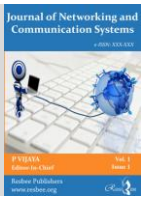
Resbee Publishers

Journal of Networking and Communication Systems

Received 3 September, Revised 22 November, Accepted 24 December



Efficient Elliptic Curve Cryptography using Glowworm Search Optimization Algorithm

Mahua Bhowmik
Department of Electronics (Digital systems)
Dr. D Y Patil Institute of Technology
Pune, Maharashtra, India
mahuabhowmik14@gmail.com

Dr. Mrs. P. Malathi
Department of Electronics and Communication
Dr. D Y Patil College of Engineering
Pune, Maharashtra, India

Abstract: With the emergence of the Internet of Things (IoT), the medical and healthcare systems experiencing the copious growth by utilizing the efficiency of IoT systems in terms of remote, non-invasive and persistent monitoring of patients. In this paper, the security of the patient data stored in IoT devices is analyzed using the renowned cryptography technique by employing the efficiency of optimization approaches. For this purpose, the encryption and decryption procedures require an optimal key to pursue the effectual security system. With the intention of accomplishing optimal key, Glowworm Swarm Optimization (GSO) model is used in Elliptic Curve Cryptography (ECC). With this implementation, the patient information can be stored securely in the IoT systems. The performance of the proposed GSO model will be compared and evaluated with the state-of-the-art models by concerning Signal-to-Noise Ratio (SNR) and similarity index.

Keywords: Internet of Things; Elliptic Curve Cryptography; Glowworm Swarm Optimization; Medical Data; Security

1. Introduction

Due to the establishment of IoT, the healthcare systems evolve a tremendous development by utilizing the efficiency of smart devices for medical diagnosis and treatments. Generally, IoT provides interconnection among the computing nodes such as smartphones, laptops, tablet, and so on with internet services which have the ability to transmit and receive data. The progressing growth of IoT devices in terms of hardware and software technologies inspire the development of IoT medical wearable devices to screen and gather several kinds of data about the patients remotely and continually. Typically, IoT devices are implemented widely in many sectors like medical devices, smart construction sites, smart transportations, etc. In particular, the IoT devices deployed in medical sector apparently provides effective and efficient assistance for the clinicians as it monitors the remote patients and informs the medical expert immediately if occurs any abnormalities which helps the patients get treated at a time.

Besides, numerous IoT Implantable Medical Devices (IMD) as well as wearable equipment such as smart watches, biosensors, etc., and imaging equipment are deployed in medical sectors which perfectly assist the doctors to treat patients as well as help the patients. Yet, the IoT devices have its limitation as all other technologies possess. It suffers owing to the issues in energy efficiency and in security aspects. Generally, the medical information gathered by the clinician is stored in the server which is needed to be kept secure as it contains sensitive data about the patients. In order to protect this data from vulnerable attacks, safe storage, as well as transmission system, is required. For this reason, the cryptographic techniques are employed to ensure security in medical IoT devices. Usually, cryptographic models have an encryption which encodes the data and decryption that decodes the data using various approaches. Traditionally, two encryption models are most widely utilized as cryptographic models such as Advanced Encryption Standard (AES) and the Rivest–Shamir–Adleman (RSA) models. The typical security models fail because of the inefficiency of the keys as it is too light which is easy to break or too long which is difficult to remember. Moreover, the IoT devices suffer due to the battery insufficiencies. These limitations lead to the development of optimal key selection to improve the encryption and decryption models. However, it encounters the efficiency of the metaheuristic optimization models [17] [18] [19] [20] [21] [22] to enhance security by choosing the optimal keys.

RFID is considered as one of the huge prospects in information technology that can change the world generally and intensely. While the RFID readers' stands through suitable communication protocols are associated to the terminal of Internet, the readers distributed all over the world can identify, track and monitor the objects attached with tags globally, automatically, and in real time, it represents Internet of Things (IOT).

With the introduction of Artificial Intelligence (AI), the Machine Learning (ML) and Deep Learning (DL) techniques become most popular in many sectors due to its efficiency in problem-solving. Moreover, the metaheuristic models such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Artificial Bee Colony (ABC), and so on were introduced to be implemented in the real-world systems. Even though the optimization models possess plenty of advantages, it suffers due to low convergence speed and local optimum issues. In the sense of cryptographic models, the key selection is a complex task as it may be symmetrical or asymmetrical key both are needed to be selected optimally. Furthermore, it should ensure the secure transmission of data among the IoT devices and the servers. These limitations draw the attention of the research and medical communities towards the development of innovative cryptographic models for IoT devices.

The main contribution of the paper is to present the encryption and decryption procedures, which requires an optimal key to pursue the effectual security system. With the intention of accomplishing optimal key, GSO model is used in ECC. The organization of this paper is in this order: Section 2 presents the literature regarding cryptographic techniques in IoT systems. Proposed cryptographic techniques in IoT systems are illustrated in Section 3. The objective function is demonstrated in Section 4. Section 5 gives the contribution of GSO models for cryptography in IoT devices. Section 6 provides the attained results, and Section 7 concludes the paper.

2. Literature Review

2.1Related Works

In 2017, Shen et al. [1] have proposed a novel Radio Frequency Identification (RFID) technique to ensure security via ECC. Moreover, this model was introduced to overcome the limitations in the traditional system. The experimentation analysis verified the efficiency of the model by means of minimized cost.

In 2018, Elhoseny et al. [2] have presented an effective cryptographic model to assure the security of the medical IoT devices using the hybridization of Grasshopper Optimization (GO) and PSO (GO-PSO) for choosing the optimal key for encryption and decryption process in ECC. The security level of this model was validated through a comparative analysis with the conventional models and the simulation results proved its efficiency.

In 2018, Kumar and Sukumar [3] have introduced an ECC model concerning energy efficiency and battery life of the IoT devices using a new scalar point-multiplication model to reduce the energy consumption. In addition to this, the encryption model provided security by ensuring the secrecy, authentication distinctiveness, as well as privacy of the data stored in IoT devices in simulation as well as the real-world scenario. Furthermore, it attained enhanced security and minimized energy utilization through fastening the system execution. The simulation work revealed efficiency through a comparative study with the traditional models by considering the battery life and energy.

In 2018, Kumari et al. [4] have established a cryptographic model to provide security in IoT devices using a novel ECC model that enabled enhanced security over Kalra and Sood model. Moreover, it was robust to malicious attacks such as offline password assumption and intruder attacks. In addition to this, it gives device secrecy, session key conformity as well as mutual verification through the Automated Validation of Internet Security Protocols with Applications tools. From the experimentation analysis, this model accomplished improved security against different malicious attacks and the comparison evaluation validated the performance with various state-of-the-art models.

In 2017, Mai and Khalil [5] have developed a cryptographic model to guarantee security, secrecy, and authentication for smart meter information in smart grid systems through homomorphic cryptography approach. Initially, the smart meter information was encrypted via the homomorphic asymmetric key technique in the IoT device i.e., before stored in the server. The applicant's invoices were considered as the homomorphic features using the overall electricity utilization which was explicitly encoded in the server. Moreover, the integration of encoded smart meter data through fixed-point number arithmetic technique provided numerous smart meter data from various households. From the simulation analysis, this model obtained improved confidentiality and security and also enhanced performance in terms of minimized fast computing and efficiency.

2.2 Review

In this section, the review of the literature is discussed. The RFID model [1] provided enhanced security and authentication and enabled safe access to IoT devices. However, it suffers due to the high computational time and high implementation cost. The GO-PSO model [2] utilized minimum memory and improved security yet, it fails to owe to the lack of tamper localization and content-based responsibility. The point-multiplication based ECC [3] model attained improved battery life and enhanced encryption and decryption process but it was vulnerable to the Denial-of-Service (DOS) attacks and computationally complex to transfer a large amount of data. The novel ECC [4] model achieved enhanced security than Kalra and Sood model and provided device secrecy still it lacks due to the expense of the IoT devices implementation and susceptible to malicious attacks. The homomorphic cryptography [5] model attained improved confidentiality and security as well as enhanced performance. However, it suffers from the abundance of smart meter data as it can afford up to 400 unique entries and required high computational time.

3. Proposed Elliptic Curve Cryptographic Model

3.1 Proposed Architecture

Fig. 1 shows the proposed architecture of the cryptographic model for IoT devices. The main objective of this paper is to provide security and data privacy by employing a hybrid encryption model for the protection of the data to be stored in the IoT devices. In this cryptographic model, asymmetric encryption (ECC) is employed which involves the use of the private and public keys. Both the keys are needed to be secured and should be chosen optimally. In ECC, the method performs on the basis of the smaller key size with improved security. It exploits plane curve as finite field, which evades the real numbers, with specific base point and with the aid of prime number function. Moreover, the encryption is performed, while maximum limit is reached on the curve. For this purpose, the GSO optimization model [16] is utilized which ensures the security of the data by generating the ciphered image. Fig. 2 depicts the typical ECC cryptographic model.

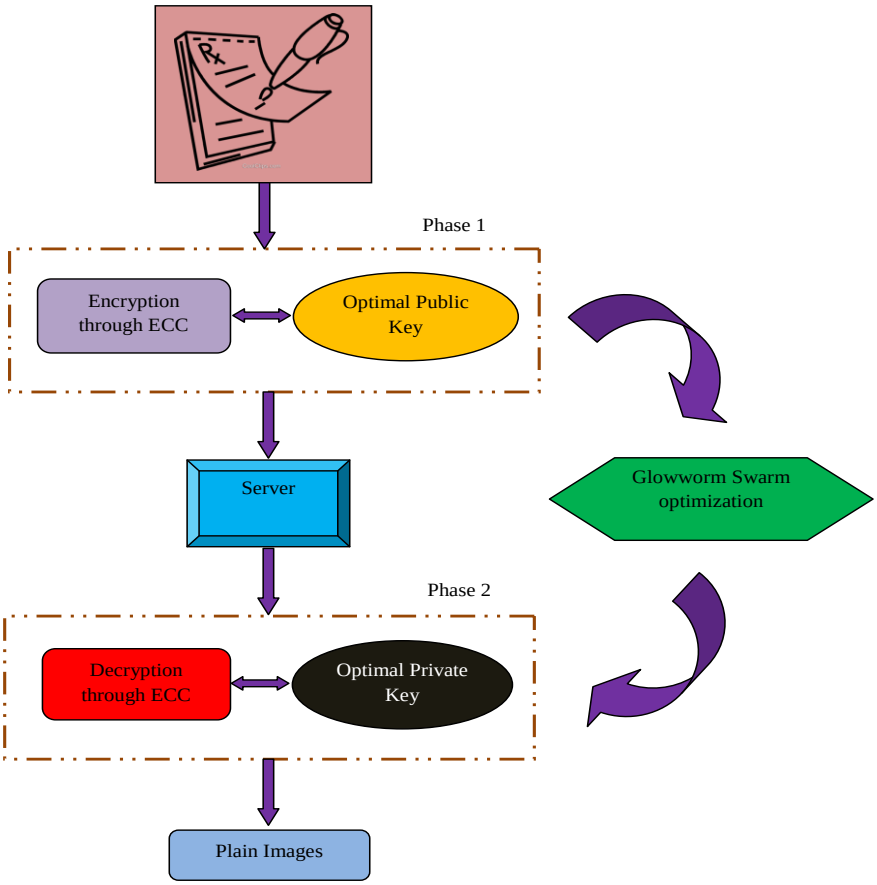


Fig. 1. *Geometrical Representation of Proposed Cryptographic Model for IoT devices*

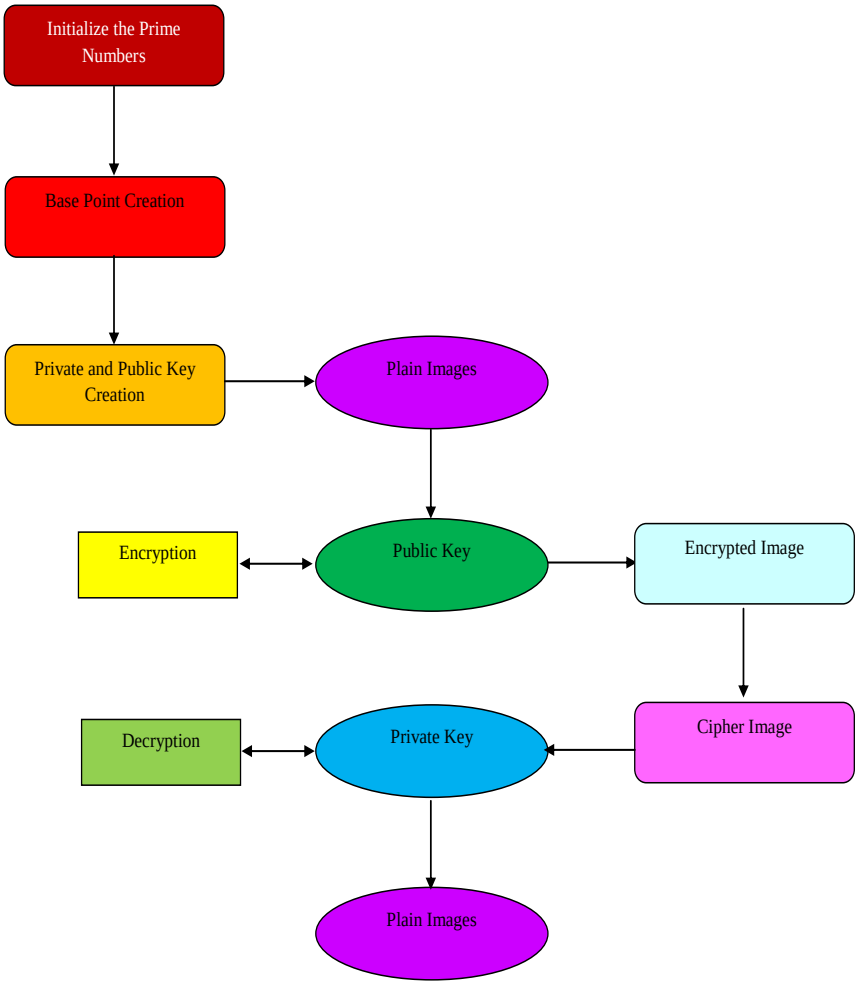


Fig. 2. *Graphical Representation of the ECC model*

4 Objective Model for Optimal Key Selection

4.1 Objective Function

The main objective of this paper is to attain an optimal key to improve the security of the data stored in IoT devices. For this purpose, the fitness function is evaluated based on the maximum key through Peak Signal Noise Ratio (PSNR) to scramble as well as unscramble information stored in IoT devices. The composition of the system is formulated based on the fitness of GSO as given in Eq. (1).

$$Ob = \max\{PSNR\} \tag{1}$$

4.2 Optimal Key Selection Model

The optimal key is chosen from the prime numbers associated with the population size of the GSO optimization model. For this purpose, ni number of solutions is attained as population size. Among them, the prime numbers are evaluated to attain the optimal key L. Fig 3 represents the solution encoding for prime number optimization.

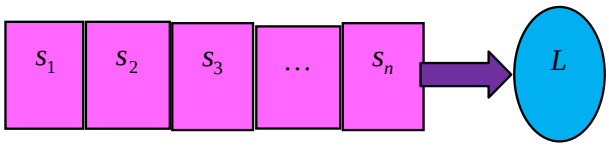


Fig. 3. *Solution encoding showing prime number optimization*

5.Optimization using Glowworm Swarm Search Algorithm

5.1 Traditional Glowworm Swarm Optimization Algorithm

Typically, for classical GSO model, a group of glowworms is arbitrarily speckled in a search space. Furthermore, they possess a special effect termed luciferin that is usually a luminescent factor and the decision domain $J_d^{xi}\left(0 < J_d^{xi} \le J_r\right)$ and $J_r\left(0 < J_d^{xi} \le J_r\right)$. Consider *xi* as the glowworm and yi as the neighbor, J_d^{xi} and J_r indicates the neighborhood range and sensor range. Normally, a glowworm *xi* recognizes a glowworm *yi* as a neighbor, when *yi* possessing the value lower than J_d^{xi}, as well as the luciferin level as $yi > xi$. Using a probabilistic function, all *xi* choose it's yi based on the luciferin value $yi > xi$ and goes towards yi i.e., xi attracts to *yi* that glows brighter. The fitness of present positions determines the luciferin intensity of the glowworms. In addition to this, the greater luciferin intensity gives the best position of xi. The length of J_d^{xi} and *xi* is balanced through the quantity of *xi* in J_d^{xi} and J_d^{xi} of *xi* is proportional to the density of *yi*. The value of J_d^{xi} is maximized, when J_d^{xi} dealt with a low density of *xi* and conversely, J_d^{xi} is minimized when it dealt with a high density of *xi*. The major four phases of GSO are given as follows.

Initial distribution of glowworms: At first, xi are arbitrarily distributed in the search space. As mentioned earlier, xi have similar luciferin intensity along with decision domain J_0.

Luciferin update: The luciferin intensity of *xi* is with respect to the fitness of its present positions. For all iteration, the location of *xi* varies and the luciferin value is required to be updated. In time *te*, the position of xi is $p^{xi}(te)$, in which, the associated objective function of the position of *xi* at the time te is $V\left(p^{x}(ti)\right)$. Additionally, the substitute $V\left(p^{xi}(te)\right)$ to the luciferin level $l^{xi}(te)$ with respect to xi in time *te* as specified in Eq. (2), in which, αi refers to luciferin decay constant $0 < \alpha i < 1$, βi represents luciferin enhancement constant.

$$l^{xi}(te) = (1-\alpha i)l^{xi}(te-1) + \beta i V\left(p^{xi}(te)\right) \tag{2}$$

Movement: Usually, all xi choose it's associated *yi* and goes in the direction of yi through a specific probability. For this purpose yi needed to possess the following 2 properties. At first, yi should be present inside the decision domain of *xi* and then l^{xi} should be greater than *xi*. Furthermore, if xi goes in the direction of *yi* that comes using $N^{xi}(te)$, then it creates a particular probability $S^{xiyi}(te)$ and it is established as stated in Eq. (3).

$$S^{xiyi}(te) = \frac{p^{yi}(te) - p^{xi}(te)}{\sum_{k \in N^{xi}(te)} p^{k}(te) - p^{xi}(te)} \tag{3}$$

For each movement of xi, Eq. (4) shows the position updation of xi, in which, si specifies the step size.

$$p^{xi}(te+1) = p^{xi}(te) + si * \left(\frac{p^{yi}(te) - p^{xi}(te)}{\left\| p^{yi}(te) - p^{xi}(te) \right\|} \right) \tag{4}$$

Neighborhood range update: After the location update of *xi*, the update of J_d^{xi} is applied. As noted above, the value of J_d^{xi} is maximized, when J_d^{xi} dealt with a low density of xi and conversely, J_d^{xi} is minimized, when it dealt with a high density of xi as specified in Eq. (5), in which, χi denotes a fixed parameter and ni^{te} represents a parameter utilized to manage a number of yi.

$$J_d^{xi}(te+1) = \min\left\{ J_r, \max\left\{ 0, J_d^{xi}(te) + \chi i\left(ni^{te} - \left| N^{xi}(te) \right| \right) \right\} \right\} \tag{5}$$

Algorithm 1 illustrated below represents the pseudo-code of GSO.

Algorithm 1: Conventional GSO
Begin
Initialize number of dimensions as ai
Initialize number of xi as bi

Size as se
Deploy- xi -arbitrarily
for $xi = 1$ to *bi*
do
$l^{xi}(0) = l^0$ $J_d^{xi}(0) = J_0$ **while** $(te < \max \ \ it)$ **do**
for all *xi*
do as per Eq. (1)
for all xi
do $N^{xi}(te) = \{yi : d^{xiyi}(te) < J_d^{xi}(te); l^{xi}(te) < l^{yi}(te);\}$ **for** all $yi \in N^{xi}(te)$
do as per Eq. (2)
$k =$ choose $xi(S)$ as per Eq. (3)
Position update as per Eq.(4)
$te = te + 1$
End

6. Result and Discussion

6.1 Simulation Setup

The proposed method of ECC cryptographic model is implemented in MATLAB 2018a and further observed the simulation results. The security of the medical data like the images of brain, heart, eyes, etc is collected from the medical IoT devices. Furthermore, the hidden data is evaluated while sending and receiving the data. Further, the performance of the GSO optimization model is compared with the state-of-the-art models like AES [10], RSA [11], ECC [12], ECC-Crow Search Algorithm (CS) [13], ECC-PSO [14], and ECC-GO [15] by concerning PSNR, Mean Square Error (MSE), Bit Error Rate (BER), and Spectral Similarity Index (SSI).

6.2 Comparison Analysis

In this section, the comparative analysis for the performance of the GSO optimization model over conventional models. Fig. 4 depicts the performance of GSO in terms of (a) PSNR, (b) MSE, (c) BER, and (d) SSI values to provide security against unauthorized attempts to access the data stored in Medical IoT devices are discussed. The performance of GSO optimization model is compared with the conventional models. The PSNR performance of GSO is 11.76%, 21.79%, 10.46%, 11.76%, 21.79%, and 20.25% better than AES, RSA, ECC, ECC-CS, ECC-PSO, ECC-GO respectively for population size 80 as shown in Fig. 4(a). Fig. 4(b) portrays the MSE performance as 11.02% better than AES, 10.25% superior to RSA, 22.02% better than ECC, 12.03% better then ECC-CS, 22.4% superior to ECC-PSO, and 15.23% better then ECC-GO for population size 60. The BER performance is 11.05%, 25.35%, 20.1%, 18.02%, 14.56%, and 12.05% better than AES, RSA, ECC, ECC-CS, ECC-PSO, ECC-GO respectively for population size 60 as shown in Fig. 4(c). The SSI performance is 8.05% better than AES, 22.58% superior to RSA, 18.25% better than ECC, 12.03% better then ECC-CS, 15.36% superior to ECC-PSO, and 6.25% better then ECC-GO for population size 40 as represented in Fig. 4(d). Thus, the performance of the GSO for enhancing the security of medical data stored in IoT devices using ECC was validated and verified.

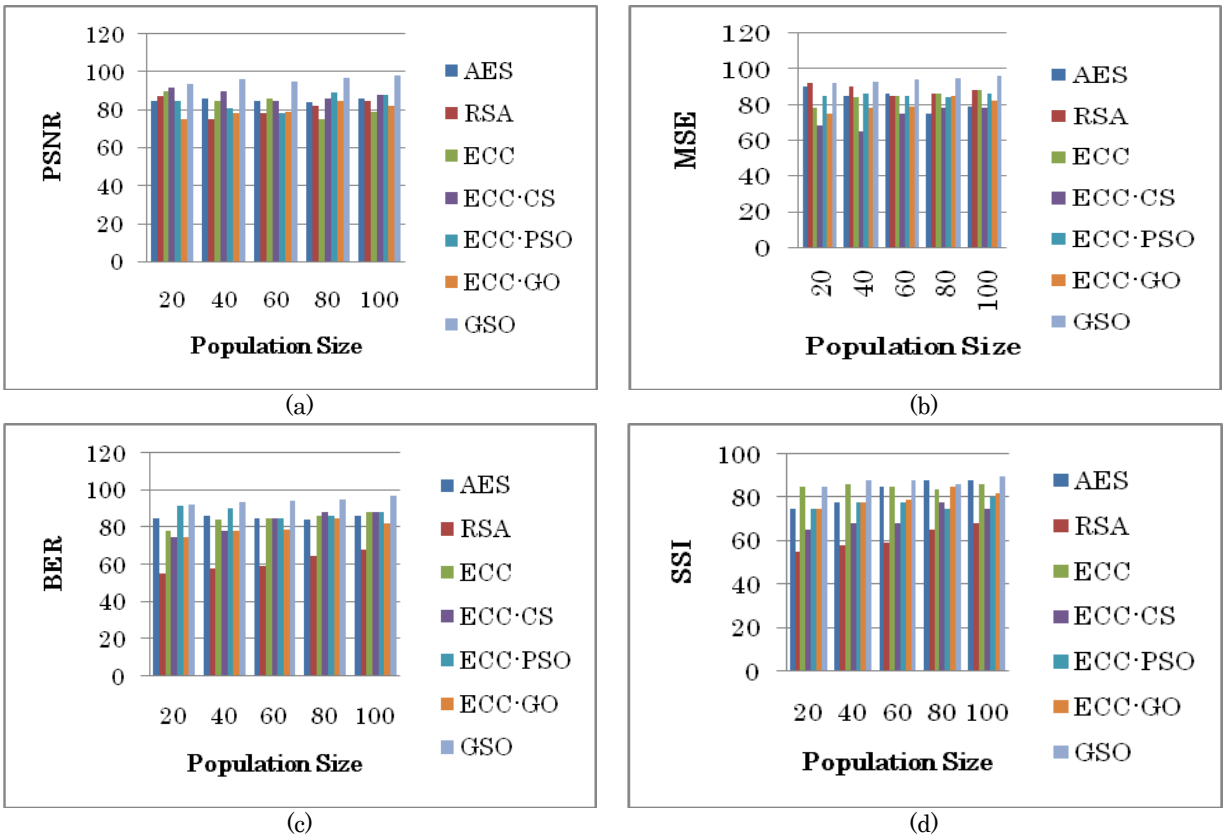
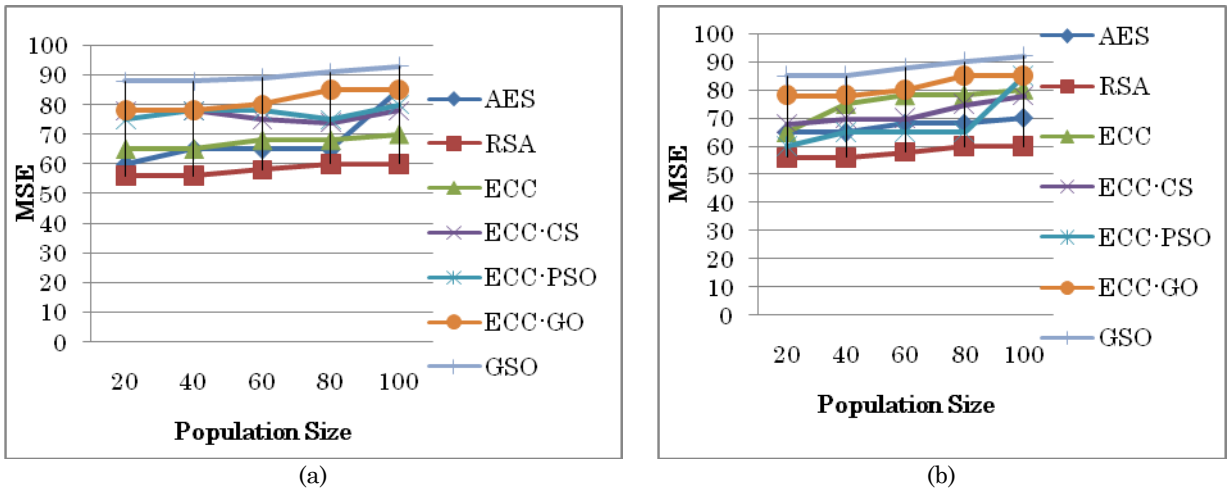
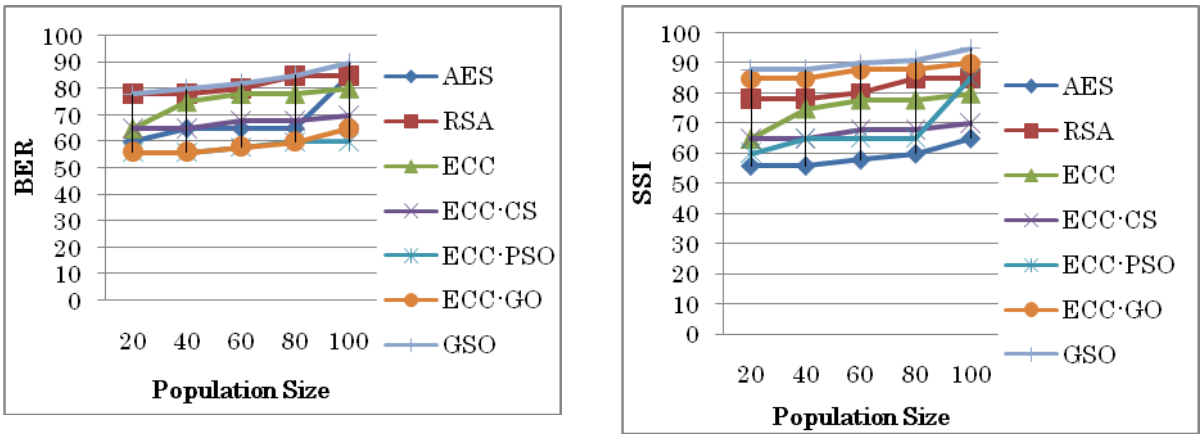


Fig. 4. *Comparison analysis for the performance of the GSO optimization model over conventional models in terms of (a) PSNR, (b) MSE, (c) BER, and (d) SSI values to provide security against unauthorized attempts to access the data stored in Medical IoT devices*

Fig. 5 depicts the performance of GSO in terms of (a) PSNR, (b) MSE, (c) BER, and (d) SSI values to provide security against malicious on the data stored in Medical IoT devices are discussed. The performance of the GSO optimization model is compared with the conventional models. The PSNR performance of GSO is 5.02%, 12.25%, 10.46%, 8.23%, 6.23%, and 14.58% better than AES, RSA, ECC, ECC-CS, ECC-PSO, ECC-GO respectively for population size 70 as shown in Fig. 5(a). Fig. 5(b) portrays the MSE performance as 23.58% better than AES, 21.85% superior to RSA, 16.98% better than ECC, 15.75% better then ECC-CS, 12.65% superior to ECC-PSO, and 12.77% better then ECC-GO for population size 50. The BER performance is 41.5%, 38.56%, 33.56%, 34.56%, 25.87%, and 26.44% better than AES, RSA, ECC, ECC-CS, ECC-PSO, ECC-GO respectively for population size 30 as shown in Fig. 5(c). The SSI performance is 8.05% better than AES, 12.55% superior to RSA, 16.45% better than ECC, 18.32% better then ECC-CS, 12.41% superior to ECC-PSO, and 15.86% better then ECC-GO for population size 60 as represented in Fig. 5(d). Therefore, the performance of the GSO for enhancing the security against malicious attacks of medical data stored in IoT devices using ECC was validated and verified.





(c) (d)

Fig. 5. *Comparison analysis for the performance of the GSO optimization model over conventional models in terms of (a) PSNR, (b) MSE, (c) BER, and (d) SSI values to provide security against malicious attacks on the data stored in Medical IoT devices*

7. Conclusion

An advanced model for securing medical data stored in IoT devices using ECC model with GSO has been proposed in this paper. The security of improved by using the encryption and decryption procedures which require an optimal key to pursue the effectual security system. For this purpose, the GSO model was used in ECC. With this implementation, the patient information was stored securely in the IoT systems. The performance of the proposed GSO model was compared and evaluated with the conventional models by concerning PSNR, MSE, BER, and SSI. The PSNR performance of GSO is 11.76%, 21.79%, 10.46%, 11.76%, 21.79%, and 20.25% better than AES, RSA, ECC, ECC-CS, ECC-PSO, ECC-GO respectively for providing security against unauthorized access. Furthermore, the PSNR performance of GSO is 5.02%, 12.25%, 10.46%, 8.23%, 6.23%, and 14.58% better than AES, RSA, ECC, ECC-CS, ECC-PSO, ECC-GO respectively for providing security against malicious attacks. Hence, the proposed GSO model with ECC provides improved security which was analyzed and verified successfully.

References

[1] Han Shen, Jian Shen, Muhammad Khurram Khan, and Jong-Hyouk Lee, "Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things", Wireless Personal Communications, vol. 96, no. 4, pp 5253–5266, 2016.

[2] Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things", Neural Computing and Applications, pp 1-15, 2018.

[3] K. Sathish Kumar, and R. Sukumar, "Achieving energy efficiency using novel scalar multiplication based ECC for android devices in Internet of Things environments", Cluster Computing, pp 1-8, 2018.

[4] Saru Kumari, Marimuthu Karuppiah, Ashok Kumar Das, Xiong Li, Fan Wu, and Neeraj Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers", The Journal of Supercomputing, vol. 74, no. 12, pp 6428–6453, 2018.

[5] Vu Mai, and Ibrahim Khalil, "Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography", Future Generation Computer Systems, vol. 72, pp 327-338, July 2017.

[6] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72-83, Feb. 2015.

[7] M. Malik, M. Dutta and J. Granjal, "A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things," IEEE Access, vol. 7, pp. 27443-27464, 2019.

[8] K. R. Choo, S. Gritzalis and J. H. Park, "Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3567-3569, Aug. 2018.

[9] L. Wei et al., "An effective differential fault analysis on the Serpent cryptosystem in the Internet of Things," China Communications, vol. 11, no. 6, pp. 129-139, June 2014.

[10] D. Bui, D. Puschini, S. Bacles-Min, E. Beigné and X. Tran, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 25, no. 12, pp. 3281-3290, Dec. 2017.

[11] S. Kaedi, M. A. Doostari and M. B. Ghaznavi-Ghoushchi, "Low-complexity and differential power analysis (DPA)-resistant two-folded power-aware Rivest–Shamir–Adleman (RSA) security schema implementation for IoT-connected devices," IET Computers & Digital Techniques, vol. 12, no. 6, pp. 279-288, 11 2018.

[12] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72-83, Feb. 2015.

[13] Oliva D, Hinojosa S, Cuevas E, Pajares G, Avalos O, and Ga ´lvez J, "Cross entropy based thresholding for magnetic resonance brain images using crow search algorithm", Expert Syst Appl, vol. 79, pp 164–180, 2017.

[14] M.E.H. Pedersen and A.J. Chipperfield, " Simplifying Particle Swarm Optimization", Applied Soft Computing, vol. 10, pp. 618–628, 2010.

[15] Neve AG, Kakandikar GM, and Kulkarni O, "Application of grasshopper optimization algorithm for constrained and unconstrained test functions", Int J Swarm Intell Evol Comput, vol. 6, no. 3, 2017.

[16] Vijayakumar Polepally, K Shahu Chatrapati,"DEGSA-VMM: Dragonfly-based exponential gravitational search algorithm to VMM strategy for load balancing in cloud computing";Kybernetes, vol.67, no.6;pp.1138-1157;2018.

[17] D. Menaga and Dr.S. Revathi,"Privacy Preserving using Bio Inspired Algorithms for Data Sanitization",International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC); pp. 201-206, 2018.

[18] MNKMSS Dr. N. Krishnamoorthy,"Performance Evaluation of Optimization Algorithm Using Scheduling Concept in Grid Environment", The IIOAB Journal 7 (9), pp. 315-323, 2016.

[19] SB Vinay Kumar, PV Rao, Manoj Kumar Singh,"Multi-culture diversity based self adaptive particle swarm optimization for optimal floorplanning",Multiagent and Grid Systems, vol14, no.1, pp.31-65, 2018.

[20] Archana H. Sable Haricharan Dhirbasi,Dr. Bondar Kirankumar Laxmanrao,"Application of Integral Transform to Recognition of Plastic Surgery Faces and the Surgery Types: an Approach with Volume based Scale Invariant Features and SVM",vol.6, no.3, pp.1061-1072, 2018.

[21] R Gupta Roy, D Baidya,"Speed Control of DC Motor Using Fuzzy-Based Intelligent Model Reference Adaptive Control Scheme",Advances in Communication, Devices and Networking, Lecture Notes in Electrical Engineering book series, Springer, vol. 462, pp.729-735, 2018.

[22] G Singh, VK Jain, A Singh, "Adaptive network architecture and firefly algorithm for biogas heating model aided by photovoltaic thermal greenhouse system",Energy & Environment, vol. 29 (7), pp.1073-1097, 2018.