International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 13, No. 2, April, 2023, pp. 325-331
Journal homepage: http://iieta.org/journals/ijsse

SLDEB: Design of a Secure and Lightweight Dynamic Encryption Bio-Inspired Model for IoT Networks

Bhavesh Kataria[1*], Harikrishna B. Jethva[2], Pushpmala Vijay Shinde[3], Satish S. Banait[4], Farhadeeba Shaikh[5], Samir Ajani[6]

[1] Department of Information Technology, LDRP Institute of Technology and Research, Kadi Sarva Vishwavidyalaya established by SVKM, Gandhinagar 382016, Gujarat, India
[2] Department of Computer Engineering, Government Engineering College, Patan 384265, Gujarat, India
[3] School of Computer Engineering and Technology, MIT-AOE, Alandi, Pune 412105, Maharashtra, India
[4] K.K.Wagh Institute of Engineering Education and Research, Nashik, SPPU Pune 422003, Maharashtra, India
[5] MIT WPU School of Polytechnic and Skill Development, Pune 411048, Maharashtra, India
[6] Department of Computer Science & Engineering (Data Science), St. Vincent Pallotti College of Engineering and Technology, Nagpur 441108, Maharashtra, India

Corresponding Author Email: bhavesh.iisc@gmail.com

(This article is part of the Special Issue **Technology Innovations and AI Technology in Healthcare**)

https://doi.org/10.18280/ijsse.130214

Received: 20 February 2023
Accepted: 14 March 2023

Keywords:
IoT, encryption, lightweight, delay, decryption, complexity, energy, security, context, elliptic, cryptic

ABSTRACT

Designing encryption models for IoT deployments requires analysis of multiple network level constraints. These include, estimation of energy requirements, security strength, encryption & decryption delay, computational complexity, etc. A wide variety of models are proposed to perform these tasks, but most of them are either highly complex, or require higher energy levels for encrypting data samples. Moreover, these models are context-independent, and cannot be used for application-specific deployments. To overcome these issues, this text proposes design of a novel secure and lightweight dynamic encryption bioinspired model for IoT networks. The proposed model initially uses an Elliptic Curve Cryptography (ECC) process for data security, and optimizes its performance via Bacterial Foraging Optimization (BFO). ECC parameters that are obtained via BFO are further fine-tuned using a Q-Learning based process, which assists in identification of context-specific parametric ranges for different network types. The combination of BFO with Q-Learning results in dynamic ECC curves, which can be used for context-specific deployments. Performance of the model was evaluated on different scaled networks, and compared with other state-of-the-art encryption models in terms of encryption delay, decryption delay, security level under different attacks, and energy consumption levels. Based on this comparison, it was observed that the proposed model showcased 8.5% lower encryption delay, 3.2% lower decryption delay, and 5.9% lower energy consumption while maintaining similar security levels. Due to these enhancements, the proposed model is useful for a wide variety of low complexity IoT deployments.

1. INTRODUCTION

As a result of advances in technology, Internet of Things (IoT) devices that are linked together are becoming increasingly widespread. Maintaining everyone's safety is the first and most important priority. When compared to the security of Internet of Things devices, the safety of transportation networks is on par, if not higher, on the priority scale [1]. Asymmetrical cryptosystems have been around since 1986, when Miller [2] and Koblitz [3] originally developed the concept of elliptic curve cryptography (ECC), which stands for elliptic curve cryptography. There are several organizations all around the globe that have given ECC its stamp of approval, including NIST [4], ANSI [5], and IEEE [6]. There have been a few different proposals for ECC hardware implementations [7]. Two of these approaches are the multiplier and the adder, and they are used in the process of putting modular multiplication into action (MM). Using the Montgomery multiplication technique is another example of multiplier-based architecture [8]. Another example is designing for a certain prime field. Interleaved multiplication is used to construct this adder-based design [9], which was described before. The central processing unit employs a Montgomery MM algorithm that has a multiplier that is r bits by r bits [10]. A multiplier that is n bits by n bits is used in the construction of the processors [11]. MM is a mathematical operation that incorporates both multiplication and quick reduction over a given prime field. It is essential to take into consideration the fact that the design based on multipliers calls for a substantial number of physical resources.

Efficient cipher chaining (ECC) also makes use of modular inversion, which is a process that takes a significant amount of time (MI). One example of this is the implementation of algorithms for binary modular inversion in hardware-efficient computers. The MM and MI units of the processor's 11-bit adder function independently from one another. The IMM approach is used by processors in order to do radix-4 booth encoding [12]. A radix-2 MM algorithm is used by the processor Durga et al. [13], Huang [14] in order to successfully complete MM while avoiding MI with projective coordinates. The software that is used for traditional cryptography algorithms has drawbacks, such as a high-power consumption and a lengthy processing time; nevertheless, these problems might be resolved with computational advancements. An ECC is similar to RSA in that it is a public-key cryptosystem, but because to developments in computers, it may be easier to use. The primary distinction between it and RSA is that it has the ability to evolve more quickly.

Similarly work in Huang [15], Wei et al. [16], Abd El-Latif et al. [17], Li et al. [18], Mamvong et al. [19], Niu et al. [20], which propose use of multiple authority attribute-based encryption, blockchain based data access control ABE (DAC ABE), controlled alternate quantum walks (CAQWs), Decisional Bilinear Diffie-Hellman (DBDH), power efficient encryption, and key aggregation searchable encryption (KASE), which assist in improving performance of encryption under different use cases. Extensions to these models are discussed in Fotovvat et al. [21], Fotovvat et al. [22], Khan et al. [23], Hussain et al. [24], Khashan [25] which propose use of Lightweight cryptography (LWC), Key-Policy Attribute Based Encryption (KPABE), Secure Surveillance Mechanism, Certificate Based Signcryption with Proxy Re-Encryption (CBSRE), and Lightweight Proxy Re-Encryption, which assists in improving security performance for different use cases. These models must be validated for large-scale networks, and can be extended via use of Compressive-Sensing-Based Lightweight Encryption [26-28], Ciphertext-Policy Hierarchical Attribute-Based Encryption [29], which aim at incorporating lightweight encryption models for IoT network scenarios. This presents those who research cryptographic algorithms with a fresh and fascinating path of exploration to pursue. It is possible to use ECC keys that are smaller and yet provide the same degree of security as RSA. The security provided by ECC, which has 163 bits rather than RSA's 1024 bits, may be considered an alternative. In addition, electronic communications work especially well as a complement to wireless media such as smart cards and mobile phones, which helps to make ECC a perfect wireless communication protocol. It has been shown that the EC point multiplication algorithm is more time and resource efficient than the RSA exponentiation algorithm. Function of Normal Distribution Extracted from an Algorithm the Elliptic Curve Cryptography (ECC) standard incorporates key exchange, agreement protocols, digital signature (ECDSA), as well as other applicable asymmetric cryptographic primitives. The operation of point multiplication, which is the foundation of all ECC primitives, is also the operation that requires the highest amount of computational work to complete. When it comes to encrypting data samples, it was discovered that the vast majority of models are either too complicated or waste an excessive amount of energy. This is despite the fact that various models have been developed to do these activities. These models are not suitable for usage in app-specific deployments since they are not sensitive to the surrounding environment. Bhattacharya and Pandey [30], Bhattacharya and Pandey [31], Wang and Liu [32], Noura et al. [33], Deb et al. [34], Zhuang et al. [35], Al-Moliki et al. [36] discuss various issues and challenges related to incorporating the Internet of Things (IoT) and green technology, as well as different encryption methods and technologies for securing IoT devices and networks. They propose solutions such as "CEaaS: Constrained Encryption as a Service in Fog-Enabled IoT" and "A Single-Pass and One-Round Message Authentication Encryption for Limited IoT Devices" to enhance security in IoT. They also propose a "Verifiable Searchable Encryption Framework Against Insider Keyword-Guessing Attack in Cloud Storage" to improve the security of cloud storage [37].

In the next section of this article, we will provide our answer to these problems, which is the creation of an innovative, bio-inspired dynamic encryption model that is both lightweight and secure for use in IoT networks. As a result, the objective of this article is to include bioinspired processes in order to offer security assurance for Internet of Things devices in a way that is as simple and uncomplicated for different use cases.

2. PROPOSED SECURE AND LIGHTWEIGHT DYNAMIC ENCRYPTION BIOINSPIRED MODEL FOR IOT NETWORKS

Based on the review of existing encryption models, it can be observed that most of these models are either highly complex, or require higher energy levels for encrypting data samples. Moreover, these models are context-independent, and cannot be used for application-specific deployments. To overcome these issues, this section proposes design of a novel secure and lightweight dynamic encryption bioinspired model for IoT networks. Flow of the model is depicted in Figure 1, where it can be observed that the proposed model initially uses an Elliptic Curve Cryptography (ECC) process for data security, and optimizes its performance via Bacterial Foraging Optimization (BFO). ECC parameters that are obtained via BFO are further fine-tuned using a Q-Learning based process, which assists in identification of context-specific parametric ranges for different network types. The combination of BFO with Q-Learning results in dynamic ECC curves, that can be used for context-specific deployments.

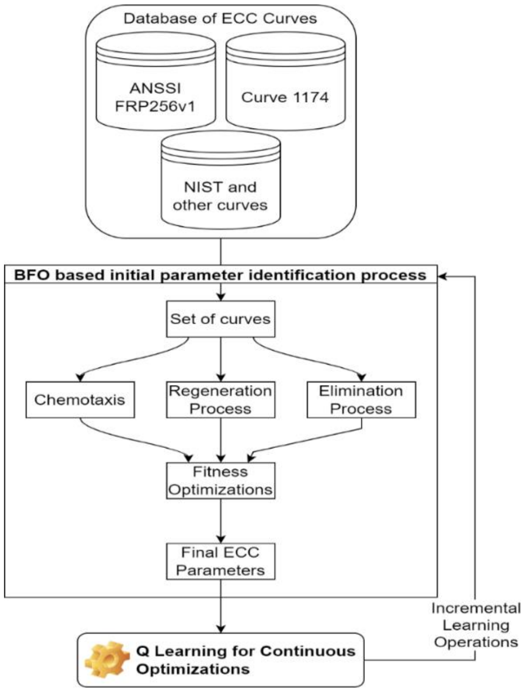

Figure 1. Overall flow of the proposed light-weight encryption process

The model initially collects information about different ECC curves, that include but are not limited to ANSSI FRP256v1, BN (2, 254), Curve1174, Curve383187, E-382, M-383, NIST P-224, secp256k1, etc. These curves have their own varying prime fields, binary fields, and Koblitz fields.

For instance, the Curve1174 is represented via Eq. (1):

$$x^2 + y^2 = 1 - 1174x^2y^2 \tag{1}$$

Which can be represented via Figure 2(a), where a quad parabolic shape can be observed for different *x* & *y* sample sets. Similarly, the secp256k1 curve, which is used by Bitcoin for block-level encryptions can be evaluated via Eq. (2), and is depicted in Figure 2(b), as follows:

$$y^2 = x^3 + 7 \tag{2}$$

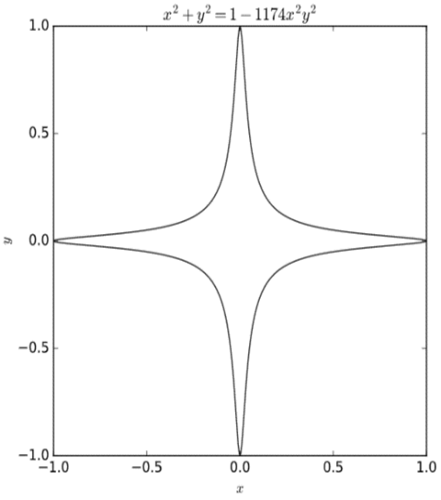

Figure 1(a). Representation of the ECC Curve1174 for different value sets

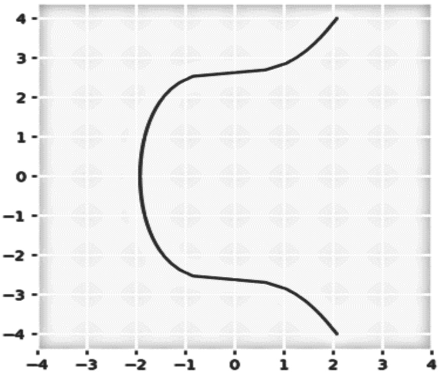

Figure 2(b). Representation of the ECC secp256k1 curve for different value sets

Based on these curve sets, it can be observed that for every value of x, the curve has 2 similar points on the Y axis. One of these points are used for encryption, while other is used for decryption process. The proposed model uses this characteristic of ECC in order to generate light-weight curves via BFO model, which works as per the following process, process. The proposed model uses this characteristic of ECC in order to generate light-weight curves via BFO model, which works as per the following process:

- Initialize optimization parameters of BFO as follows:

○Total number of bacteria particles used during optimization (N_p);

○Total optimization iterations for BFO (N_i);

○Chemotaxis rate (L_c);

○Rate at which particles regenerate (L_r);

○Rate of elimination (L_e);

○Total available ECC curves and their parameters (N_c).

- Initially generate bacterial swarm as per the following process:

○Select a stochastic curve from the set of curves, and estimate its fields as per Eqns. (3), (4), and (5).

$$p = STOCH(L_c * p_{max}, p_{max}) \tag{3}$$

$$b = STOCH(L_r * b_{max}, b_{max}) \tag{4}$$

$$k = STOCH(L_e * k_{max}, k_{max}) \tag{5}$$

where, *STOCH* represents a Markovian stochastic process, used to generate numbers between given range sets, while *p*, *b* & *k* represents prime field values, binary field values, and Koblitz field values for the given curve sets.

○The generated sub-curve is further processed if it follows the rule of ECC, that for every value of *x*, there should be exactly 2 values of y, which assists in encryption and decryption processes;

○If the curve doesn't follow these rules, then it is regenerated via Eqns. (3), (4), and (5) till the conditions are fulfilled for different value sets;

○This new sub-curve is evaluated, and its fitness levels are estimated via Eq. (6):

$$f = \frac{1}{N_i}\sum_{i=1}^{N_i}\frac{d_{e_i} + d_{d_i}}{d_{ref}} + \frac{e_{e_i} + e_{d_i}}{e_{ref}} \tag{6}$$

where, d_e & d_d represents delay needed for encryption & decryption, while d_{ref} represents combined encryption & decryption for the reference curve, while, e_e & e_d represents energy needed for encryption & decryption, while e_{ref} represents combined encryption & decryption energy for the underlying reference curve sets.

○This process is repeated for all particles, and a particle fitness threshold is estimated via Eq. (7):

$$f_{th} = \sum_{i=1}^{N_p} f_i * \frac{L_c + L_r + L_e}{3 * N_p} \tag{7}$$

○Particles with $f < f_{th}$ are marked as 'not to be reconfigured', while others are marked as 'to be reconfigured'.

- Once initial configurations are generated, then all particles are scanned for N_i iterations, and the particles marked as 'to be reconfigured' are regenerated via Eqns. (3), (4), (5) and (6), which assists in generation of new curve sets.

- At the end of each iteration, fitness threshold levels are recalculated, and the process is continued for N_i iterations.

At the end of final iteration, select all curves that are marked as 'not to be reconfigured', and use a Q-Learning based model to identify optimal curve sets for different IoT use cases. To perform this task, setup target delay d_t and target energy levels e_t that are required by the IoT deployment, and evaluate the curve for *N* dummy communication requests. For each of the requests, calculate curve's Q-Level via Eq. (8):

$$Q = \frac{d_e + d_d}{d_e(Orig) + d_d(Orig)} + \frac{e_e + e_d}{e_e(Orig) + e_d(Orig)} \tag{8}$$

where, *d*(*Orig*) & *e*(*Orig*) represents original levels of delay and energy for given curve sets. For each of the encryption and decryption requests, evaluate reward factor via Eq. (9):

$$r = \frac{Q_{i+1} - Q_i}{L_r} - L_c * Max(Q) + Q_i \tag{9}$$

where, Q_i & Q_{i+1} represents current and next values of Q-Levels. This process is repeated for *N* requests and for each 'not to be configured' curve sets. Variance levels of reward is estimated via Eq. (10):

$$v = \frac{\sum_{i=1}^{N} r_i - \sum_{j=1}^{N} \frac{r_j}{N}}{N} \tag{10}$$

Once this process is repeated for every curve, then a variance threshold is estimated via Eq. (11):

$$v_{th} = L_e * \sum_{i=1}^{N_c} \frac{v_i}{N_c} \tag{11}$$

where, N_c represents number of curves used for the evaluation process. All curves that fulfil condition in Eq. (12), are selected for the IoT deployment, while others are removed from the selection process.

$$v < v_{th} * (L_c + L_r) \tag{12}$$

Based on this process, curves are selected for low energy and low delay operations. These curves were evaluated on different IoT networks, and their performance was compared w.r.t. standard encryption models in the next section of this text.

3. STATISTICAL COMPARISON AND ANALYSIS

The proposed model uses a combination of BFO with Q-Learning to continuously optimize the ECC curve generation and selection process for IoT deployments. To validate performance of this model, it was evaluated on a standard set of following network configurations:

Type of Channel: Wireless
Type of Propagation: Two Ray Ground
Type of Interface: Wireless Physical
Used MAC: 802.16a
Queue Type: Priority Queue with Drop Tailing
IoT Nodes: 500
Underlying router: TORA based routers
Network Dimensions: 300m×300m
Size of Packet: 500 bits per packet
Interval of communication: 0.0005 seconds per packet

Values for end-to-end communication latency, per-communication energy consumption, packet delivery ratio (PDR) per-communication, and communication throughput are assessed based on these common wireless network metrics. The performance of the individual models used for validation is shown by their labels in the accompanying tables, which tabulate these data. The suggested model's performance was compared with respect to DAC ABE [16] and CBS RE [23], which helped to validate its performance under various Number of Communication (NC) sequence sets (Table 1).

Table 1. Communication delay with the proposed encryption model averaged over different communication sets

NC	Delay (ms) DAC ABE [16]	Delay (ms) CBS RE [23]	Delay (ms) Proposed
100	0.44	0.50	0.26
150	0.52	0.60	0.31
200	0.63	0.72	0.38
250	0.72	0.83	0.43
300	0.81	0.93	0.49
350	0.90	1.04	0.54
400	1.00	1.14	0.60
450	1.09	1.24	0.65
500	1.17	1.34	0.70

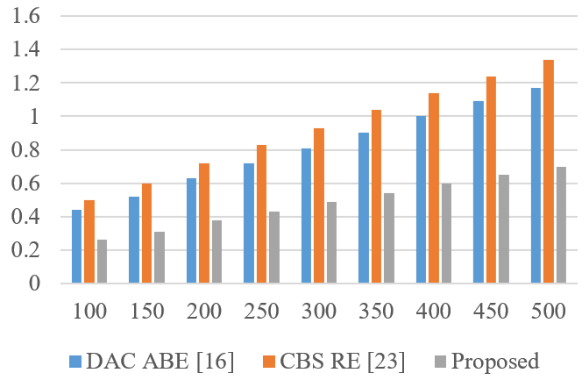

Figure 2. Communication delay with the proposed encryption model averaged over different communication sets

Based on this evaluation, and Figure 3, it can be observed that the proposed model showcased 18.5% lower delay when compared with DAC ABE [16], and 25.9% lower delay when compared with CBS RE [23], which makes it useful for high-speed IoT network scenarios. This is due to incorporation of encryption & decryption delays during selection of sub-curve parameters, which assists in improving communication performance under real-time IoT communication sets. Similarly, the energy consumption can be observed from Table 2 as follows:

Table 1. Communication energy levels with the proposed encryption model averaged over different communication sets

NC	Energy (mJ) DAC ABE [16]	Energy (mJ) CBS RE [23]	Energy (mJ) Proposed
100	6.25	7.19	3.73
150	6.62	7.61	3.95
200	6.95	8.00	4.15
250	7.28	8.38	4.35
300	7.62	8.76	4.55
350	7.98	9.18	4.76
400	8.36	9.61	4.99
450	8.70	10.00	5.20
500	9.03	10.38	5.39

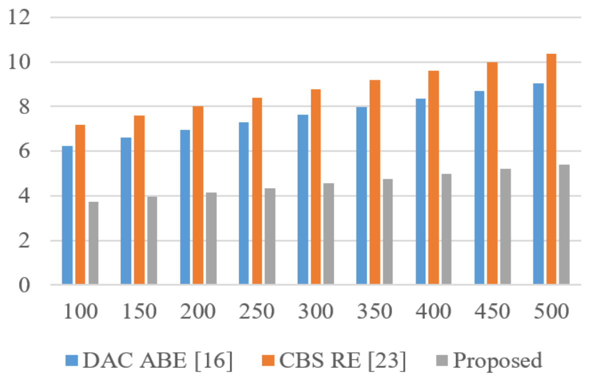

Figure 3. Communication energy levels with the proposed encryption model averaged over different communication sets

Based on this assessment and Figure 4, it can be seen that the proposed model demonstrated 28.3% and 34.2% reduced energy usage, respectively, when compared with DAC ABE [16] and R2, which makes it beneficial for high-lifetime IoT network situations. This is because real-time IoT communication sets help to improve communication performance by including encryption & decryption energy levels while choosing sub-curve parameters. Similarly, the throughput of these communications can be observed from Table 3 as follows:

Table 2. Communication throughput with the proposed encryption model averaged over different communication sets

NC	Thr (kbps) DAC ABE [16]	Thr (kbps) CBS RE [23]	Thr (kbps) Proposed
100	336.50	292.61	524.26
150	340.83	296.38	531.01
200	343.67	298.84	535.43
250	346.67	301.45	540.10
300	350.03	304.38	545.34
350	353.49	307.39	550.73
400	357.04	310.47	556.26
450	360.85	313.78	562.19
500	364.41	316.89	567.75

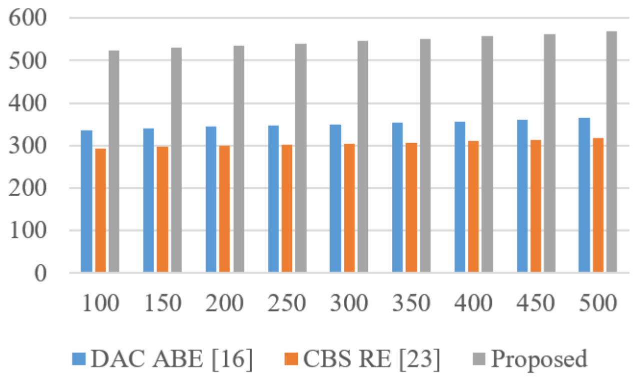

Figure 4. Communication throughput with the proposed encryption model averaged over different communication sets

The proposed model demonstrated 19.5% greater communication throughput when compared with DAC ABE [16] and 14.9% higher communication throughput when compared with CBS RE [23], which makes it ideal for high data-rate IoT network situations, as can be seen from this assessment in Figure 5. This is because real-time IoT communication sets help to improve communication performance by including processing delay levels and evaluating temporal performance while choosing sub-curve parameters. Similarly, the PDR of these communications can be observed from Table 4 as follows:

Table 3. Communication PDR with the proposed encryption model averaged over different communication sets

NC	PDR (%) DAC ABE [16]	PDR (%) CBS RE [23]	PDR (%) Proposed
100	98.92	99.02	98.97
150	99.05	99.15	99.10
200	99.17	99.27	99.22
250	99.27	99.37	99.32
300	99.36	99.46	99.41
350	99.47	99.57	99.52
400	99.59	99.69	99.64
450	99.71	99.81	99.76
500	99.83	99.93	99.88

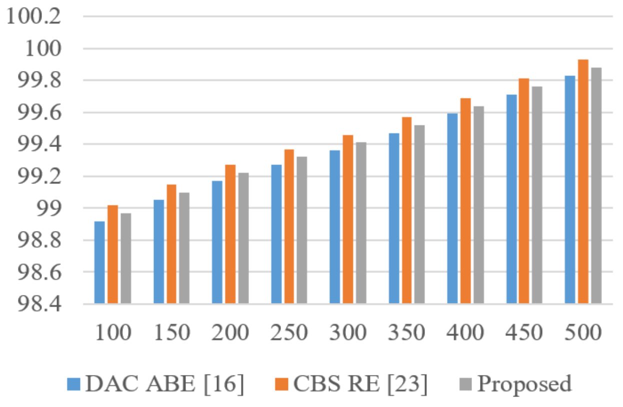

Figure 5. Communication PDR with the proposed encryption model averaged over different communication sets

Based on this assessment and Figure 6, it is apparent that the proposed model demonstrated comparable PDR when compared with DAC ABE [16] and CBS RE [23], making it appropriate for real-time IoT network applications. Due to the adoption of high-efficiency encryption methods, which decrease packet losses by mitigating various network threats, the PDR is often high. As a result, the suggested model is extremely effective and can be used for IoT networks with lower complexity and improved energy efficiency and larger data rates, making it scalable for various network situations.

4. CONCLUSION AND FUTURE SCOPE

The proposed model uses a combination of BFO for estimation of initial ECC sub-curves, and optimizes it via continuous Q-Learning operations. The model uses encryption & decryption delay, encryption & decryption energy, and reference curve performance levels in order to identify efficient sub-curve sets. The proposed model therefore demonstrated 18.5% reduced latency in comparison to DAC ABE [16] and 25.9% lower delay in comparison to CBS RE [23], making it effective for high-speed IoT network situations. This is because encryption and decryption delays are taken into account while choosing sub-curve parameters, helping to improve communication performance for real-time IoT communication sets. It is advantageous for high-lifetime IoT network situations as the proposed model's energy usage was 28.3% and 34.2% less than that of DAC ABE [16] and [R2, respectively]. This is because real-time IoT communication sets help to improve communication performance by including encryption & decryption energy levels while choosing sub-curve parameters. Secondary measures revealed that the proposed model had 19.5% greater communication throughput compared to DAC ABE [16] and 14.9% higher communication throughput compared to CBS RE [23], making it appropriate for high data-rate IoT network applications. This is because real-time IoT communication sets help to improve communication performance by including processing delay levels and evaluating temporal performance while choosing sub-curve parameters. When compared to DAC ABE [16] and CBS RE [23], the proposed model also showed comparable PDR, which makes it appropriate for real-time IoT network applications. Due to the adoption of high-efficiency encryption methods, which decrease packet losses by mitigating various network threats, the PDR is often high. As a result, the suggested model is very effective and suitable for low-complexity and high energy efficiency applications. Higher data rates on IoT networks make it scalable for many network situations. In future, the model's performance can be optimized via integration of hybrid bioinspired models that will assist in improving parameter selection for different scenarios. The model must be validated w.r.t. large-scale network sets, and its performance can be further improved via deployment of other encryption techniques which will make it useful for large-scale network scenarios.

REFERENCES

[1] Hao, J., Liu, J., Wu, W., Tang, F., Xian, M. (2019). Secure and fine-grained self-controlled outsourced data deletion in cloud-based IoT. IEEE Internet of Things Journal, 7(2): 1140-1153. https://doi.org/10.1109/JIOT.2019.2953082

[2] Gu, Z., Li, H., Khan, S., Deng, L., Du, X., Guizani, M., Tian, Z. (2021). Iepsbp: A cost-efficient image encryption algorithm based on parallel chaotic system for green IoT. IEEE Transactions on Green Communications and Networking, 6(1): 89-106. https://doi.org/10.1109/TGCN.2021.3095707

[3] Zhong, H., Zhang, S., Cui, J., Wei, L., Liu, L. (2021). Broadcast encryption scheme for V2I communication in VANETs. IEEE Transactions on Vehicular Technology, 71(3): 2749-2760. https://doi.org/10.1109/TVT.2021.3113660

[4] Sun, Y., Chatterjee, P., Chen, Y., Zhang, Y. (2021). Efficient identity-based encryption with revocation for data privacy in internet of things. IEEE Internet of Things Journal, 9(4): 2734-2743. https://doi.org/10.1109/JIOT.2021.3109655

[5] Sadhukhan, R. (2022). A classical and machine learning-based reliability analysis on catalan object encryption scheme. IEEE Transactions on Reliability, 71(2): 1022-1032. https://doi.org/10.1109/TR.2022.3156478

[6] Liu, S., Yu, J., Xiao, Y., Wan, Z., Wang, S., Yan, B. (2020). BC-SABE: Blockchain-aided searchable attribute-based encryption for cloud-IoT. IEEE Internet of Things Journal, 7(9): 7851-7867. https://doi.org/10.1109/JIOT.2020.2993231

[7] Al-Moliki, Y.M., Alresheedi, M.T., Al-Harthi, Y., Alqahtani, A.H. (2021). Robust lightweight-channel-independent OFDM-based encryption method for VLC-IoT networks. IEEE Internet of Things Journal, 9(6): 4661-4676. https://doi.org/10.1109/JIOT.2021.3107395

[8] Khan, S., Lee, W.K., Hwang, S.O. (2021). Scalable and efficient hardware architectures for authenticated encryption in IoT applications. IEEE Internet of Things Journal, 8(14): 11260-11275. https://doi.org/10.1109/JIOT.2021.3052184

[9] Cui, J., Lu, J., Zhong, H., Zhang, Q., Gu, C., Liu, L. (2021). Parallel key-insulated multiuser searchable encryption for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 18(7): 4875-4883. https://doi.org/10.1109/TII.2021.3110193

[10] Ramesh, S., Govindarasu, M. (2020). An efficient framework for privacy-preserving computations on encrypted IoT data. IEEE Internet of Things Journal, 7(9): 8700-8708. https://doi.org/10.1109/JIOT.2020.2998109

[11] Kuldeep, G., Zhang, Q. (2021). Design prototype and security analysis of a lightweight joint compression and encryption scheme for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(1): 165-181. https://doi.org/10.1109/JIOT.2021.3098859

[12] Gupta, N., Jati, A., Chattopadhyay, A. (2020). MemEnc: A lightweight, low-power, and transparent memory encryption engine for IoT. IEEE Internet of Things Journal, 8(9): 7182-7191. https://doi.org/10.1109/JIOT.2020.3040846

[13] Durga, R., Poovammal, E., Ramana, K., Jhaveri, R.H., Singh, S., Yoon, B. (2022). CES blocks—A novel chaotic encryption schemes-based blockchain system for an IoT environment. IEEE Access, 10: 11354-11371. https://doi.org/10.1109/ACCESS.2022.3144681

[14] Huang, K. (2021). Accountable and revocable large universe decentralized multi-authority attribute-based encryption for cloud-aided IoT. IEEE Access, 9: 123786-123804. https://doi.org/10.1109/ACCESS.2021.3110824

[15] Huang, K. (2021). Secure efficient revocable large universe multi-authority attribute-based encryption for cloud-aided IoT. IEEE Access, 9: 53576-53588. https://doi.org/10.1109/ACCESS.2021.3070907

[16] Wei, X., Yan, Y., Guo, S., Qiu, X., Qi, F. (2021). Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT. IEEE Internet of Things Journal, 9(11): 8143-8153. https://doi.org/10.1109/JIOT.2021.3111012

[17] Abd El-Latif, A.A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., Venegas-Andraca, S.E. (2020). Secure data encryption based on quantum walks for 5G Internet of Things scenario. IEEE Transactions on Network and Service Management, 17(1): 118-131. https://doi.org/10.1109/TNSM.2020.2969863

[18] Li, L., Wang, Z., Li, N. (2020). Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT. IEEE Access, 8: 176738-176749. https://doi.org/10.1109/ACCESS.2020.3025140

[19] Mamvong, J.N., Goteng, G.L., Zhou, B., Gao, Y. (2020). Efficient security algorithm for power-constrained IoT devices. IEEE Internet of Things Journal, 8(7): 5498-5509. https://doi.org/10.1109/JIOT.2020.3033435

[20] Niu, J., Li, X., Gao, J., Han, Y. (2019). Blockchain-based anti-key-leakage key aggregation searchable encryption for IoT. IEEE Internet of Things Journal, 7(2): 1502-1518. https://doi.org/10.1109/JIOT.2019.2956322

[21] Fotovvat, A., Rahman, G.M., Vedaei, S.S., Wahid, K.A. (2020). Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. IEEE Internet of Things Journal, 8(10): 8279-8290. https://doi.org/10.1109/JIOT.2020.3044526

[22] Fotovvat, A., Rahman, G.M., Vedaei, S.S., Wahid, K.A. (2020). Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. IEEE Internet of Things Journal, 8(10): 8279-8290. https://doi.org/10.1109/ACCESS.2020.3048192

[23] Khan, J., Li, J.P., Ahamad, B., Parveen, S., Haq, A.U., Khan, G.A., Sangaiah, A.K. (2020). SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. IEEE Access, 8: 15747-15767. https://doi.org/10.1109/ACCESS.2020.2966656

[24] Hussain, S., Ullah, I., Khattak, H., Adnan, M., Kumari, S., Ullah, S.S., ... & Khattak, S.J. (2020). A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid. IEEE Access, 8: 93230-93248. https://doi.org/10.1109/ACCESS.2020.2994988

[25] Khashan, O.A. (2020). Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment. IEEE Access, 8: 66878-66887. https://doi.org/10.1109/ACCESS.2020.2984317

[26] Xue, W., Luo, C., Shen, Y., Rana, R., Lan, G., Jha, S., ... & Hu, W. (2020). Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things. IEEE Transactions on Mobile Computing, 20(10): 3049-3065. https://doi.org/10.1109/TMC.2020.2992737

[27] Unde, A.S., Deepthi, P.P. (2019). Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(1): 167-171. https://doi.org/10.1109/TCSII.2019.2897839

[28] Khattabi, Y.M., Matalgah, M.M., Olama, M.M. (2020). Revisiting lightweight encryption for IoT applications: Error performance and throughput in wireless fading channels with and without coding. IEEE Access, 8: 13429-13443. https://doi.org/10.1109/ACCESS.2020.2966596

[29] Chen, X., Liu, Y., Chao, H.C., Li, Y. (2020). Ciphertext-policy hierarchical attribute-based encryption against key-delegation abuse for IoT-connected healthcare system. IEEE Access, 8: 86630-86650. https://doi.org/10.1109/ACCESS.2020.2986381

[30] Bhattacharya, S., Pandey, M. (2021). Issues and Challenges in Incorporating the Internet of Things with the Healthcare Sector. Data Engineering and Communication Technology: Proceedings of ICDECT 2020: 639-651. https://doi.org/10.1007/978-981-16-0081-4_64

[31] Bhattacharya, S., Pandey, M. (2021). Internet of things for green technology. Green Eng. Technol., pp. 243–258. https://doi.org/10.1201/9781003176275-14

[32] Wang, X., Liu, P. (2021). A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Transactions on Circuits and Systems I: Regular Papers, 69(3): 1291-1301. https://doi.org/10.1109/TCSI.2021.3133318

[33] Noura, H.N., Salman, O., Couturier, R., Chehab, A. (2022). A single-pass and one-round message authentication encryption for limited IoT devices. IEEE Internet of Things Journal, 9(18): 17885-17900. https://doi.org/10.1109/JIOT.2022.3161192

[34] Deb, P.K., Mukherjee, A., Misra, S. (2022). CEaaS: Constrained encryption as a service in fog-enabled IoT. IEEE Internet of Things Journal, 9(20): 19803-19810. https://doi.org/10.1109/JIOT.2022.3167832

[35] Zhuang, E.S., Fan, C.I., Kuo, I.H. (2022). Multiauthority attribute-based encryption with dynamic membership from lattices. IEEE Access, 10: 58254-58267. https://doi.org/10.1109/ACCESS.2022.3179110

[36] Al-Moliki, Y.M., Alresheedi, M.T., Al-Harthi, Y., Alqahtani, A.H. (2021). Robust lightweight-channel-independent OFDM-based encryption method for VLC-IoT networks. IEEE Internet of Things Journal, 9(6): 4661-4676. https://doi.org/10.1109/JIOT.2021.3107395

[37] Miao, Y., Tong, Q., Deng, R.H., Choo, K.K.R., Liu, X., Li, H. (2020). Verifiable searchable encryption framework against insider keyword-guessing attack in cloud storage. IEEE Transactions on Cloud Computing, 10(2): 835-848. https://doi.org/10.1109/TCC.2020.2989296