Computers, Materials & Continua
DOI: 10.32604/cmc.2022.027858
Article

Tech Science Press

An Effective Signcryption with Optimization Algorithm for IoT-enabled Secure Data Transmission

A. Chinnappa* **and C. Vijayakumaran**

Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology,
Kattankulathur, 603203, Tamilnadu, India
*Corresponding Author: A. Chinnappa. Email: ca5461@srmist.edu.in

Received: 27 January 2022; Accepted: 01 April 2022

Abstract: Internet of Things (IoT) allows several low resources and controlled devices to interconnect, calculate processes and make decisions in the communication network. In the heterogeneous environment for IoT devices, several challenging issues such as energy, storage, efficiency, and security. The design of encryption techniques enables the transmission of the data in the IoT environment in a secured way. The proper selection of optimal keys helps to boost the encryption performance. With this motivation, the study presents a signcryption with quantum chaotic krill herd algorithm for secured data transmission (SCQCKH-SDT) in IoT environment. The proposed SCQCKH-SDT technique aims to effectively encrypts the data by the use of optimal keys generated by the CQKH algorithm. The proposed SCQCKH-SDT technique initially employs the signcryption technique for the encryption of data. In order to optimize the secrecy, the optimal key generation process is carried out using Chaotic Krill Herd (CQKH) algorithm. The CQKH algorithm incorporates the concept of quantum computing and chaotic theory into the traditional KH algorithm. The performance validation of the SCQCKH-SDT technique is performed using benchmark dataset. An extensive comparative analysis reported the superior performance of the SCQCKH-SDT technique over the recent approaches.

Keywords: Security; Internet of Things; encryption; optimal key generation; metaheuristics

1 Introduction

Recently, with the expansion of new network advancements and a constant updating of terminal devices [1], Internet of Things (IoT) has become widespread. It is estimated that IoT would attain fifty billion devices by 2020. IoT is the effect of tremendous growth, beginning with computerization of some processes, utilizing electronic gadgets, and the procedure is updated with transmission capacity [2]. Owing to the development in remote transmission, embedded framework, and sensor IoT system is widely utilized in some spaces. While the high accessibility of IoT systems is proportionate to increasing security and privacy risks [3]. Although efficiency of IoT systems must improve the lives of many people, customary digital attack on IoT framework is feasible [4]. The use of system privacy and security highlight to increase in worth issues, on the ground that IoT method has different elements: User Interface (UI) component, implanted gadget, device control, cloud computing for data processing, etc. [5]. Privacy-preserving is a security problem confronted by end-client when managing IoT-enabled applications. Cloud computing (CC) provides the basis and storing IoT data processing. Cryptographic-based methodology was presented as a standout amongst other methods to guarantee the privacy of IoT information. Cryptosystem supplies components to ensure data integrity and classification. When the information is continuously encrypted in the cloud, then the suspicions are evacuated, and control isn't lost [6]. The security necessity for data and algorithms has become extremely challenging in the past few years. The different types of attacks in IoT environment is shown in Fig. 1.

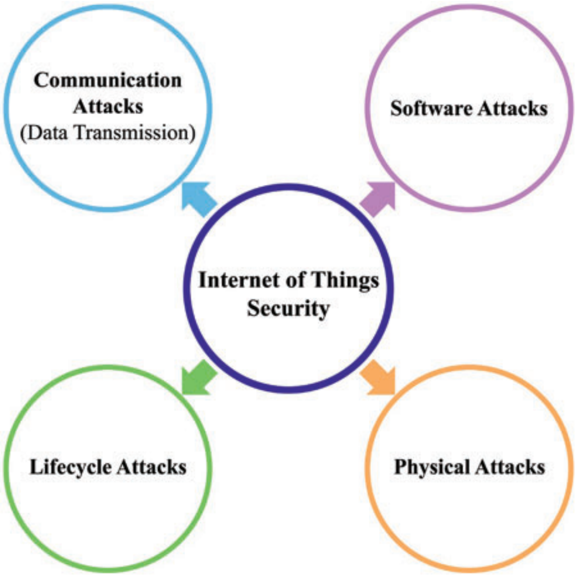
Communication Attacks (Data Transmission)
Software Attacks
Internet of Things Security
Lifecycle Attacks
Physical Attacks

Figure 1: Types of attacks in IoT security

In such scenarios, it is crucial to frame a powerful method for guarantying the trustworthiness and safety of the patient symptomatic information that is received and transmitted from IoT [7]. 'Encryption cryptography' is the method where the message is encrypted so that the programmer could not read it, yet that is permitted by the presented faculty. Rivest–Shamir–Adleman (RSA) and Advanced Encryption Standard (AES) approaches are employed for data encryption. Consequently, the IoT offer ascent to different restorative application includes remote healthcare monitoring [8]. For example, in light of the patient healthcare information, a social insurance specialist cooperative could enhance by examining the person's condition and could recommend the earlier intercession and optimal treatment. Traditional security systems won't be capable of obliging IoT devices completely because a major part of this device has battery-restricted assets and limitations; in other cases, this component requires further resources [9]. Long key makes the figure hard to break, and also, it approves a systematic 'scramble and decodes' procedure. In general, RSA is an open key calculation that is widely used as a part of individual communication and business areas [10]. Jang et al. [11] presented an approach to partially encrypt secured data in images with FF1 and FF3-1. The presented approach encodes secured data without raising the data size, resolving the issue of unused memory space. Further, certain section of encrypted image is recognized and decrypted beforehand decryption of whole data, which address the problem of attacking image encryption and privacy masking approaches. Medileh et al. [12] introduced a scalable encryption method named Flexible encryption method (FlexenTech), to secure IoT data. The presented method is appropriate for resource-limited networks and devices. It provides a lower encryption time, protects against popular attacks namely replay attacks and determines configurable modes, whereas another amount of key sizes of rounds might be utilized. Jeong et al. [13] verified optimum lightweight cryptography for privacy improvement in an IoT based Environment Monitoring Scheme which controls and monitors the nearby humidity and temperature. Then, compared processing time and CPU usage while different lightweight cryptography has been employed. This assisted us to accomplish that the optimum lightweight cryptography for IoT based method is Lightweight Encryption Algorithm (LEA) that is block cipher. Chowdhury et al. [14] proposed Modified AES (MAES), a lightweight version of AES that meets the requirement. A One Dimensional (1D) Substitution Box is presented by creating a square matrix in affine transformation stage of MAES. The authors in [15] presented a hybridization of data encrypting method for sheltering the data diagnoses in healthcare images. The presented method is proposed by integrating 2-Dimensional (2D)-Discrete Wavelet Transform (DWT)-2 L or 2D-DWT-1 L steganography. The hybrid encryption is constructed by strategically using AES and RSA approaches to secure diagnoses data to be embedded with Red Green Blue (RGB) channel. The main novelty is the usage of Adoptive Genetic Algorithm with Optimum Pixel Adjustment Process (AGA-OPAP) improves data hiding capacity and imperceptibility feature.

This paper presents a signcryption with quantum chaotic krill herd algorithm for secured data transmission (SCQCKH-SDT) in IoT environment. The proposed SCQCKH-SDT technique initially employs the signcryption technique for the encryption of data and optimal key generation process using the CQKH algorithm. The CQKH algorithm incorporates the concept of quantum computing and chaotic theory into the traditional KH algorithm. The performance validation of the SCQCKH-SDT technique is performed using benchmark dataset and the results are examined under various aspects.

2 The Proposed Model

This paper has developed a novel SCQCKH-SDT to effectively encrypt the data by the use of optimal keys generated by the CQKH algorithm in the IoT environment. The workflow of proposed model is given in Fig. 2. The proposed SCQCKH-SDT technique follows a 2-stage process namely signcryption based encryption and CQKH based optimal key generation process. The CQKH algorithm incorporates the concept of quantum computing and chaotic theory into the traditional Kill Herd (KH) algorithm.

2.1 Stage 1: Encryption Process

At the initial stage, the signcryption technique can be employed to encrypt the data before transmission process. It is a public key cryptographic technique that concurrently fulfills the digital signature and opens key encryption with minimal complexity. It involves several subprocesses as defined in the following section [16]:

The key generating method: The probabilistic approach takes 2 prime numbers (p, q) as input and gives private key $S_k(n, d)$ and symmetric key C_k (p, q) and the output public key $P_k(n, e)$

Key generating method $\rightarrow (P_k, S_k, C_k)$.

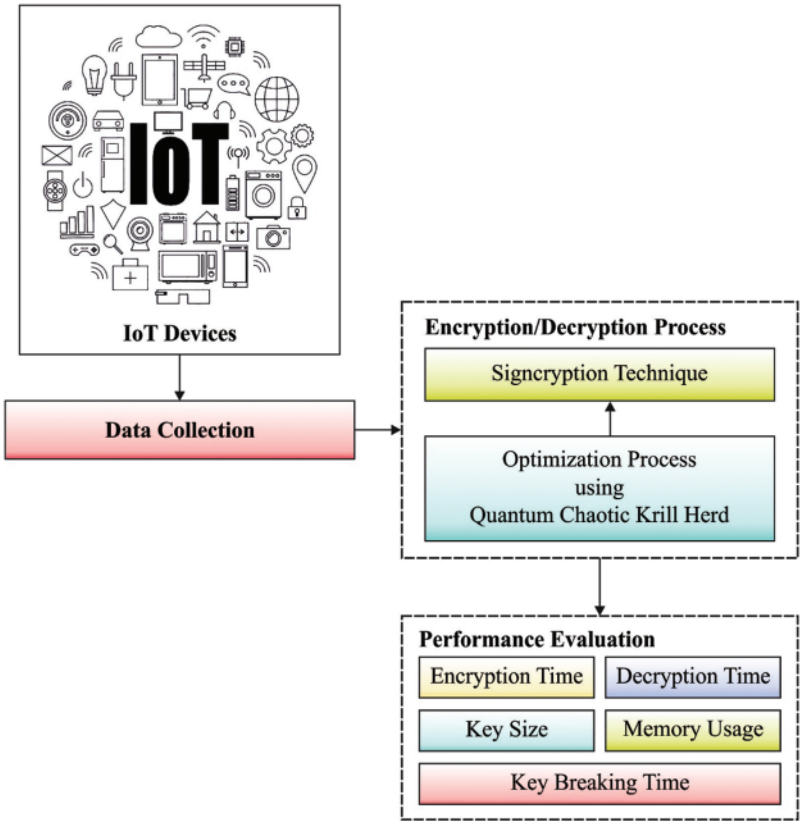

Figure 2: Workflow of SCQCKH-SDT technique

Data encrypting method (DEM): The probabilistic approach takes the symmetric key C_k and original message M and give output ciphertext CM. (M, C_k)

Key generating method → (CM).

Key derivative key: The probabilistic approach take input as length of integer $nLen$ and integer n and give output (z, Z) whereas z represents arbitrary integer is carefully selected from zero to $n - 1$ and Z represent $nLen$ string values as important bit first that is converted from z. $(n, nLen)$

Key derivative $key \rightarrow (z, Z)$

Encryption: The probabilistic approach takes input as receivers public key P_k (n, e) and arbitrary integer z produce the output (c, C) whereas c represents the ciphertext of z and C denotes $nLen$ string values as important bit first that is converted from c. $(P_k, (n, e))$ Encrypted → (c, C). In the presented approach, the encryption is performed using Elliptic Curve Cryptography (ECC) method.

Key derivative function: The probabilistic approach (hash function – Message Digest(MD5)) takes length of key encryption key $kekLen$ and input integer Z is acquired from Z as well give the output (KEK) key encrypted key. $(Z$, kekLen)

Key derivative function → (KEK)

Wrapped function: The probabilistic approach (Wrapping) takes input as key encrypting key (KEK) and symmetric key C_k and give output wrapping key WK. (C_k, KEK)

Wrapped function → WK

Concatenation: The probabilistic approach takes input ciphertext C, wrapping key WK, and output encapsulation key EK.

Signcryption: The probabilistic approach takes senders private key $S_k\ (n, d)$, input ciphertext CM, encapsulated key EK and output of the signcryption data (δD). $(CM, S_k, (n, d), EK)$

Signcryption → (δD)

Unsigncryption procedure

Signature authentication: The probabilistic approach takes input senders public key $S(P_k)$, signcryption data δD, and produce output as 1 followed by the signature is valid otherwise return $\perp$ that indicates invalid signature. $(S(P_k), \delta D)$ Signature confirmation → 1 $or\perp$.

Detach: The probabilistic approach takes input EK and outputs the wrapped key WK, ciphertext C.

Decryption: The probabilistic approach takes input ciphertext C the receivers private key $S_k(n, d)$ produce the output Z.

Key derivative function: The probabilistic approach (hash function (MD5)) take input random integer Z and length of key encrypted key kekLen is acquired from Z and give the output (KEK) *key* encrypted key. $(Z,$ kekLen)

Key derivative function → (KEK)

Unwrapped function: The probabilistic approach (Wrapping) takes input as key encrypting key (KEK) and wrapped key WK and give the output symmetric key C_k. (WK, KEK)

Wrapped function → C_k.

Data encrypting method (DEM): The probabilistic approach (AES) takes ciphertext CM and the symmetric key C_k and give the output original message $M.(CM, C_k)$

Key generating method →(M).

2.2 *Stage 2: Optimal Key Generation Process*

During the encryption process, the choice of keys plays a vital role and can be optimally generated by the use of CQKH algorithm. Krill herd (KH) is a metaheuristic optimization approach to resolve optimization issues that is depending on the stimulation of the KH swarm regarding environmental and biological methods [17]. The time- based location of an individual krill in two-dimensional surface is given below:

- Motion influenced by krill individual;
- Foraging movement
- Random or Physical diffusion

The Lagrangian method is generalized to d-dimension decision area.

$$\frac{dX_i}{dt} = N_i + F_i + D_i \tag{1}$$

In which D_i denotes the physical diffusion of i-th krill individual; F_i represent the foraging movement; and N_i indicates the movement influenced by krill individual. Fig. 3 shows the flowchart of KH algorithm [18]. The motion influenced by krill individual, the direction of influenced movement,

α_i, is evaluated using a local swarm density (local effect), repulsive swarm density (repulsive effect), and the targeted swarm density (targeted effect).

$$N_i^{new} = N^{max}\alpha_i + \omega_n N_i^{\mathrm{old}} \tag{2}$$

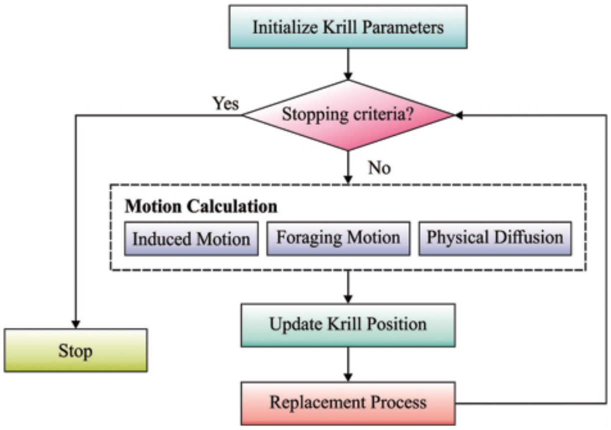

Figure 3: Flowchart of KH algorithm

Let N^{maks} be the maximal induced speed, N^{old} represent the final movement induced, ω_n implies the inertia weight of movement induced within [0, 1]. The foraging movement can be defined by the two major factors. Previous experience and Food position regarding the food position:

$$F_i = V_f \beta_j + \omega_{\mathrm{f}} F_i^{\mathrm{old}} \tag{3}$$

whereas

$$\beta_j = \beta_j^{food} + \beta_j^{best} \tag{4}$$

ω_f denotes the inertia weight of foraging movement among [0,1], F_i^{old} indicates the final foraging movement and V_f represent the foraging speed. The physical diffusion of krill individuals is processed as an arbitrary method. This movement is determined based on arbitrary directional vector and maximal diffusion speed.

$$D_i = D^{max}\delta \tag{5}$$

whereas δ indicates the random directional vector, and D^{max} represent the maximal diffusion speed and in the range of [1,1]. From the abovementioned motions, efficient parameter of the motion, the location vector of a krill individual at time t to $t + \Delta t$ can be expressed as follows:

$$X_i(t + \Delta t) = X_i(t) + \Delta t \frac{dX_i}{dt} \tag{6}$$

where Δt represents constant and must be regulated interms of optimization problem. The variable is considered as a scaling factor of the speed vector. Δt based on the searching region and attained from the subsequent formula:

$$\Delta t = c_t \sum_{j=1}^{NV} \left(UB_j - LB_j\right) \tag{7}$$

In which NV represent the overall amount of parameters, UB_j and LB_j denotes upper and lower limits of the jth parameter ($j = 1, 2, \ldots;, NV$), correspondingly. Therefore, the absolute subtraction displays the searching region. Lower values of C_ζ makes the krill individual implement the searching in the space. In random-based optimization method, the method utilizing chaotic variable rather than random variable is named chaotic optimization approach (COA). In this algorithm, chaos has the features of ergodicity and non-repetition, it could implement entire searching at high speed when compared to stochastic search that is based on probability. To satisfy this, here 1-D non-invertible map is utilized for producing chaotic set [19]. Therefore, the CKH algorithm is derived by the integration of KH algorithm with chaotic concept.

The QCKH algorithm is derived by the use of QC, which is a current domain in computer science that is concerned in quantum computer with the phenomena of quantum mechanism namely entanglement, quantum gate, and state superposition [20]. The basic data unit in quantum computation is Q-bit. A Q-bit might be in the state $|1>$, in the state $|0>$, or superposition state $|0> and |1>$. Based on Dirac notation, the Q-bit is denoted as integration of states $|0> and\ 1>$:

$$|Q>=\alpha|0>+\beta|1> \text{ thus } |\alpha|^2+|\beta|^2=1 \tag{8}$$

whereas α and β represent complex values. $|\alpha|^2$ (resp. $|\beta|^2$) denotes the likelihood to identify the Q-bit in state zero. Then, A quantum register of size n is constituted from n Q-bits. It characterizes a superposition of n Q-bits, that is, it comprises up to 2^n probable values. It can be characterized as follows:

$$\Psi=\sum_{x=0}^{2^n-1} C_X|X> \tag{9}$$

The amplitude C_X satisfies the subsequent property:

$$\sum_{x=0}^{2^n-1}|C_X|^2=1 \tag{10}$$

The state of Q-bit is altered using quantum gate. A Q-gate refers to a reversible gate and characterized by a unitary operator U which acts on Q-bit basis state satisfies $U^+U=UU^+$, in which U^+ denotes the Hermitian adjoint of U. It contains numerous Q-gates, namely NOT gate, controlled NOT gate, Hadamard gate, rotation gate, and so on. In order to optimally generate the keys for the signcryption process, the CQKH algorithm is employed. It computes a fitness function by maximizing the PSNR values for scrambling and unscrambling the data. The CQKH algorithm can be employed for choosing the keys and the fitness function can be defined using Eq. (11):

$$Fitness=MAX\{PSNR\} \tag{11}$$

3 Results and Discussion

This section inspects the security analysis of the SCQCKH-SDT technique under various dimensions [21–24]. The results are investigated under distinct file sizes [25–27]. Tab. 1 offers the overall encryption result analysis of the SCQCKH-SDT technique under distinct file sizes. The results denoted that the SCQCKH-SDT technique has accomplished effective security in the IoT environment. Fig. 4 demonstrates the encryption time (ET) and decryption time (DT) analysis [28] of the SCQCKH-SDT technique under various file sizes. The figure reported that the SCQCKH-SDT technique has resulted to effectual outcome with least ET and DT. For instance, with 10kb file size, the SCQCKH-SDT technique has attained ET and DT of 550.943 and 86.548 s respectively. Simultaneously, with 30 kb file size, the SCQCKH-SDT technique has obtained ET and DT of 581.053 and 88.371 s respectively.

Concurrently, with 50 kb file size, the SCQCKH-SDT technique has achieved ET and DT of 597.168 and 101.130 s respectively.

Table 1: Encryption performance analysis of SCQCKH-SDT technique

File size (kb)	Encryption time (s)	Encryption memory (kb)	Key size (kb)	Key breaking time (s)	Decryption time (s)	Decryption memory (kb)
10	550.943	1080.370	25.000	0.097	86.548	607.730
20	570.027	1139.350	31.000	0.097	85.637	596.700
30	581.053	1099.220	44.000	0.099	88.371	597.100
40	582.749	1087.370	56.000	0.099	90.649	618.170
50	597.168	1152.240	64.000	0.095	101.130	621.370

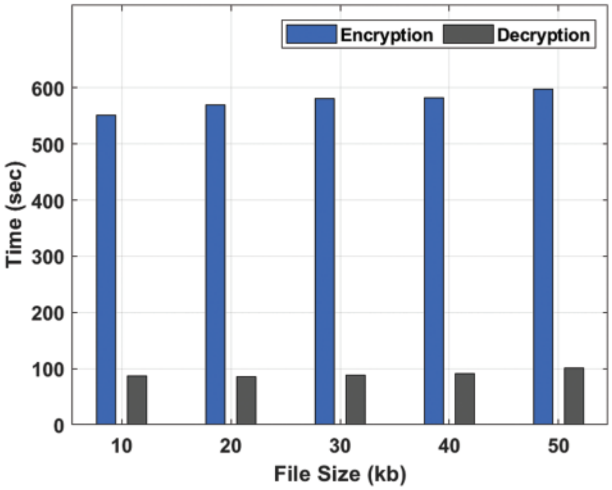

Figure 4: ET and DT analysis of SCQCKH-SDT technique

A brief encryption memory (EM) and decryption memory (DM) analysis [29] of the SCQCKH-SDT technique takes place under varying file sizes in Fig. 5. The results indicated that the SCQCKH-SDT technique has required minimal EM and DM under all files. For instance, with 10kb file size, the SCQCKH-SDT technique has needed EM and DM of 1080.370 and 607.730 kB respectively. Along with that, with 30 kb file size, the SCQCKH-SDT technique has offered EM and DM of 1099.220 and 597.100 kB respectively. In line with, with 50 kb file size, the SCQCKH-SDT technique has resulted to ET and DT of 1152.240 and 621.370 kb respectively.

An extensive comparative result analysis of the SCQCKH-SDT technique with other techniques take place in Tab. 2 and Fig. 6. The table values implied that the SCQCKH-SDT technique has reached lower ET over the other methods under all file sizes. For instance, with 10 kb file size, the SCQCKH-SDT technique has provided least ET of 550.943 s whereas the ECC, HE, and OHE techniques have offered increased ET of 589.958, 574.692 and 561.121 s respectively. Moreover, with 30kb file size, the SCQCKH-SDT technique has gained reduced ET of 581.053 s whereas the ECC, HE, and OHE techniques have obtained increased ET of 626.005, 606.073 and 598.864 s respectively. Furthermore, with 50 kb file size, the SCQCKH-SDT technique has resulted to lower ET of 597.168 s whereas the ECC, HE, and OHE techniques have reached higher ET of 648.481, 636.183 and 611.586 s respectively.

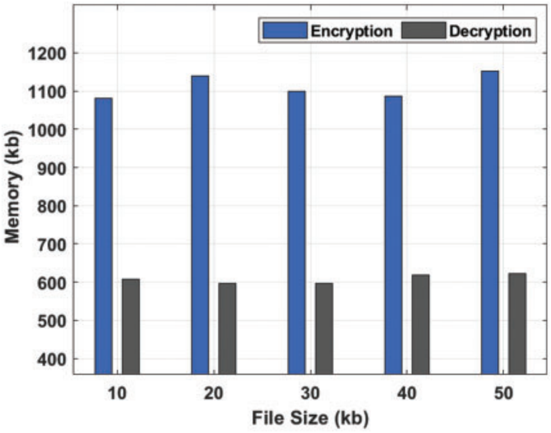

Figure 5: EM and DM analysis of SCQCKH-SDT technique

Table 2: Comparative ET analysis of SCQCKH-SDT technique with other techniques

	Encryption time (s)			
File size (kb)	ECC	HE	OHE	SCQCKH-SDT
10	589.958	574.692	561.121	550.943
20	601.409	598.864	584.87	570.027
30	626.005	606.073	598.864	581.053
40	636.607	618.796	600.985	582.749
50	648.481	636.183	611.586	597.168

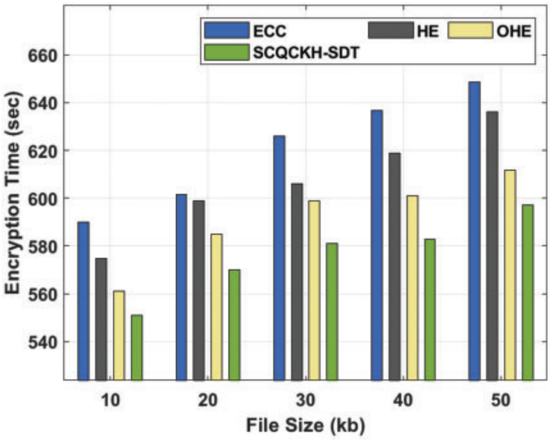

Figure 6: ET Analysis of SCQCKH-SDT technique under distinct file sizes

A comparison study of the SCQCKH-SDT technique in terms of DT is offered in Tab. 3 and Fig. 7. The experimental results reported that the SCQCKH-SDT technique has accomplished minimal DT over the other methods under all file sizes.

Table 3: Comparative DT analysis of the SCQCKH-SDT technique under distinct file sizes

Decryption time (s)				
File size (kb)	ECC	HE	OHE	SCQCKH-SDT
10	113.433	103.408	97.940	86.548
20	112.066	105.687	99.307	85.637
30	122.091	115.256	101.586	88.371
40	131.205	125.737	113.433	90.649
50	137.129	137.584	125.281	101.13

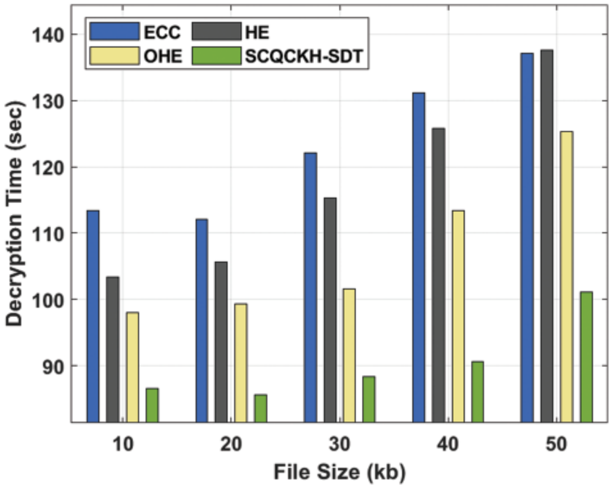

Figure 7: DT analysis of the SCQCKH-SDT with existing techniques

For instance, with 10 kb file size, the SCQCKH-SDT technique has accomplished lower DT of 86.548 s whereas the ECC, HE, and OHE techniques have attained higher DT of 113.433, 103.408 and 97.940 s respectively. Concurrently, with 30 kb file size, the SCQCKH-SDT technique has depicted minimum DT of 88.371 s whereas the ECC, HE, and OHE techniques have exhibited maximum DT of 122.091, 115.256 and 101.586 s respectively. Eventually, with 50 kb file size, the SCQCKH-SDT technique has resulted to lower DT of 101.13 s whereas the ECC, HE, and OHE techniques have demonstrated higher DT of 137.129, 137.584 and 125.281 s respectively.

Tab. 4 and Fig. 8 inspects the key breaking time (KBT) analysis [30] of the SCQCKH-SDT technique with the recent methods. The results demonstrated that the SCQCKH-SDT technique has demonstrated better KBT under all files. For instance, with 10 s file size, the SCQCKH-SDT technique has offered raised KBT of 0.097 s whereas the ECC, HE, and OHE techniques have obtained reduced KBTs of 0.090, 0.094 and 0.096 s respectively. Similarly, with 30 s file size, the SCQCKH-SDT technique has resulted to better KBT of 0.099 s whereas the ECC, HE, and OHE techniques have accomplished decreased KBTs of 0.090, 0.094 and 0.097 s respectively. Likewise, with 50 s file size, the

SCQCKH-SDT technique has provided increased KBT of 0.095 s whereas the ECC, HE, and OHE techniques have obtained reduced KBTs of 0.090, 0.092, and 0.094 respectively.

Table 4: Comparative KBT analysis of the SCQCKH-SDT technique under distinct file sizes

	Key breaking time (s)			
File size (kb)	ECC	HE	OHE	SCQCKH-SDT
10	0.090	0.094	0.096	0.097
20	0.085	0.092	0.095	0.097
30	0.090	0.094	0.097	0.099
40	0.092	0.095	0.098	0.099
50	0.090	0.092	0.094	0.095

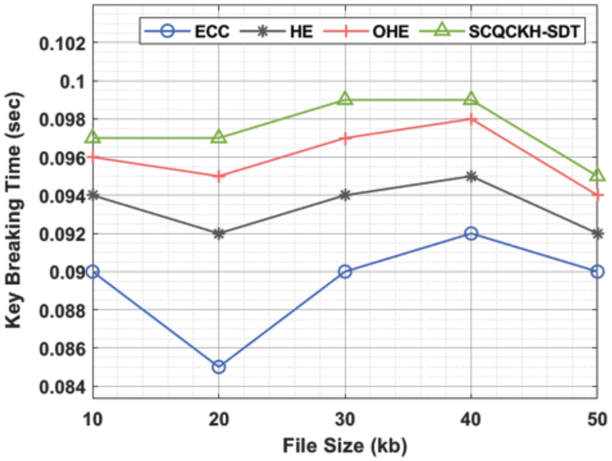

Figure 8: KBT analysis of the SCQCKH-SDT with existing techniques

The key size analysis of the SCQCKH-SDT technique is compared with the recent methods in Tab. 5 and Fig. 9. The experimental results indicated that the SCQCKH-SDT technique has accomplished increased key size under all files. For instance, with 10 kb file size, the SCQCKH-SDT technique has provided increased key size of 25 kb whereas the ECC, HE, and OHE techniques have obtained reduced key sizes of 20, 21 and 22 kb respectively. Along with that, with 30 kb file size, the SCQCKH-SDT technique has resulted to better key size of 44 kb whereas the ECC, HE, and OHE techniques have accomplished decreased key sizes of 36, 40 and 42 kb respectively. In line with, with 50 kb file size, the SCQCKH-SDT technique has provided increased key size of 64 kb whereas the ECC, HE, and OHE techniques have obtained reduced key sizes of 58, 60 and 62 kb respectively.

Finally, a brief EM and DM analysis of the SCQCKH-SDT technique with existing methods take place in Tab. 6 and Fig. 10. The results shown that the ECC algorithm has shown worse outcome with the EM and DM of 1022.26 and 510.294 kb respectively. Followed by, the HE and OHE techniques have obtained slightly increased values of EM and DM. However, the SCQCKH-SDT technique has accomplished effective performance with the higher EM and DM of 1152.24 and 621.37 kb respectively.

Table 5: Comparative Key size analysis of the SCQCKH-SDT with existing techniques

Key size (kb)				
File size (kb)	ECC	HE	OHE	SCQCKH-SDT
10	20.00	21.00	22.00	25.00
20	24.00	26.00	29.00	31.00
30	36.00	40.00	42.00	44.00
40	48.00	51.00	53.00	56.00
50	58.00	60.00	62.00	64.00

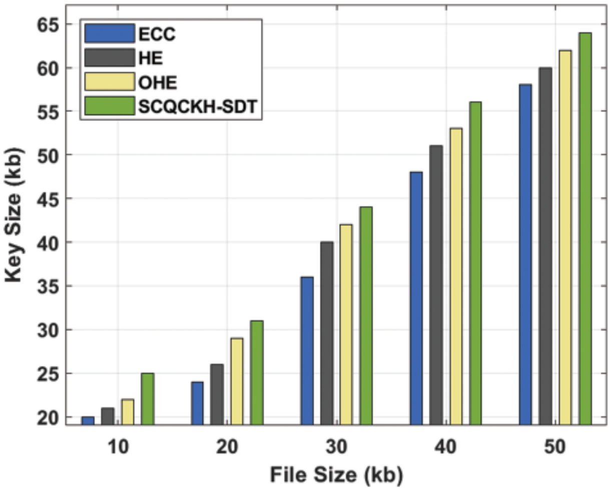

Figure 9: Key size analysis of the SCQCKH-SDT with existing techniques

Table 6: Comparative Memory Analysis of the SCQCKH-SDT with existing techniques

	Memory (kb)	
Methods	Encryption	Decryption
ECC algorithm	1022.26	510.294
HE algorithm	1066.54	526.898
OHE algorithm	1088.68	560.106
SCQCKH-SDT	1152.24	621.37

From the detailed results and discussion, it is obvious that the SCQCKH-SDT technique has outperformed the other techniques under diverse aspects. Therefore, the SCQCKH-SDT technique can be utilized as an effective tool for accomplishing security in the IoT environment.

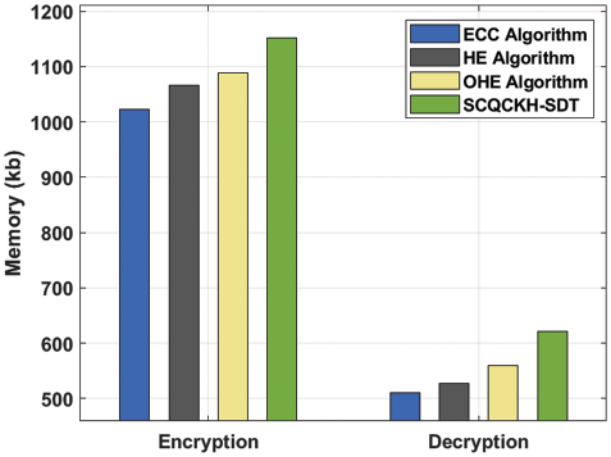

Figure 10: Comparative EM and DM analysis of the SCQCKH-SDT with existing techniques

4 Conclusion

This paper has developed a SCQCKH-SDT to effectively encrypted the data by the use of optimal keys generated by the CQKH algorithm in the IoT environment. The proposed SCQCKH-SDT technique follows a 2-stage process namely signcryption based encryption and CQKH based optimal key generation process. The CQKH algorithm incorporates the concept of quantum computing and chaotic theory into the traditional KH algorithm. The performance validation of the SCQCKH-SDT technique is performed using benchmark dataset and the results are examined under various aspects. An extensive comparative analysis reported the superior performance of the SCQCKH-SDT technique over the recent approaches. In future, lightweight cryptographic techniques with classification models can be designed.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Rajesh, V. Paul, V. G. Menon and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, pp. 293– 312, 2019.

[2] S. Kim and I. Lee, "IoT device security based on proxy re-encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1267–1273, 2018.

[3] A. Hameed and A. Alomary, "Security issues in IoT: A survey," in *Proc. Int. Conf. on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Bahrain, pp. 1–5, 2019.

[4] N. Pakniat, D. Shiraly and Z. Eslami, "Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial IoT," *Journal of Information Security and Applications*, vol. 53, no. 5, pp. 102525–102540, 2020.

[5] B. Y. Sung, K. B. Kim and K. W. Shin, "An AES-GCM authenticated encryption crypto-core for IoT security," in *Proc. Int. Conf. on Electronics, Information, and Communication (ICEIC*, Hawaii, USA, pp. 1–3, 2018.

[6] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang *et al.,* "IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT," *Future Generation Computer Systems*, vol. 95, no. 7, pp. 344–353, 2019.

[7] D. A. T. Toledo, O. R. L. Bonilla, E. E. G. Guerrero, E. T. Cuautle, D. L. Mancilla *et al.,* "Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps," *Chaos, Solitons & Fractals*, vol. 153, no. 3, pp. 111506–111520, 2021.

[8] M. A. F. Al-Husainy, B. Al-Shargabi and S. Aljawarneh, "Lightweight cryptography system for IoT devices using DNA," *Computers & Electrical Engineering*, vol. 95, pp. 107418, 2021.

[9] M. sarac, N. Pavlovic, N. Bacanin, F. Al-Turjman and S. Adamovic, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Reports*, vol. 7, no. 18, pp. 8075–8082, 2021.

[10] M. S. Kang, "Design of AES-based encryption chip for IoT security," *The Journal of the Institute of Internet, Broadcasting and Communication*, vol. 21, no. 1, pp. 1–6, 2021.

[11] W. Jang and S. Y. Lee, "Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment," *International Journal of Distributed Sensor Networks*, vol. 16, no. 3, pp. 1–16, 2021.

[12] S. Medileh, A. Laouid, R. Euler, A. Bounceur, M. Hammoudeh *et al.,* "A flexible encryption technique for the Internet of Things environment," *Ad Hoc Networks*, vol. 106, no. 1, pp. 102240–102258, 2020.

[13] J. Jeong, L. Bajracharya and M. Hwang, "Optimal lightweight cryptography algorithm for environmental monitoring service based on IoT," in *Proc. Int. Conf. on Information Science and Applications*, Singapore, pp. 361–367, 2018.

[14] A. R. Chowdhury, J. Mahmud, A. R. M. Kamal and M. A. Hamid, "MAES: Modified advanced encryption standard for resource constraint environments," in *Proc. IEEE Sensors Applications Symp. (SAS)*, Seoul, Korea, pp. 1–6, 2018.

[15] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21165–21202, 2021.

[16] R. B. Nishanth, B. Ramakrishnan and M. Selvi, "Improved signcryption algorithm for information security in networks," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 3, pp. 151–157, 2015.

[17] G. G. Wang, L. Guo, A. H. Gandomi, G. S. Hao, H. Wang *et al.,* "Chaotic krill herd algorithm," *Information Sciences*, vol. 274, no. 2, pp. 17–34, 2014.

[18] P. Niveditha, M. S. Sujatha and M. Vijaya Kumar, "Implementation of krill herd algorithm for optimal sizing and placing of DG in radial distribution system," *International Journal of Grid and Distributed Computing*, vol. 11, no. 9, pp. 51–64, 2018.

[19] S. Li and Y. Tian, "Krill herd algorithm with chaotic time interval and elitism scheme," *Systems Science & Control Engineering*, vol. 7, no. 2, pp. 71–84, 2019.

[20] R. K. Agrawal, B. Kaur and S. Sharma, "Quantum based whale optimization algorithm for wrapper feature selection," *Applied Soft Computing*, vol. 89, no. 1, pp. 106092–106106, 2020.

[21] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in Internet of Things using the optimum authentication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.

[22] N. Krishnaraj, M. Elhoseny, E. L. Lydia, K. Shankar and O. ALDabbas, "An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment," *Software: Practice and Experience*, vol. 51, no. 3, pp. 489–502, 2021.

[23] J. Yan, L. Wang, L. Wang, Y. Yang and W. Yao, "Efficient lattice-based signcryption in standard model," *Mathematical Problems in Engineering*, vol. 2013, no. 702539, pp. 1–19, 2013.

[24] K. Tamilarasi and A. Jawahar, "Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm," *Wireless Personal Communications*, vol. 114, no. 3, pp. 1–16, 2020.

[25] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi *et al.,* "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Computer Networks*, vol. 177, no. 1, pp. 107333–107347, 2020.

[26] R. K. Mahendran and P. Velusamy, "A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things," *Computer Communications*, vol. 153, no. 1, pp. 545–552, 2020.

[27] C. Vijayakumaran, B. Muthusenthil and B. Manickavasagam, "A reliable next generation cyber security architecture for industrial Internet of Things environment," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 387–395, 2020.

[28] B. Muthusenthil, C. Vijayakumaran and H. Kim, "Security and privacy framework for academic monitoring system," in *Proc. 8th Int. Conf. on Security Technology (SecTech)*, Jeju Island, South Korea, pp. 5–8, 2015.

[29] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[30] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.