DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

Proposed Secure Key for Healthcare Platform

Mutaz Haqi Ismael[1], Abeer Tariq Maolood[2]

[1,2]Department of Computer Science, University of Technology, Baghdad, Iraq

[1]muataz.haqi@gmail.com, [2] abeer.t.maolood@uotechnology.edu.iq

Abstract— *The automation of medical systems is one of the most important topics and that takes the highest priority in our time due to the COVID-19 pandemic, which has caused human disasters without knowing the exact diagnosis of patients and other diseases. Therefore, it has been recently started to rely on sensors to support medical results and monitor the patient throughout the day, and this in itself is an application of Internet of Things (IoT) which is called Internet of Medical Things (IoMT). The expansion and reliability of this type of systems need to secure the systems, infrastructure, devices and used sensors. This paper focuses on the proposal key to encrypt the data stored in the database by relying on artificial intelligence algorithms and Bezier curves based on the dynamic number generated in the medical platform as an input to it. The Particle Swarm Optimization (PSO) algorithm was chosen because it is fast to implement and to support limited devices within the used network. Also, the logistic map function was used to generate the randomness of the generated key. The proposed key has also been examined and it has passed the five randomness tests and succeeded in 13 out of 16 tests within the NIST tests.*

Index Terms*— Bezier Curve, healthcare system, Internet of Medical Things, Optimization Swarm Optimization.*

I. INTRODUCTION

The Internet has infiltrated our daily lives in recent years. The way we manage our lives has been altered in many ways. On this list, the Internet of Things IoT is at the top. IoT is commonly referred to as IoMT in the medical field and it has changed the medical field with the newly established remote healthcare system concerning social merits, perception, and effective illness diagnostics. Thanks to IoT's permanent computing [1], [2] IoMT is straightforward to handle clinical objectives such as doctor's advice, remedies, medical instruments, and patient data. IoMT also offers real-time medical services and help via Internet-enabled smart devices such as smart phones, smart medical wearable implanted devices and electronic medical reports (EMR), to reduced health-care expenditures, prompt medical answers, quick decision-making, and increased medical treatment quality are all advantages of IoMT. Currently, the Internet of Things IoT connects billions of devices for a variety of purposes, including healthcare. Users' privacy and security have become the most problematic challenges in IoT (particularly in IoMT) as a result of this exponential expansion, and they must be taken into account[3]. Unauthorized access to vast amounts of sensitive patient data (i.e., personal and medical information) that aids in making life-changing choices is one of the potential securities and privacy breaches that might occur in healthcare systems[4]–[6].

An algorithm (or encryption approach) and an encryption key are the two main components of encryption. The produced key's security strength depends on the method employed and the key size[7]. New cryptographic methods developed from chaotic systems and possessing crucial chaotic traits such as sensitive dependency on beginning circumstances and a quasi-random matrix that is difficult to predict after

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

certain proposed iterations to overcome this challenge. Robert and J. Matthews [8] were the first to coin the term “anarchic cryptography”. Some prerequisites for the encryption technique include a vast key space, sensitive reliance on secret keys, and no association between two neighboring pixels [9], [10].

We propose a key generation method based on chaotic systems' unique features. The remainder of this work is organized in the following manner. PSO is mentioned in the first section (particle swarm optimization). Section two discusses the Bezier Curve and Logistic Map Chaotic described in section three, while Section 4 illustrated the suggested picture coding algorithm and its mathematical model. Some conclusions are drawn in *Fig. 2*. Moreover, this paper proposes generate random keys by using the PSO, Bezier Curve and Chaotic ciphers.

II. LITERATURE REVIEW

This section will review some studies interested in generating a random key, as well as other applications about the possibility of the PSO algorithm as shown in Table I.

TABLE I. LITERATURE REVIEW FOR SOME STUDIES

Author	**Years**	**Methodology**	**Outcomes**
Raja Rajeshwari K .et al, [11]	2020	PSO-IoT	Improves grouping precision with expanding attributes, however with irrelevant qualities, the exactness rate is diminished.
Vivek Anil Pandey et al.,[12]	2020	PSO	The use of a heuristic (partial search algorithm) approach that may present us with a proper satisfactory result to an optimization dilemma of key selection, or generation.
Abdulameer A. Karim et al.[13]	2019	Bezier Curve	This algorithm give a high random distribution to the pixels of the secure image when hiding it on the pixels of the cover image.
Majed Ismael Sameer[14]	2019	PSO Chaotic map	the results show the high sensitivity for proposed scheme depending on the secret Keys. The speed and performance of encryption and decryption operations for color images are excellent and very close to real time.
Hanaa Mohsin1*,et al. [15]	2018	Cubic Spline Curve and Blum Blum Shub Algorithm	Create a random number to create the curve to detect, as well as the pace at which different shapes in a cubic spline curve may be identified. Assurance provides confirmation of appropriate security and a simple approach to complex security applications.
Wesam Samier Bhaya [16]	2016	Cubic Bezier Curve	symmetry key depending on the ridges curvatures of fingerprint

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

III. BACKGROUND THEORY

A. Particle Swarm Optimization (PSO)

PSO is a ciphering process that's made up of two scientific components: computer science and social science. Furthermore, PSO practices the swarm intelligence approach, a characteristic of a system, in which cumulative acknowledgements of the naive agents that are socializing regionally among their surroundings. Produces compatible global utilitarian exemplars. PSO's foundations are built on the following principles:

- ***Social Concepts:*** "Human intellect emerges from social interactions," as the phrase goes.
- ***Swarm Intelligence***: It's the collective behavior of decentralized and self-organizing systems. These systems might be either natural or man-made [15].

In PSO. The term "particles" is referred to the members of the population group that need an optimized result for locating the food for themselves. These particles are considered to possess an arbitrary negligible mass and volume and are constrained to velocities and acceleration to a better mode of behavior. PSO is not largely affected by the size of the group (or swarm) and non-linearity of the function. It converges to a global optimum result for the problem where most of the analytical methods fail to focalize. The flocking of birds and schooling of fish are the two main examples of PSO[11].

The particle(s) swarm optimization works in such a way that a difficult situation is being given. Also, a path to appraise the recommended explication to the given problem endures in the torso of a robustness function. A connection fabrication or chain is formed, allowing next-door neighbor for every particle(s) to communicate amidst. The robustness of the candidate result is iteratively evaluated and thus they memorize the position to the place where they found of the best result. The best result for the particle(s) is known as the personal best or the local best. The information accomplished by each particle(s) is shared among its every neighbor. The methodology in performing the PSO can be recapitulated likewise:

- Social Concepts: It can be referred to as "human intelligence results from social interactions".
- Swarm Intelligence: It may be described as the collective behavior of decentralized, self-organized systems. These systems can be natural or artificial [12].

B. Cubic Bezier Curve

The Bezier curve is a polynomial function of the parameter t and is a parametric curve P (t). The degree of the polynomial is determined by the number of points used to identify the curve. Control points are used to construct an approximation curve via the method. The curve is drawn to the local points rather than passing through them. It's as though the points are pulling on the curve. Every point influences the curve's orientation by drawing it toward itself, and this attraction is stronger when the curve approaches the point as closely as possible. A cubic polynomial is a curve with four points that can be recognized. One reason for its popularity is because it is simple to alter, tweak, and alter the curve [16]. It's also possible to alter the curve by adding or removing points.

C. Logistic Map

The logistic map was proposed by P. Verhulst in the year of 1845. It is a simple map of a non-linearity. It's one of the simplest commonly utilized chaotic maps that became quite popular after using it by the biologist R. M. May in the year of 1979 [9], [10]. The logistic map is a complicated polynomial of a chaotic system, the behavior in which may be a result of the non-linear dynamic of simple formulas) [17]. The equation of this map is depicted bellow:

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

$$g(x_n) = g(x_{n+1}) = r * x_n(1 - x_n) \tag{1}$$

IV. PROPOSED SYSTEM

The general scheme that represents the Architecture of the platform of IOMT that consists of four parts and all the parts is presented sequentially in a top-down style as shown in *Fig. 1*. In the marked part (third component) within the backend layer, the proposed key is used to encrypt the stored data.

A. Layers of the platform

The platform has three types of customers, the highest authority is the system's admin, who has the highest privilege in terms of managing users (Adding users and editing permissions) with a rich dashboard that includes statistics for all medical centers. As for the doctor, His privilege is limited by adding a new visit with the patient's approval, (the second development of the letter), and he also has a dashboard that is specialized in his own patient's statistics. Finally, the subscriber to the medical platform who owns the right to authorize the doctor via mobile applications through Quick Response (QR) or by the One Time Password (OTP).

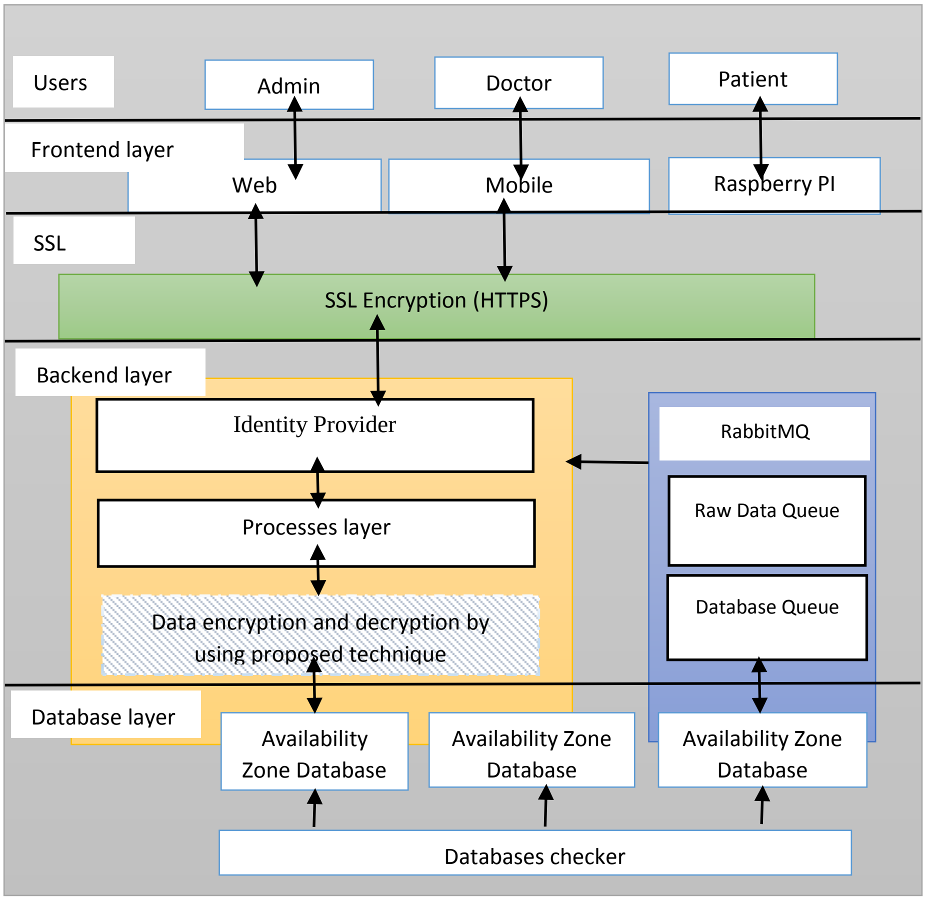

FIG. 1. GENERAL SCHEME THAT REPRESENTS THE ARCHITECTURE OF THE PLATFORM.

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

B. SSL layer

SSL relies on public key cryptography to function. To send secure data between two systems, public key cryptography requires two keys: a private and a public key. These keys are required for decoding and encoding secure data respectively.

Here's how SSL works, step by step:

1. An SSL-enabled service, such as a website, is accessed.
2. In exchange for its own public key, the user's application asks the server's public key. This public key exchange allows both parties to encrypt messages that can only be viewed by the other.

3. When a user sends a message to the server, the application encrypts the message using the server's public key.
4. The server gets the user's communication and uses its private key to decode it. Messages transmitted back to the browser are encrypted in the same way, with the user's application's public key.

Using public key cryptography is analogous to locking your door with a padlock. The public key is the padlock itself, whereas the private key is the combination. The server distributes a padlock that can be used to lock a door or a box by anyone. The padlock, on the other hand, cannot be unlocked without the combination, which is only known by the server.

C. Availability Zone layer

In order to ensure the security of data in more than one site and as support to enhance the platform architecture for the “distributed systems”, a specialized layer has been created in databases only to ensure the continuity of the system’s work in the event that the work of a particular site stops working depending on the rest of the active sites. During the addition of new databases. This architecture also included the use part of the databases with specific application in front layer to ensure second concept, which is “decentralized”.

As presented, a special section has been added to monitor entries in databases to ensure that a specific database is not tampered with in real time, and also this file illustrates the flaw in the non-conformity at the database, table, and record level.

V. BACKEND LAYER (PROPOSED KEY GENERATION)

Depends on proposed architect which supports the microservices design model, each action or event within the platform will be encrypted. The fact that the devices used on the platform have limited technical specifications as we mentioned in the introduction, and at the same time the importance of securing data, especially medical, has increased due to its privacy. So that the proposed key will be generated in high performance, runtime and not stored in the database with Particle Swarm Optimization algorithm (PSO). In *Fig. 2* the steps of generating key will be illustrated.

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

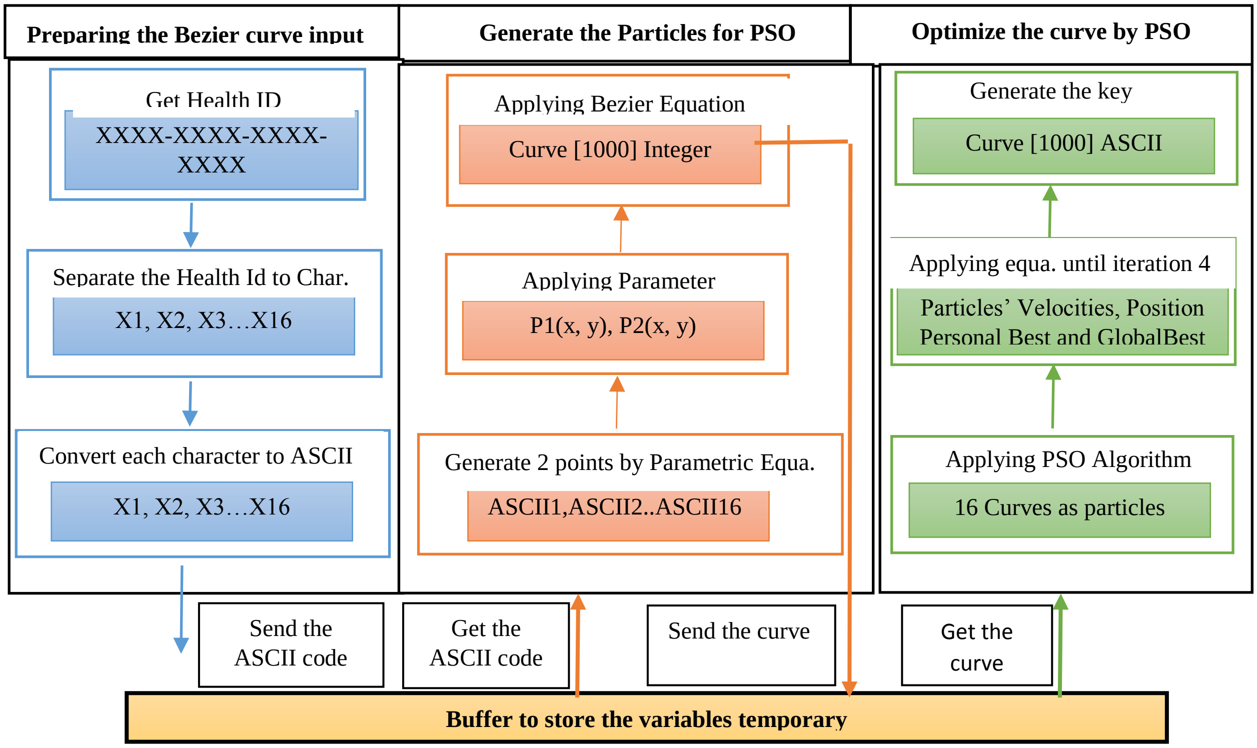
Preparing the Bezier curve input
Generate the Particles for PSO
Optimize the curve by PSO
Get Health ID
XXXX-XXXX-XXXX-XXXX
Separate the Health Id to Char.
X1, X2, X3…X16
Convert each character to ASCII
X1, X2, X3…X16
Applying Bezier Equation
Curve [1000] Integer
Applying Parameter
P1(x, y), P2(x, y)
Generate 2 points by Parametric Equa.
ASCII1,ASCII2..ASCII16
Generate the key
Curve [1000] ASCII
Applying equa. until iteration 4
Particles' Velocities, Position
Personal Best and GlobalBest
Applying PSO Algorithm
16 Curves as particles
Send the ASCII code
Get the ASCII code
Send the curve
Get the curve
Buffer to store the variables temporary

FIG. 2. ALGORITHM OF THE HYPER SECURITY

The Health ID generated within the proposed platform will be split into 16 characters and in order to be dealt with mathematically in the second step, it must be converted to ASCII codes. One ASCII code will generate four points, then applying the parameter equation, and applying the Bezier equation, which provides the Bezier curve. The main idea of increasing the length of the Health ID was to increase the number of curves that are inserted into the algorithm. Since PSO belongs to the swarm algorithms, it is preferable to increase inputs (particles) to improve the results as much as possible. After that, the algorithm will be run and the variables are updated for four iterations as mentioned before. Finally, the accumulative curve will represent the proposed key, the bellow steps describe with example the methodology as:

1- Generate Health ID

In this process we generate the Health ID after enroll the subscriber as the bellow structure:

transaction id (4 digits)	last visit id (3 digits)	date of birth (4 digits)	serial number (2digits)	session id (3 digits)

2- Convert HealthID to Bezier curve

Here, the Health ID will be split into 16 characters. After separating the characters, each character will be converted into ASCII code. To get a good numbers of features, the ASCII code will enter to the parametric equation then enter to the Bezier equation to get finally array of 1000 elements as illustrated in *Fig. 3* that represents sample of curves. While *Fig. 4* represents the fully curve for the example below.

3- Send Bezier curves as particles

PSO Algorithm will get the 16 particles, which a good amount of inputs for Swarm algorithm. We can increase the number of inputs by increase the length of Health ID.

4- Generate the key

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

PSO algorithm will start their training to optimize the randomness of particles based on chaotic logistic map 1D. The last updated position multiply by subscriber device number and current date to get the proposed key.

Example: -

1- Generate Health ID

Transaction_Id: 617a6b01c5994701aba83e1e19e08b4c

Last_visit_id: 002

Birthdate: 642891600.0

Serial number: 111111

Session token: eyJleHAiOjE2MjI0MTEwMjEsImlhdCI6MTYyMjMyNDYxNiwic3ViIjoxfQ

The HealthID will be: 617a002642811eyJ

2- Convert HealthID to Bezier curve.

3- In this step the 16 Bezier curve be ready for trading for each ASCII code.

4- Generate the key: Run the PSO algorithm.

Sample of the key, then be XOR with plaintext as the bellow:

0000001010001111000010010101110101001010000000101010010101011001110010000000100100011
1011010010011100010001101000111010100011011100001110111000100101110010011100010111011
0001001011100111011000101101000001001010100100111000101111000001110010100110111000001
1010000011100110101001110000011101000010100110101111001111111011000010100101101001001
0000111111100101110111011000011010110101100101111110100000010000111010000101110111100
0100111110101010001100010111000000100101011010001110011101000000110111010011101010011
1101110001001010100111100110101011000001111101111000010110101111100001001011010100010
1001110110010010000111011100110110101011111

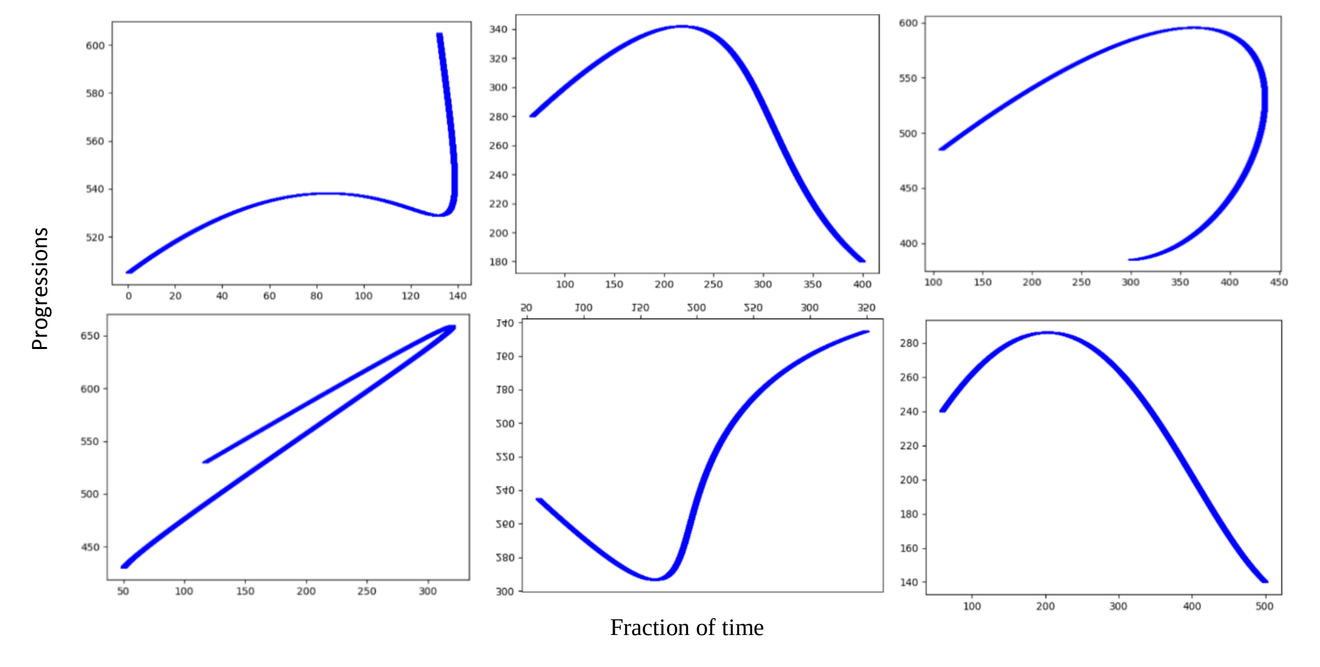

FIG. 3. SAMPLE OF BEZIER CURVE

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

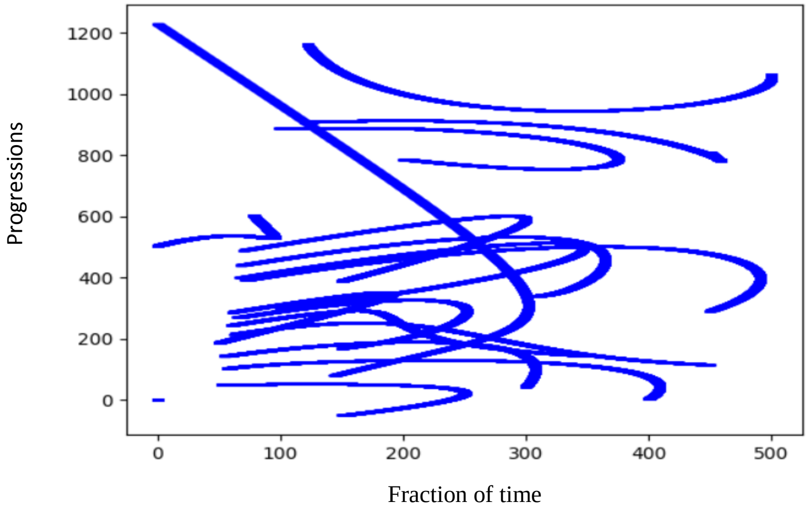

FIG. 4. BEZIER CURVES FOR EXAMPLE

VI. EXPERIMENTAL RESULTS

The key generated from the proposed platform has been tested using Randomness five tests and we note that all tests have been successfully passed after four iteration. Table II and Table III shown the results of five randomness tests in first and fifth iteration, while Table IV represents the NIST tests.

TABLE II. RANDOMNESS TEST FIRST ITERATION

Iteration	**Health ID**	**Execution time/Second**	**Randomness test (Failed) of 5 Tests**
First Iteration	11111111111	0.3842	RUN TEST T0, RUN TEST T1, SERIAL TEST, AUTO_CORRELATION TEST
	aaaaaaaaaaaaaaaa	0.3718	RUN TEST T0, RUN TEST T1, SERIAL TEST, POKER TEST AUTO_CORRELATION TEST
	1234567890123456	0.3713	RUN TEST T0, RUN TEST T1, SERIAL TEST, AUTO_CORRELATION TEST
	abcdefghijklmnop	0.4168	RUN TEST T0, RUN TEST T1, SERIAL TEST, POKER TEST AUTO_CORRELATION TEST
	a1b2c3d4e5f6g7h8	0.3973	RUN TEST T0, RUN TEST T1, SERIAL TEST, POKER TEST AUTO_CORRELATION TEST
	1698790124935791	0.3745	RUN TEST T0, RUN TEST T1, SERIAL TEST, AUTO_CORRELATION TEST
	zeBaqXaQwKlaOPyT	0.4368	RUN TEST T0, RUN TEST T1, SERIAL TEST, POKER TEST AUTO_CORRELATION TEST
	AABBCCDDaabbccdd	0.4678	RUN TEST T0, RUN TEST T1, SERIAL TEST, POKER TEST AUTO_CORRELATION TEST

Received 16/June/2021; Accepted 30/August/2021

	@G1K5QWuy\w12$z%	0.4920	RUN TEST T0, RUN TEST T1, SERIAL TEST, POKER TEST AUTO_CORRELATION TEST
	a1b2c3b7h6j9k0g1	0.4198	RUN TEST T0, RUN TEST T1, SERIAL TEST, AUTO_CORRELATION TEST

TABLE III. FIVE RANDOMNESS TEST FIFTH ITERATION

Iteration	**Health ID**	**Execution time/ Second**	**Randomness test (Failed)**
Fourth Iteration	11111111111	0.3940	None
	aaaaaaaaaaaaaaaa	0.4129	None
	1234567890123456	0.4374	None
	abcdefghijklmnop	0.4626	None
	a1b2c3d4e5f6g7h8	0.4908	None
	1698790124935791	0.5106	None
	zeBaqXaQwKlaOPyT	0.5984	None
	AABBCCDDaabbccdd	0.5239	None
	@G1K5QWuy\w12$z%	0.5980	None
	a1b2c3b7h6j9k0g1	0.5728	None

TABLE IV. NIST TEST FIFTH ITERATION

NO.	**Test name**	**Result**
1	Frequency	success
2	Block Frequency	success
3	Cumulative Sums	success
4	Runs	success
5	Longest Run	success
6	Rank	success
7	Discrete Fourier Transform	success
8	Non-periodic Templates	success
9	Overlapping	success
10	Universal	Discard
11	Approximate Entropy	success
12	Random Excursions	Test not applicable
13	Random Excursions Variant	Test not applicable
14	Seri al	success
15	Lempel-Ziv Compression	success
16	Linear Complexity	success

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

VII. CONCLUSION

In this paper, we highlight security issues in IoMT. Anti-IoT in safety measures are also provided in terms of authentication, encryption and IoMT. A method to generate an encrypted key to maintain security standards was proposed for stored data was constructed using the PSO and the Bezier Curve techniques. The use of PSO was great idea to generate keys as the PSO is a stochastic method which is based on random initialization with the chaotic logistic maps. The use of the PSO in key generation is considered as one of the greatest methods, and these results have been tested and found to be very strong in the process of scattering and encryption data. The contribution in this paper can be represented by employment PSO algorithm with Bezier curves to increase the length of the proposed keys, which means increasing the features for the inputs of PSO algorithm.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests regarding the publication of this paper.

ACKNOWLEDGMENT

The publication of this article was funded by the University of technology,Computer science department.

REFERENCES

[1] A. Seno and S. Alshammari, “A Cooperation of Fog Computing and Smart Gateways in a Secure and Efficient Architecture for IoT-Based Smart Homes,” *Eng. Technol. J.*, vol. 37, no. 7A, pp. 290–301, 2019, doi: 10.30684/etj.37.7a.10.

[2] M. Azhar and A. Seno, “A Group Authentication Protocol on Multilayer Structure for Privacy-Preserving IoT Environment,” *Eng. Technol. J.*, vol. 37, no. 5A, pp. 172–180, 2019, doi: 10.30684/etj.37.5a.4.

[3] B. Mostafa, A. Miry, and T. Salman, “Healthcare Monitoring and Analytic System Based Internet of Thing,” *Iraqi J. Electr. Electron. Eng.*, vol. sceeer, no. 3d, pp. 30–36, 2020, doi: 10.37917/ijeee.sceeer.3rd.5.

[4] M. S. Mahdi, N. F. Hassan, and G. H. Abdul-Majeed, “An improved chacha algorithm for securing data on IoT devices,” *SN Appl. Sci.*, vol. 3, no. 4, pp. 1–9, 2021, doi: 10.1007/s42452-021-04425-7.

[5] M. Vijayalakshmi, S. Mercy Shalinie, M. H. Yang, and U. Raja Meenakshi, “Web phishing detection techniques: A survey on the state-of-the-art, taxonomy and future directions,” *IET Networks*, vol. 9, no. 5, pp. 235–246, 2020, doi: 10.1049/iet-net.2020.0078.

[6] M. M. Rahma and A. D. Salman, “a Wearable Medical Monitoring and Alert System of Covid-19 Patients,” *Iraqi J. Comput. Informatics*, vol. 47, no. 1, pp. 12–17, 2021.

[7] M. S. Fadhil, A. K. Farhan, M. N. Fadhil, and N. M. G. Al-Saidi, “A New Lightweight AES Using a Combination of Chaotic Systems,” in *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*, 2020, pp. 82–88.

[8] A. L. R. A. Ali, “Random Number Generator based on Hybrid Algorithm between Particle Swarm Optimization (PSO) Algorithm and 3D-Chaotic System and its Application,” *Iraqi J. Inf. Technol. V*, vol. 8, no. 3, 2018.

[9] D. Chen and Y. Chang, “A novel image encryption algorithm based on logistic maps,” vol. 3, pp. 364–372, Aug. 2011, doi: 10.4156/aiss.vol3.issue7.43.

[10] B. Schneier and P. Sutherland, "*Applied Cryptography: Protocols, Algorithms, and Source Code in C*," 2nd ed. USA: John Wiley &amp; Sons, Inc., 1995.

[11] M. Ramakrishnan and K.Raja, “Internet of Trust Things using Particle-Swarm Optimisation (PSO-IoT),” International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS), 2021.

[12] V. A. Pandey, P. Pulastiya, I. Kaur, and S. Rastogi, “A survey on key management using particle swarm optimization in MANET,” ^{3rd} International on Innovative Computing and communication (ICICC),India,2020.

[13] M. A. AbdulAmir Abdullah Karim, Abdul Mohsin J, Abdul Hussein, “Image Steganography System Using Bezier Curve,”

Received 16/June/2021; Accepted 30/August/2021

DOI: https://doi.org/10.33103/uot.ijccce.22.1.3

AL-MANSOUR J., p. 111, 2019, doi: 10.36541/0231-000-031-009.

[14] M. I. Sameer, "Good bye for random functions in equation PSO and welcome for chaotic functions in equation PSO," *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 7, 2019.

[15] H. Mohsin and A. Oday, "User Authentication Secure by Randomly Cubic Spline Curve and Blum Blum Shub Algorithm," Al-Mustansiriyah Journal of Science , Volume 30, Issue 1, 2019.

[16] W. S. Bhaya and W. M. Brich, "Secure Exchange of Generated Key by Fingerprint Ridges Depend on Cubic Bezier Curve," no. 2, pp. 285–298, 2016.

[17] S. Yin and H. Li, "GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system," *Evol. Intell.*, vol. 14, no. 4, pp. 1817–1829, 2021.

Received 16/June/2021; Accepted 30/August/2021