Comparative Assessment on Privacy Preservation in Health Care Sectors coupled with IoT

Pravin N.Kathavate, J.Amudhavel

ABSTRACT--- Safe and high-quality healthcare service is of supreme significance to patients. Security and patients' privacy of healthcare data are imperative problems that will have a large impact on the upcoming accomplishment of Healthcare with IoT. A major problem in the IoT dependent healthcare system is the fortification of privacy. Usually, a healthcare service contributor receives data from its patients and distributes them with healthcare experts or registered clinics. The contributor may perhaps share out the data to pharmaceutical companies and health insurance companies. Hence, for overcoming the challenges existing in security, this paper has come out with a privacy-preserving technique with significant data extraction from IoT devices linked with healthcare sector. According to the adopted scheme, the information obtained from IoT devices is processed for preserving the sensitive data, such that unknown people are prohibited to access them. Here, Grey Wolf Optimization (GWO) scheme is proposed to recognize the optimal key. The objective of the proposed scheme is to minimize hiding failure rate, modification degree, and true positive value for better preservation of sensitive data. Moreover, the implemented technique is distinguished with conventional schemes like Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Bee Colony (ABC), Firefly (FF) and Differential Evolution (DE) algorithms in terms of performance. Also, the statistical analysis of the presented method is measured for three test cases, and the effectiveness of the implemented method is revealed.

Keywords—Internet of Things; Healthcare; Privacy Preservation; Sanitization; Hidden rate; Modification Degree, True Positive rate.

1. INTRODUCTION

IoT has raised as major powerful interaction systems of the 21st century. In the IoT surroundings, the entire objects in the routine life turn out to be a part of the internet owing of their computing and communication abilities, which permits them to interact with various objects. IoT widens the hypothesis of the internet and develops it in an enhanced mode. In the IoT surrounding, the faultless interactions between various kinds of devices such as home appliances, medical sensors, vehicles, monitoring cameras, etc., have led to the rise of several applications like home automation, smart city, traffic management, smart grid, etc.

Accordingly, healthcare patients' privacy and data security are significant problems, which will have a large influence on the upcoming success of Health IoT. A major problem in the IoT dependent healthcare system is the privacy protection. Usually, a healthcare service provider obtains data from its patients and distributes them with authenticated clinics or healthcare experts. The provider also shares the information to pharmaceutical and health insurance companies. In addition, patient data can be susceptible to hackers while synchronizing with interlinked devices.

In the healthcare region, IoT comprises of several types of cheap sensors, which facilitates elderly people to offer medical healthcare any time at anywhere. They offer convenience to medical employees and also improve the quality of elderly people's life in a better way. Moreover, the increased exploitation of smart devices and communication apps in healthcare monitoring, related to patients and healthcare fields are witnessed. It is essential to safeguard this information from unauthenticated access that may influence in the public domain, or in accordance with required medical equipment, for e.g., pacemaker. A security breach of a patient's data may perhaps influence the patient's mental disorders, social embarrassment, or adverse physical effects like a fatal heart attack. Therefore, protection of data in the form of authentication and watermarking is very essential in an IoT-dependent healthcare system.

The Body Sensor Network (BSN) scheme is exploited in IoT- dependent healthcare system. It is a collection of lightweight and low-power wireless sensor nodes which are exploited to monitor the functions of human body and environment. As BSN nodes are deployed to gather sensitive information and may function in hostile surroundings, accordingly, they desire strict security methods to avoid malicious communication with the system [2]. Recently, Health IoT is still in its initial stages with respect to modeling, deployment, and development; anyhow, IoT-dependent solutions are offering a specific impact presently and carving out a developing market in the present healthcare industry and upcoming IoT- dependent healthcare monitoring solutions. IoT has the capability to protect 50,000 people every year in US by deaths caused owing to hospital error. Research exposes that IoT in the healthcare industry can enable enhanced care with minimized costs, minimized direct staff-patient communication, and ubiquitous quality care access. Thus these limitations have to be focused keenly to overcome the challenges in healthcare IoT systems. This paper contributes an efficient data preservation policy in healthcare sector connected with IoT. According to the suggested scheme, the data that has to

Revised Manuscript Received on March 10, 2019.

Mr.Pravin N.Kathavate, Research Scholar, K L University(Deemed To be University), Vaddeswaram, Guntur, Andhra Pradesh, India-522502 (Email: pravin.kathavate@gmail.com)

Dr.J.Amudhavel, Research Supervisor, K L University(Deemed To be University), Vaddeswaram, Guntur, Andhra Pradesh,India – 522502 (Email: amudhavel@kluniversity.in)

be preserved is sanitized, thus hindering the data from unauthorized users. Moreover, GWO algorithm is adopted for an optimal key generation. The objective of the suggested method is to minimize the parameters such as hiding failure rate, modification degree, and true positive value for better preservation of sensitive data.Further, the proposed model is compared with conventional algorithms like, GA, PSO, ABC, FF, and DE, correspondingly and the results are obtained. This paper is organized as follows. Section II analyses the related works and reviews done under this topic. Moreover, section III describes the modeling of privacy preservation for healthcare preservation of data and section IV explains the suggested objective model and optimal key generation. In addition, section V discusses the results, and section VI concludes the paper.

2. LITERATURE SURVEY

A. Related works

In 2017, J. H. Abawajy and M. M. Hassan [1] introduced a scheme which offers a pervasive patient health monitoring (PPHM) infrastructure. PPHM was dependent on IoT and cloud computing technologies, which were integrated. With the intention to illustrate the adoptability of the suggested PPHM structure, an analysis for real-time monitoring of a patient enduring from congestive heart failure by means of ECG was offered. Investigational evaluation of the implemented PPHM design had revealed that PPHM was a scalable, flexible, and energy-effective health monitoring system for patients.

In 2016, Prosanta Gope and Tzonelih Hwang [2] had established a novel technology in applications of healthcare devoid of regarding security which in turn makes patient privacy vulnerable. Accordingly, the main security necessities were highlighted in BSN dependent modern healthcare system. Consequently, a protected IoT dependent healthcare structure by means of BSN, known as BSN-Care that can resourcefully bring about those needs was presented.

In 2016, M. S. Hossain and G. Muhammad [3] has suggested a Health IoT-enabled monitoring structure, in which ECG and various data of healthcare were composed by sensors and Mobile Healthcare Networks (MHN) devices and safely transmitted to the cloud for faultless access by experts of healthcare. Watermarking, signal improvement, and various associated analytics were exploited to evade clinical error or identity theft by experts in healthcare. The appropriateness of this technique has been authenticated by both investigational assessment and simulation by employing an IoT-driven ECG- dependent health monitoring facility in the cloud.

In 2015, K. Zhang *et al.* [4] has introduced a structural design of MHN and indicates the privacy and security limitations from the viewpoint of QoP. Moreover, certain countermeasures for privacy and security fortification in MHNs, together with health data aggregation in privacy-preserving, misbehavior recognition, and protected health data processing. At last, certain open inconveniences and pose upcoming research directions in MHNs were presented.

In 2017, Mahmud Hossain *et al.* [5] have introduced a scheme that contributes to the group of characteristics of telemedicine by implementing a design for an IoT-dependent Health Prescription Assistant (HPA) that assists every patient to pursue the doctor’s suggestion appropriately. In addition, this method models a security system which guarantees user validation and confined access to services and resources. The security system validates a user dependent on the standard Open ID. Moreover, a control access system was proposed to avoid illegal access to medical policies.

In 2017, M. A. Salahuddin *et al.* [6] has established a enhanced structural design, a new platform with Machine-to-Machine (M2M) messaging, rule- dependent beacons, for faultless data administration, and the exploitation of decision fusion and data fusion to assist smart-healthcare applications and services. Experimentations have shown that the suggested model has revealed cost-effective, flexible, private, and secure IoT deployment for smart-healthcare services and applications.

In 2018, Ming Tao *et al.* [7] have introduced a scheme by means of numerous capable opportunities offered by the progression in Cloud Computing and IoT technologies for confronting the limitations. Here, a new multi-layer cloud design was introduced to facilitate efficient and faultless interoperations on heterogeneous services offered by diverse retailers in IoT- dependent smart home. Moreover, enhanced resolving techniques regarding the heterogeneity problems in the layered cloud platform were proposed in this technique.

In 2015, He and S. Zeadally [8] have described security needs of RFID confirmation systems, and specifically, a reassess of ECC- dependent RFID confirmation systems with respect to security and performance. Even though the majority of them cannot gratify the entire security needs and have suitable performance, it was established that there are three ECC- dependent methods in recent times appropriate for the healthcare surroundings regarding their security and performance.

B. Review

Table 1 shows the methods, features, and challenges of conventional techniques based on skin cancer detection using dermoscopic image processing. At first, Classical Naive Bayes was adopted in [1] that attains high accuracy with better average F-measure. However, there was no contemplation on verifying it in a real-life environment. Similarly, AES-CBC encryption was implemented in [2] that are significantly valuable for the resource-constrained sensor devices. It also offers least computational cost with reduced execution time, but there was no assurance of value for aged people’s life. Moreover, Fast Fourier Transform (FFT) was proposed in [3] which offer increased patient care quality with reduced attacks. Anyhow, there was no implementation of test trial with real-world patients and health professionals. In addition, Hidden Markov Model (HMM) was suggested in [4] that presents lightweight data sensing and security with greatly enviable human intelligence. However, this method necessitates more research effort in QoP viewpoint. Further, Security Access Token (SAT) was presented in [5], which Executes a

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

condition script and Outperforms in computation latency and communication. Anyhow, there was deficiency in security schemes to protect medical campaigns. Machine learning was suggested in [6] that were developed to improve patient experience and healthcare quality with reduced latency and Minimized costs, but there are Chances of blocked transactions. Moreover, Semantic Web Rule Language (SWRL) was proposed in [7] that offers increased scalability with better security and privacy, but it is highly complex. Finally, Elliptic Curve Cryptography (ECC) was implemented in [8] that satisfy the entire security requirements with minimized performance cost, but it is Susceptible to various kinds of malicious attacks. These above mentioned challenges were considered for motivating the improvement of the IoT in healthcare systems.

Author [citation]	**Adopted methodology**	**Features**	**Challenges**
J. H. Abawajy and M. M. Hassan [1]	Classical Naive Bayes	❖Attains high accuracy ❖Better average F-measure	❖No contemplation on verifying it in a real-life environment.
Prosanta Gope and Tzonelih Hwang [2]	AES-CBC encryption	❖Significantly valuable for the resource-constrained sensor devices ❖Least computational cost ❖Reduced execution time	❖No assurance of value for aged people
M. S. Hossain and G. Muhammad [3]	FFT	❖Increased patient care quality ❖Reduced attacks	❖No implementation of test trial with real-world patients and health professionals
K. Zhang *et al.* [4]	HMM	❖Lightweight data sensing and security ❖Greatly enviable human intelligence	❖Necessitates more research effort in QoP viewpoint
Mahmud Hossain *et al.* [5]	SAT	❖Executes a condition script ❖Outperforms in computation latency and communication	❖Deficient security scheme to protect medical campaigns
M. A. Salahuddin *et al.* [6]	Machine learning	❖developed patient experience and healthcare quality ❖Reduced latency ❖Minimized costs	❖Chances of blocked transactions
Ming Tao *et al.* [7]	SWRL	❖Increased scalability ❖Better security and privacy	❖Increased complexity
He and S. Zeadally [8]	ECC	❖satisfy the entire security requirements ❖minimized performance cost	❖Susceptible to various kinds of malicious attacks.

3. MODELLING PRIVACY PRESERVATION FOR HEALTHCARE DATA

A. Proposed Architecture

The suggested novel architecture for preserving the sensitive data regarding the healthcare sector is demonstrated by Fig. 1.The most important objective of the implemented model is to preserve the healthcare information, which is extracted from the IoT sensor or devices. The original database $\hat{D}$ is sanitized, and it offers the sanitized database $\overline{D}$. In addition, the sanitization procedure is made by converting the time series data to another structure. At last, the converted data d_T is uploaded to IoT.

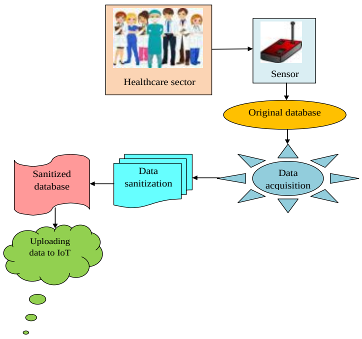


Fig. 1. Overall framework of the implemented Privacy preservation model

B. Sanitizing Phase

The sanitization procedure is for hiding the sensitive information, which is available in $\hat{D}$. Accordingly, $\overline{D}$ is the outcome of the process with less similarity as given in Eq. (1), in which N_d is the entire number of data in $\hat{D}$. The sanitization procedure is specified in Algorithm 1. Moreover, Fig. 2 demonstrates the data sanitization procedure of the suggested representation.

$$\overline{D} \leftarrow \sum_{i=1}^{N_d} d_{Ti} \qquad (1)$$

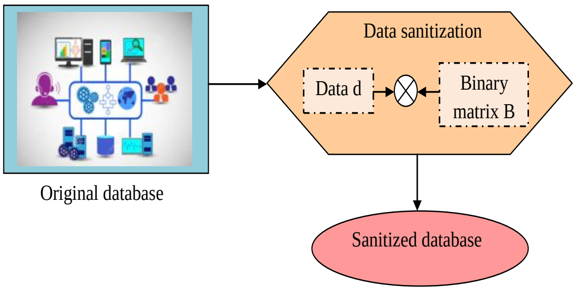


Fig. 2. Layout of sanitization

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

```
Algorithm 1: Data Sanitization process
Input: Original database $\hat{D}$
Output: Sanitized database $\overline{D}$
For every $d$ from $\hat{D}$
    $d_T$ is configured by Eq.(1)
    Update $\overline{D}$ by Eq.(1)
End
```

C. Restoring Phase

Data restoration is the inverse procedure of the data sanitization, where the original database $\hat{D}$ is recovered from $\overline{D}$ that can be further known as retrieved database D''.

4. SUGGESTED OBJECTIVE MODEL AND OPTIMAL KEY GENERATION

A. Objective Function

The data d are obtained from the sensor $s : s = s_1,.....s_n$. The data preservation is practiced by converting the acquired data that are in time series structure to another structure, known as the transformed form d_T. The d_T transformation is described as specified in Eq. (2), in which B indicates the binary matrix. The size of d and d_T is transformed to 1×4 as given in Eq. (3), Eq. (4) and Eq. (5) correspondingly.

$$d_T = d \times B \tag{2}$$

$$G_1 = \sum_{i=1}^{M} (d_i) \tag{3}$$

$$G_2 = \sum_{i=1}^{M} (d_{Ti}) \tag{4}$$

$$D = \frac{G_1}{G_2} \tag{5}$$

The objective of the proposed research work, W is described in Eq. (10), where the parameters R, H (hiding failure rate), O (modification degree)and TP (true positive value) are given by Eq. (6), Eq. (7), Eq. (8) and Eq. (9) respectively. In Eq. (6), Q_{val} is the value in all the sensors, which has to be preserved. In Eq. (7), N_S denotes the number of sensitive data in sanitized data and N_T is the total number of data in field. In Eq. (8), ED indicates the Euclidean distance and in Eq. (9), N_{NS} is the number of non-sensitive data in sanitized data and N_{NO} is the number of non sensitive data in original data.

$$R = \sum \exp(D - Q_{val}) \tag{6}$$

$$H = \frac{N_S}{N_T} \tag{7}$$

$$O = ED(D, \overline{D}) \tag{8}$$

$$TP = \frac{N_{NS}}{N_{NO}} \tag{9}$$

$$W = \min\left(R + H + O + \frac{1}{TP} \right) \tag{10}$$

For achieving the objective model, the optimal key is recognized by means of well-known optimization technique known as GWO. The development of A for data transformation is described with the given subsequent illustration: Assume a data volume [data volume= 100,000 $\times$ 4], in which '4' represent the sensor field, and 100,000 indicate the instant data. Therefore, the value which to be preserved can be assigned as $P_{val} = [1 \times 4]$. As the data volume is 100,000, the chromosome length is considered as [$1 \times$ 10,000]. Four values are extracted from the chromosome each time, and the values are transformed into binary to attain [40×4]. The similar procedure is executed for the entire 25000 rounds, and the binary matrix A of size [$100{,}000 \times 4$] is obtained.

B. Novel Key Extraction Process

The key appropriate for the authentication is obtained by GWO [26] algorithm, which is said to be a population dependent meta-heuristic technique that plays a major role in the leadership of grey wolves in addition to their hunting process in nature. This hierarchy includes four stages, i.e., the initial level is known as α that remains as the leaders of the group. The second stage is β which assists α in taking decisions. The third level is δ, that is known as the subordinates. The final or last level is ω, that is regarded as the scapegoat in the group.

The wolf, α is regarded as the best solution and β and δ obtains the second and third levels correspondingly. Accordingly, the hunting process is assisted by α, β and δ .The pseudo code of the GWO algorithm is revealed by Algorithm 1. The first stage involves parameter initialization, in which Q indicates the population size, the parameter is indicated by z, the coefficient vectors are denoted by M and N and $I^{(\max)}$ signifies the maximum iteration. The numerical encircling is given by Eq. (11), Eq. (12), Eq. (13) and Eq. (14), in which t indicates the current iteration and P_l symbolizes the prey's position vector and P represents the grey wolf's position vector.

$$B = \mid MP_l(t) - P(t) \mid \tag{11}$$

$$P(t+1) = P_l(t) - N \times B \tag{12}$$

The parameters N and M coefficients are calculated as given by Eq. (13) and (14), in which a_1 and a_2 are the arbitrary vectors lying between [0, 1]. The arithmetical representation of the hunting nature of wolves can be considered as given subsequently. The three initial best fittest solutions are stored and the positions are updated depending on the position of best search agent, as shown by Eq. (15), Eq. (16) and Eq. (17).

$$N = 2Z \cdot a_1 - Z \tag{13}$$

$$M = 2.a_2 \tag{14}$$

$$\begin{aligned} B_\alpha &= \mid M_1 \cdot P_\alpha - P \mid \\ B_\beta &= \mid M_2 \cdot P_\beta - P \mid \\ B_\delta &= \mid M_3 \cdot P_\delta - P \mid \end{aligned} \tag{15}$$

$$\begin{aligned} P_1 &= P_\alpha - N_1 \cdot (B_\alpha) \\ P_2 &= P_\beta - N_2 \cdot (B_\beta) \\ P_3 &= P_\delta - N_3 \cdot (B_\delta) \end{aligned} \tag{16}$$

$$P(t+1) = \frac{P_1 + P_2 + P_3}{3} \tag{17}$$

The vector N is an arbitrary value lying between $[-2Z, 2Z]$, in which the element of Z is lessened from 2 to 0 for increasing iterations. Therefore, P_α is considered as the best key obtained that is exploited to achieve the minimized objective function. The pseudocode for key extraction using GWO scheme is given by algorithm 2.

```
Algorithm 2: Procedure of Key extraction using GWO algorithm
Step1  Initialize $Q$, $Z$, $N, M$ and $I^{(\max)}$
       Assign $q := 0$ (counter initialization)
Step2  for $(i = 1 : i \le Q)$ do
           Create a initial random population $P_i(q)$
           Calculate the fitness function $f(P_i)$
       End for
Step3  Set the first, second and third best solution $P_\alpha, P_\beta, P_\delta$
       correspondingly.
Step4  Repeat
           for $(i = 1 : i \le Q)$ do
           Update all the search agents present in the population
           Minimize the variable $Z$ from 2 to 0
           Update the $N$ and $M$ coefficients
           Calculate the fitness function of all the search agents $f(P_i)$
           End for
           Update the vectors $P_\alpha, P_\beta, P_\delta$
           Assign $q = q + 1$
Step5  until $(q < I^{(\max)})$
       Generate the best solution $P_\alpha$ (best key)
```

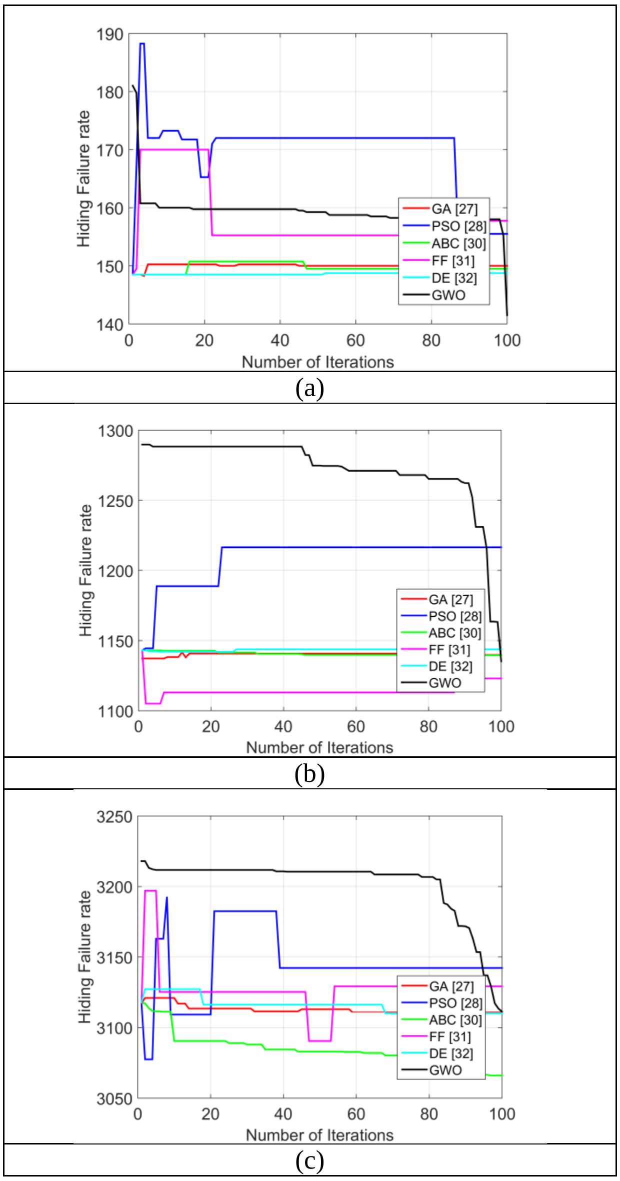
5. RESULTS AND DISCUSSIONS

A. Simulation Procedure

The proposed data sanitization representation was simulated in MATLAB 2015a, and the experimental results were noticed. Three test cases were exploited for verifying the performance of the suggested design. Each test case includes 25000 data with four sensor fields. Data sanitization was attained by accomplishing an adaptive GWO algorithm. In addition, the implemented model was distinguished with the traditional techniques like GA [27], PSO [28], ABC [30], FF [31] and DE [32] correspondingly. Moreover, the analysis on hiding failure rate, modification degree, and true positive value was done. The statistical analysis was furthermore measured depending on five cases like best, worst, mean, median and standard deviation correspondingly.

B. Hiding Failure Rate

The HF rate of the proposed GWO model for three test cases for healthcare data preservation in IoT is given by Fig. 3. From Fig. 3(a), the cost function regarding the HF rate at 100th iteration is 7% better than GA, 9.15% better than PSO, 6.33% better than ABC, 11.26% better than FF and 4.22% better than DE schemes. Also from Fig. 3(b), the HF rate at 100th iteration is 0.8% superior to GA, 8.84% superior to PSO, 0.8% superior to ABC and 1.32% superior to DE techniques. Moreover, from Fig. 3(c), the HF rate of proposed model at 100th iteration is 0.64% better than PSO and 0.16% better than FF methods. Thus the HF rate analysis of the proposed method in has been observed clearly.



(a)

(b)

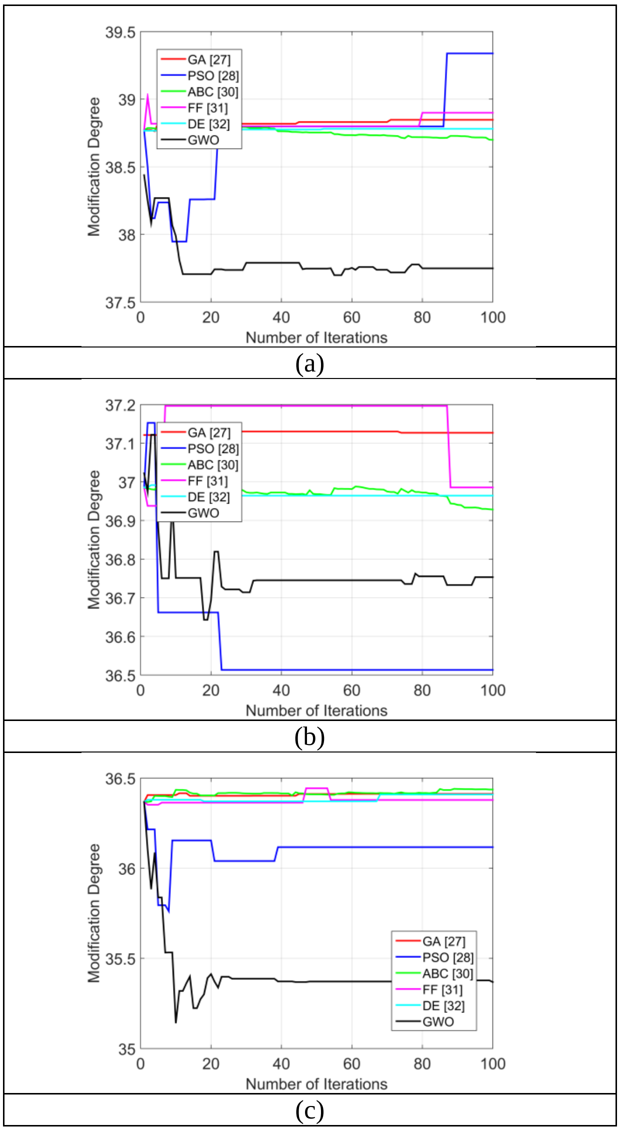
(c)

Fig. 3. HF rate analysis of the proposed over conventional models (a) Test case 1 (b) Test case 2 (c) Test case 3

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

C. Modification Degree Rate

The MD rate of the implemented GWO scheme in healthcare data preservation in IoT for three test cases is given by Fig. 4. Accordingly, from Fig. 4(a), for test case 1, the suggested method at 80th iteration is 3.12% superior to GA, 2.72% superior to PSO, 2.59% superior to ABC, 2.72% superior to FF and 2.7% superior to DE schemes. In addition, from Fig. 4(b), for test case 2, the proposed method at100th iteration is 1% better than GA, 0.46% better than ABC, 0.62% better than FF and 0.54% better than DE schemes. Similarly, from Fig. 4(c), for test case 3, the presented model at 100th iteration is 2.97% superior to GA, 2.4% superior to PSO, 3.02% superior to ABC, 2.82% superior to FF and 2.97% superior to DE algorithms. Thus the MD rate of the proposed model has minimized when compared over the conventional methods.



(a)

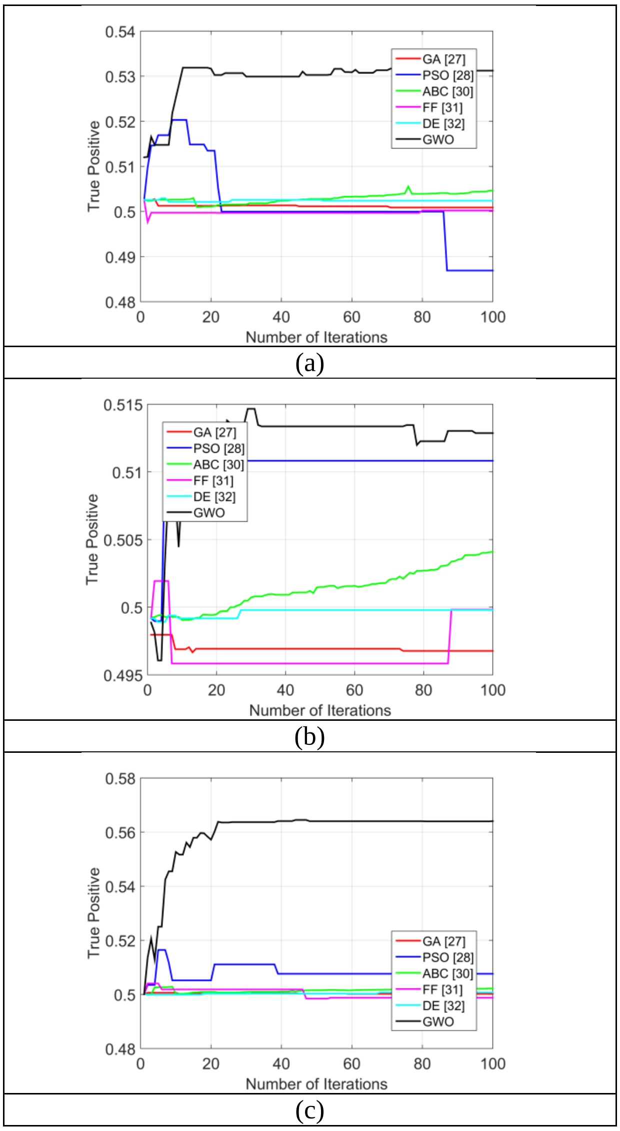
(b)

(c)

Fig. 4. MD analysis of the proposed over conventional models (a) Test case 1 (b) Test case 2 (c) Test case 3

D. True positive rate

The TP rate for data preservation in healthcare IoT using GWO model is given by Fig. 5. From Fig. 5(a), the suggested scheme for test case 1 is 5.83%, 9%, 5.27%, 5.83% and 5.46% better than GA, PSO, ABC, FF and DE algorithms. Also, from Fig. 5(b), for test case 2, the presented method is 3.11% better than GA, 0.38% better than ABC, 1.75% better than FF and 2.5% better than DE schemes. Finally, from Fig. 5(c), for test case 3, the implemented method is 11.5% superior to GA, 9.73% superior to PSO, 10.61% superior to ABC, 11.68% superior to FF and 11.5% superior to DE algorithms. Thus, from the analysis, the improvement of the TP rate of proposed GWO scheme has been confirmed effectively.



(a)

(b)

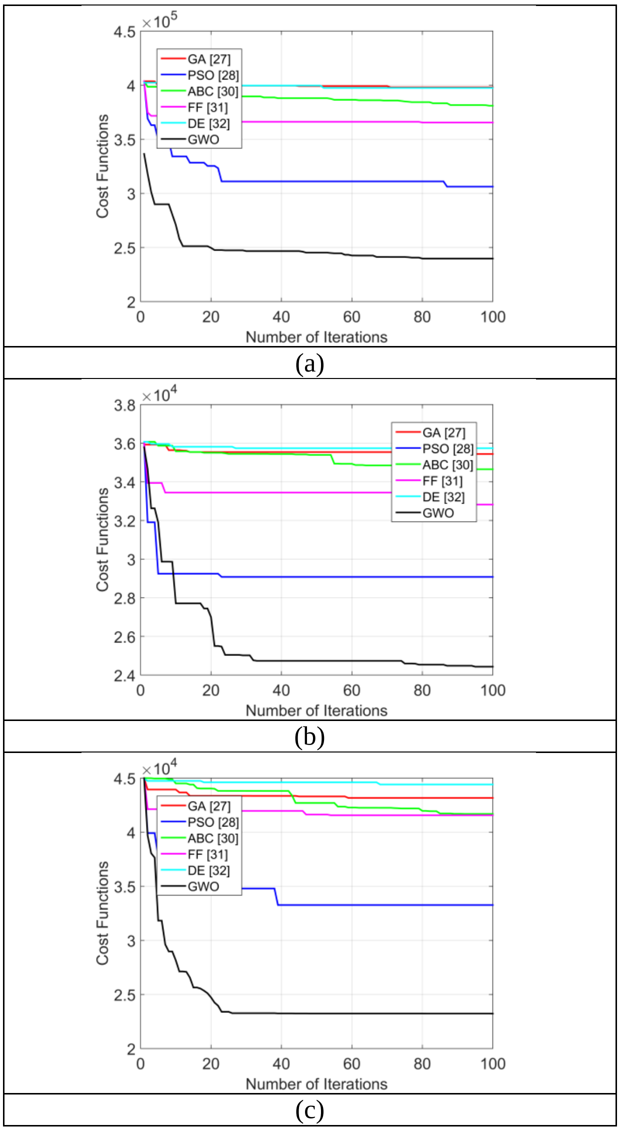
(c)

Fig. 5. TP analysis of the proposed over conventional models (a) Test case 1 (b) Test case 2 (c) Test case 3

E. Convergence analysis

The convergence analysis of the proposed model for data preservation in IoT is given by Fig. 6. From Fig. 6(a), the suggested scheme for test case 1 at 100th iteration is 70.83% superior to GA, 29.16% superior to PSO, 58.33% superior to ABC, 54.16% superior to FF and 66.66% superior to DE techniques. Moreover, on considering test case 2, for 100th iteration, the suggested scheme is 47.32% better than GA, 19.34% better than PSO, 44% better than ABC and 35.8% better than FF, 47.73% better than DE systems. Also, for test case 3, the implemented model for 100th iteration is

79.16% superior to GA, 41.66% superior to PSO, 77% superior to ABC, 77% superior to FF and 83.33% superior to DE models. Therefore the enhancement of the proposed scheme in terms of cost function has been substantiated in a better way.



(a)

(b)

(c)

Fig. 6. Convergence analysis of the proposed over conventional models (a) Test case 1 (b) Test case 2 (c) Test case 3

F. Key Sensitivity Analysis

The key sensitivity analysis of the suggested GWO scheme for data preservation in healthcare for three test cases is given by Table II-IV. From Table II, the proposed method for 10th learning percentage is 1.25% superior to GA, 7.9% superior to PSO, 1.77% superior to ABC, 1.25% superior to FF and 5.68% superior to DE models. Similarly, for 30th learning percentage, the presented scheme is 0.12% better than GA, 0.23% better than PSO, 0.19% better than ABC and 0.29% better than FF, 0.244% better than DE systems. Also, the suggested method for test case 2 is given by Table III, where the implemented model at 40th iteration is 0.27% superior to GA, 5.48% superior to PSO, 5.16% superior to ABC, 0.16% superior to FF and 0.17% superior to DE algorithms. In addition, for 70th learning percentage, the suggested scheme is 0.64% better than GA, 0.18% better than PSO, 0.41% better than ABC and 0.29% better than FF, 0.41% better than DE methods. Also, the key sensitivity analysis for test case 3 is given by Table IV, where the presented scheme for 10th learning percentage is 0.15% superior to GA, 2.86% superior to PSO, 7.19% superior to ABC, 2.8% superior to FF and 3.04% superior to DE techniques. Similarly, for 80th learning percentage, the implemented method is 0.4% better than GA, 0.43% better than PSO, 0.54% better than ABC and 0.3% better than FF, 7.58% better than DE algorithms. Thus the effectiveness of the proposed model in terms of key sensitivity is confirmed successfully.

TABLE II Key sensitivity analysis of proposed model Test case 1

Methods	10%	30%	40%	70%	80%
GA [27]	0.992058	0.966954	0.935376	0.88658	0.829146
PSO [28]	0.99266	0.96867	0.933548	0.883524	0.826104
ABC [30]	0.991792	0.967799	0.933308	0.885459	0.828625
FF [31]	0.992203	0.968598	0.93496	0.884727	0.827198
DE [32]	0.992442	0.968194	0.93402	0.883104	0.826281
GWO	0.991876	0.965779	0.931839	0.881905	0.825605

TABLE III Key sensitivity analysis of proposed model Test case 2

Methods	10%	30%	40%	70%	80%
GA [27]	0.991989	0.969881	0.941546	0.890199	0.8371
PSO [28]	0.992485	0.971123	0.939674	0.886581	0.834497
ABC [30]	0.991737	0.970286	0.938949	0.888716	0.833309
FF [31]	0.992461	0.970174	0.940167	0.887782	0.834934
DE [32]	0.99228	0.970251	0.940451	0.888306	0.832737
GWO	0.991941	0.969292	0.938485	0.884349	0.828696

TABLE IV Key sensitivity analysis of proposed model Test case 3

Methods	10%	30%	40%	70%	80%
GA [27]	0.994065	0.975021	0.948223	0.890188	0.844802
PSO [28]	0.994081	0.97453	0.947932	0.888286	0.845153
ABC [30]	0.99356	0.974023	0.94679	0.88983	0.845942
FF [31]	0.994046	0.974414	0.948133	0.890195	0.844985
DE [32]	0.994018	0.975207	0.948793	0.88942	0.842893
GWO	0.993715	0.973662	0.9465	0.885651	0.841362

G. Statistical Analysis

As the met heuristic algorithms are stochastic in nature, it is necessary to execute the proposed and traditional schemes for five times, and the best solution was obtained. The statistical analysis of the presented GWO model for data preservation in IoT healthcare for three test cases is given in this section. From Table V, the statistical analysis for the proposed model for test case 1 in terms of best performance is 70.35% better than GA, 30.87% better than PSO, 62.62% better than ABC and 57.15% better than FF, 72.42% better than DE systems. Also, the worst performance of the proposed model is 51.73% superior to GA, 24.59% superior to PSO, 85.22% superior to ABC, 42.49% superior to FF and 52.14% superior to DE schemes. Moreover, the mean of the suggested technique is 62.01% better than GA, 26.53%

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

better than PSO, 56.34% better than ABC and 49.76% better than FF, 62.90% better than DE systems. Similarly, test case 2 can be obtained from Table VI, where the implemented scheme for best performance is 55.28% superior to GA, 219.91% superior to PSO, 51.42% superior to ABC, 43.12% superior to FF and 55.64% superior to DE methods. Also, the worst performance of the proposed scheme is 33.48% better than GA, 8.39% better than PSO, 30.83% better than ABC and 25.04% better than FF, 32.96% better than DE algorithms. Also, the median of the presented scheme is 46.64% superior to GA, 16.64% superior to PSO, 42.87% superior to ABC, 37.34% superior to FF and 45.55% superior to DE techniques. Furthermore, the test case 3 of suggested model is given by Table VII, where the proposed method is 54.29% better than GA, 64.09% better than PSO, 52.72% better than ABC and 50.84% better than FF, 55.82% better than DE systems. Also, the standard deviation for the implemented method is 64.73% superior to GA, 47.60% superior to PSO, 78.22% superior to ABC, 66.82% superior to FF and 93.36% superior to DE algorithms. Thus from the statistical analysis, the effectiveness of the presented privacy preservation model has been verified successfully.

TABLE V Statistical analysis of proposed and conventional methods for test case 1

Measures	GA [27]	PSO [28]	ABC [30]	FF [31]	DE [32]	GWO
Best	392428.7	301482	374619.1	362007.6	397182.7	230354.1
Worst	398021.6	326823.9	387642.9	373770.1	399091.7	262312.6
Mean	395994.8	309270.2	382136.4	366069.6	398177.3	244421.7
Median	396836	306182.2	380986.2	364767.9	398243	239718.7
Standard deviation	2215.384	10056.28	5340.785	4494.549	870.0179	12508.25

TABLE VI Statistical analysis of proposed and conventional methods for test case 2

Measures	GA [27]	PSO [28]	ABC [30]	FF [31]	DE [32]	GWO
Best	35417.37	27349.21	34536.42	32642.37	35499.15	22807.94
Worst	35947.91	29190.08	35235.35	33676.69	35805.9	26930.17
Mean	35701.07	28382.47	34863.07	33256.15	35630.29	24820.64
Median	35781.03	28498.7	34908.92	33557.11	35564.34	24432.94
Standard deviation	255.8514	800.8913	277.5553	483.6044	133.6668	1902.604

TABLE VII Statistical analysis of proposed and conventional methods for test case 3

Measures	GA [27]	PSO [28]	ABC [30]	FF [31]	DE [32]	GWO
Best	42701.39	32026.31	41284.36	39706.54	44177.88	19516.62
Worst	44892.63	35464.67	42646.54	41561.79	44550.53	25920.39
Mean	43549.64	33565.81	41841.54	40556.11	44317.36	23147.16
Median	43307.39	33505.58	41683.33	40359.69	44232.04	23226.22
Standard deviation	829.373	1231.786	512.0773	780.33	156.7796	2351.04

6. RESULTS AND DISCUSSION

This paper has presented a data sanitization model in IoT for privacy data preservation in the healthcare sector. Accordingly, the optimal key generation for the data sanitization process was recognized by means of the GWO algorithm. The constraints such as hiding failure rate, modification degree, and true positive value were minimized to obtain the objective, i.e., enhanced preservation of sensitive data. Moreover, the proposed method was compared with the conventional algorithms such as GA, PSO, ABC, FF and DE correspondingly and the results were obtained. From the convergence analysis, the suggested scheme for test case 1 at 100th iteration was 70.83% better than GA, 29.16% better than PSO, 58.33% better than ABC, 54.16% better than FF and 66.66% better than DE techniques. Also, from the key sensitivity analysis, the proposed method for 10th learning percentage was 1.25% superior to GA, 7.9% superior to PSO, 1.77% superior to ABC, 1.25% superior to FF and 5.68% superior to DE techniques. In addition, the statistical analysis for the proposed model for test case 1 in terms of best performance was 70.35% superior to GA, 30.87% superior to PSO, 62.62% superior to ABC and 57.15% superior to FF, 72.42% superior to DE systems. Thus the enhancement of the implemented GWO model has been proved proficiently.

REFERENCES

1. J. H. Abawajy and M. M. Hassan, "Federated Internet of Things and Cloud Computing Pervasive Patient Health Monitoring System," IEEE Communications Magazine, vol. 55, no. 1, pp. 48-53, January 2017.
2. Prosanta Gope and Tzonelih Hwang,"A Fog Based Middleware for Automated Compliance With OECD Privacy Principles in Internet of Healthcare Things," IEEE Access, vol. 4, pp. 8418-8441, 2016.
3. M. S. Hossain and G. Muhammad, "Cloud-Assisted Industrial Internet of Things (IIoT)- Enabled Framework for Health Monitoring," Computer Networks, vol. 101, pp.192–202, June 2016.
4. K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen and H. H. Luo, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," IEEE Wireless Communications, vol. 22, no. 4, pp. 104-112, August 2015.
5. Mahmud Hossain, S.M. Riazul Islam, Farman Ali, Kyung-Sup Kwak, Ragib Hasan," An Internet of Things-based health prescription assistant and its security system design",Future Generation Computer Systems, 2 December 2017.

6. M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib and F. Sallabi, "Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare," in Computer, vol. 50, no. 7, pp. 74-79, 2017.
7. Ming Tao, Jinglong Zuo, Zhusong Liu, Aniello Castiglione, Francesco Palmieri, “Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes”, Future Generation Computer Systems, vol. 78, Part 3, pp. 1040-1051, January 2018.
8. D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72-83, Feb. 2015.
9. Bahar Farahani, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Kunal Mankodiya, “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare”, Future Generation Computer Systems, vol. 78, Part 2, pp. 659-676, January 2018.
10. Min Woo Woo, JongWhi Lee, KeeHyun Park, “A reliable IoT system for Personal Healthcare Devices”, Future Generation Computer Systems, vol. 78, Part 2, pp. 626-640, January 2018.
11. YangSun Lee, Junho Jeong, Yunsik Son, “Design and implementation of the secure compiler and virtual machine for developing secure IoT services”, Future Generation Computer Systems, vol. 76, pp. 350-357, November 2017.
12. Munish Bhatia, Sandeep K. Sood, “A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective”, Computers in Industry, vol. 92–9, pp. 50-663, November 2017.
13. Suwon Kim, Seongcheol Kim, “User preference for an IoT healthcare application for lifestyle disease management Telecommunications Policy, 23 March 2017.
14. Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Hannu Tenhunen, “SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways”, Procedia Computer Science, vol. 52, pp. 452-459, 2015.
15. Sandeep K. Sood, Isha Mahajan, “Wearable IoT sensor based healthcare system for identifying and controlling chikungunya virus”, Computers in Industry, vol. 91, pp. 33-44, October 2017.
16. Gunasekaran Manogaran, R. Varatharajan, Daphne Lopez, Priyan Malarvizhi Kumar, Chandu Thota, “A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system”, Future Generation Computer Systems, 16 November 2017.
17. Yi Liu, Yinghui Zhang, Jie Ling, Zhusong Liu, “Secure and fine-grained access control on e-healthcare records in mobile cloud computing”, Future Generation Computer Systems, vol. 78, Part 3, pp. 1020-1026, January 2018.
18. Richard K. Lomotey, Joseph Pry, Sumanth Sriramoju, “Wearable IoT data stream traceability in a distributed health information system”, Pervasive and Mobile Computing, vol. 40, pp. 692-707, September 2017.
19. Suwon Kim, Seongcheol Kim, “A multi-criteria approach toward discovering killer IoT application in Korea”, Technological Forecasting and Social Change, vol. 102, pp. 143-155, January 2016.
20. Sravani Challa, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Athanasios V. Vasilakos, “An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks”, Computers & Electrical Engineering, 18 August 2017.
21. Amir M. Rahmani, Tuan Nguyen Gia, Behailu Negash, Arman Anzanpour, Pasi Liljeberg, “Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach”, Future Generation Computer Systems, vol. 78, Part 2, pp. 641-658, January 2018.
22. Yuehong YIN, Yan Zeng, Xing Chen, Yuanjie Fan, “The internet of things in healthcare: An overview”, Journal of Industrial Information Integration, vol. 1, pp. 3-13, March 2016.
23. Samir V. Zanjal, Girish. R. Talmale, “Medicine Reminder and Monitoring System for Secure Health Using IOT”, Procedia Computer Science, vol. 78, pp. 471-476, 2016.
24. Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir M. Rahmani, Jouni Isoaho, “End-to-end security scheme for mobility enabled healthcare Internet of Things”, Future Generation Computer Systems, vol. 64, pp. 108-124, November 2016.
25. Asif Qumer Gill, Nathan Phennel, Dean Lane, Vinh Loc Phung, “IoT-enabled emergency information supply chain architecture for elderly people: The Australian context”, Information Systems, vol. 58, pp. 75-86, June 2016.
26. Seyedali Mirjalili, Seyed Mohammad Mirjalili and Andrew Lewis, "Grey Wolf Optimizer", Advances in Engineering Software, vol.69, pp.46–61, 2014.
27. Holland, J.H.: Adaptation in Natural and Artificial Systems “Genetic Algorithm”, University of Michigan Press, Ann Arbor, Michigan; re-issued by MIT Press, 1992.
28. Kennedy, J.; Eberhart, R. . "Particle Swarm Optimization". Proceedings of IEEE International Conference on Neural Networks. IV. pp. 1942–1948, 1995.
29. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi and G. Marrocco, "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces," in IEEE Internet of Things Journal, vol. 1, no. 2, pp. 144-152, April 2014.
30. Dervis Karaboga and Bahriye Basturk, " A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm", vol. 39, no. 3, pp. 459–471, 2007.
31. Xin-She Yang, " Firefly algorithm, stochastic test functions and design optimisation", Int. J. Bio-Inspired Computation, vol. 2, n0. 2, 2010.
32. A. Glotic, N. Sarajlic, M. Kasumovic, M. Tesanovic, M. Sarajlic and J. Pihler, "Identification of thermal parameters for transformer FEM model by differential evolution optimization algorithm," 2016 International Conference Multidisciplinary Engineering Design Optimization (MEDO), pp. 1-6, 2016.