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.

I. 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 to their computing and communication abilities, which permit 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 HealthIoT. 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 severaltypes 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 the 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 BodySensorNetwork (BSN) schemes 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, IoT in the healthcare industry 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
be preserved or 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. Section VI concludes the paper.

II. 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 adaptability 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 Hossainet 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. Salahuddinet al. [6] has established an 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
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.

### III. 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 \( \tilde{D} \). In addition, the sanitization procedure is made by converting the time series data to another structure. At last, the converted data \( d_f \) is uploaded to IoT.

![Fig. 1. Overall framework of the implemented Privacy preservation model](image)

#### B. Sanitizing Phase

The sanitization procedure is for hiding the sensitive information, which is available in \( \hat{D} \). Accordingly, \( \tilde{D} \) 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.

\[
\tilde{D} \leftarrow \sum_{i=1}^{N_d} d_f
\]

![Fig. 2. Layout of sanitization](image)
Algorithm 1: Data Sanitization process

**Input:** Original database $\tilde{D}$

**Output:** Sanitized database $\bar{D}$

For every $d$ from $\tilde{D}$

$d_1$ is configured by Eq.(1)

Update $\bar{D}$ by Eq.(1)

End

### C. Restoring Phase

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

### IV. 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 $A$ indicates the binary matrix. The size of $d$ and $d_T$ is transformed to $1 \times 4$ as given in Eq. (3), Eq. (4) and Eq. (5) correspondingly.

$$d_T = d \times B$$

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

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

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

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.

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

For achieving the objective model, the optimal key is recognizedby 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 × 4], in which ‘4’ represent the sensor field, and 100,000 indicate the instant data. Therefore, the value which to be preserved can be assignedas $P_{val} = [4 \times 4]$. 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 $\alpha$ that remains as the leaders of the group. The second stage is $\beta$ which assists $\alpha$ in taking decisions. The third level is $\delta$, that is known as the subordinates. The final or last level is $\omega$, that is regarded as the scapegoat in the group. 

The wolf, $\alpha$ is regarded as the best solution and $\beta$ and $\delta$ obtains the second and third levels correspondingly. Accordingly, the hunting process is assisted by $\alpha, \beta$ and $\delta$. 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 $t^{(max)}$ 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 $P_t$ symbolizes the prey’s position vector and $P$ represents the grey wolf’s position vector.

$$B = |MP_t(t) - P(t)|$$

$$P(t + 1) = P_t(t) - N \times B$$

The parameters $N$ and $M$ coefficients are calculated as given by Eq. (13) and (14), in which $a_t$ and $a_t$ 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).

$$N = 2Z \cdot a_1 - Z$$
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, $P_\alpha$ 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 $f^{(max)}$
Assign $q := 0$ (counter initialization)

**Step2** for ($i = 1 : i \leq Q$) 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 ($i = 1 : i \leq Q$) 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 ($q < f^{(max)}$)
Generate the best solution $P_\alpha$ (best key)

V. 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 100\textsuperscript{th} 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 100\textsuperscript{th} 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 100\textsuperscript{th} 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.

![Fig. 3. HF rate analysis of the proposed over conventional models (a) Test case 1 (b) Test case 2 (c) Test case 3](image-url)
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 the 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 at the 100th 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 the 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.

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 schemes. 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.

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 the 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.

![Convergence analysis of the proposed over conventional models](image)

**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**

<table>
<thead>
<tr>
<th>Test case 1</th>
<th>10%</th>
<th>30%</th>
<th>40%</th>
<th>70%</th>
<th>80%</th>
</tr>
</thead>
<tbody>
<tr>
<td>GA [27]</td>
<td>0.992058</td>
<td>0.969954</td>
<td>0.935376</td>
<td>0.886585</td>
<td>0.829146</td>
</tr>
<tr>
<td>PSO [28]</td>
<td>0.99266</td>
<td>0.96867</td>
<td>0.933548</td>
<td>0.883524</td>
<td>0.826104</td>
</tr>
<tr>
<td>ABC [30]</td>
<td>0.991792</td>
<td>0.967799</td>
<td>0.933308</td>
<td>0.885459</td>
<td>0.828625</td>
</tr>
<tr>
<td>FF [31]</td>
<td>0.992203</td>
<td>0.968598</td>
<td>0.93496</td>
<td>0.884727</td>
<td>0.827198</td>
</tr>
<tr>
<td>DE [32]</td>
<td>0.992442</td>
<td>0.968194</td>
<td>0.93402</td>
<td>0.883104</td>
<td>0.826281</td>
</tr>
<tr>
<td>GWO</td>
<td>0.991876</td>
<td>0.965779</td>
<td>0.931839</td>
<td>0.881905</td>
<td>0.825605</td>
</tr>
</tbody>
</table>

**TABLE III Key sensitivity analysis of proposed model**

<table>
<thead>
<tr>
<th>Test case 2</th>
<th>10%</th>
<th>30%</th>
<th>40%</th>
<th>70%</th>
<th>80%</th>
</tr>
</thead>
<tbody>
<tr>
<td>GA [27]</td>
<td>0.991989</td>
<td>0.969881</td>
<td>0.941546</td>
<td>0.890199</td>
<td>0.8371</td>
</tr>
<tr>
<td>PSO [28]</td>
<td>0.992485</td>
<td>0.971123</td>
<td>0.939674</td>
<td>0.886581</td>
<td>0.834497</td>
</tr>
<tr>
<td>ABC [30]</td>
<td>0.991737</td>
<td>0.970286</td>
<td>0.938949</td>
<td>0.88716</td>
<td>0.833309</td>
</tr>
<tr>
<td>FF [31]</td>
<td>0.992461</td>
<td>0.970174</td>
<td>0.940167</td>
<td>0.887782</td>
<td>0.834934</td>
</tr>
<tr>
<td>DE [32]</td>
<td>0.99228</td>
<td>0.970251</td>
<td>0.940451</td>
<td>0.888306</td>
<td>0.832737</td>
</tr>
<tr>
<td>GWO</td>
<td>0.991941</td>
<td>0.969292</td>
<td>0.938485</td>
<td>0.884349</td>
<td>0.828696</td>
</tr>
</tbody>
</table>

**TABLE IV Key sensitivity analysis of proposed model**

<table>
<thead>
<tr>
<th>Test case 3</th>
<th>10%</th>
<th>30%</th>
<th>40%</th>
<th>70%</th>
<th>80%</th>
</tr>
</thead>
<tbody>
<tr>
<td>GA [27]</td>
<td>0.994065</td>
<td>0.975021</td>
<td>0.948223</td>
<td>0.890188</td>
<td>0.844802</td>
</tr>
<tr>
<td>PSO [28]</td>
<td>0.994081</td>
<td>0.97453</td>
<td>0.947932</td>
<td>0.888286</td>
<td>0.845153</td>
</tr>
<tr>
<td>ABC [30]</td>
<td>0.99356</td>
<td>0.974023</td>
<td>0.94679</td>
<td>0.88983</td>
<td>0.845942</td>
</tr>
<tr>
<td>FF [31]</td>
<td>0.994046</td>
<td>0.974414</td>
<td>0.948133</td>
<td>0.890195</td>
<td>0.844985</td>
</tr>
<tr>
<td>DE [32]</td>
<td>0.994018</td>
<td>0.975207</td>
<td>0.948793</td>
<td>0.88942</td>
<td>0.842893</td>
</tr>
<tr>
<td>GWO</td>
<td>0.993715</td>
<td>0.973662</td>
<td>0.9465</td>
<td>0.885651</td>
<td>0.841362</td>
</tr>
</tbody>
</table>

**G. Statistical Analysis**

As the meta 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% better than PSO, 41.66% better than 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.
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, 1.25% superior to FF and 5.68% 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 VI Statistical analysis of proposed and conventional methods for test case 1**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Best</td>
<td>392428.7</td>
<td>301482</td>
<td>374619.1</td>
<td>362007.6</td>
<td>397182.7</td>
<td>230354.1</td>
</tr>
<tr>
<td>Worst</td>
<td>398021.6</td>
<td>326823.9</td>
<td>387642.9</td>
<td>373770.1</td>
<td>399091.7</td>
<td>262312.6</td>
</tr>
<tr>
<td>Mean</td>
<td>395994.8</td>
<td>309270.2</td>
<td>382136.4</td>
<td>366096.9</td>
<td>398177.3</td>
<td>244421.7</td>
</tr>
<tr>
<td>Median</td>
<td>396836</td>
<td>306182.2</td>
<td>380986.2</td>
<td>364767.9</td>
<td>398243</td>
<td>239718.7</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>2215.384</td>
<td>10056.28</td>
<td>5340.785</td>
<td>4494.549</td>
<td>870.0179</td>
<td>12508.25</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Best</td>
<td>35417.37</td>
<td>27349.21</td>
<td>34536.42</td>
<td>32642.37</td>
<td>35499.15</td>
<td>22807.94</td>
</tr>
<tr>
<td>Worst</td>
<td>35947.91</td>
<td>29190.08</td>
<td>35235.35</td>
<td>33676.69</td>
<td>35805.9</td>
<td>26930.17</td>
</tr>
<tr>
<td>Mean</td>
<td>35701.07</td>
<td>28382.47</td>
<td>34863.07</td>
<td>33256.15</td>
<td>35630.29</td>
<td>24820.64</td>
</tr>
<tr>
<td>Median</td>
<td>35781.03</td>
<td>28498.7</td>
<td>34908.92</td>
<td>33557.11</td>
<td>35564.34</td>
<td>24432.94</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>255.8514</td>
<td>800.8913</td>
<td>277.5553</td>
<td>483.6044</td>
<td>133.6668</td>
<td>1902.604</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Best</td>
<td>42701.39</td>
<td>32026.31</td>
<td>41284.36</td>
<td>39706.54</td>
<td>41477.88</td>
<td>19516.62</td>
</tr>
<tr>
<td>Worst</td>
<td>44892.63</td>
<td>35464.67</td>
<td>42646.54</td>
<td>41561.79</td>
<td>44550.53</td>
<td>25920.39</td>
</tr>
<tr>
<td>Mean</td>
<td>43549.64</td>
<td>33565.81</td>
<td>41841.54</td>
<td>40556.11</td>
<td>44317.36</td>
<td>23147.16</td>
</tr>
<tr>
<td>Median</td>
<td>43307.39</td>
<td>33505.58</td>
<td>41683.33</td>
<td>40359.69</td>
<td>44232.04</td>
<td>23226.22</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>829.373</td>
<td>1231.786</td>
<td>512.0773</td>
<td>780.33</td>
<td>156.7796</td>
<td>2351.04</td>
</tr>
</tbody>
</table>

**VI. 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**


