

Article

Privacy Preservation in Edge Consumer Electronics by Combining Anomaly Detection with Dynamic Attribute-Based Re-Encryption

Eunmok Yang ¹, Velmurugan Subbiah Parvathy ², P. Pandi Selvi ³, K. Shankar ⁴,
Changho Seo ⁵, Gyanendra Prasad Joshi ^{6,*} and Okyeon Yi ^{7,*}

¹ Department of Financial Information Security, Kookmin University, Seoul 02707, Korea; emyang@kongju.ac.kr

² Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Srivilliputhur, Tamil Nadu 626128, India; s.p.velmurugan@klu.ac.in

³ Department of Computer Science, Mangayarkarasi College of Arts and Science for Women, Madurai, Tamil Nadu 625018, India; selvim11215@gmail.com

⁴ Department of Computer Applications, Alagappa University, Karaikudi, Tamil Nadu 630003, India; drkshankar@ieee.org

⁵ Department of Convergence Science, Kongju National University, Gongju 32588, Korea; chseo@kongju.ac.kr

⁶ Department of Computer Science and Engineering, Sejong University, Seoul 05006, Korea

⁷ Department of Information Security, Cryptology, and Mathematics, Kookmin University, Seoul 02707, Korea

* Correspondence: joshi@sejong.ac.kr (G.P.J.); oyyi@kookmin.ac.kr (O.Y.); Tel.: +82-2-6935-2481 (G.P.J.); +82-02-910-5120 (O.Y.)

Received: 7 September 2020; Accepted: 19 October 2020; Published: 29 October 2020



Abstract: The expanding utilization of edge consumer electronic (ECE) components and other innovations allows medical devices to communicate with one another to distribute sensitive clinical information. This information is used by health care authorities, specialists and emergency clinics to offer enhanced medication and help. The security of client data is a major concern, since modification of data by hackers can be life-threatening. Therefore, we have developed a privacy preservation approach to protect the wearable sensor data gathered from wearable medical devices by means of an anomaly detection strategy using artificial intelligence combined with a novel dynamic attribute-based re-encryption (DABRE) method. Anomaly detection is accomplished through a modified artificial neural network (MANN) based on a gray wolf optimization (GWO) technique, where the training speed and classification accuracy are improved. Once the anomaly data are removed, the data are stored in the cloud, secured through the proposed DABRE approach for future use by doctors. Furthermore, in the proposed DABRE method, the biometric attributes, chosen dynamically, are considered for encryption. Moreover, if the user wishes, the data can be modified to be unrecoverable by re-encryption with the true attributes in the cloud. A detailed experimental analysis takes place to verify the superior performance of the proposed method. From the experimental results, it is evident that the proposed GWO–MANN model attained a maximum average detection rate (DR) of 95.818% and an accuracy of 95.092%. In addition, the DABRE method required a minimum average encryption time of 95.63 s and a decryption time of 108.7 s, respectively.

Keywords: edge consumer electronics (ECE); dynamic attribute-based re-encryption (DABRE); modified artificial neural network (MANN); Internet of medical things (IoMT); anomaly detection

1. Introduction

Edge consumer electronics (ECE) are advanced gadgets that have tremendous computational capabilities when used with the Internet. They have transformed the computing framework used by the network of end clients all over the globe. The Internet of things (IoT) allows ECEs like smart cars, smart machines, smart appliances and so forth to transfer information from one another, and from other gadgets or systems, using a distinctive Internet address (IP). These smart appliances can be used in a home (referred to as a smart home) by structuring a networked system to do a variety of tasks automatically [1]. Moreover, the expanding utilization of edge consumer electronic components and innovations in vehicles has drastically changed not only transportation, but also the idea of security in the automotive industry over the last few decades [2,3]. The ongoing advancement is the Internet of medical things (IoMT), a sub-division of the IoT where clinical gadgets, like smart blood pressure monitors, smart glucometers, smart bands, smart pacers, smart pulse rate monitors and so on, are connected and exchange data with one another to share sensitive clinical information. The information is then used by health care authorities, specialists and emergency clinics to offer enhanced medication and help [4,5].

In all cases, the development of smart ECE devices with storage and handling capacities presents serious difficulties for most real-time applications, such as receiving a high throughput with diminished delay, the price of getting a service and so on. Cloud computing can be used to provide on-demand services to consumers in a cost-effective way in minimal time [6]. However, the cloud-based application building model does not work well in time-sensitive situations where high latency can bring about catastrophic results [7].

Thanks to the wide availability of advanced embedded equipment, along with the advancement of smart medical gadgets for universal health care, the IoMT has drastically changed health care services worldwide [8]. The wearable wireless sensor devices (ECSs) gather patients' information, encrypt it through an associate node and then transfer it to medical cloud storage. Medical staff can monitor the condition of every patient at the workstation in real time to screen treatment procedures and handle urgent situations [9,10]. Furthermore, the ongoing advancement of deep learning models has brought forth a revolution in consumer electronics, with progressively more intelligent smart gadgets performing at or about the human level of exactness in an assortment of tasks [11].

However, an advanced IoT should guarantee conditions like trust, security and privacy [12]. The danger of network attacks, such as the number of requests sent to the IoT services within a short time or unapproved access to services, may lead to tragic outcomes. Intruder detection systems (IDSs) can be used to identify intruders, as well as to keep the IoT networks secure and accessible. An IDS can reduce cybersecurity threats in edge computing. However, because resources and energy are limited for IoT gadgets, it is not always possible to use complex IDSs [13,14]. Security and privacy are considered central to the consumer electronics (CE) industry [15].

To achieve security and privacy, this paper develops a privacy preservation approach to protect the wearable sensor data gathered from wearable medical devices by means of an anomaly detection strategy, using artificial intelligence combined with a novel dynamic attribute-based re-encryption (DABRE) method. Anomaly detection is accomplished through a modified artificial neural network (MANN) based on a gray wolf optimization (GWO) technique, where the training speed and classification accuracy are improved. In this study, the GWO algorithm is preferred over other optimization parameters, owing to the few random and user-defined parameters. Some of the other advantages of the GWO algorithm are simplicity, speed, high accuracy, ease of implementation and the ability to be integrated with practical engineering problems. Once the anomaly data are removed, the data are stored in the cloud, secured through the proposed DABRE approach for future use by the doctors. Furthermore, in the proposed DABRE, the biometric attributes chosen dynamically are considered for encryption. Moreover, if the user wishes, the data can be modified to be unrecoverable by re-encryption with the true attributes in the cloud.

The remaining sections of the paper are arranged as follows. Section 2 provides a brief review of existing works related to the study. Section 3 discusses the proposed method, and Section 4 explains the performance validation of the proposed method. Finally, Section 5 concludes the study.

2. Related Works

Alexia Dini Kounoudes and Georgia M. Kapitsaki [16] recognized the fundamental requirements for an IoT security system to ensure protection of individual client information while supporting the General Data Protection Regulation (GDPR) prerequisites. They also identified the unsolved problems in client security.

Bhabendu Kumar Mohanta et al. [17] published a review of the IoT technology and its applications. They identified the essential security concerns, known as CIA (confidentiality, integrity, availability), as well as layer-wise problems. They then focused on three essential tools—artificial intelligence, machine learning and blockchain—for tackling the security problem in the IoT.

Syed Rizvi et al. [18] analyzed critical gadgets and their vulnerabilities, emphasizing the necessity of thorough security controls. They also examined possible attacks on IoT gadgets in three main domains: health care, commerce and at home. Their work included identifying exposures at the device level, considering attacks and risks due to known vulnerabilities and using proper security controls to reduce vulnerabilities and limit threats.

Vishal Sharma et al. [19] proposed a methodology that depends on edge-crowd integration to ensure trust and privacy in the social Internet of things (SIoT). Their approach uses crowd sources as mini edge servers and entropy modeling for characterizing trust among the entities. Fission managers were responsible for keeping up the security rules for each SIoT application.

Partha Pratim Ray et al. [20] considered the essential job of industrial guidelines and the components of edge computing for the scattering of overpowering, enlarged user involvement with the union of the IoT. First, they introduced a taxonomical classification and investigated which industrial aspects could profit simultaneously from the IoT and edge computing. Second, they presented two realistic case studies that used the edge IoT paradigm to take care of urban smart living issues. Third, they proposed a design based on edge IoT design for e-health care.

Ajaya K. Tripathy et al. [21] introduced a smart consumer electronics solution for a safe and progressive reopening after stay-at-home limitations are lifted. An IoMT-enabled wearable called an Easy Band was launched to limit the development of new positive cases via auto contact tracing and to encourage basic social distancing.

Tejasvi Alladi et al. [22] described the regular attacks faced by consumer IoT devices and proposed potential mitigation methods. The authors also emphasized the dangers presented by unsecured gadgets found throughout the community (e.g., smart city, smart home and critical infrastructure installations).

Prateek Jain et al. [23] presented an IoMT-empowered edge gadget for exact, noninvasive blood glucose estimation. The gadget was called an Intelligent Glucose Meter (iGLU) and used near-infrared (NIR) spectroscopy and an AI model of high precision. iGLU was validated in a medical clinic, and blood glucose estimates were put away in an IoMT stage for remote checking by endocrinologists.

Lei Xu et al. [24] proposed two different plans for cryptocurrency mobile payments. One involves a centralized bank, and the other does not require any centralized party. They also suggest a solution allowing the bank to meet know your customer (KYC) and anti-money laundering (AML) agreement requirements for cryptocurrency mobile payment processing.

3. Proposed Privacy Preservation Model in Edge Consumer Electronics

Edge consumer electronics (ECEs) include devices with contemporary hardware designs, used solely for communication, entertainment and home office events. ECEs help us with our everyday tasks, offering comfort, efficiency, effectiveness and promptness to ensure client satisfaction. Security and protection are challenging, although in many applications, they are considered the most basic features of the IoT. Security vulnerabilities encouraged intruders to abuse them

for their own advantage. In addition, the IoMT has tremendously rigid resource constraints. Accordingly, lightweight health data security and protection are essential necessities.

In treatment centers, monitoring the condition of elderly patients continuously is a significant challenge. In clinical practice, numerous sensors have been used to screen the health of a patient in real time and automatically alert the patient in case of a problem. If this information is leaked or altered during transmission, this is not only a breach of patient privacy, but also a threat to the patient's life. A basic problem with securing streaming health data is that the patient's data must be protected and authenticated efficiently throughout the networking environment.

In this paper, we present a new anomaly detection strategy using artificial intelligence (AI) combined with a novel dynamic attribute-based re-encryption (DABRE) method for processing and protecting wearable sensor data. It is assumed that the data are periodically sent to physicians for medical advice whenever a particular range of data is collected or any abrupt change in data occurs. During the transmission, the data are checked for anomalies using a modified artificial neural network (MANN), where a gray wolf optimization (GWO) algorithm is used to increase the training speed and anomalous data are removed. Once the anomalous data are removed, they are forwarded for encryption using the proposed dynamic attribute-based re-encryption strategy. The structure of the proposed privacy preservation model for ECEs is shown in Figure 1.

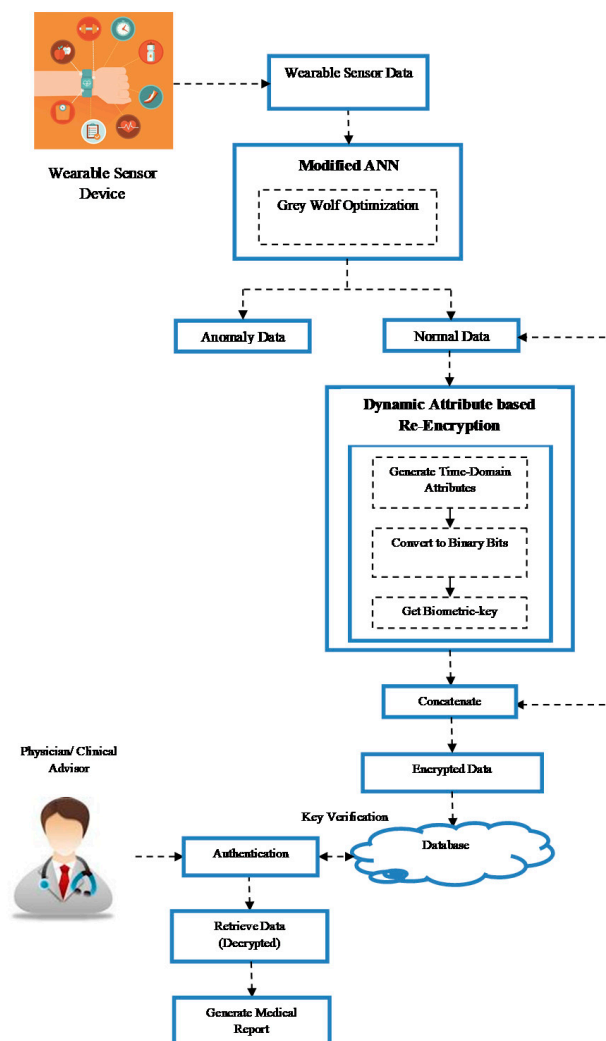


Figure 1. The structure of the proposed privacy preservation model for edge consumer electronics (ECEs).

The proposed encryption model encrypts the data based on the data's own attributes, which work as a biometric key. The data attributes are collected dynamically during the last few time periods, and they are processed (by binary bit conversion) and concatenated with the original data, so as to encrypt the data. The nature of this biometric key is dynamic, and during every encryption, the key is generated with a new set of time domain data. The encrypted data are securely stored in the databases, which physicians can use to generate medical reports for patients. Moreover, the proposed encryption model re-encrypts the data (by verifying the biometric key) whenever the client feels unsafe. This enhances the security of the data, in addition to increasing client satisfaction.

3.1. Anomaly Detection by a Modified ANN

An artificial neural network (ANN) is the algebraic equivalent of the human brain, used for complex pattern recognition [25]. ANN classification uses a three-layered, feedforward artificial neural network, where the sets of input neurons are mapped onto a set of computational outputs and a training algorithm (usually a backpropagation (BP) algorithm). The structure of an ANN consists of one input layer, one output layer and one or more hidden layers. Every layer is composed of various neurons or nodes interconnected by weights. Generally, the data sent as input to ANNs are trained, with or without providing the target output. The output pattern is registered by varying the weights to reduce the error between the actual and desired output patterns. The training process ends once the error is minimized to the desired range. Our proposed anomaly detection scheme takes the data from wearable sensor devices and processes this data to sort the output classes of data as normal or anomalous. Moreover, the proposed ANN-based anomaly detection scheme uses a GWO algorithm to optimize the weights by minimizing the training error. This improves the accuracy, training speed and performance of the existing BP algorithm. The structure of the proposed GWO-based modified ANN is shown in Figure 2.

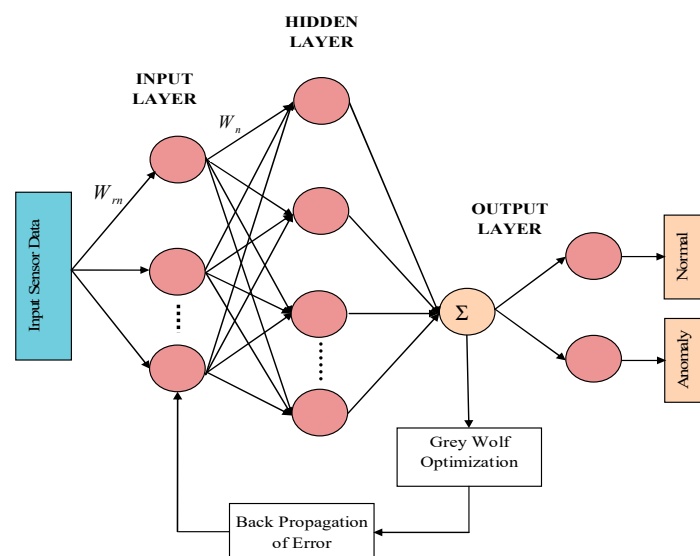


Figure 2. The structure of the proposed gray wolf optimization (GWO)-based modified artificial neural network (ANN).

Let $A = \{a_1, a_2, \dots, a_n, \dots, a_N\}$ denote the set of sensor data given as inputs to the ANN, and let the outputs be $B = \{b_1, b_2\}$, defining the data classes (normal and anomalous). The set of hidden layers is denoted as $H = \{h_1, h_2, \dots, h_r, \dots, h_R\}$. The operations taking place while the ANN is trained are listed below:

1. First, the number of neurons is initiated for the hidden layer, and then the input vector is fed to the input layer;

- Then, the neural network is generated with the input amount of neurons in the input layer, equivalent to the number of inputs, and with an output layer with two neurons, corresponding to the two output classes;
- The hidden layer input is calculated using the weighted sum of the outputs from the input layer by using the bias function of the input layer, which is specified as

$$h_r = \beta_r + \sum_{n=0}^{N-1} W_{rn} a_n \quad (1)$$

- Then, the output for the hidden layer is also found with the activation function of h_r :

$$h_r^{(out)} = AF(h_r) \quad (2)$$

Here, the activation function is a sigmoid transfer function, which can be given as

$$AF(h_r) = \frac{1}{1 + \exp^{-(h_r)}} = \frac{1}{1 + \exp^{(-\beta_r - \sum_{n=0}^{N-1} W_{rn} a_n)}} \quad (3)$$

- Once the hidden output is found, the training error ξ is established between the expected and obtained outputs as

$$\xi = \frac{1}{R} \sum_{r=0}^{R-1} h_r^{(out)}(expected) - h_r^{(out)}(actual) \quad (4)$$

where $h_r^{(out)}(expected)$ and $h_r^{(out)}(actual)$ represent the expected and obtained outputs, respectively.

- Finally, the BP algorithm is used to find the new weights of each neuron $\hat{W}_{rn}$:

$$\hat{W}_{rn} = W_{rn} + \partial W_{rn} \quad (5)$$

The term ∂W_{rn} is responsible for the formation of newer weights and is dependent on the backpropagation error:

$$\partial W_{rn} = \lambda h_r \delta \quad (6)$$

where δ illustrates the back propagation error and λ denotes the learning rate, with a value of $0.2 < \lambda < 0.5$.

- The above steps are repeated until the backpropagation error δ becomes smaller than 0.1.

3.2. Gray Wolf Optimization (GWO)

GWO is an algorithm inspired by the group hunting and social hierarchy behavior of gray wolves. They follow a strict social dominance hierarchy where the wolves are considered as alphas, betas, deltas and omegas. The alphas (dominant wolves) are responsible for decision-making. The betas get the second rank in the hierarchy and support the alphas in choice management. The beta wolves control the other lower-ranking wolves and send feedback to the alpha. They can also replace the alphas when an alpha wolf passes away or becomes very old. The third rank in the wolf hierarchy is the deltas (scouts, sentinels, elders, hunters and caretakers), which report to the alphas and betas. The lowest-ranking wolves are omegas, which maintain the dominance structure and serve the entire pack.

The GWO algorithm is designed to perform optimization through mathematical modeling of the social hierarchy behavior and group hunting technique of gray wolves. The group hunting is done in following steps: prey encircling, hunting and attacking prey (exploitation). The proposed privacy

preservation scheme in edge consumer electronics uses the GWO algorithm to improve the training speed of the modified ANN, so as to detect and remove the anomalous data. The GWO algorithm picks the optimal sets of weights for the ANN and solves the error minimization problem.

Step 1: Initialization

During initialization, the population of gray wolves (Z_j , where $j = 1, 2, \dots, m$), representing the set of weights used for an ANN training model, is initiated randomly. The coefficient vectors $\vec{C}$, $\vec{c}$ and $\vec{E}$, used for the optimization problem, are also initiated. In addition, the wolf hierarchy of α (alpha), β (beta) and χ (delta) are also initiated.

Step 2: Fitness Calculation

At this stage, the fitness of all the input solutions is evaluated, and the best solutions are chosen. The fitness function is designed according to the optimization problem and, therefore, the fitness can be defined as the minimization of error:

$$fitness(Z_j) = \min(\xi) \quad (7)$$

where ξ depicts the training error of the ANN. During every iteration, the training error is calculated with all possible sets of weights generated by the algorithm. Then, the set of weights with the smallest training error is saved as the fittest, and the algorithm tries to further improve or maintain the maximum fittest value.

At the end of the fitness evaluation stage, the social hierarchy of wolves is assigned numerically by designating the three best solutions as alpha (α), beta (β) and delta (χ). The remaining solutions are considered omegas (ω).

Step 3: Encircling Prey

Gray wolves encircle prey when hunting, and this behavior is mathematically modeled by the following equations:

$$\vec{F} = |\vec{E} \cdot \vec{Z}^l(x) - \vec{Z}(x)| \quad (8)$$

$$\vec{Z}(x+1) = \vec{Z}^l(x) - \vec{C} \cdot \vec{F} \quad (9)$$

where x represents the current iteration and $\vec{Z}(x)$ and $\vec{Z}^l(x)$ denote the location vectors of the wolf and the prey (optimum), respectively, at the x^{th} iteration. The coefficient vectors $\vec{C}$ and $\vec{E}$ are calculated as

$$\vec{C} = 2\vec{c} \cdot \vec{u}_1 - \vec{c} \quad (10)$$

$$\vec{E} = 2 \cdot \vec{u}_2 \quad (11)$$

Here, $\vec{u}_1$ and $\vec{u}_2$ define the random vectors distributed within the range $[0, 1]$, and the values of $\vec{c}$ are gradually decreased from 2 to 0 through the succession of iterations.

Step 4: Hunting

The hunting behavior is modeled by assuming that the alpha, beta and delta gray wolves have a superior ability to find and encircle prey. Therefore, the position of each solution is updated according to the location of the three best solutions. The formulas are

$$\vec{F}_\alpha = |\vec{E}_1 \cdot \vec{Z}^\alpha - \vec{Z}| \quad (12)$$

$$\vec{F}_\beta = |\vec{E}_2 \cdot \vec{Z}^\beta - \vec{Z}| \quad (13)$$

$$\vec{F}_\chi = |\vec{E}_3 \cdot \vec{Z}^\chi - \vec{Z}| \quad (14)$$

Using Equations (12–14), the search for prey is done by modifying the position vectors of other wolves based on the positions of the alpha $\vec{Z}^\alpha$, beta $\vec{Z}^\beta$ and delta $\vec{Z}^\chi$ wolves:

$$\vec{Z}_1 = \vec{Z}^\alpha - \vec{C}_1 \cdot \vec{F}^\alpha \quad (15)$$

$$\vec{Z}_2 = \vec{Z}^\beta - \vec{C}_2 \cdot \vec{F}^\beta \quad (16)$$

$$\vec{Z}_3 = \vec{Z}^\chi - \vec{C}_3 \cdot \vec{F}^\chi \quad (17)$$

Finally, the new solution $\vec{Z}(x+1)$ is generated with the combination of $\vec{Z}_1$, $\vec{Z}_2$ and $\vec{Z}_3$ as follows:

$$\vec{Z}(x+1) = \frac{\vec{Z}_1 + \vec{Z}_2 + \vec{Z}_3}{3} \quad (18)$$

Step 5: Attacking Prey (Exploitation)

During hunting, the position of the wolves is updated based on the alpha, beta and delta wolves. Once the optimal position of the prey is found, the wolves start attacking. This is mathematically modeled by decreasing $\vec{c}$ when approaching the prey. This variation range of $\vec{c}$ also impacts $\vec{C}$ so that the value of $\vec{C}$ is between $[-2c, 2c]$ and decreases over successive iterations as the $\vec{c}$ vector decreases. As the value of $\vec{C}$ comes within $[-1, 1]$, the wolves come closer to the prey.

Step 6: Search for Prey (Exploration)

To find the optimal solution, the gray wolf tries to search for prey by deviating from the previous position vector, and then the wolves converge to attack the prey. This divergence is mathematically modeled by modifying the value as $|\vec{C}| > 1$. This permits the GWO algorithm to search globally.

Step 7: Termination Phase

The above steps are repeated until the maximum iteration is reached or the best solution fulfilling the necessary rule is achieved.

The algorithm ends when the training error is reduced, and the training procedure is also halted to frame the training structure with the saved optimal set of weights. Afterward, the trained ANN with GWO can be generalized to predict the anomalous data for any set of data from the wearable sensor devices.

3.3. Dynamic Attribute (Biometric Key)-Based Re-Encryption

Attribute-based encryption (ABE) is a kind of public key encryption where the characteristic features (data attributes) are used to create the secret key (private key) for the client and, subsequently, create the ciphertext. In these methods, the decryption of a ciphertext is probable only if the set of attributes of the client key is successfully matched with the attributes of the ciphertext. This improves data confidentiality. By taking advantage of ABE, we have proposed a type of dynamic attribute-based re-encryption with a biometric key, used for securing the wearable sensor data that is already checked for anomalies.

The attributes that serve as the biometric key are chosen dynamically, according to the time-varying sensor data. Typically, the proposed algorithm selects the data (attributes) of last few time periods when data was transmitted to the cloud storage. Then, the data are converted to binary bits. During encryption, the binary converted attributes, as well as the public key, are concatenated with the sensor data that needs to be sent securely. The users with true attributes can also be allowed to confidently re-encrypt the encrypted data and make them unrecoverable if the data owner feels unsafe or does not want to keep the encrypted data. This is done by generating a re-encryption request, and then a re-encryption key is developed using that re-encryption request and the master private key. The re-encryption key is then used to re-encrypt the encrypted data. This re-encryption is done

at the cloud server. The dynamic attribute-based re-encryption scheme adds three more steps—the re-encryption request, Re-KeyGen (for re-encrypted key generation) and the re-encryption phase—in addition to the conventional attribute-based encryption scheme. All steps involved in the proposed dynamic attribute-based re-encryption scheme are listed below.

Setup Phase (n)

In this phase, a public key K_{pub} and a master key K_{pub}^M are generated arbitrarily, using the security parameter n by the trusted authority.

$$KeyGen(K_{pub}, K_{pvt}^M)$$

Here, the private key K_{pvt} that is used for decryption is generated from the input master key K_{pvt}^M and the public key K_{pub} .

$$Encrypt(K_{pub}, A(t), D_{(S)})$$

Now, the elements, including the public key K_{pub} , the time-domain attributes $A(t)$ and the sensor data $D_{(S)}$, are input to develop the cipher text $E[D_{(S)}]$. Finally, the encrypted data are updated to the cloud with the label $\{E[D_{(S)}], L\}$.

$$Re-Encrypt\ Request(A(t))$$

To enhance data security, the data owner requests re-encryption by providing the attributes $A(t)$. The attributes are validated by the cloud, and a re-encryption request $Req(ReE)$ is generated with some information about the key update.

$$ReKeyGen(Req(ReE), K_{pvt}^M)$$

During this section, the $Req(ReE)$ obtained is sent along with the master key K_{pvt}^M , and the trusted authority generates a re-encryption key $Re(K)$ for the data owner.

$$ReEncrypt(E[D_{(S)}], Re(K))$$

Finally, the re-encryption key $Re(K)$ is given with the encrypted data $E[D_{(S)}]$ in order to re-encrypt the encrypted data $E[D_{(S)}]$. This results in the re-encrypted data $ReE[D_{(S)}]$.

3.4. Data Retrieval and Medical Advisory Report Generation

Physicians retrieve the data to give medical advice. The authorized physicians have the public key K_{pub} and the private key K_{pvt} and decrypt the data using the function $Decrypt(K_{pub}, E[D_{(S)}], K_{pvt})$.

$$Decrypt(K_{pub}, E[D_{(S)}], K_{pvt})$$

During decryption, the original sensor data $D_{(S)}$ are retrieved when the public key K_{pub} , the secret key K_{pvt} and the encrypted data $E[D_{(S)}]$ are provided.

Now, the physicians get the original data $D_{(S)}$, and they can analyze it to generate proper medical advisory reports. The reports are then transmitted to the data owners. Once the owners receive the report, they can re-encrypt the data directly at the cloud server by providing only the attributes so that no one can understand the data. This enhances the security of edge consumer devices.

4. Results and Discussion

The results in this section were obtained by executing the proposed method on a PC with the following specifications: CPU Intel® Pentium 1.9 GHz; 64-bit operating system; Microsoft® Windows 10; 4 GB of RAM; and Java JDK 1.8. The experiments were done on the dataset used in [26]. The dataset is composed of continuous glucose monitor (CGM) data collected from 40 successive patients who have type 1 diabetes. For experimental validation, different validation processes (50–50, 60–40, 70–30, 80–20 and 90–10) were employed to split the dataset into training and testing sets. The parameter settings of the proposed method were given as follows: iteration count, 5000; learning rate, 0.001; momentum rate, 0.4; error, 0.001; activation function, sigmoid; and epoch count, 50.

4.1. Performance Metrics

For performance analysis, the metrics considered were accuracy, false alarm rate and detection rate.

Detection Rate

The proportion of true positives (TPs) to the summation of TPs and false negatives (FNs) is known as sensitivity:

$$DR = \frac{TP}{TP + FN} \times 100 \quad (19)$$

False Alarm Rate (FAR)

The false alarm rate (FAR) is the proportion of false positives (FPs) to the summation of true negatives (TNs) and false positives (FPs):

$$FAR = \frac{FP}{TN + FP} \times 100 \quad (20)$$

Classification Accuracy

Accuracy can be evaluated using the measures of specificity and sensitivity. It is denoted as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \quad (21)$$

where TP is the number of true positives, TN is the number of true negatives, FP is the number of false positives and FN is the number of false negatives.

4.2. Result Analysis

First, the performance of the proposed anomaly detection approach using a GWO-MANN was compared with an ANN using metrics like accuracy, false alarm rate and detection rate. The values are compared by varying training-testing rates and are presented in Table 1.

Table 1. Detection rate, false alarm rate and accuracy values of the proposed gray wolf optimization-based modified artificial neural network (GWO-MANN) and an existing artificial neural network (ANN) for varying training-testing ratios.

Training-Testing Ratio (%)	DR (%)		FAR (%)		Accuracy (%)	
	ANN	Proposed GWO-MANN	ANN	Proposed GWO-MANN	ANN	Proposed GWO-MANN
50–50	84.7	93.59	5.28	1.31	86.52	96.62
60–40	88.16	95.48	4.62	0.99	83.35	87.07
70–30	90.4	95.83	2.7	1.57	86.97	97.4
80–20	91.35	97.27	5.26	1.13	83.35	98.48
90–10	94.26	96.92	2.14	1.64	95.41	95.89

The training-testing ratio was varied by values of 50–50, 60–40, 70–30, 80–20 and 90–10. The respective detection rates for the proposed GWO-MANN were, respectively, 93.59, 95.48, 95.83, 97.27 and 96.92. For the existing ANN, the rates were substantially lower, being 84.7, 88.16, 90.4, 91.35 and 94.26, respectively. Likewise, the accuracy values obtained for the GWO-MANN were 96.62, 87.07, 97.4, 98.48 and 95.89, respectively, while the existing method provides values of only 86.52, 83.35, 86.97, 83.35 and 95.41. The FAR for the proposed GWO-MANN was 1.31, 0.99, 1.57, 1.13 and 1.64, which are lower than the values for the existing ANN.

In summary, the DR and accuracy values are higher, and the FAR values are lower, for the proposed GWO-MANN method, compared with the existing method. Furthermore, the detection rate is high when the training data ratio is increased.

Next, the performance of the proposed dynamic attribute-based re-encryption (DABRE) approach is compared with the existing attribute-based encryption scheme by varying the size of the input attributes (i.e., attributes computed for varying time periods in seconds). Here, we compared the encryption time, decryption time and re-encryption time.

It was observed that the encryption time needed for the proposed DABRE approach was 56, 59, 62, 77, 89, 98, 111, 119, 121, 128 and 132 ms from Table 2. The existing method took more time, measured at 60, 64, 76, 84, 90, 102, 118, 124, 136, 142 and 150 ms, respectively. The decryption time for the DABRE approach was 57, 69, 76, 82, 95, 103, 121, 135, 149, 152 and 157 ms, and the time for existing scheme was higher, being 80, 92, 100, 112, 124, 132, 142, 154, 162, 170 and 182 ms. Moreover, the re-encryption time was only measured for the proposed DABRE approach, and the values recorded were 114, 121, 125, 128, 130, 132, 133, 135, 136, 138 and 139 ms. These values show that both the encryption time and decryption time of the proposed DABRE approach increase gradually when the attribute size is increased. However, the encryption time and decryption time required for the proposed DABRE approach was smaller than that needed for the existing ABE. The re-encryption time also increased gradually when the attribute size increased.

Table 2. Encryption time, decryption time and re-encryption time analysis of the proposed dynamic attribute-based re-encryption (DABRE) with attribute-based encryption (ABE) for varying time periods.

Attributes Taken for Time Period (s)	Encryption Time (ms)		Decryption Time (ms)		Re-encryption Time (ms)	
	Existing ABE	Proposed DABRE	Existing ABE	Proposed DABRE	Existing ABE	Proposed DABRE
5	60	56	80	57	-	114
6	64	59	92	69	-	121
7	76	62	100	76	-	125
8	84	77	112	82	-	128
9	90	89	124	95	-	130
10	102	98	132	103	-	132
11	118	111	142	121	-	133
12	124	119	154	135	-	135
13	136	121	162	149	-	136
14	142	128	170	152	-	138
15	150	132	182	157	-	139

5. Conclusions

In this paper, we developed an efficient, privacy-preserving model for the security of data storage for edge consumer devices, especially wearable sensor medical devices. Our model checks the data for anomalies using a gray-wolf-optimization-based modified artificial neural network GWO–MANN. The data are then encrypted using our novel dynamic attribute-based re-encryption model before being stored in a cloud database. Re-encryption is done at the cloud, ensuring that the data are unrecoverable. This is an important feature for secondary data protection. We assessed the efficiency of the proposed anomaly detection method using the detection rate (DR), false alarm rate (FAR) and accuracy. We compared the values with those obtained using an existing ANN method. We also assessed the time required for the proposed encryption strategy. The results show that for our method, the DR and accuracy rate are higher and the FAR is lower than those of the existing method. The proposed method also takes less time. From the experimental results, it is evident that the proposed GWO–MANN model has attained a maximum average DR of 95.818% and an accuracy of 95.092%. In addition, the DABRE method has required a minimum average encryption time of 95.63 s and decryption time of 108.7 s, respectively. This shows that the proposed method outperforms the existing method in every aspect. As a part of the future scope, the MANN-based anomaly detection technique can be replaced by the use of deep learning (DL) models, such as recurrent neural networks (RNNs) and software-defined networks (SDNs). Besides that, the limitations of the GWO algorithm, such as a low solving accuracy, lower local searching ability and slow convergence rate, can be resolved by the use of quasi-oppositional-based learning strategy.

Author Contributions: Conceptualization, E.Y. and G.P.J.; data curation, E.Y.; formal analysis, K.S.; funding acquisition, O.Y.; investigation, E.Y. and V.S.P.; methodology, V.S.P.; project administration, C.S. and

G.P.J.; resources, P.P.S., C.S. and G.P.J.; software, E.Y.; supervision, G.P.J. and O.Y.; validation, P.P.S., C.S. and O.Y.; visualization, K.S.; writing—original draft, K.S.; writing—review and editing, G.P.J. All authors have read and agreed to the published version of the manuscript.

Funding: The work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Government (MSIT) (No.2020-0-00085, Research on Security Technology for 6G Telecommunication with 5G+).

Acknowledgments: K. Shankar would like to thank RUSA PHASE 2.0, Dept. of Edn. Govt. of India.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Farooq, M.O.; Wheelock, I.; Pesch, D. IoT-Connect: An Interoperability Framework for Smart Home Communication Protocols. *IEEE Consum. Electron. Mag.* **2019**, *9*, 22–29. [\[CrossRef\]](#)
2. Dibaei, M.; Zheng, X.; Jiang, K.; Abbas, R.; Liu, S.; Zhang, Y.; Xiang, Y.; Yu, S. Attacks and defences on intelligent connected vehicles: A survey. *Digit. Commun. Netw.* **2020**. [\[CrossRef\]](#)
3. Bernardini, C.; Asghar, M.R.; Crispo, B. Security and privacy in vehicular communications: Challenges and opportunities. *Veh. Commun.* **2017**, *10*, 13–28. [\[CrossRef\]](#)
4. RM, S.P.; Praveen Kumar Reddy Maddikunta, M.P.; Koppu, S.; Reddy, T.; Chowdhary, C.L.; Alazab, M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput. Commun.* **2020**, *160*, 139–149.
5. Greco, L.; Ritrovato, P.; Xhafa, F. An edge-stream computing infrastructure for real-time analysis of wearable sensors data. *Future Gener. Comput. Syst.* **2019**, *93*, 515–528. [\[CrossRef\]](#)
6. Garg, S.; Kaur, K.; Batra, S.; Aujla, G.S.; Morgan, G.; Kumar, N.; Zomaya, A.Y.; Ranjan, R. En-ABC: An ensemble artificial bee colony based anomaly detection scheme for cloud environment. *J. Parallel Distrib. Comput.* **2020**, *135*, 219–233. [\[CrossRef\]](#)
7. Pešić, S.; Ivanović, M.; Radovanović, M.; Badić, C. CAAVI-RICS Model for Observing the Security of Distributed IoT and Edge Computing Systems. *Simul. Model. Pract. Theory* **2020**, *105*, 102125. [\[CrossRef\]](#)
8. Greco, L.; Percannella, G.; Ritrovato, P.; Tortorella, F.; Vento, M. Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern Recognit. Lett.* **2020**, *135*, 346–353. [\[CrossRef\]](#)
9. Ge, C.; Yin, C.; Liu, Z.; Fang, L.; Zhu, J.; Ling, H. A privacy preserve big data analysis system for wearable wireless sensor network. *Comput. Secur.* **2020**, *96*, 101887. [\[CrossRef\]](#)
10. Zhu, H.; Wu, C.K.; Koo, C.H.; Tsang, Y.T.; Liu, Y.; Chi, H.R.; Tsang, K.-F. Smart Healthcare in the Era of Internet-of-Things. *IEEE Consum. Electron. Mag.* **2019**, *8*, 26–30. [\[CrossRef\]](#)
11. Lemley, J.; Bazrafkan, S.; Corcoran, P. Learning data augmentation for consumer devices and services. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE; IEEE), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–3.
12. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137. [\[CrossRef\]](#)
13. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion detection systems in the Internet of things: A comprehensive investigation. *Comput. Netw.* **2019**, *160*, 165–191. [\[CrossRef\]](#)
14. Lin, F.; Zhou, Y.; An, X.; You, I.; Choo, K.-K.R. Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of Internet of Things devices. *IEEE Consum. Electron. Mag.* **2018**, *7*, 45–50. [\[CrossRef\]](#)
15. Lee, J.-H.; Kim, H. Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consum. Electron. Mag.* **2017**, *6*, 134–136. [\[CrossRef\]](#)
16. Kounoudes, A.D.; Kapitsaki, G.M. A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet Things* **2020**, *11*, 100179. [\[CrossRef\]](#)
17. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [\[CrossRef\]](#)
18. Rizvi, S.; Pipetti, R.; McIntyre, N.; Todd, J.; Williams, I. Threat model for securing internet of things (IoT) network at device-level. *Internet Things* **2020**, *11*, 100240. [\[CrossRef\]](#)
19. Sharma, V.; You, I.; Jayakody, D.N.K.; Atiquzzaman, M. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. *Future Gener. Comput. Syst.* **2019**, *92*, 758–776. [\[CrossRef\]](#)

20. Ray, P.P.; Dash, D.; De, D. Edge computing for Internet of Things: A survey, e-healthcare case study and future direction. *J. Netw. Comput. Appl.* **2019**, *140*, 1–22. [[CrossRef](#)]
21. Tripathy, A.K.; Mohapatra, A.G.; Mohanty, S.P.; Kougianos, E.; Joshi, A.M.; Das, G. EasyBand: A Wearable for Safety-Aware Mobility during Pandemic Outbreak. *IEEE Consum. Electron. Mag.* **2020**, *9*, 57–61. [[CrossRef](#)]
22. Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.-K.R. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 17–25. [[CrossRef](#)]
23. Jain, P.; Joshi, A.M.; Mohanty, S.P. iGLU: An Intelligent Device for Accurate Noninvasive Blood Glucose-Level Monitoring in Smart Healthcare. *IEEE Consum. Electron. Mag.* **2019**, *9*, 35–42. [[CrossRef](#)]
24. Xu, L.; Chen, L.; Gao, Z.; Carranco, L.; Fan, X.; Shah, N.; Diallo, N.; Shi, W. Supporting Blockchain-Based Cryptocurrency Mobile Payment with Smart Devices. *IEEE Consum. Electron. Mag.* **2020**, *9*, 26–33. [[CrossRef](#)]
25. Dhanalaxmi, B.; Naidu, G.A.; Anuradha, K. Adaptive PSO based association rule mining technique for software defect classification using ANN. *Procedia Comput. Sci.* **2015**, *46*, 432–442. [[CrossRef](#)]
26. Fox, I.; Ang, L.; Jaiswal, M.; Pop-Busui, R.; Wiens, J. Deep multi-output forecasting: Learning to accurately predict blood glucose trajectories. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, London, UK, 19–23 August 2018; pp. 1387–1395.

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).