

Research Article

Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications

Rajesh Kumar Kaushal ¹, Rajat Bhardwaj ², Naveen Kumar ¹, Abeer A. Aljohani ³,
Shashi Kant Gupta ⁴, Prabhdeep Singh ⁵, and Nitin Purohit ⁶

¹Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

²Department of CSE, Faculty of Engineering & Technology, Jain University, Bengaluru, India

³Computer Science Department, Applied College, Taibah University, Saudi Arabia

⁴CSE Department, Integral University, Lucknow, India

⁵School of Computer Applications, BBD University, Lucknow, India

⁶Department of Computer Science, Kebri Dehar University, Ethiopia

Correspondence should be addressed to Nitin Purohit; nitinpurohit111@kdu.edu.et

Received 24 August 2022; Accepted 9 September 2022; Published 6 October 2022

Academic Editor: Akshi Kumar

Copyright © 2022 Rajesh Kumar Kaushal et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mobile computing and technology are becoming more common in many parts of private life and public services, and they are playing an increasingly important role in healthcare, not just for sensory devices but also for communication, recording, and display. They are used for more than only sensory devices but also for communications, recording, and display. Numerous medical indications and postoperative days must be monitored carefully. As a result, the most recent development in Internet of Things- (IoT-) based healthcare communication has been embraced. The Internet of Things (IoT), which is employed in a wide range of applications, is a catalyst for the healthcare industry. Healthcare data is complicated, making it difficult to handle and evaluate in order to derive useful information for decision-making. On the other hand, data security is a vital requirement in a healthcare data systems. Determining the need for a smart and secure IoT platform for healthcare applications, we create one in this study. Here, a cutting-edge encryption algorithm is used to protect the health data. Normalization is first used to preprocess the data and remove any irrelevant information. Using principal component analysis and logistic regression, the data's features are extracted (LR-PCA). To choose the pertinent features, a feature selection process based on genetic algorithms is used. We have put out a brand-new kernel homomorphism. To increase the security of the IoT network, use the two-fish Encryption algorithm (KHTEA). EBSMO (exponential Boolean spider monkey optimization) is used to further boost the encryption process' effectiveness. Utilizing the MATLAB simulation tool, the proposed system is assessed, and the metrics are contrasted with the accepted practices. Our suggested solution has been shown to be effective in protecting medical healthcare data. The effectiveness of the proposed and existing approaches is assessed using metrics for encryption time, execution time, and security level. The security precautions we suggested for healthcare data worked well.

1. Introduction

Mobile computing offers IoT services via mobile wireless services, applications, and the m-healthcare system. M-health helps the Internet of Things by offering features like compactness, IP connection, low battery utilization, and security. Because of their low cost and ease of use, IoT, mobile, and network connections are the ideal options. The

fundamental goal of IoT-based healthcare services is to deliver a rich user experience at a reasonable cost while also improving quality of life. In the medical area, the Internet of Things (IoT) introduces smart healthcare systems, which are typically made up of smart sensors, a remote server, and a network [1]. Mobile computing is a crucial sector that is critical in healthcare applications. Mobile computing offers both hardware and software-based solutions for IoT device

security. Individuals are not involved in a machine-to-machine (M2M) interaction among IoT systems, but human-to-computer interaction makes mobile computing extremely advanced. IoT networks' vulnerabilities could be easily exposed; thus, IoT mobile applications can help limit that risk. Furthermore, since such apps integrate online, mobile, and networking components, they might be difficult to create. Mobile computing is now being prioritized by healthcare businesses because it reduces IT costs and improves service and technological infrastructure [2]. Mobile computing enables movable and context-aware systems to change conventional towns and civilizations into technology-driven smart metropolises by using urban functions that are digitized. Despite its advantages and services, mobile computer systems and manner have several significant obstacles, including restricted hardware and data security and privacy concerns. Security refers to the principles, policies, and procedures in mobile computing environments that safeguard the confidentiality and integrity of users' and gadgets' data by prohibiting unauthorized access to data [3]. Several technological solutions have been developed in recent years to meet the demand for trusted mobile computing, including handset solutions such as Secure Element (SE), Trusted Platform Module (TPM), and Trusted Execution Environment (TEE). Software-based solutions have recently emerged as a result of the performance of integrated multicore processors, particularly for Virtualization Environments (VE) [4]. Figure 1 shows the representation of mobile computing for healthcare in the IoT framework.

The term "mobile computing" includes technologies that allow data, phones, and multimedia to be transmitted wirelessly from a computer device. It does not rely on a permanent physical network or connectivity. It lets people transition from one physical place to the other while communicating.

With the advent of mobile computing, customers' needs for high-quality, dependable services and support have grown. Many new applications for smart environments have emerged as both a consequence of the increasing number of distributed services available and resources [5]. For healthcare applications, we created a smart and secure IoT platform. A unique encryption method is used to protect the health data throughout this case.

The objectives of the IoT aid medical personnel in providing superior care to patients. It establishes a consolidated database for all of a hospital's digitally recorded actions, and other forms of data analytics can be applied to the problem-solving process. If patients are more at ease throughout their treatment, they are more likely to be pleased with the results and will heal more quickly. Internet of Things (IoT) healthcare equipment, wearable technologies, and data access enable doctors to keep closer tabs on their patients and administer more tailored care.

1.1. Contribution

- (i) Healthcare input-based datasets
- (ii) Preprocessing data by use of normalization

- (iii) Logistic regression-principal component analysis for feature extraction
- (iv) Features are selected using a genetic algorithm
- (v) Suggested a unique kernel homomorphism two-fish encryption algorithm (KHTEA) with exponential Boolean spider monkey optimization (EBSMO) to improve the security of the IoT network

Hence, in this paper, the research using mobile computing to provide a smart and secure Internet of things framework for medical applications was described. The further part of this article is categorized as follows: the related works and problem statement are presented in part 2; part 3 explains the proposed method; part 4 explains the results and discussion; part 5 explains the conclusion.

2. Related Works

In [6], the author suggests a unique electronic health record (EHR) sharing architecture on a blockchain-based mobile cloud service with a decentralized interplanetary file system (IPFS). To enable secure EHR sharing among patients and healthcare providers, a consistent user access solution concept of smart programs was developed. In [7], the authors discussed a security framework for mobile health apps based on two algorithms: (i) patient priority autonomous call and (ii) location distance-based switch and compared it to current frameworks. In [8], it is mentioned that the public cloud, cloud technology, big data analytics, the Internet of things, and cellphone apps are one of the most rapidly evolving technology in personalized medical systems. In [9], the author suggests the Claudio-Health as an innovative strategy for merging cloud computing (CC) and IoT for smart healthcare, known as the Claudio-Health paradigm. To present a realistic vision for integrating existing CC and IoT components in healthcare systems, this article defines the term Claudio-Health and examines various key complexities. In [10], the proposed method can handle a high number of users without significantly increasing the mean processing time. In [11], the author discussed IoT-based E-health applications, and a safe cluster key exchange system has been developed. For IoT-based healthcare applications, the paradigm should provide verification as well as efficiency and processing. In [12], a description of the primary technologies and paradigms in connection to healthcare, as well as their main application scenarios, and an analysis of the advantages and emerging cross-disciplinary obstacles are explained. In [13], the author suggests Petri net-based resource preservation net (RPN) architecture for early development (ED) systems, which is coupled with bespoke cloud and edge computing [14]. The suggested framework is technically explained and verified and is aimed at representing nonconsumable resources. In [15], the author suggests IoT security in embedded controllers (EC). First, the current state of research is discussed, as well as certain key terms. After that, they discuss the IoT service framework and EC. In [16], the author discussed the UCI dataset and medical

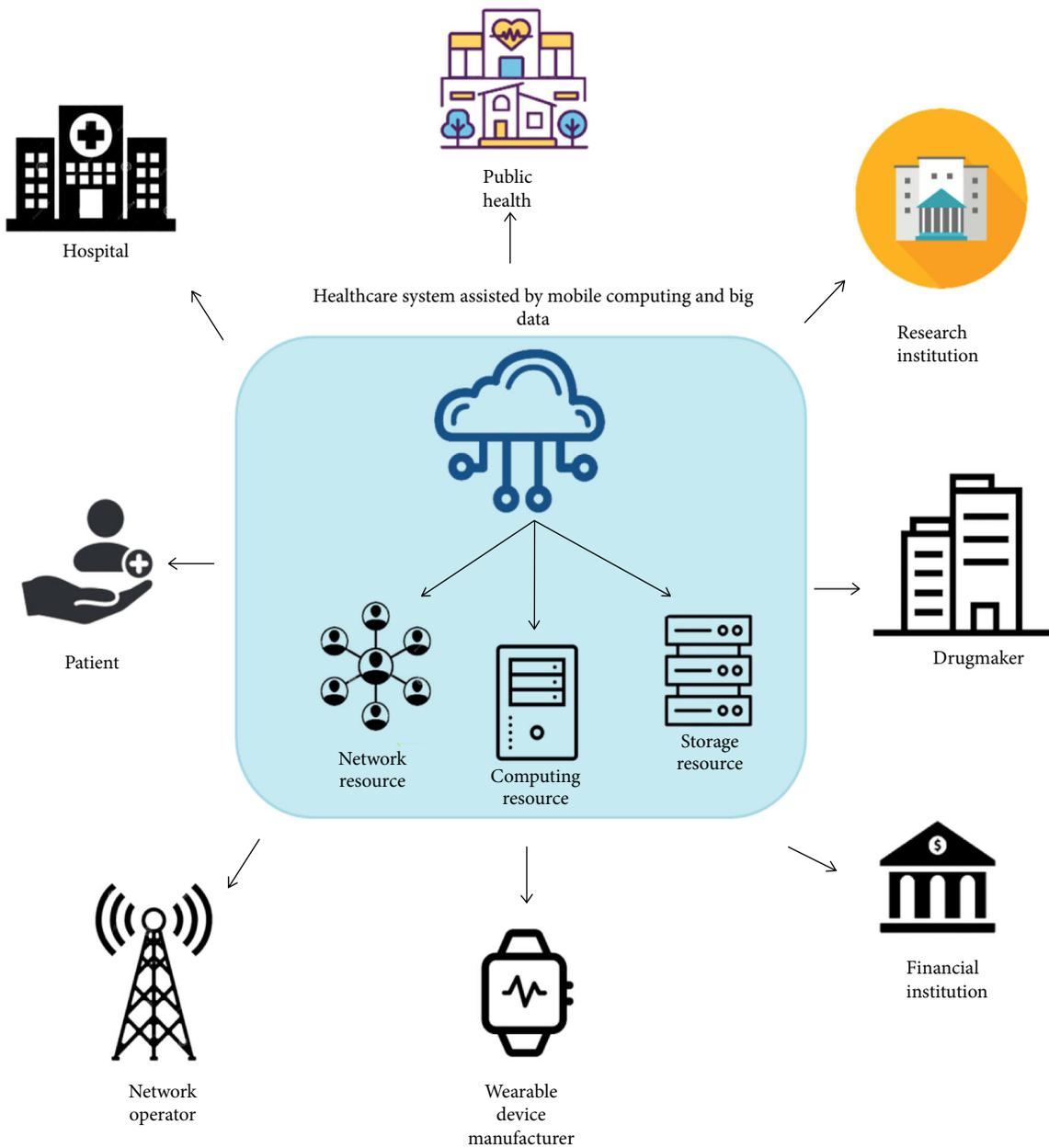


FIGURE 1: Mobile computing for healthcare in IoT.

sensors to create systematic student perspective health data to forecast students with varying illness severity. In [17], the author used the computer-based simulations to assess the proposed framework. The framework is superior for IoT-enabled healthcare systems. In [18], the author compared the diabetes disorders and associated medical data developed utilizing the UCI repository dataset and medical sensors to forecast persons who are seriously impacted by diabetes. In [19], the author suggested a specialized framework for one digital healthcare system based on IoT, with a particular emphasis on connectivity issues. In [20], the author develops an edge-based automated patient monitoring system that allows for remote monitoring and rapid detection of significant medical events. Then, to maximize

medical data exchange between different organizations, they combine this approach with blockchain architecture [21]. In [22], the author provides a complete overview of the Internet of medial things (IoMT) and its associated machine learning- (ML-) based development frameworks that were built or are now being used, throughout the previous decade, from 2010 to 2019. In [23], the author suggests that the Internet of Things (IoT) is rapidly developing in medical systems including health monitoring and fitness programs; assessments including IoT-based medical systems are being conducted. Many analyses have been undertaken to improve the surveillance efficiency of the IoT-based health service. In [24], an IoT BIOS Data Area (BDA) has aided in the creation of new health-related apps and services. This research

contributes to a corpus of knowledge in the domains of medical informatics and telecommunications and also the awareness about how these technologies are applied in true hospital healthcare. In [25], recent progress in the usage of the IoT in tackling different health concerns was already presented from the standpoint of technological solutions, healthcare facilities, and software products. An IoT system's possible obstacles and problems are identified. In [26], the author suggests an identification of mobile cloud techniques in the area of medical IoT networks. In [27], the author covers a variety of IoT difficulties and concerns, as well as architecture and major application areas. The article also highlights current literature and shows how it contributes to various facets of the Internet of Things. In [28], the author presented an improved routing protocol as the basis for a secure and scalable Internet of Things (IoT) architecture for transmitting healthcare data. A variety of Internet of Things (IoT) devices, such as wearables and sensors, are initially used to collect health data. In [29], there is combined recurrent neural networks (RNNs) and grey wolf optimization (GWO) to provide a novel quantitative approach to anticipate HR demand. To identify and disprove rumours spread online on Twitter about prominent international figures, including world leaders and politicians, a novel ReputeCheck technique is proposed [30]. The most frequent bullying method used against prominent figures, such as politicians and celebrities, is denigration, in which false information is spread online through the publication of rumours, images, and videos [31]. In [32], the author analysed the MMBD computing stack and draws parallels between the big data and MMBD computing ecosystems (MMBD). An application of three deep learning architectures—Deep Belief Networks, Convolutional Neural Networks, and Recurrent Neural Networks—in the area of speech recognition is surveyed [33]. Examine two collaborative filtering algorithms that address the sparsity and scalability difficulties at the same time: the first is based on the weighted slope one scheme and item clustering, while the second is based on item classification and item clustering [34].

2.1. Problem Statement. The health monitoring system allows patients to update current medical records through mobile telephone, and clinicians may efficiently handle the information of the patients. During an emergency, this is quite handy. A drawback of this technique was that patient welfare could not be monitored in real time. Due to the huge complexity of health records, the security of healthcare data transmission through the rise of mobile phones is difficult. The patient's hospital (PH) keeps every one of the patient's records in actual life. Healthcare data contains delicate data of patients, yet mobile phones have restrictions (limited computational capacity, difficult computations, etc.). The purpose of secured healthcare exchanging data is to protect individuals' sensitive medical records against data leakage while also making them accessible to allowed individuals because they need access. The use of the Internet and cloud equipment and devices is a growing section of healthcare

that finds a solution with quick and effective sharing of patient data as well as improved patient care. Mobile devices and the Internet are open to confidentiality, in addition to providing quicker and more effective related healthcare information.

3. Proposed Work

In the latest innovations in short-range wireless networks, a new location known as the Internet of Things (IoT) has emerged. The Internet of Things is currently producing new academic fields and technological transformations. The Internet of things based on the healthcare system is used for continually monitoring the patient's condition and diagnosing the patient in times of emergency. Several systems that form to monitor patient's health are included in the existing approaches. Due to their Internet communication, such systems are vulnerable to unauthorized users. There are numerous threats from preps that can put computer networks at risk. In this paper, the existing methods like orthogonal particle swarm optimization-optimal deep neural network (OPSP-DNN), escrow-free-identity based-aggregate signcryption (EF-IDAS), temporal health index-Bayesian belief network (THI-BBN), and grey filter Bayesian-convolution neural network (GFB-CNN) are compared. Figure 2 shows the representation of the suggested methods.

3.1. Input Healthcare Dataset. Organizational, economic, and medical info can be found in the initial files of an AIH and APAC databases, as indicated in Table 1 which lists all key data items. Every file format includes additional factors that differentiate a unique healthcare activity and is reflected supplementary to such fundamental attributes. In particular, average urine output over time and BMI measurements are only found in the critical care and weight loss surgery data files, but the mortality indicated data element is still only found in the hospitalized database objects. Table 1 describes the healthcare data elements of the AIH and APAC [35].

3.2. Data Processing Using Normalization. As the device dataset contains certain incorrect or incomplete data, as well as duplication in form during personal potential by both datasets, we execute data preprocessing, which comprises normalization, and handle all incorrect data, inaccuracies, and similar data. An equation was used to normalize data medical information DF^{mg} within domain $[0, 1]$, which decreased computing complexity:

$$Data_{U_{norm}} = \frac{DF^{mg} - Data_{U_{min}}}{Data_{U_{max}} - Data_{U_{min}}} \times [\max_{value} - \min_{value}] + \min_{value}, \quad (1)$$

where $Data_{U_{norm}}$ denotes the normalized value of a data source, $Information_{U_{min}}$ denotes the minimum value of a data source, $Data_{U_{max}}$ denotes the maximum value of a dataset, DF^{mg} denotes the original value of the medical data source, \max_{value} and \min_{value} denote the range of a

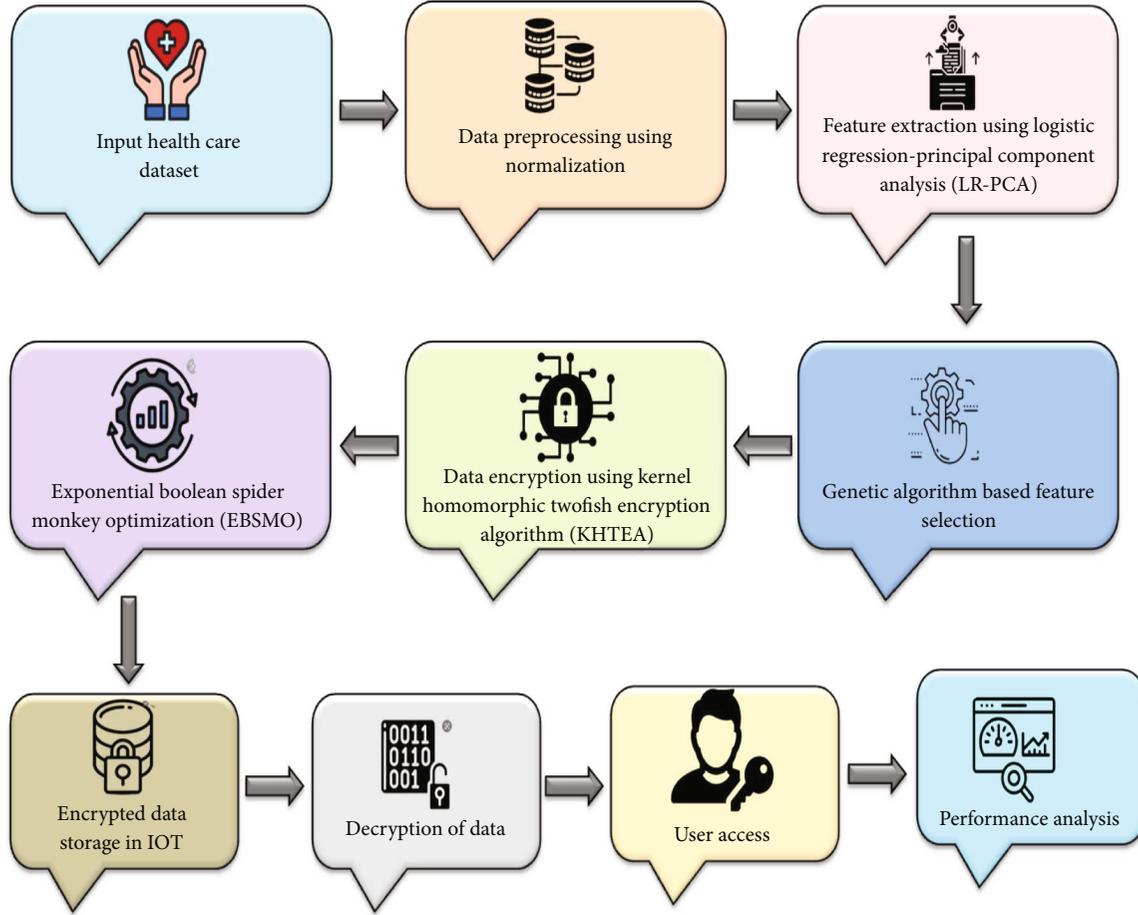


FIGURE 2: Schematic representation of the suggested methodology.

TABLE 1: Healthcare data elements of the AIH and APAC datasets.

Serial no.	Data element	Group	Data type
1	Data of discharge	Administrative	Data
2	Healthcare unit	Administrative	Code (CNES)
3	Issues data	Administrative	Data
4	Reason for discharge	Administrative	Code (local)
5	Age	Demographic	Numerical
6	Gender	Demographic	Code (local)
7	Nationality	Demographic	Code (local)
8	State	Demographic	Code (local)
9	Performance procedure	Action	Code (SIGTAP)
10	Main diagnosis	Evaluation	Code (ICD 10)
11	Secondary diagnosis	Evaluation	Code (ICD 10)

normalized input data, with $\max_{\text{value}} = 1$ and $\min_{\text{value}} = 0$, and DF denotes the initial price of a medical data source.

3.3. Feature Extraction Using Logistic Regression-Principal Component Analysis. Identifying all of the correlations between variables in data analysis might be tough. PCA

transforms a great deal of information included in initial datasets into a series of important three components, allowing for the discovery of hidden connections, enhanced information visualization, feature extraction, and categorization in new definition dimensions. If a learning algorithm is needed on the dataset, PCA can be quite useful because it aids in effectively initializing coordinates for grouping. To optimize the PCA output, first initially normalize the dataset upon a unit scale (mean = 0 and variance = 1), which would be a condition again for maximum efficiency of several neural network models. Our goal is to convert the p -dimensional database x together into different total sample y with lower size (Lp), wherein x is just the principal component of y .

$$x = TD(y). \quad (2)$$

With y containing a collection containing n dimensions.

(a) Organize into given data

With y containing a collection containing n dimensions.

(b) To use the equations, take the average

$$\bar{y} = \frac{\sum_{j=1}^m y_j}{m}. \quad (3)$$

(c) Determine variability:

$$R^2 = \frac{\sum_{j=1}^m (y_j - \bar{y})^2}{(m-1)}. \quad (4)$$

(d) Determine the correlation coefficients:

$$Y^{m \times m} = \left(y_{i,j}, y_{i,j} = \text{cov}(\text{Dim}_j, \text{Dim}_i) \right). \quad (5)$$

(e) Determine the principal components

The principal component and natural frequencies of a matrix are at the heart of a PCA. Its principal components would define the major feature design's orientations, whereas the principal components would decide its intensity. When is again a matrix, because if BY is an integer complex number of y , a nonnegative variable x in n is called an equal zero of B .

$$BY = \lambda y. \quad (6)$$

A number is referred to as a component of B , as well as the matrix y was referred to as a basis vector equal with. Because the positive integer matrices that meet the equations are the principal components related to a component of matrices B .

$$(\lambda I - B)y = 0. \quad (7)$$

For the equivalent evaluation spaces, let us identify the collection B like all matrices y that meet

$$F = \{y : (B - \lambda I)y = 0\}. \quad (8)$$

A logistic regression model was used extensively in a variety of fields, including evolutionary biology. Whenever the goal is to categorize collected data into groups, the multinomial logistic approach is applied. In most cases, the data point in logistic regression is basic, meaning this only holds information that can be categorized as 1 or 0, which then in our situation corresponds to an individual who is favorable or unfavorable for disease. The goal of the logistic regression technique is to obtain the best fit for describing the relationship between the target attribute and the predicted values that is analytically acceptable.

A regression analysis algorithm is based on calculation (9), which would be a regression analysis equation.

$$x = g_\theta(y) = \theta^P y. \quad (9)$$

Because equation (9) would be expensive in predicting our numeric code ($yI0$ and 1), we propose the function in equation (11) to assess the probability that a specific corresponds to the "1" (positive) class vs. the "0" (negative) class.

$$p(x = 1 | y) = g_\theta(y) = \frac{1}{1 + \exp(-\theta^P y)} = \sigma(\theta^P y), \quad (10)$$

$$p(x = 0 | y) = 1 - P(x = 1 | y) = 1 - g_\theta(y). \quad (11)$$

Creators can maintain that frequency of y^P inside the $[0, 1]$ range by using equation (12), sometimes known as the sigmoid function. Now will look for just a frequency of these because when x corresponds to the "1" class, the probability $p(x = 1 | y) ==$ is big, and then, when y corresponds to the "0" class, the probability $p(x = 0 | y)$ is low.

$$\sigma(p) = \frac{1}{(1 + f^{-p})}. \quad (12)$$

The data and outcome of our logistic regression technique are detailed in the next part after it has been effectively modeled or executed.

3.4. Genetic Algorithm-Based Feature Selection. Genetic algorithms (GAs) are a subset of simulated annealing, a rapid expansion subject of machine learning. Genetic algorithms are based on optimization algorithms that are founded on biological evolution. Proposed solutions to these problems are seen in a chromosomal group in GAs. Resolved bits are found on each and every chromosome. The basic chromosomal population consists of 1s and 0s distributed at randomness. Various ranges are given ranging between 0 and 1. Chromatids are parts in strings (1s and 0s); their duration is measured by the number of main components in the area at the top of this encoding scheme. Every chromosomal suggests a solution or a collection of important components again for the contender. The species expands by searching for genetic algorithms. Figure 3 shows genetic algorithms' workflow.

We derived the overall fitness function within described genetic algorithm by employing random function-dependent probability, as indicated in the equation:

$$\text{Fitness}(H | b) = \frac{\text{sumy} \text{in} b H b(y)}{H} * (H b(y)), \quad (13)$$

where $Hb(y)/H$ denotes the association between the number of things within the data source, vectors b hold the property H , and $H * (Hb(y))$ denotes the team probability of the items with the property b .

3.5. Data Encryption Using Kernel Homomorphic Two-Fish Encryption Algorithm. The set of all elements that are

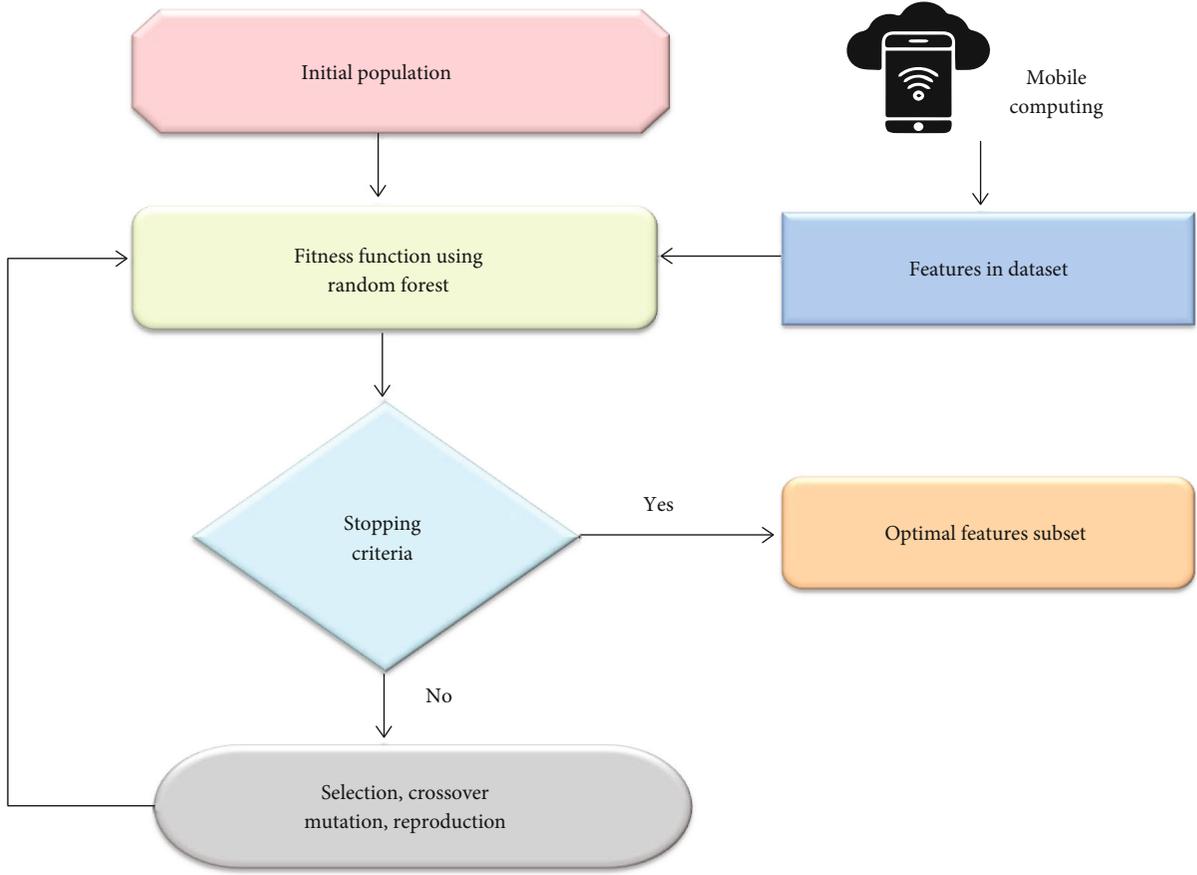


FIGURE 3: Genetic algorithm workflow.

mapped to an identity element of a group homomorphism constitutes its kernel. An identity element of is always present in the kernel, a regular subgroup of. If it is injective, it is reduced to an identity element. Data encryption methods have succeeded a previous data encryption standard. Validity, identification, or nonrepudiation is a few of the safety precautions that algorithms protect. To validate the source of communication, we have suggested kernel homomorphic two-fish encryption algorithm (KHTEA). A kernel is a method for representing a dataset in a flexible manner. Kernel’s main feature is plaintexts of various sizes. A clustering algorithm is the only name for a basic function of i , where the characteristic variable (i) and the integer value with the functions are known as a kernel.

$$S(i, i^x) = \phi(i) \cdot \phi(i^x). \quad (14)$$

We implement a kernel homomorphism toward a homomorphism that fails the drug and one function. Something like kernel homomorphism can be used to test the extent of the input component. As a function of using kernel and kernel homomorphism, users will be protected against loss or disturbance while encryption and decryption. Also, it controls the encryption complexity of the encrypt and prevents sounds or faults. The strategy’s security depends on term or condition, which would be difficult for a transmitter

to crack and allows them to obtain the initial encoded data. This significantly reduces computation and communication costs compared to the smooth curve’s tiny block cipher. According to this perspective, the most widely used kernel work is the linear kernel, polynomial kernel, quadratic kernel, sigmoid, and radial basis activities. These terminologies again for different kernel works are the following:

$$\text{linear}_l(I, J) = i^p j + a. \quad (15)$$

If i, j are still the linear kernel’s internal components, while (a) is a constant

$$\text{quad}_l(I, J) = 1 - \frac{\|i - j\|^2}{\|i - j\|^2 + a}. \quad (16)$$

If i, j is the given input variables of a polynomial kernel function

$$\begin{aligned} \text{poly}_l(I, J) &= (\lambda i^p j + a)^d, \lambda > 0, \\ \text{sig}_l(I, J) &= \text{tang}(\lambda i^p j + a), \lambda > 0. \end{aligned} \quad (17)$$

The data encryption efficacy was regularly focused on the kernel’s uniqueness. Within the event that now the

feature difference was continuously separable, then the radial basis task kernel must convert it into a multidimensional difference for the data to look linear and moveable.

When a homomorphism fails to inject or map exactly one object to another, we use a kernel homomorphism to fix it. The degree of an injective function can be quantified by employing a kernel homomorphism. In this context, the kernel of a homomorphism is trivial if and only if a homomorphism is injective.

The data encryption efficacy was constantly orientated just on kernel's diversity. Within the event that feature difference is continuously inseparable, the radial basis work kernel must convert into a higher-quality dimensional separation in order for the data to look sequentially separate. This encryption is performed using an optimal two-fish encryption technique in this application. Two-fish is a 128-bit block cipher with a changeable key size. To construct homomorphic connectivity including an input kernel function consisting of four crucial 8-by-8-bit S-boxes, a fixed 4-by-4 maximal value separated matrices on finite fields, a morph transformation, Boolean rotations, and a correct alignment managing and supporting makes up the cipher (Figure 4).

3.6. Exponential Boolean Spider Monkey Optimization. Our proposed work was inspired by exponential Boolean spider monkey optimization. The spider monkeys' group interactions create a randomized optimization method that models their feeding activity. This methodology to spider monkey feeding behavior reveals that such monkeys belong to the fission-fusion social structure (FFSS) oriented mammal class. As a function, the suggested algorithm may be adequately discussed in terms of fission-fusion social structure. Spider monkey optimization is separated into seven various steps, which are clearly explained as follows.

Spider monkey optimization (SMO) is a population-based algorithm inspired by spider monkey social interactions. It is based on spider monkeys' sophisticated foraging techniques, which mirror fission-fusion social organization. The members of fission-fusion social system (FFSS) individuals' transient small groups are drawn from a larger, more stable society. Based on the availability and scarcity of food supplies, monkeys separate themselves into larger and smaller groups and vice versa. SMO is a swarm intelligence metaheuristic algorithm that draws inspiration from spider monkeys' social organization. The algorithm imitates spider monkeys' foraging techniques. Based on the theory of spider monkeys' fission-fusion social structure (FFSS), this behavior can be divided into four categories. The party begins food foraging after assessing the distance to the food. The positions of the group members and the estimated distance from the food sources are updated in the second stage. The local leader then updates its best standing within the group in the following phase. When the local leader fails to update them on the optimal position, the entire gang begins looking for food.

3.6.1. Initialization Phase. A group of spider monkeys (SM) starts to increase, where $x = 1, 2, \dots, m$. As illustrated in

equation (18), each spider monkey is divided at probability sampling.

$$RN_{xy} = RN_{\min xy} + \text{rand} [0, 1] * (RN_{\max xy} - RN_{\min xy}). \quad (18)$$

RN_{xy} refers to the spider monkeys in the $y * RN$ variable. The boundaries of RN_{xy} in the $y * \text{variable}$ are $RN_{\max xy}$ and $RN_{\min xy}$, respectively, while $\text{rand} [0, 1]$ is a special variable in the domain $(0, 1)$.

3.6.2. Local Leader Phase. A spider monkey modifies its present role based on the behavior of the local leader and local team members. A fitness value of a newly acquired location is computed. If a fresh position comes fitness value is better than the previous one can be, $RN_{\text{new}xy}$ replaces its old position also with the unique thing.

$$RN_{\text{new}xy} = RN_{xy} + T_x * (KK_{ly} - RN_{xy}) + (1 - T_x) * (RN_{sy} - RN_{xy}). \quad (19)$$

RN_{xy} is the x^{th} SM in the y^{th} vector, and kk_{ly} is the l^{th} leader of the local assembling position within the y^{th} aspect. RN_{ry} specifies the r^{th} RN, which would be selected randomly from the T^{th} unit and has the value $T \in 1$ in the y^{th} variable.

$$\text{Prob}_x = 0.9 * \left(\frac{\text{Fitness}_x}{\text{Fitness}_{\max}} \right) + 0.1. \quad (20)$$

A given phrase can be used to compute the probability prob_x . And Fitness_x is the x^{th} spider monkey's fitness value. Furthermore, the overall fitness of a newly created spider monkey's positioning is calculated and recalculated location, with the higher position being selected.

3.6.3. Global Leader Phase. During the global leader phase, the spider monkeys utilize equation (21) and evaluate their success based on the global leader and the group has expanded members' interaction.

$$RN_{\text{new}xy} = RN_{xy} + \text{Prob}_x * (HK_y - RN_{xy}) + (1 - \text{Prob}_x) * (RN_{sy} - RN_{xy}). \quad (21)$$

If HK_y has been the global leader type of position y^{th} vector, y is taken randomly, and y is $1, 2, 3, \dots, D$.

3.6.4. Global Leader's Learning Phase. A new global leader is picked from among the spider monkeys with the best fitness. Furthermore, regardless of whether the global leader's position is modified or otherwise, the GlobalLimitCount number rises by one.

3.6.5. Local Leader Learning. Every member of the group changes their center before and during the stage, with community officials becoming the post with both the fittest. If the performance cost of the assets regional leadership role

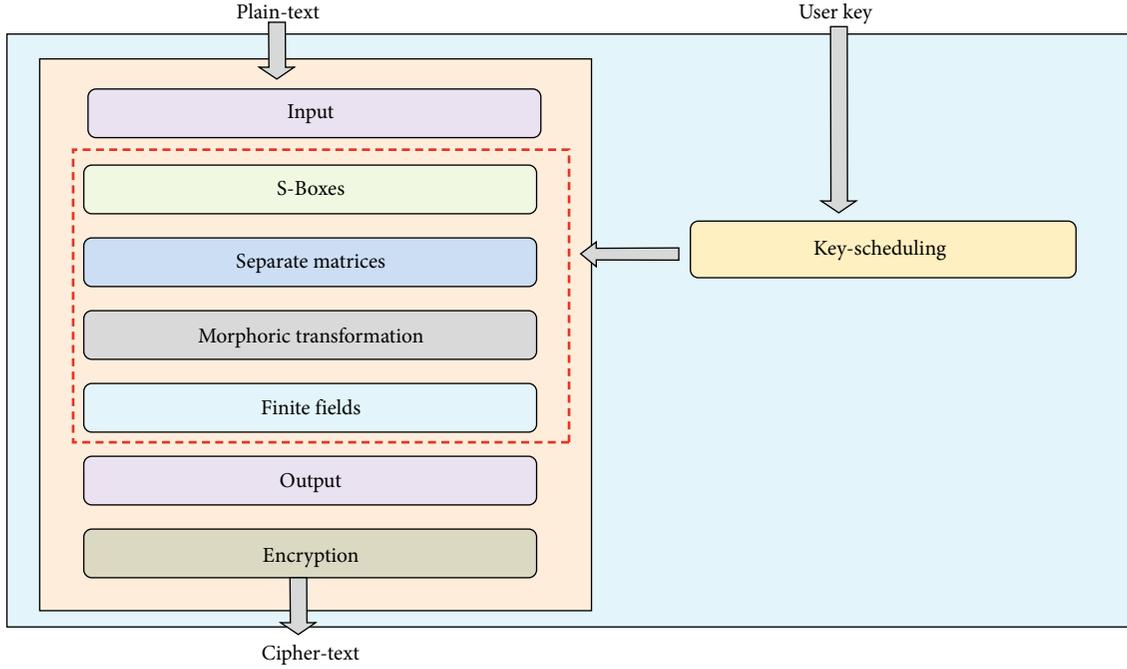


FIGURE 4: Two-fish algorithm steps in kernel homomorphism.

is smaller than the previous place, then the Local Limit Count value rises by individuals.

3.6.6. Local Leader Decision Phase. If the local leader viewpoint is still not changed to a Local Limit Count value, every group member will show changes at randomized or through merging global and local leader data.

$$RN_{newxy} = RN_{xy} + Prob_x * (HK_y - RN_{xy}) + (1 - Prob_x) * (RN_{sy} - KK_{ly}). \quad (22)$$

3.6.7. Global Leader Decision. If global leader status is not updated to a Local Limit Count quantity in this stage, the data is divided into two and three segments and so forth, till the maximal group (MG) is achieved.

The encrypted data is then stored in the IoT database, and the decryption process is done once the user accesses the data.

4. Result and Discussion

The kernel of a homomorphism (function that maintains structure) in algebra is typically the mirror image of 0. Foraging spider monkeys served as inspiration for spider monkey optimization (SMO), a global optimization technique that uses a fission-fusion social (FFS) structure. SMO beautifully illustrates the key ideas of self-organization and division of labor in swarm intelligence. In our paper, the proposed methods of kernel homomorphism two-fish encryption algorithm enhance the security of the IoT network. Exponential Boolean spider monkey optimization is compared with the existing methods. In this novel, we proposed the kernel homomorphism two-fish encryption algorithm (KHTEA) to enhance the security of the IoT

network. Exponential Boolean spider monkey optimization (EBSMO) is used to further increase the efficiency of the encryption process. Our paper compared the existing works like orthogonal particle swarm optimization-optimal deep neural network (OPSP-DNN), escrow-free-identity based-aggregate sing encryption (EF-IDAS), temporal health index-Bayesian belief network (THI-BBN), and grey filter Bayesian-convolution neural network (GFB-CNN).

4.1. Encryption Time. An encryption time is the time taken for data encryption that generates a key stream from plain-text. The overall flow of an encryption method is computed using encryption time, usually denotes its encryption speed. Figure 5 shows the comparison of encryption time.

The results of suggested and existing approaches' encryption time calculations are shown in Figure 5. According to the aforementioned graph, the proposed approach of KHTEA+EBSMO has a lower encryption time when compared to the existing methods like OPSO-DNN, EF-IDSC, THI-BBN, and GFB-CNN.

4.2. Decryption Time. Decryption is the process of restoring encrypted information to its initial state. In most cases, it was a reversal of the symmetric encryption. Since decryption needs a hidden key card, it decrypts its encrypted files so only a valid user accesses the decrypt. Figure 6 shows the comparison of decryption time.

Figure 6 represents the decryption time results with the proposed and existing approaches. Figure 6 shows that the proposed method of kernel homomorphism two-fish encryption algorithm with exponential Boolean spider monkey optimization has a low decryption time when compared to the existing methods such as OPSO-DNN, EF-IDSC, THI-BBN, and GFB-CNN.

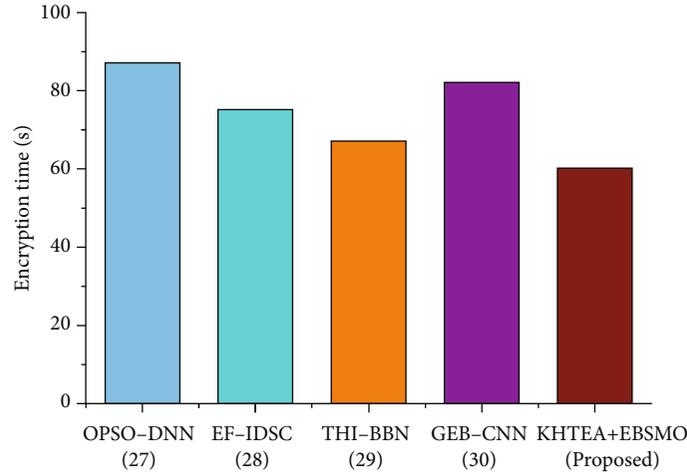


FIGURE 5: Comparison of encryption time(s).

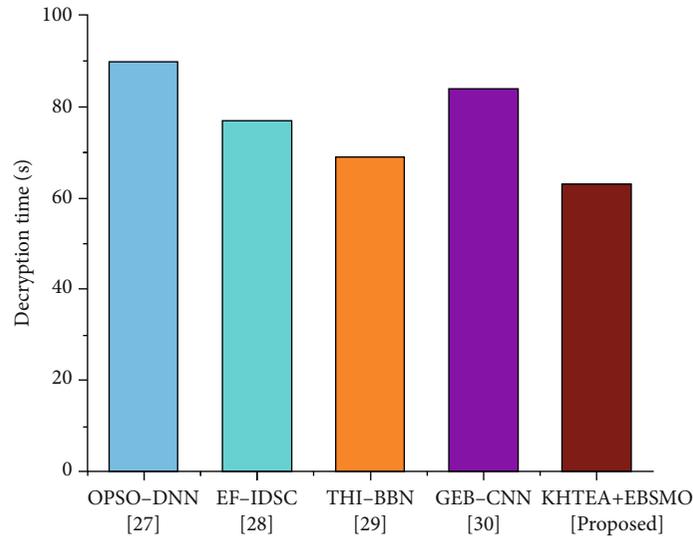


FIGURE 6: Comparison of decryption time(s).

4.3. Execution Time. An execution time of a process is the amount of time it spends proactively utilizing computer capabilities. Every work occurrence from the same assignment is likely to be taking a different amount of time to complete. Figure 7 shows the comparison of execution time.

Figure 7 represents the execution time results with the proposed and existing approaches. Figure 7 shows that the existing methods like OPSO-DNN, EF-IDSC, THI-BBN, and GFB-CNN have a high execution time when compared to the proposed methods of advanced KHTEA+EBSMO.

4.4. Security Level. Data security is combined with the requirement to preserve the data's integrity and authentication at the security level. There are three degrees of security: high, medium, and low. Figure 8 shows the comparison of security levels.

The results of suggested and existing approaches' security level calculations are shown in Figure 8. According to the aforementioned graph, the proposed approach of

KHTEA+EBSMO has the highest security level with 85% when compared to the existing methods like OPSO-DNN, EF-IDSC, THI-BBN, and GFB-CNN.

5. Discussion

In this part, we discuss the effectiveness of our proposed technique by assessing the above-mentioned performance metrics regarding mobile computing for the given data. Our proposed method is matched with other standard techniques OPSO-DNN [36], EF-IDSC [37], THI-BNN [38], and GFB-CNN [39]. In OPSO-DNN [36], for high-dimensional space, it is simple to slip into a local optimum, and the iterative process has a poor convergence rate. When directed weighted complex network particle swarm optimization (DWCNPSO) is used to address high-dimensional and difficult problems, its computational complexity is tolerated. In EF-IDSC [37], to prevent specific attack vectors that might allow unauthorized spending of cash,

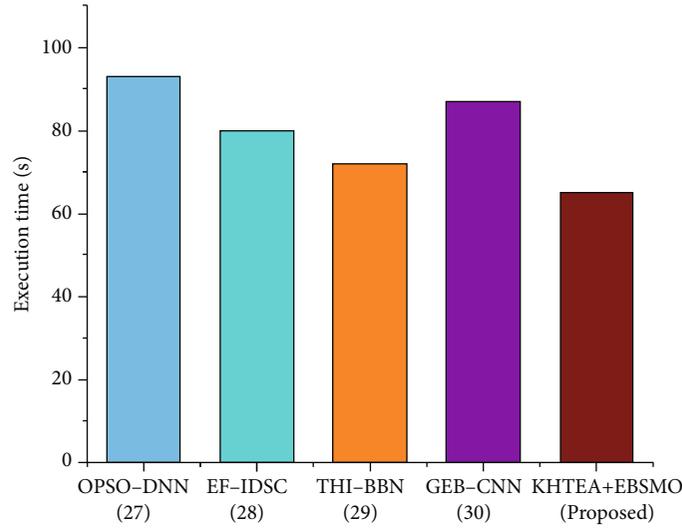


FIGURE 7: Comparison of execution time.

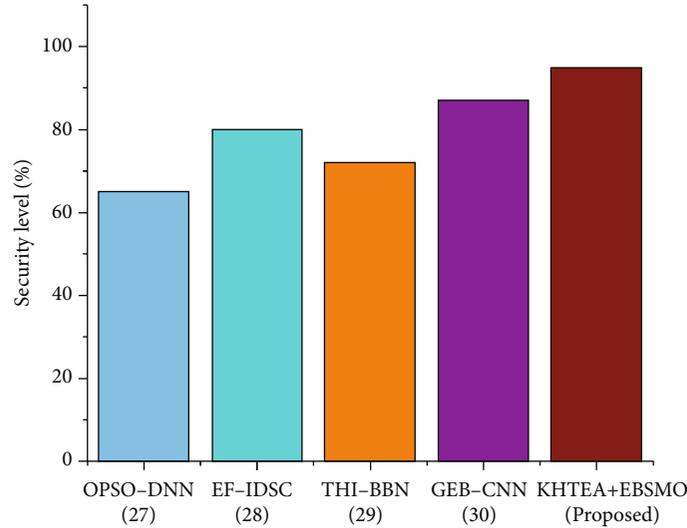


FIGURE 8: Comparison of security level.

careful implementation is essential. The use of signature aggregation to cover all transactions within a block is a possibility. The attacker can easily calculate a valid digital signature for an aggregate signature method using this information. In that manner, you can steal money from an address that you do not have authority over. In THI-BNN [38], there have been numerous breakthroughs in this regard, but no conqueror has emerged in a long time. In comparison, neural networks have an advantage because they can learn multiple patterns and are not confined to the originator. The pressure is dependent on the deflection, and the deflection is dependent on the pressure. This network fails to define and make decisions on a tightly coupled problem. In GFB-CNN [39], the cable network's top dense layers will incorporate very greater data and generate classifying predictions. It detects important aspects in an image's pixels. The surface layer will incorporate simple features into even more complex features, while hidden

levels may learn to detect simple features like boundaries and color gradients. There are no improvements in parameter selection and adjustment and also in the selection of criteria and data samples. These specified restrictions are properly resolved by using our proposed technique. In this part, the investigation analysis was demonstrated regarding the KHTEA. From this assessment, we accomplished the proposed approach with the greatest level of security than OPSO-DNN [36], EF-IDSC [37], THI-BNN [38], and GFB-CNN [39].

6. Conclusion

Medical healthcare organizations can now offer greater smart and easy applications and services because of advances in data technology and data computing. Medical systems will potentially play an integral role as a manual to health behavior, a resource to support business processes, and a

differentiator in the expanding health system, with the help of computer vision, data analysis, machine learning, and other modern approaches. In this paper, the proposed exponential Boolean spider monkey optimization (EBSMO) is used to further increase the efficiency of the encryption process. Our proposed work proved to be efficient for securing healthcare data.

Data Availability

There are no relevant data to be made available.

Conflicts of Interest

The authors declare no conflict of interest.

References

- [1] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of things for healthcare using effects of mobile computing: a systematic literature review," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 5931315, 20 pages, 2019.
- [2] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing-based healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 457–468, 2019.
- [3] A. Ahmad, A. W. Malik, A. Alreshidi, W. Khan, and M. Sajjad, "Adaptive security for self-protection of mobile computing devices," *Mobile Networks and Applications*, vol. 24, pp. 1–20, 2019.
- [4] M. A. Bouazzouni, E. Conchon, and F. Peyrard, "Trusted mobile computing: an overview of existing solutions," *Future Generation Computer Systems*, vol. 80, pp. 596–612, 2018.
- [5] C. H. Hsu, S. Wang, Y. Zhang, and A. Kobusinska, "Mobile edge computing," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7291954, 3 pages, 2018.
- [6] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE access*, vol. 7, pp. 66792–66806, 2019.
- [7] S. A. Butt, T. Jamal, M. A. Azad, A. Ali, and N. S. Safa, "A multivariant secure framework for smart mobile health application," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 8, article e3684, 2022.
- [8] V. Jagadeeswari, V. Subramaniaswamy, R. Logesh, and V. Vijayakumar, "A study on medical Internet of things and big data in personalized healthcare system," *Health information science and systems*, vol. 6, no. 1, pp. 1–20, 2018.
- [9] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 4151–4166, 2019.
- [10] M. A. Rahman, M. S. Hossain, G. Loukas et al., "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.
- [11] M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," in *2018 20th International Conference on advanced communication technology (ICACT)*, pp. 481–487, Chunchon, Korea (South), 2018.
- [12] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and health: Internet of things, big data, and cloud computing for Healthcare 4.0," *Journal of Industrial Information Integration*, vol. 18, article 100129, 2020.
- [13] S. Oueida, Y. Kotb, M. Aloiaily, Y. Jararweh, and T. Baker, "An edge computing based smart healthcare framework for resource management," *Sensors*, vol. 18, no. 12, p. 4307, 2018.
- [14] M. P. S. Bhatia and S. R. Sangwan, "Soft computing for anomaly detection and prediction to mitigate IoT-based real-time abuse," *Personal and Ubiquitous Computing*, vol. 25, pp. 1–11, 2021.
- [15] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: a survey," *Security and communication networks*, vol. 2020, Article ID 8872586, 13 pages, 2020.
- [16] P. Verma and S. K. Sood, "Cloud-centric IoT based disease diagnosis healthcare framework," *Journal of Parallel and Distributed Computing*, vol. 116, pp. 27–38, 2018.
- [17] J. Li, J. Cai, F. Khan et al., "A secured framework for sdn-based edge computing in IOT-enabled healthcare system," *IEEE Access*, vol. 8, pp. 135479–135490, 2020.
- [18] P. M. Kumar, S. Lokesh, R. Varatharajan, G. C. Babu, and P. Parthasarathy, "Cloud and IoT based disease prediction and diagnosis system for healthcare using fuzzy neural classifier," *Future Generation Computer Systems*, vol. 86, pp. 527–534, 2018.
- [19] M. Pasha and S. M. W. Shah, "Framework for E-health systems in IoT-based environments," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6183732, 11 pages, 2018.
- [20] A. A. Abdellatif, L. Samara, A. Mohamed et al., "Medge-chain: leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15762–15775, 2021.
- [21] N. K. Rajagopal, N. I. Qureshi, S. Durga et al., "Future of business culture: an artificial intelligence-driven digital framework for organization decision-making process," *Complexity*, vol. 2022, Article ID 7796507, 14 pages, 2022.
- [22] I. U. Din, A. Almogren, M. Guizani, and M. Zuair, "A decade of Internet of things: analysis in the light of healthcare applications," *Ieee Access*, vol. 7, pp. 89967–89979, 2019.
- [23] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," *SN Applied Sciences*, vol. 2, no. 1, pp. 1–8, 2020.
- [24] T. Saheb and L. Izadi, "Paradigm of IoT big data analytics in the healthcare industry: a review of scientific literature and mapping of research trends," *Telematics and Informatics*, vol. 41, pp. 70–85, 2019.
- [25] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-based applications in healthcare devices," *Journal of healthcare engineering*, vol. 2021, Article ID 6632599, 18 pages, 2021.
- [26] A. A. Mutlag, M. K. AbdGhani, N. A. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019.
- [27] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big data*, vol. 6, no. 1, pp. 1–21, 2019.
- [28] E. Refaee, S. Parveen, K. M. Begum et al., "Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications," *Wireless*

- Communications and Mobile Computing*, vol. 2022, Article ID 5665408, 12 pages, 2022.
- [29] N. K. Rajagopal, M. Saini, R. Huerta-Soto et al., "Human resource demand prediction and configuration model based on grey wolf optimization and recurrent neural network," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 5613407, 11 pages, 2022.
- [30] M. P. S. Bhatia and S. R. Sangwan, "Debunking online reputation rumours using hybrid of lexicon-based and machine learning techniques," *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*, Lecture Notes in Networks and Systems, vol. 121, P. Singh, W. Pawłowski, S. Tanwar, N. Kumar, J. Rodrigues, and M. Obaidat, Eds., Springer, Singapore, 2020.
- [31] S. R. Sangwan and M. P. Bhatia, "Denigration bullying resolution using wolf search optimized online reputation rumour detection," *Procedia Computer Science*, vol. 173, pp. 305–314, 2020.
- [32] A. Kumar, S. R. Sangwan, and A. Nayyar, "Multimedia social big data: mining," in *Multimedia Big Data Computing for IoT Applications*, S. Tanwar, S. Tyagi, and N. Kumar, Eds., vol. 163 of Intelligent Systems Reference Library, Springer, Singapore, 2020.
- [33] A. Kumar, S. Verma, and H. Mangla, "A survey of deep learning techniques in speech recognition," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 179–185, Greater Noida, India, 2018.
- [34] A. Kumar and A. Sharma, "Alleviating sparsity and scalability issues in collaborative filtering based recommender systems," *2013 Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*, Advances in Intelligent Systems and Computing book series (AISC, volume 199), Springer, Berlin Heidelberg, 2013.
- [35] D. Teodoro, E. Sundvall, M. João Junior, P. Ruch, and S. Miranda Freire, "ORBDA: an openEHR benchmark dataset for performance assessment of electronic health record servers," *Plo S one*, vol. 13, no. 1, article e0190028, 2018.
- [36] T. Veeramakali, R. Siva, B. Sivakumar, P. C. Senthil Mahesh, and N. Krishnaraj, "An intelligent Internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing*, vol. 77, no. 9, pp. 9576–9596, 2021.
- [37] M. Kumar and S. Chand, "A secure and efficient cloud-centric Internet-of-medical-things-enabled smart healthcare system with public verifiability," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10650–10659, 2020.
- [38] A. Haiter Lenin, S. Mary Vasanthi, and T. Jayasree, "Automated recognition of hand grasps using electromyography signal based on LWT and DTCWT of wavelet energy," *International Journal of Computational Intelligence Systems*, vol. 13, no. 1, pp. 1027–1035, 2020.
- [39] R. Patan, G. P. Ghantasala, R. Sekaran, D. Gupta, and M. Ramachandran, "Smart healthcare and quality of service in IoT using grey filter convolutional based cyber physical system," *Sustainable Cities and Society*, vol. 59, article 102141, 2020.