Journal of Intelligent Systems and Internet of Things
Vol. 13, No. 01, PP. 31-45, 2024
DOI: https://doi.org/10.54216/JISIoT.130103

Revolutionizing Healthcare: A Comprehensive Framework for Personalized IoT and Cloud Computing-Driven Healthcare Services with Smart Biometric Identity Management

S. Phani Praveen*[1], Chandra Shikhi Kodete[2], Saibaba velidi[3], Srikanth Bhyrapuneni[4], Suresh Babu Satukumati[5], Vahiduddin Shariff[6]

[1]Department of CSE, PVP Siddhartha Institute of Technology, Kanuru, Vijayawada, A.P, India
[2]Department of School of Technology, Eastern Illinois University, Charleston, Illinois, USA
[3]Department of Information Technology, SRKR Engineering College, Bhimavaram, A.P, India
[4]Department of CSE (IOT&CSBT), PACE Institute of Technology and Sciences, Valluru, Prakasam D.T, Andhrapradesh, India
[5]Computer Science and Engineering, Vignan's Foundation for Science, Technology and Research (Deemed to be University), Vadlamudi, Guntur District, A.P, India
[6]Department of Computer Science and Engineering, Sir C R Reddy College of Engineering, Eluru, A.P, India.

Emails: sppraveen@pvpsiddhartha.ac.in*[1]; chandrashikhi@gmail.com[2]; sai.velidi@gmail.com[3]; srikanth_b@pace.ac.in[4]; suresh.satukumati83@gmail.com[5]; shariff.v@gmail.com[6]

Abstract

Medical care conveyance has been transformed by the Internet of Things (IoT's) combination into wellbeing systems, which provides doctors and patients with continuous on-request services. However, this coordination poses questions with respect to the precision of the information and possible security risks. This research expects to present a sharp character the executives structure planned for IoT and distributed computing based personalized medical care frameworks. The purpose is to upgrade confirmation processes while restricting security threats through the double-dealing of multimodal encoded biometric features. The suggested approach incorporates biometric-based continuous authentication together with combined and concentrated personality access strategies. To safeguard patient information in the cloud, it combines electrocardiogram (ECG) and photoplethysmogram (PPG) signals for authentication, which is further bolstered by homomorphic encryption (HE). An AI (ML) model was used to assess the system's reasonability including a dataset of 20 clients in various seating configurations. The merged based biometric structure defeated standalone ECG or PPG signal-based procedures in perceiving and authenticating every client with 100% exactness. The proposed framework makes significant improvements to the privacy and security of personalized healthcare frameworks. It fulfills the essential security necessities and is by the by viable enough to run on low-end processors. It guarantees trustworthy authentication and protects against conventional security threats by utilizing multimodal biometric features and cutting-edge encryption techniques.

Received: March 22, 2024 Revised: May 02, 2024, Accepted: June 28, 2024

Keywords: Healthcare; Internet of Things (IoT); Cloud computing; Smart biometric identity management; electrocardiogram(ECG); photoplethysmogram (PPG); Homomorphic Encryption (HE); Machine learning (ML).

1. Introduction

Throughout the course of recent years, the utilization of Internet of Things (IoT) innovation has developed considerably across a range of organizations, and the healthcare area is no special case [1]. The Internet of Things has the potential to change the healthcare business by making it conceivable to gather and analyze real-time patient data dramatically. More accurate diagnosis, individualized treatment plans, and far off health checking could result from this [2]. The safe checking of patient health data is one of the main purposes of the Internet of Things in healthcare, and it necessitates cloud based IoT arrangements. Cloud-based IoT for safe health observing reforms healthcare by giving real-time capabilities to data gathering, evaluation, and independent direction. Therefore, costs drop, and efficiency rises [3].

The notable advancements made in 2022 and 2023 made it workable for these advancements to be broadly adopted by decreasing stresses over privacy, data security, and interoperability. Working on patient care, distinguishing health issues early, and encouraging more teamwork are all beneficial to patients, health care suppliers, and

researchers. Since cloud based IoT holds the way to revolutionizing the way we track and manage our personal health, it presents huge open doors for the advancement of healthcare.

To address some of the issues, this article suggests the CloudIoT PersonalCare identity management architecture. For access control, it combines the Federated and Centralized Identity Management Systems (IDMS). To safeguard security and privacy, it authenticates clients utilizing scrambled biometric features. To defend the security of the patient information, homomorphic encryption is used to scramble both the biometric boundaries and the patient information [4]. The as of late demonstrated system has been picked above elective methodologies since it is normally suitable for shielding clinical information examination.

In this work, the electrocardiogram (ECG) and photoplethysmogram (PPG) signals are consolidated to think up the confirmation procedure. Since most of IoT devices in a PH network can peruse these signs, these two qualities were picked. Because it is easily falsified and is likely to spoofing, utilizing a solitary trait-based biometric for authentication, like an ECG, is inadequately safe. By the by, joining these two signals utilizing mathematical mean and communicating to PH cloud services via homomorphic encryption will increase the security and trouble of manufacturing or falsifying their utilization for authentication.

Transforming Healthcare: The Synergistic Impact of IoT and Cloud Technologies

The state of the healthcare industry has greatly improved from previously. In addition to helping patients, modern medical equipment, diagnostics, and treatment options also simplify the lives of physicians, hospitals, and insurance providers [5]. Let's examine how the Internet of Things is changing the healthcare sector.

IoT for Doctors

Wearable IoT technology and home monitoring tools help physicians treat patients more successfully. They can monitor patients' health in real time and ascertain whether they are following treatment regimens and medication schedules. Healthcare providers will be notified of any irregularity detected by these devices, enabling them to offer emergency medical aid. Doctors will be able to select the course of treatment and have greater communication with their patients thanks to Internet of Things devices connected to the cloud.

IoT for Patients

Patients receive individualized care using wearable technology, which includes fitness bands, smart watches, blood pressure monitors, heart rate monitoring cuffs, and more. These devices allow them to monitor their heart rate, number of calories burned, blood pressure fluctuations, amount of exercise, and more [6]. Patients can record their own observations with these Internet-connected devices and forward them to a hospital or their physician for professional advice. These devices can notify the patient's doctor, other concerned healthcare practitioners, and their family members in the event of an emergency or any disruption to usual activities.

IoT for Hospitals

Hospitals can gain much from IoT devices in addition to physicians and patients. In addition to keeping track of the inventory of medical equipment, such as wheelchairs, nebulizers, oxygen pumps, defibrillators, and other monitoring devices, they can also monitor patient health and alert physicians [7]. Real-time visibility of hospital medical staff is another benefit that IoT may offer. Monitoring and stopping the spread of illnesses is one of the biggest areas where IoT helps hospitals [8]. Hygiene monitoring devices with Internet of Things capabilities can record infected patients and stop such gadgets from being reused.

IoT for Health Insurance Companies

Intelligent IoT devices are used by health insurance firms for underwriting, risk management, processing and executing claims, and identifying fraudulent claims [9]. By using the information gathered by a patient's medical equipment, they can make better judgments. By facilitating greater openness between the client and the insurance provider, these gadgets enable precise claim processing and underwriting.

Objectives of the Study

The primary aims of this study are outlined below:

- To design and build a state-of-the-art identity management system for Internet of Things and cloud computing-based personalized health care solutions.
- Examine whether, under the suggested framework, multimodal encrypted biometric features might improve authentication procedures.
- To evaluate the security gains made possible by combining biometric-based continuous authentication with federated and centralized identity access strategies.
- To assess the effectiveness and dependability of the suggested framework for user authentication utilizing a combination of photoplethysmogram (PPG) and electrocardiogram (ECG) signals, backed by homomorphic encryption (HE) for cloud processing data security.

2. Review Of Literature

Saif et al. [10] analyzed dependable healthcare inside the framework of IoT and give a comprehensive analysis of standards in addition to a case study demonstrating IoT's application in secure health checking. Their review features the need of powerful information security, confidentiality, and access control techniques to safeguard the honesty and privacy of healthcare data.

Bikku et al examined how the Internet of Things can alter the field of healthcare checking. Their review emphasizes the importance of real-time data assortment and analysis made conceivable by IoT and how it has the potential to totally change the way healthcare services are given [11]. Their research features the need of scalable and dependable IoT advances to guarantee secure health checking.

Butpheng et al. gave a valuable example of consolidating IoT and cloud computing in an e-health climate. The authors gave proof that it is feasible to proficiently integrate and carry out cloud computing and Internet of Things (IoT) innovations. Through this integration, costs are decreased while health results, treatment practicality, and diagnostic accuracy are all gotten to the next level [12]. Identification, authentication, and authorization are only a couple of the privacy/security necessities that the authors of a comprehensive technical architecture with a comprehensive rundown of prerequisites for e-health frameworks that utilization IoT-cloud innovation accommodated associated smart hardware, custom frameworks, and custom applications that communicate over the Internet. By analyzing and distinguishing vulnerabilities from each security aspect, security arrangements that are in accordance with the proposed architecture can be actually worked to lessen the probability of an attack.

Wang and Cai suggested the use of Edge-cloud computing (SHNIE) and Internet of Things (IoT) to give a safe, fast, and financially savvy way to transmit medical data by joining Named Data Networking (NDN) with healthcare data[13]. From the nearest edge gadgets that have the necessary medical data, SHNIE may successfully disseminate aggregated NDN-medical data to several shoppers. To maintain privacy and security, the NDN uses a hash ciphertext of the supplier's name and IDs as a verification token to guarantee communication security.

Rahmani et al. Haze computing is used to add a geographically disseminated intermediate knowledge layer between cloud gadgets and sensor gadgets in e-health frameworks that leverage IoT-cloud innovation [14]. Their approach tackles issues related to adaptability, scalability, and stability. , It was found that the smart e-health gateway health observing framework model was fruitful in further developing framework knowledge, energy productivity, portability, performance, security convention interoperability, and dependability.
Begum et al. created a framework for the Internet of Things called the Smart Healthcare Observing Framework. This framework's main goal is to make it workable for individuals who have heart issues to exactly measure their internal heat level, heart rate (in beats each moment), and body act in a clean climate[15]. The framework is evaluated on a worker who voluntarily takes part in the research. Various physiological markers, including heart rate and internal heat level, are evaluated during the evaluation. In addition, the participant's developments are checked, and serial plotting software housed on a local server is used to evaluate the ECG graph.

Praveen et al. examined a cloud-based, Internet of Things-based electrocardiogram (ECG) checking framework. Their review's goal was to foster an innovation that may be used in keen healthcare settings. The researchers suggested a state-of-the-art method for tracking ECG via the Internet of Things [16]. A wearable surveillance hub is used to gather ECG data, which are consequently remotely shipped off the Internet of Things cloud. The IoT cloud uses the MQTT and HTTP conventions to give users access to graphical representations of real-time ECG data. The ease with which internet browser-prepared smart terminals may get ECG data has decreased the challenge of cross-platform interoperability. Human subjects healthy are used in analyses to evaluate the framework's dependability. Empirical data demonstrates that the proposed strategy is exceptionally reliable with regards to acquiring and introducing ECG data in real time.

3. Proposed Methodology

3.1 Cloud IoT Personal Care Identity Management System (IDMS) Framework

Numerous opportunities arise when personalized healthcare systems are integrated with other IoT systems and cloud technology. A few of the potential smart applications that could arise from the Internet of Things' integration of personalized healthcare (PH) are shown in Figure 1.

IoT sensors, wearables, and other smart devices assemble patient information at the contraption layer, where information procurement happens, and they move that information to the cloud data set through the IoT entryway (the passage layer). A variety of networking devices with Internet access make up the Gateway layer. In order to do the authentication computations, these devices autonomously create a local cloud. In order to authenticate the patient later, they encrypt the biometric template and store it. In order to guarantee proper permission in the healthcare database, the encrypted template is also sent by the Gateway layer to the hospital cloud [17]. This results in a number of apps that can use this data to their advantage. In addition to giving other healthcare applications the ability to offer intelligent services like emergency alert systems, community-based engagement services, and smart medication management, among many others, it allows medical practitioners to view the data remotely. When additional IoT apps are added to the cloud IoT system, the prospects grow enormous. The device layer, entryway layer, and clinic/public healthcare cloud layer contain the three levels of the proposed CloudIoT based healthcare framework. The patient's association contains the Device layer, where contraptions are verified through a focal passage. The patient's confirmation accreditations, encryption, and some other primer calculations are kept at the Entryway layer.

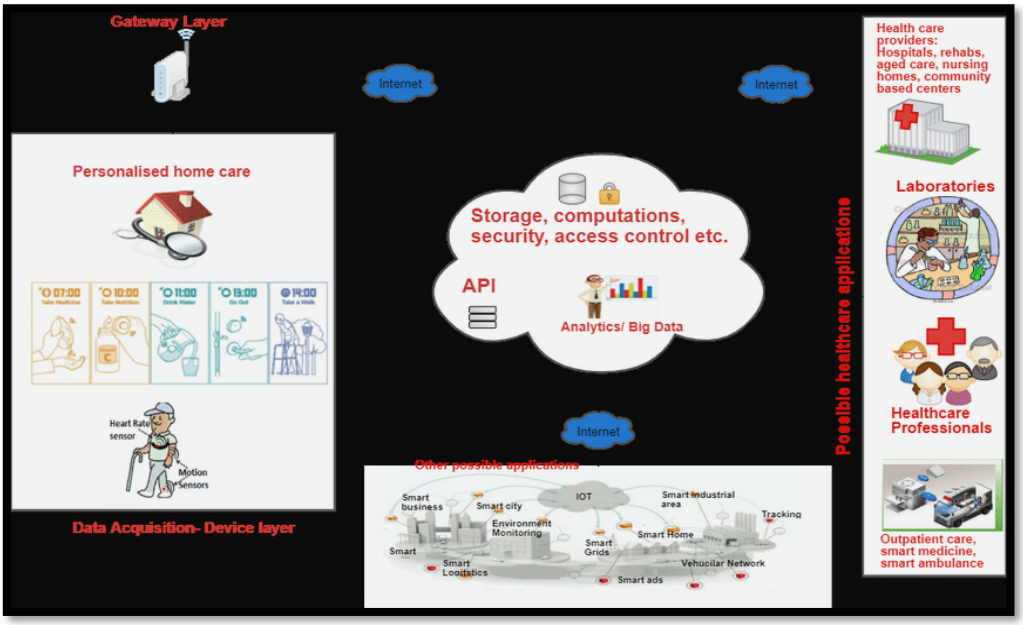


Figure 1: Architecture of CloudIoT Philippines offerings

Table 1: The Cloud IoT Personal Care Identity Management System (IDMS) Framework's Layer Description

Layer	Description
Device Layer	Patients' biometric information is gathered by sensors and sent to the gateway layer.
Gateway Layer	To ensure authenticity, biometric templates are saved and encrypted using homomorphic encryption (HE) techniques.
Clinic/Public Healthcare Cloud Layer	In addition to processing and analysing patient data, authentication information is saved.

The Authentication Framework

Figures 2 and 3 portray the enrolment and authentication phases, which are the two stages of the authentication techniques engaged with the hospital cloud layer and gateway, separately.

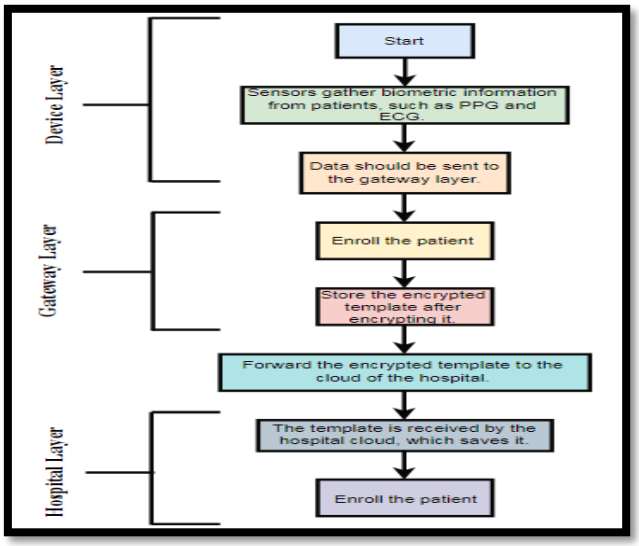


Figure 2: The process of enrolling

- Device Layer: The sensors pass the biometric data on to the gateway layer after gathering it from the patients at various times and in various positions, such sitting or resting.
- Gateway Layer: The patient is enlisted and the template is saved by the gateway layer. The homomorphic algorithm is used to get the biometric template. The hospital cloud gets the encoded template after that.

- Hospital Layer: To approve the patient later on, this layer keeps the authentication information that it obtained from the Gateway layer. Additionally, this layer is in charge of handling and analyzing the patient's data.

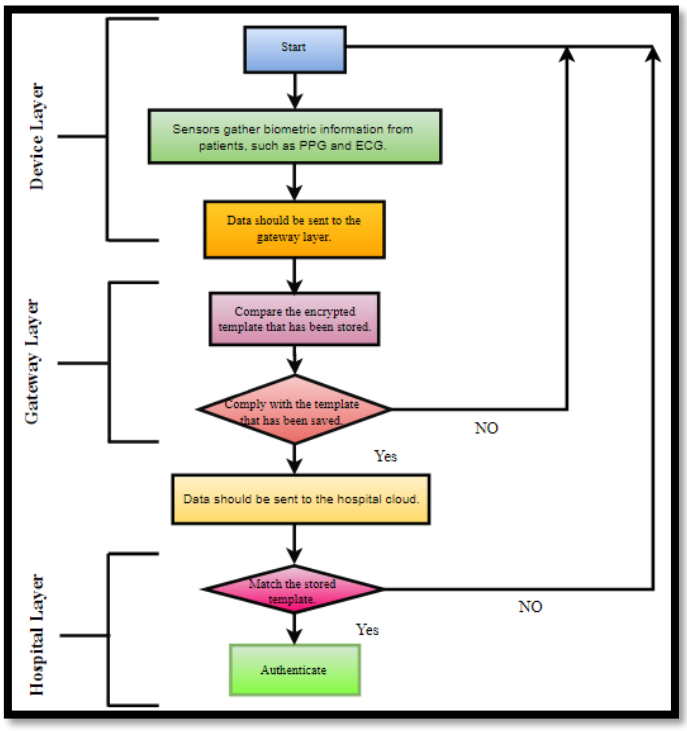


Figure 3: The authentication stages

The means engaged with the authentication cycle can be summarized as follows:

- The patient transmits new information and their biometric characteristics to the passage layer through the apparatus door.
- The mixed biometric format is attempted by the Door layer against the encoded layout that is saved in the database. The client is then verified expecting the format matches.
- Data is delivered off the emergency clinic cloud through the door layer. Then, at that point, the recently shown up layout got from the door is contrasted with the mixed biometric layout that has been taken care of for the client's validation. The user has total authentication on the off chance that the template matches.

3.2 Encryption for Biometric Template

Homomorphic encryption (HE) is used by the suggested authentication system to protect patient data. To guard against theft and unauthorized use, the patient data and biometric template are encrypted. The HE technique has the advantage of allowing calculation to be done straightforwardly on encoded data without expecting access to the mystery key. The computation's result is also protected in an encoded format. Subsequently, the ciphertext can be used for the computation without the need to decode the plaintext. For example, homomorphic encryption can calculate on CT_i and CT_j without uncovering PT_i and PT_j if the comparing ciphertext for a plaintext PT_i is CT_i, and the relating ciphertext for PT_j is CT_j. The addition or multiplication strategy frames the basis of the computation. The homomorphic encryption for the plaintexts PT_i and PT_j is calculated as follows on the off chance that HEA(x) is a capability to scramble them.

$$CT_i = HEA(PT)_{ii} \quad (1)$$

$$CT_j = HEA(PT)_{jj} \quad (2)$$

$$CT_i \times CT_j = HEA(PT + PT)_{ijij} \quad (3)$$

The enrolment level encryption encrypts the stored biometric template using the procedures listed below, which are based on the aforementioned notions:

- The sensor transmits the gathered biometric template during the enrolment step. A vital pair — public key pki and secret key ski — is used to get the template. The biometric feature ECG/PPG is used as contribution for the KGen(κ) capability, which generates the key

$$KGen(\kappa_{ECG}) = pk_i, sk_i \quad (4)$$

However, another key is generated using the patient data and biometric highlights such as PPG or ECG, or a mix of both, when the patient transmits actual health data following the enrollment period.

$$KGen(\kappa_{BT,Data}) = pk_j, sk_j \quad (5)$$

where BT = biomeric traits, data = health data.

- Encryption technique: After that, the encryption function is used to encrypt the biometric template:

$$C_{BioTemp} = Enc\ (pk_i\ ,\ P_{BioTemp}) \quad (6)$$

This function accepts two arguments, a public key (pk_i) and the plaintext of a biometric template ($P_{BioTemp}$), and returns the encrypted version of the template (ciphertext). The $C_{BioTemp}$

- Decryption technique: The following is the process of decrypting the template using the decryption function:

$$P_{BioTemp} = Dec\ (sk_i\ ,\ C_{BioTemp}) \quad (7)$$

This method accepts a secret key ski as input and returns the corresponding plaintext $P_{BioTemp}$ after encrypting the biometric template ciphertext $C_{BioTemp}$.

- Evaluation function: The evaluation capability Ev(pk,χ,σ) is the ensuing capability. This evaluation capability takes the public key that is generated from the biometric traits and uses it in a circuit with m data sources. The sources of info incorporate the plaintext for the biometric template, $P_{BioTemp}$, and a bunch of ciphertexts, $C_{BioTemp1}$, $C_{BioTemp2...}$, CBioTempm, from which it generates a ciphertext. The result is CBioTemp

Using the HE approaches; the patient data is also scrambled.

3.3 Long Short-Term Memory (LSTM) Model

The Long Short-Term Memory (LSTM) architecture is a form of recurrent neural network (RNN) that was developed to solve the problem of disappearing gradients and to identify long-term dependencies in sequential data. Since their introduction, LSTMs have found widespread application in a variety of natural language processing tasks, including speech recognition, time series analysis, and others [18]. It is possible for LSTM to store and retrieve information over lengthy sequences because its architecture has specialized mechanisms that make this possible.

Four neural networks and other memory blocks called cells make up the LSTM architecture's chain structure.

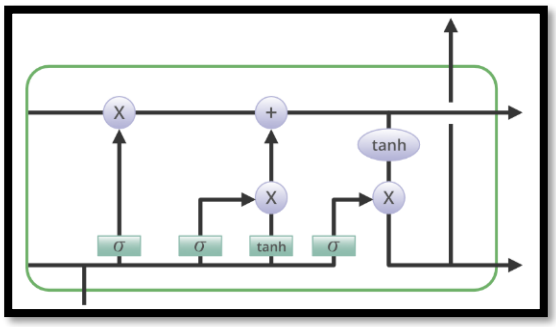


Figure 4: Architecture and Working of LSTM

The gates perform memory modifications, whereas the cells store information. Three gates are present.

- **Forget Gate**

Once the cell state no longer requires certain data, the forget gate removes it. Two inputs, xt (the current input) and ht-1 (the output of the preceding cell), are passed into the gate. Prior to bias being added, they are multiplied by weight matrices. Its binary output is the result of passing it through an activation function. When a cell state's output is 0, all of the associated data is erased; on the other hand, when it's 1, the data is stored for future use. The formula for the forget gate is an:

$$f_t = (W_f[h_{t-1}, x_t] + b_f)$$

Where:

- The weight matrix connected to the forget gate is denoted by W_f.
- The concatenation of the current input and the prior hidden state is indicated by the notation [h_t-1, x_t]
- The bias with the forget gate is denoted by b_f.
- σ is the activation function of the sigmoid.

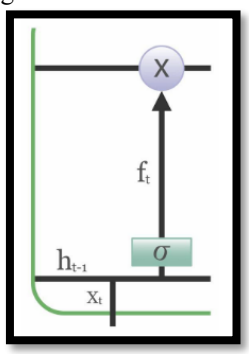


Figure 5: Forget gate architecture

- **Input gate**

The input gate adds relevant data to the cell state, changing it. Inputs ht-1 and xt are utilized to control the data, which is subsequently filtered using the sigmoid function in a forget gate-like fashion. The next step is to generate a vector containing all possible values between ht-1 and xt by using the tanh function, which returns an integer between -1 and +1. Multiplying the vector values by the regulated values is the final step in acquiring the pertinent data. The equation for the input gate is

$$i_t = (W_i[h_{t-1}, x_t] + b_i)$$
$$\hat{C}_t = \tanh(W_c[h_{t-1}, x_t] + b_c)$$

We take the information we had previously decided to ignore and multiply the previous condition by foot. We then incorporate i_t*C_t. This shows the revised candidate values, each of which has been adjusted for the degree to which we decided to update each state value.

$$C_t = f_t C_{t-1} + i_t \hat{C}_t$$

where

- ⊙ indicates multiplication of elements;
- tanh is the activation function.

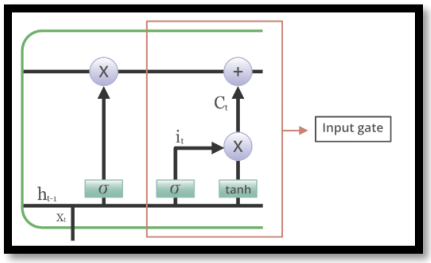


Figure 6: Input gate architecture

- **Output gate**

The output gate's function is to show meaningful data obtained from the cell's current state. First, the cell uses the tanh function to create a vector. After the data has been filtered using the values that need to be remembered using the inputs ht-1 and xt, it is then regulated using the sigmoid function. The last step is to multiply the vector and controlled values so that they can be sent as input and output, respectively, to the cell after it. The output gate's equation is:

$$O_t = (W_o[h_{t-1}, x_t] + b_o)$$

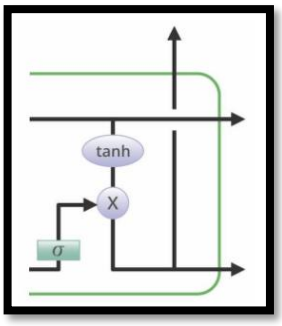


Figure 7: Output gate architecture

3.4 Bidirectional Long Short-Term Memory (BiLSTM) algorithm

Bidirectional long short-term memory (LSTM) recurrent neural networks (Bi LSTM/BLSTM) can process sequential data in both the forward and backward directions[19]. In contrast to conventional LSTMs, Bi LSTMs can learn longer-range dependencies in sequential data, as they can analyze sequential input in both directions.
The suggested architecture uses Bidirectional Long Short-Term Memory (BiLSTM) for biometric authentication because of its capacity to grasp complicated temporal patterns in sequential data. Electrocardiograms (ECGs) and photoplethysmograms (PPGs) are examples of physiological signals that display unique patterns that are used in biometric verification. For user authentication, these patterns include crucial information.

To catch conditions from both past and future settings simultaneously, BiLSTM is chosen for this undertaking because of its capacity to examine input successions in both forward and in reverse directions (Paulraj, 2021). By handling information in the two headings, the model can more likely handle the successive idea of the biometric information, this works on its precision in person recognizable proof.

The melded signals got from the clients' ECG and PPG information are handled by BiLSTM inside the proposed structure. The model figures out how to recognize individual biometric designs by handling this information utilizing BiLSTM layers. The model can recognize genuine clients and frauds involving the examples in the

biometric information, on account of the learned information that frames the premise of authentication. Eventually, BiLSTM is major areas of strength for an authentication device inside the system since it precisely distinguishes clients utilizing their unmistakable biometric highlights and catches the transient elements of physiological signs.

Algorithm 1: BiLSTM

```
ALGORITHM: Define BiLSTM model for biometric authentication
Input: fused ECG and PPG signals
class BiLSTM_Model:
 initialize():
 # Initialize model parameters
input_dim = Dimensionality of input features (e.g., fused ECG and PPG signals)
hidden_dim = Dimensionality of hidden states
num_classes = Number of output classes (e.g., valid user or impostor)
forward_lstm = LSTM(input_dim, hidden_dim)  # Forward LSTM layer
backward_lstm = LSTM(input_dim, hidden_dim)  # Backward LSTM layer
fully_connected_layer = FullyConnectedLayer(2 * hidden_dim, num_classes)  # Fully connected layer for classification

forward_pass(input_sequence):
forward_hidden_states = []  # Forward hidden states
backward_hidden_states = []  # Backward hidden states

 # Forward pass through forward LSTM layer
forward_hidden_state = forward_lstm.initial_state()
       for input_token in input_sequence:
forward_hidden_state = forward_lstm.forward_pass(input_token, forward_hidden_state)
forward_hidden_states.append(forward_hidden_state)

     #Backward pass through backward LSTM layer
backward_hidden_state = backward_lstm.initial_state()
       for input_token in reversed(input_sequence):
backward_hidden_state = backward_lstm.forward_pass(input_token, backward_hidden_state)
backward_hidden_states.prepend(backward_hidden_state)

       # Combine forward and backward hidden states
combined_hidden_states = []
       for i in range(length(input_sequence)):
combined_hidden_state = concatenate(forward_hidden_states[i], backward_hidden_states[i])
combined_hidden_states.append(combined_hidden_state)
 # Forward pass through fully connected layer for classification
output_logits = fully_connected_layer.forward_pass(combined_hidden_states)

       return output_logits
```

3.5 The Experimental Work

Here we detail the analyses that demonstrated the proposed authentication model was right. Information utilized in the biometric authentication investigate came from a dataset that was open to general society. To prepare and test the proposed biometric-based authentication structure, this dataset is utilized. Twenty users' electrocardiograms and photograms (PPGs) from an examination are remembered for the assortment. A model contraption, which looked like a smartwatch, was worn by the members. Alongside other sensors like Galvanic Skin Response (GSR) sensors, the model gadget had an electrocardiogram (ECG) and reasonable open equipment PPG sensors. Twenty workers sat in different situations while we recorded their important bodily functions (ECG and PPG signals[20]). Every member's information was gathered throughout five minutes and remembered for the dataset. Around 26,000 examples of PPG and ECG signal adequacy values were produced by every member. The authentication methodology was tested in two stages to ensure its validity and durability. Using the data obtained from 8 participants, we trained and evaluated the authentication model in the first step. We expanded the dataset size to 20 people in the second phase to test and assess the experiment's scalability. What follows is a detailed description of these experiments.

Table 2: Phases of Experiments and Synopses for Model Training and Validation

Experiment Phase	Description

Phase One	Training and assessment of an LSTM model using a 20-user dataset.
Phase Two	Testing for scalability and validation with a larger dataset with 20 users.

3.5.1 Dataset Pre-Processing

Users were asked to sit while combination signals were calculated and recorded. A fused signal Fs was created from the PPG and ECG data utilizing the accompanying formula:

$$F_s = \sqrt{P_s^2 + E_s^2} \quad (8)$$

At any given second, the PPG amplitude point (Ps) and the ECG amplitude point (Es) are both represented in Equation (8). An unmistakable data record containing the fused signal, PPG, and ECG signals was created and saved in advance of the first and second stages of this trial ("mergedTable1.mat"). You can track down this and the code for processing the data on GitHub. It ought to be referenced that to forestall an imbalance in the valid user samples, the minor class parameters were repeated all through the model's training.

3.5.2 Phase One of the Experiment

We utilized the Long Short-Term Memory (LSTM), a progression design that matches significant brain associations, to do biometric validation. Time series data distinguishing proof and assumption are two typical purposes for this learning technique. We took advantage of the bidirectional LSTM layer to make the LSTM net check the ECG and PPG signal successions both forward and in reverse to ensure that they matched a genuine client. For every member, the example window size for every progression was set at 1400. Every client produced around thirteen example successions. As a result, the 10 users generated a total sample size of more than 172 sequences of fused samples. To increase the model's training bias, a couple of duplicates of the minor class data were also used. The organization model architecture is displayed in Figure 4.

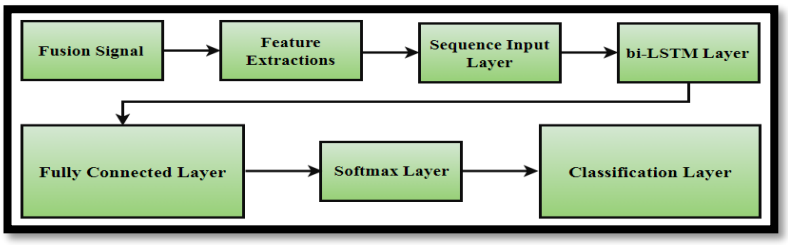
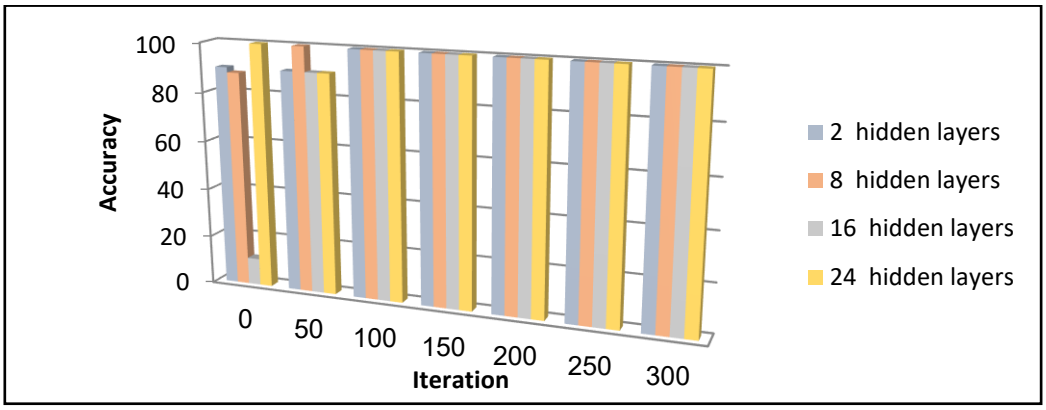


Figure 8: The architecture of the biometric model that incorporates integration of PPG and ECG

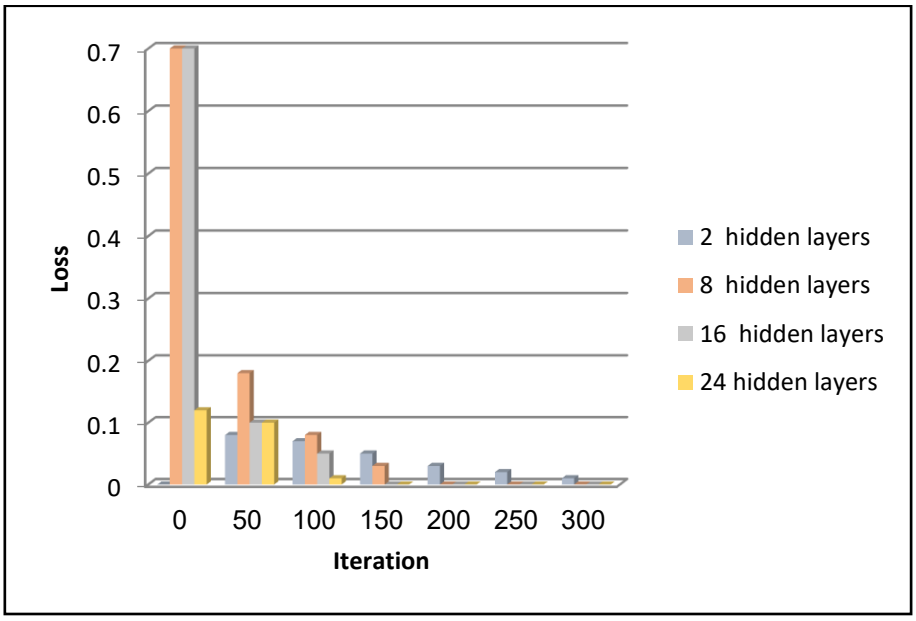
We portrayed the LSTM layer with a variable number of hid away neurons to determine the amount of ideal mystery layers expected for this model. In other words, the calculation cost decreased as the quantity of neurons decreased. The completely associated layer was attached to this layer. There were just two categories of commendable result: users who were valid or invalid. To indicate two classes, we hence incorporated a completely associated layer of two neurons. This was followed by an order layer, a softmax layer that dissipated the likelihood of each class, etc. Furthermore, the softmax layer played out the gig of a brain move. These exchange capacities determined the consequence of the softmax layer in light of its net data.

The Model Training Setup

The classifier had numerous training possibilities. Here are a portion of those that we set: To train the organization and set up the neurons, the maximum age was set to 100. The association was told to consider 32 data focuses at a time by configuring a minibatch size of 32. The preparation cycle was advanced quickly by setting the underlying learning rate to 0.01. The gradient edge was assembled to 1 to hold the gradients back from being excessively gigantic and to balance out the preparation interaction. The Stochastic Gradient Descent with the Momentum (SGDM) enhancer was likewise utilized. Figure 9 shows the training progress utilizing different secret layer charts.



(a) Results from training with 2,8,16, and 24 hidden layers with pinpoint accuracy



(b) Deterioration in training results when using 2, 8, 16, or 24 hidden layers

Figure 9: Making progress with different hidden layers throughout training

3.5.3 Phase Two of the Experiment

We entered the combined sign from the imported record "mergedTable1.mat" into the ML model during the investigation's ensuing stage. The architecture of the ML model during this phase was comparable to that found in Figure 4. Each user had 172 sample sequences with a sample recurrence of 150 Hz. As a result, the 20 users' total sample size of data consisted of more than 4500 fused signal sequences.

Model Training Options

In the second part of the review, the secret layer of the model contained 100 neurons. For the training, a maximum age of 20 and a batch size of 32 were chosen. The gradient limit was set to one and the underlying learn rate was set at 0.01. One person was chosen after numerous tries as a legitimate user to compare their biometric information to that of the other users. Afterwards, the model was trained using 60% of the data, and it was tested using the remaining 30% of the data. Consequently, the model was trained and tested using 180 samples of data from legitimate users and 4500 samples of data from attacker signals.

4. Analysis And Experimental Results

To make the preliminary more straightforward, the pre-handled dataset was isolated into preparing and testing portions in a 70/30 proportion. The melded sign of a genuine client was prepared to be perceived from that of other clients by the model. The test subset of the data was used to evaluate the model following the training phase. After then, the model's ability to identify legitimate users was observed and verified.

4.1 Results: Phase 1

Tables 3 and 4 display the outcomes of the experiment's initial phase. The four probable outcomes are indicated by the acronyms TN, TP, FN, and FP: False positive, false negative, true positive, and true negative[21]. TN

indicates that an attack is determined to be successful based on Tables 1 and 2. TP indicates a successful authentication of the valid user. Tables 3 and 4 show that by utilizing just two mystery layers of LSTM, the preparation and test model could accomplish a most extreme exactness and precision of 100%. Consequently, we see that a more modest LSTM network is accepted to be fitting for reasons for approving biometric authentication. Where,

$$True\ Positive\ Rate\ (TPR) = \frac{TP}{Actual\ Positive} = \frac{TP}{TP + FN}$$

$$False\ Negative\ Rate\ (FNR) = \frac{FN}{Actual\ Positive} = \frac{FN}{TP + FN}$$

$$True\ Negative\ Rate\ (TNR) = \frac{TN}{Actual\ Positive} = \frac{TN}{TN + FP}$$

$$False\ Positive\ Rate\ (FNR) = \frac{FP}{Actual\ Positive} = \frac{FP}{TN + FP}$$

Table 3: Experiment phase 1: A comparison of model training using 100 iterations

Size of LSTM	TN	FN	FP	TP	Sensitivity	Specificity	Precision	Accuracy	F Score
2 Layers	109	0	0	74	100%	100%	100%	100%	100%
8 Layers	110	0	0	73	100%	100%	100%	100%	100%
16 Layers	110	0	0	73	100%	100%	100%	100%	100%
24 Layers	109	0	0	74	100%	100%	100%	100%	100%

We also sampled data with a grouping size of 14 s in phase 1 of the trial, which equated to 1400 amplitude points. The outcomes showed that the model could authenticate a user with 14 seconds of fused PPG and ECG readings.

Table 4: Examining the findings of various tests

Size of BiLSTM	TN	FN	FP	TP	Sensitivity	Specificity	Precision	Accuracy	F Score
2 Layers	48	0	0	32	100%	100%	100%	100%	100%
8 Layers	47	0	0	33	100%	100%	100%	100%	100%
16 Layers	47	0	0	33	100%	100%	100%	100%	100%
24 Layers	48	0	0	34	100%	100%	100%	100%	100%

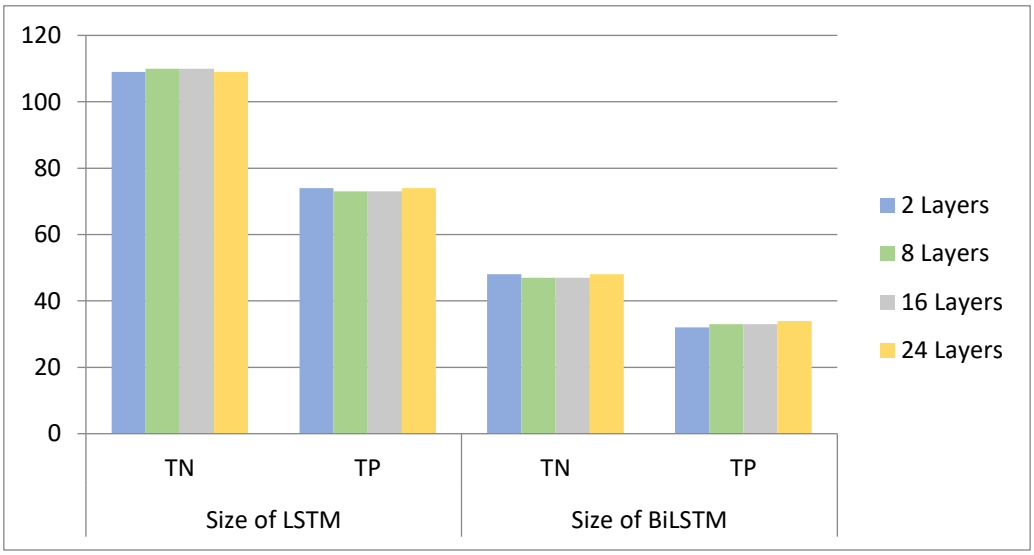


Figure 10: Visual depiction of TN vs. TP comparison for LSTM and BiLSTM models with varying layer sizes

Tables 3 and 4 demonstrate that with just two hidden layers, the suggested biometric authentication scheme might get 100% accuracy. At 100 epochs, the model reached its ideal state. The exactness and equal error rate (EER) of the model's presentation have been contrasted with those of other equivalent works. As a result, our model—which combined PPG and ECG signals to authenticate clients—performed better than the model that was presented using three physiological signs—namely, the GSR, PPG, and ECG—in conditions that were indistinguishable, such as sitting positions and similar data sources. Table 5 presents the disclosures. The model's exactness in checking the personalities of the ten subjects was 100% while relying essentially upon the PPG signal. The results of the examination showed that the recommended model likewise achieved a 100% precision rate. Notwithstanding, our model was accepted to be more secure and less vulnerable to parodying assaults since it

depended upon a combined ECG and PPG signal. Contrasted with simply faking the ECG or PPG signal, it is more trying for an aggressor to make the two signs, intertwine them, and calibrate them.

Table 5: Comparison of biometric models

Biometric Trait	Accuracy	EER	Subjects
PPG, ECG	100%	0.00%	27
PPG	100%	0.00%	12
ECG, PPG, GSR S1a	0%	0.07%	27
ECG	0%	0.13%	80
ECG	0%	0.03%	32

4.2 Results of Phase 2 of the Experiment

The preliminary's ensuing stage saw an expansion in the dataset test size from 10 to 25 people. This allowed us the opportunity to test the proposed model further and approve its usefulness. Figures 7 and 8 showcase the outcomes as a chaos lattice. The presentation of the testing and preparing settings both arrived at 100% exactness, as shown in Figures 7 and 8. For sure, even in the wake of cutting down the train/test proportion to 20/80, we found that a diminished example size was at this point satisfactory to prepare the model to recognize genuine clients, in spite of the examination's 70 to 30 train to test proportion.

Table 6: Experiment two for training precision

		Target Class	
		Attacker	valid user
Output class	Attacker	3394 98.0%	0 0.0%
	valid user	0 0.0%	135 6.0%

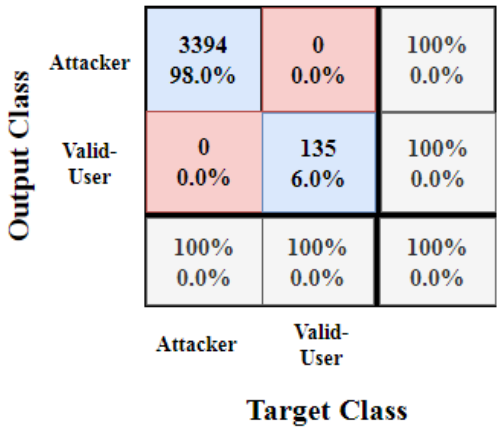


Figure 11: Experiment two Confusion Matrix for training precision

In Experiment 2, the goal classes are classified as "Attacker" and "Valid User," and the output classes are the model's predictions. The findings are shown in Table 6. Based on 3,469 cases that were categorised as "Attacker," the model successfully predicted 3,394 instances, yielding a 98.0% accuracy rate, according to the table. This shows that throughout the training phase, the model was able to accurately identify and classify cases that belonged to the attacker class. On the other hand, the model accurately predicted 135 out of 2,235 instances for cases classified as "Valid User," yielding a 6.0% precision rate. Even though the validity user class's precision is much lower than the attacker class's, this suggests that the model was still able to detect legitimate user instances with some accuracy even when there was more data present. In general, the table demonstrates the way that well the model can separate between cases of aggressors and real users; all through the preparation stage, an especially high accuracy rate was noted for the aggressor class.

Table 7: Experiment two for testing precision

		Target Class	
		Attacker	valid user
Output class	Attacker	1570 98.0%	0 0.0%
	valid user	0 0.0%	59 6.0%

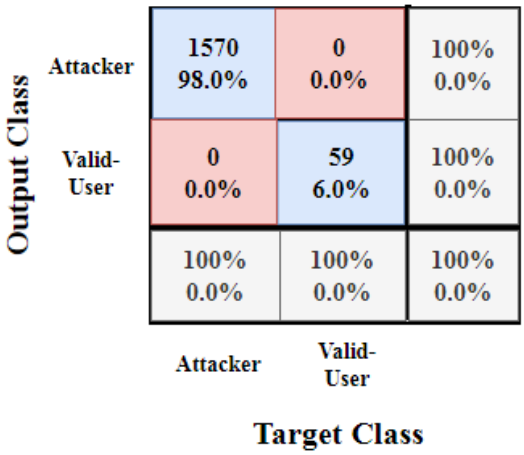


Figure 12: Experiment two Confusion matrix for testing precision

The results of Trial 2, what split the objective classes into "Aggressor" and "Substantial Client," are displayed in Table 7. The result classes compare to the model's forecasts. As per the table, the model accomplished an accuracy pace of 98.0% by precisely foreseeing each of the 1,570 cases that were classed as "Assailant." This proposes that all through the testing stage, the model was profoundly exact in perceiving occurrences that had a place with the assailant class. On the other hand, for the cases classified as "Valid User," the precision rate was 6.0% as the model only predicted 59 out of 985 cases accurately. Even while the valid user class's precision is noticeably less than the attacker class's, this still indicates that the model was able to identify valid user instances during testing even though there was more data available.

Overall, the table highlights the model's ability to discriminate between legitimate and attacker user instances; throughout the testing phase, a particularly high precision rate was noted for the attacker class. It is obvious from the uncovered consequences of the two phases of the assessment completed in this work that clients can be authenticated in light of their biometric credits using a melded sign of ECG and PPG without forfeiting the precision of the model. Results from comparing the suggested combined-based biometric model to those from using either ECG or PPG signals revealed a significant improvement in the safety and protection of the whole personalized healthcare system.

5 Discussion

In light of the discoveries of this review, a novel methodology has been proposed with the goal of helping personalized healthcare systems by consolidating Internet of Things (IoT) innovation and cloud computing. The Internet of Things (IoT) Personal Care Identity Management System (IDMS) Structure that has been created utilizes Internet of Things (IoT) sensors, wearables, and smart gadgets to gather patient information. This information is then shipped off the cloud data set for capacity and examination[22]. Through this connection point, different intelligent applications, including local area based commitment administrations, crisis ready systems, and smart medicine management, are made conceivable. Furthermore, this joining makes it more straightforward for clinical professionals to remotely get to their patients.

The Gadget Layer, the Passage Layer, and the Center/Public Healthcare Cloud Layer are the three levels that make up the structure. The Gadget Layer is liable for the gathering of biometric information from patients using sensors. This information is then shipped off the Passage Layer for authentication and encryption through the usage of homomorphic encryption (HE) procedures. Following the authentication cycle, the information is then saved and handled in the Center/Public Healthcare Cloud Layer. This layer is liable for the support of authentication data as well as the investigation of patient information.

Both enlistment and authentication are expected for the structure's authentication cycle to be finished effectively. While the enlistment stage includes the assortment and encryption of biometric information using HE techniques, the authentication stage includes the examination of the encoded information with recently put away layouts with the end goal of approval. Inside the setting of the healthcare system, this technique ensures the authenticating of patients in a protected and exact way.

The use of homomorphic encryption ensures the wellbeing of patient data by empowering calculations to be completed straightforwardly on scrambled information without the need of unscrambling[23][24]. The tasks of encryption and decoding are completed with the help of public and confidential keys that are created from the biometric characteristics and health information of the patients. This guarantees that the information is kept secret and that it isn't compromised in any capacity.

The exploration additionally concentrates on the organization of Long Short-Term Memory (LSTM) models for biometric authentication, explicitly centered around the mix of electrocardiogram (ECG) and photoplethysmogram (PPG) signals. LSTM networks are suitable for the examination of physiological signs as a result of their ability to perceive long-term conditions in consecutive information[25]. This capacity is the justification behind their determination. To work on the precision of the model in distinguishing users in light of their biometric characteristics, bidirectional LSTM (BiLSTM) calculations are used to handle input successions in both forward and in reverse directions.

The progress of the recommended system is exhibited by the aftereffects of the analyses, which show that elevated degrees of precision were achieved in both the preparation and testing stages. When it comes to biometric authentication, the use of LSTM and BiLSTM models gives phenomenal outcomes, with correctnesses surpassing 100 percent in different settings. Furthermore, the adaptability of the model is demonstrated through tests that include higher dataset sizes. This exhibits the model's power and pertinence for applications really happen in reality.

A comprehensive structure for personalized healthcare benefits that are driven by cloud computing and the Internet of Things is introduced by the examination. This system integrates intelligent biometric identity management approaches. The structure that has been proposed offers significant advances in the security, protection, and productivity of personalized healthcare systems. These increases are made conceivable by incorporating modern advancements like the Internet of Things (IoT), cloud computing, and LSTM models. Through the execution of biometric authentication, patients are destined to be distinguished in a way that is both precise and reliable, hence working on the general nature of healthcare administrations.

6 Conclusion

The review offers an essential movement in the field of clinical innovation. The proposed design effectively lessens related security takes a chance by executing smart biometric identity management as well as meeting the expanded requirement for individualized and on-demand healthcare administrations made conceivable by IoT and cloud computing. A system for overseeing biometric characters was proposed in this work model. The Homomorphic Encryption technique and multi-modular IDMS structure the groundwork of the system. It allows patients' identities to be uniquely identified in contexts of individualized healthcare. Biometric data that can be recognised and verified forms the basis of the authentication procedure. It employs a cutting-edge technique that combines ECG and PPG data to provide identification, making it a dependable, quick, and—above all—secure solution. The majority of senior patients typically lack technology experience; thus, the suggested strategy helps to relieve many of the problems experienced in the health area. When a fused-based biometric method is utilized, many of the security gambles — like spoofing attacks — that accompany utilizing a solitary biometric trait — like PPG signals — are decreased. The experimental results presented in this research further validate the framework's ability to successfully distinguish users utilizing their biometric profiles, generally obtained by consolidating their ECG and PPG signals. Twenty clients in sitting positions were utilized to test the exhibition of the proposed biometric authentication strategy, which showed 0% EER and 100% precision. All things considered, this research paves the way for a more connected and individualized approach to healthcare conveyance by working on the effectiveness, security, and accessibility of healthcare services in the digital age. In subsequent research, we'll examine the suggested model using a bigger dataset of users in various roles. It is also intended to do more research to assess the suggested model's end-to-end security performance.

References

[1] Abdulmalek, S.; Nasir, A.; Jabbar, W.A.; Almuhaya MA, M.; Bairagi, A.K.; Khan, M.A.; Kee, S.H. IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. Healthcare 2022, 10, 1993.

[2] Akhbarifar, S.; Javadi HH, S.; Rahmani, A.M.; Hosseinzadeh, M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. Pers. Ubiquitous Comput. 2020, 27, 697–713.

[3] Awotunde, J.B.; Jimoh, R.G.; Folorunso, S.O.; Adeniyi, E.A.; Abiodun, K.M.; Banjo, O.O. Privacy and security concerns in IoT-based healthcare systems. In The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care; Springer International Publishing: Cham, Switzerland, 2021; pp. 105–134.

[4] S. Phani Praveen , Thulasi Bikku, P. Muthukumar, K. Sandeep, Jampani Chandra Sekhar, V. Krishna Pratap. (2024). Enhanced Intrusion Detection Using Stacked FT-Transformer Architecture. Journal of Cybersecurity and Information Management, 13(2), 19-29 (Doi : https://doi.org/10.54216/JCIM.130202).

[5] G. Gardaˇsevi´c, K. Katzis, D. Baji´c, and L. Berbakov, “Emerging wireless sensor networks and internet of ,ingstechnologiesfoundations of smart healthcare,” Sensors, vol. 20, no. 13, p. 3619, 2020.

[6] Hathaliya, J.J.; Tanwar, S.; Evans, R. Securing electronic healthcare records: A mobile-based biometric authentication approach. J. Inf. Secur. Appl. 2020, 53, 102528.

[7] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," Computer Communications, vol. 153, no. 1, pp. 311–335, 2020.
[8] Joseph, T.; Kalaiselvan, S.; Aswathy, S.; Radhakrishnan, R.; Shamna, A. A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. J. Ambient. Intell. Humaniz. Comput. 2020, 1–9.
[9] M. A. D. Shewale and S. V. Sankpal, "IOT based smart and secure health care system Analysis & data comparison," International Journal for Research in Applied Science and Engineering Technology, vol. 8, no. 1, pp. 394–398, 2020.
[10] Saif, S.; Bhattacharjee, P.; Karmakar, K.; Saha, R.; Biswas, S. IoT-Based Secure Health Care: Challenges, Requirements and Case Study. In Internet of Things Based Smart Healthcare: Intelligent and Secure Solutions Applying Machine Learning Techniques; Springer Nature Singapore: Singapore, 2022; pp. 327–350.
[11] Bikku, T., Chandolu, S. B., Praveen, S. P., Tirumalasetti, N. R., Swathi, K., & Sirisha, U. (2024). Enhancing Real-Time Malware Analysis with Quantum Neural Networks. Journal of Intelligent Systems and Internet of Things, 12(1), 57-7.
[12] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and privacy in IoT-cloud-based e-health systems-A comprehensive review," Symmetry, vol. 12, no. 7, pp. 1191–1235, 2020.
[13] X. Wang and S. Cai, "Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud," Future Generation Computer Systems, vol. 112, pp. 320–329, 2020.
[14] A. M. Rahmani, T. N. Gia, B. Negash et al., "Exploiting smart e-Health gateways at the edge of healthcare Internet-of- ,ings: a fog computing approach," Future Generation Computer Systems, vol. 78, pp. 641–658, 2018.
[15] Begum, V.; Vajubunnisa Begum, R.; Dharmarajan, D.K. Smart Healthcare Monitoring System in IoT. Eur. J. Mol. Clin. Med. 2020, 7, 2647–2661.
[16] S. P. Praveen, B. Thati, C. Anuradha, S. Sindhura, M. Altaee, and M. A. Jalil, "A novel approach for enhance fusion based healthcare system in cloud computing," Journal of Intelligent Systems and Internet of Things, vol. 12, no. 1, pp. 88–100, 2023, doi: 10.54216/JISIoT.090106.
[17] Phani Praveen, S., Hasan Ali, M., Musa Jaber, M., Buddhi, D., Prakash, C., Rani, D. R., & Thirugnanam, T. (2023). IOT-enabled healthcare data analysis in virtual hospital systems using Industry 4.0 smart manufacturing. *International Journal of Pattern Recognition and Artificial Intelligence*, *37*(02), 2356002.
[18] Paulraj, G.J.L.; Jebadurai, I.J.; Jebadurai, J.; Samuel, N.E. Cloud-based real-time wearable health monitoring device using IoT. In Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020; Springer: Singapore, 2021; pp. 1081–1087.
[19] Shakil, K.A.; Zareen, F.J.; Alam, M.; Jabin, S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. J. King Saud Univ. Comput. Inf. Sci. 2020, 32, 57–64.
[20] T. B. M. Krishna, S. P. Praveen, S. Ahmed, and P. N. Srinivasu, "Software-driven secure framework for mobile healthcare applications in IoMT," Intelligent Decision Technologies, vol. 17, no. 2, pp. 377–393, May 2023, doi: 10.3233/IDT-220132.
[21] A. Madhuri, T. Umadevi. (2024). Role of Context in Visual Language Models for Object Recognition and Detection in Irregular Scene Images. *Fusion: Practice and Applications*, 15(1), 250-261 (**Doi :** https://doi.org/10.54216/FPA.150120).
[22] Praveen, S. P., Jyothi, V. E., Anuradha, C., VenuGopal, K., Shariff, V., & Sindhura, S. (2022). Chronic kidney disease prediction using ML-based Neuro-Fuzzy model. International Journal of Image and Graphics, 2340013.
[23] Madhuri, A., Jyothi, V. E., Praveen, S. P., Altaee, M., & Abdullah, I. N. (2023). Granulation-Based Data Fusion Approach for a Critical Thinking Worldview Information Processing. *Journal of Intelligent Systems and Internet of Things*, *9*(1), 49-68.
[24] Toomula, S., Paulraj, D., Bose, J., Bikku, T., & Sivabalaselvamani, D. (2022). IoT and wearables for detection of COVID-19 diagnosis using fusion-based feature extraction with multikernel extreme learning machine. In *Wearable Telemedicine Technology for the Healthcare Industry* (pp. 137-152). Academic Press.
[25] Bikku, T., Sree, K. S., Jarugula, J., & Sunkara, M. (2022, March). A novel integrated IoT framework with classification approach for medical data analysis. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 710-715). IEEE.