Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2206530, 14 pages
https://doi.org/10.1155/2022/2206530

Research Article

Energy Efficient and Secure Information Dissemination in Heterogeneous Wireless Sensor Networks Using Machine Learning Techniques

Deepak Dudeja,[1] Sabeena Yasmin Hera,[2] Nitika Vats Doohan,[3] Nilesh Dubey,[4] R. Mahaveerakannan,[5] Tariq Ahamed Ahanger,[6] and Simon Karanja Hinga[7]

[1]*Department of Computer Science and Engineering, Geeta University, Panipat, Haryana, India*
[2]*Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India*
[3]*Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India*
[4]*Department of Computer Science & Engineering, Devang Patel Institute of Advance Technology and Research, Charotar University of Science and Technology, Gujarat, India*
[5]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India*
[6]*College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Saudi Arabia*
[7]*Department of Electrical and Electronic Engineering, Technical University of Mombasa, Mombasa, Kenya*

Correspondence should be addressed to Simon Karanja Hinga; kahinga@tum.ac.ke

Received 5 March 2022; Revised 14 April 2022; Accepted 20 April 2022; Published 7 June 2022

Academic Editor: Mohammad Farukh Hashmi

The extensive use of sensor technology in every sphere of life, along with the continuous digitization of society, makes it realistic to anticipate that the planet will soon be patched with small-sized devices all over the place in the not-too-distant future. These devices give monitoring and surveillance capabilities, as well as access to a vast digital universe of information, among other things. Finding data and information, as well as processing enquiries, is made much easier thanks to the seamless transmission of information over wireless media, which is based on the "anywhere, anytime, everywhere" paradigm that allows information to be sent anywhere, at any time. Sensing networks came into existence as a consequence of the downsizing of wireless devices that are capable of receiving information from a source, transferring it, and processing it. Sensor networks, although they share many of the features, uses, and limits of ad hoc networks, have their own set of capabilities that are unique to them. While performing their responsibilities, sensor networks must contend with a variety of security issues, including unsecured wireless channels, physical compromise, and reprogramming. Because of the small size and ubiquitous availability of wireless sensor networks, compromise attacks are the most severe kind of attack in this environment (WSNs). With the proliferation of wireless sensor networks (WSNs), it is becoming more difficult to rely only on machine learning techniques. We sought to tackle the security challenge by developing a key management system as well as a secure routing mechanism. We are building scalable key management approaches that are resistant to node compromise and node replication attacks, which we will demonstrate in our proposed study, by using deployment-driven localization of security information and leveraging distributed key management. Using a security-aware selection of the next hop on the route to the destination, we were able to design safe routing algorithms that were effective.

1. Introduction

Generally speaking, a wireless sensor network (WSN) is a collection of resources that may be used for a range of inaccessible tasks like monitoring, surveillance, tracking, and recording in a variety of environments. A wireless sensor network (WSN) is comprised of a large number of sensing stations, which are collectively referred to as sensor nodes (SNs) in the network. In addition, SNs are resource-constrained devices that must transmit sensed data from the sensing fields to a remote base station (BS) that is securely located in a different area to function properly. This is done via the use of multihop routes, which incorporate wireless networks and intermediated SNs as part of the routing protocol. It is conceivable that BS can handle it locally, or that BS is connected to distant processing capability in other networked systems, depending on the situation. Sensors may be either fixed or mobile in their function depending on their design. SNs may or may not be equipped with electronics that enable them to be tracked down to a specific spot. The setup of WSNs might result in either homogeneous or heterogeneous WSNs, depending on the state of the network. A very limited number of SNs are given individual global sensor identifiers, and these are only given to a small number of SNs. WSNs are networks that are only dedicated to the transmission of data. A well-defined group of nodes or a certain quality in data must be targeted by any sort of communication in WSNs if it is to be successful. Because of the presence of a limited number of high-end sensors (H-sensors) in WSNs, it is possible to take advantage of heterogeneity in the assignment of complex computation to H-sensors, resulting in an improvement in performance. Heterogeneous wireless sensor networks (HWSNs) are a subset of wireless sensor networks (WSNs) that are distinguished by the heterogeneity of its components (HWSNs).

When it comes to network security, key management is an important weapon in any organization's arsenal. Despite the fact that they share a number of characteristics with ad hoc networks, wireless sensor networks (WSNs) vary from one another in a variety of ways. We suggest key management systems as a viable solution to the ever-changing security challenges that we are experiencing. When the chance presents itself, one should make advantage of postdeployment location information in order to make any type of compromising effort in WSNs that are much more difficult to do. Throughout this chapter, we have discussed two essential management alternatives.

Following deployment, the first technique relies on SNs to generate keys on the fly while utilizing HBT on generating keys that have already been installed in the system, while the second technique relies on SNs to generate keys on the fly while utilizing HBT on generating keys that have already been installed in the system (GKs). By using a location-based key generation approach, the suggested key generation method is able to effectively prevent both node compromise attacks and node replication assaults. The second approach is a pair-wise key management system that is based on a localized matrix and is used to protect sensitive information.

Medical services [1] are a highly information-intensive industry that is strongly reliant on technological advances. In recent years, the ever-increasing pattern of medical care information has unintentionally sparked a tremendous development that has been unavoidable. For example, it is predicted that the amount of information held within the medical services sector alone in the USA would approach the Zettabyte scale in a very short period of time [2]. Furthermore, the development of big data in medical services writing is a symptom of the rising significance of vast scope informational indexes in medical care and biomedicine ([3], as shown by the expansion of big data in medical services writing).

A rising number of individuals are also becoming aware of the potential function that big data may play in logical and clinical study [4], as well as the importance of data in general. It is projected that medical care information would continue to grow in a number of forms, including electronic health records (EHR), patient-reported outcomes, biometric information, clinical imaging, and wearable devices. Clinical benefit suppliers and pharmaceutical ventures, as well as public medical services organizations, analysts, and clinical protection, are some of the most essential providers of medical care information, among other things.

In terms of resources, the H-sensor outperforms the L-sensor by a factor of several hundred. In highly capable wireless communication devices, H-sensors are equipped with robust batteries, large quantities of storage, a powerful radio antenna, and enough processing capabilities. H-sensors are used in a variety of applications. They are also reasonably priced.

CHS is able to connect with other networks without the need of a third-party gateway since it uses single-hop communication and a data forwarder for its cluster members and base station (BS).

Anchor nodes (ANs) are nodes that serve as anchors for other nodes. Nodes called anchor nodes (ANs) are H-sensors that are capable of transmitting data at a number of various power levels. ANs placed in triangular or hexagonal locations enable the implementation of a novel clustering/localization approach, which is advantageous.

Sink/base station (SINK/BS): A sink or a base station is a station where water is disposed of. Every network node in a WSN is capable of communicating with one another through BS. A secure location, which may be in the center of the network or at one of its corners, is used by BS to monitor the functioning of the WSN. The position is determined by the application's requirements and may be either in the center of the network or at one of its corners.

Incorporating massive, real-world clinical informational indexes from the "Electronic Medical Record" (EMR) with omics information and focused biochemical and hormonal examinations makes it possible to discover new indicative and restorative apparatuses ([5], as well as recognize the full complexity of diseases) and to recognize the full complexity of diseases [6]. Over 800 people took part in a magnificent model [7], which included continuous monitoring of blood glucose levels, as well as assessments of the participants' anthropometrics and dietary habits, as well as assessments of the participants' gut microbiota, medications, and a

variety of laboratory tests. Feldman et al. [8] report that there are multiple unintegrated clinical information pools that are constrained by six partners: suppliers, payers, scientists and engineers, buyers, and marketers. According to the principles of the CCA (Creative Commons Attribution 4.0 License), this framework may be used without authorization. The fact that these sources have been giving medical care information for a long period of time has resulted in the capacity for medical services information growing into a sector that is consistently growing in size. A growing number of researchers are looking into the Internet media, including Twitter, as a potential information source that can provide a wide range types and quantities of information of great value to medical services proposed work on a variety of different illnesses [9], including but not limited to cancer. Since these bits of information are informative, Twitter is rapidly becoming a vital source of information on medical services. In any case, it is vital that Twitter information be distributed as quickly as possible (speed). A greater quantity of information is accessible, and the degree of risk grows as a result of data coming from a greater diversity of heterogeneous sources. Vulnerability is concerned about the sort of information that is being collected. The nature of medical care information is a basic part in the field of medical care information. It is critical to undertake compelling information inquiry in order to identify vital insight that will be valuable in dynamic settings from other information. In addition to standard quality indicators such as estimation clamor, choice predisposition, and test size [10], it is important to consider the nature of the evidence to be inferred. This will be dependent on the information sources to be incorporated, such as interpersonal organization [11] or public archives [12]. A huge difficulty exists in the realm of big data when it comes to the availability of data. Unstructured content is abundant in the sphere of medical services, and it includes well-crafted video, magnetic resonance imaging (MRI), and text and audio recordings of patients' talks with their physicians, among other things. Structured information, such as that included in an electronic health record, exists in a similar way. This debate will proceed on the assumption that technology advancements in the medical care industry will have the capability of managing information in a variety of different formats. As a result of the discussion, it was discovered that medical care information had four characteristics: a huge quantity, a high volume of data, incredible speed, and considerable vulnerability (veracity). These features all contributed to the notion of big health-care information. As a consequence of these features, a wide variety of obstacles or roadblocks arise for both the customers of medical services information and the innovators who work in the medical care field, as a result of which the medical care sector suffers. Data analysis, information management, and information mix are the three most pressing issues faced by organizations when dealing with large amounts of big health-care data. It is true that when it comes to medical knowledge, joining is a major roadblock. This is mostly because to the large volume of information accessible and the rapidity with which it is gained. According to Martin and colleagues [4], the coordination of unstructured information is a crucial problem for the big data professional. Although structured EHR information has a broad reach, there are a variety of mixed obstacles [13] to overcome, despite the fact that the information has a clear structure. As a result, intelligent data integration solutions are badly needed in the medical industry to cope with the plethora of medical data that is being generated.

WSNs may be differentiated from ad hoc networks in a number of ways, which are discussed below. As an example, SNs are resource-constrained devices that do not have a unique identifier that is recognized throughout the globe. When SNs fail, a multitude of causes contribute to their demise, including energy constraints, malicious attacks, and changing topology. Comparing SNs to ad hoc networks, SNs are more densely dispersed and include a higher number of nodes. We shall provide a brief summary of the properties of WSNs as follows:

Sensors are small devices that collect information largely from their immediate surroundings and have limited resource capabilities. Because of its small size, the amount of resources that can be supported in terms of transmission range, storage capacity, and processing capabilities is limited to a small number.

Sensors use their batteries to detect, configure, and report data in a dynamic topology, and they do it with the help of their batteries.

Because of a shortage of accessible battery resources, the battery of sensors may fail after they have been deployed. This leads in a change in the network's topology and is a frequent activity in wireless sensor networks.

In WSNs, data must be routed to surrounding nodes because of the limited bandwidth available and the remote position of the BS. Multihop communication is thus employed in the communication of sensor networks as a consequence of this.

It is the goal of this research to develop novel optimum deep learning models for effective data integration and storage in warehouse ideas, which will be discussed in more depth in the next section. As a contribution to the debate, the article makes the following points:

An important result of this research is the creation of a data integration technique based on multimodal hybrid deep learning models for dealing with medically heterogeneous health-care data. This is one of the most significant contributions of this research.

The integration of the analytics engine will allow for enhanced diagnoses for those suffering from various cardiac diseases in the future.

In addition, this technique is being employed as a storage medium in data warehouses, which will be used more often in the future.

The following are the most important management schemes: In the case of HWSNs, we have proposed two key management strategies, the first of which is explained in this section.

Using the underlying deployment and local node connection as a starting point, the first key management approach seeks to optimize efficiency. The method is meant to be used in conjunction with hierarchical architecture in

the HWSN environment. However, despite the fact that the system allows for connection in a probabilistic environment, it needs the involvement of a third party such as CH.

Aside from that, the localization effect makes the approach more resistant to assaults such as node compromise and node duplication. The technique generates randomization via tree-based key generation, which results in a significant reduction in computing cost.

Using a pair-wise key scheme that is based on a localized matrix, the second key management system may be implemented with a small amount of storage. The construction of pair-wise keys is ensured without the requirement for any active participation on the part of the key generation algorithm. Localization was employed to provide resistance to compromise assaults, and a matrix-based architecture was used to provide entire connectivity via the usage of pair-wise keys that were located in the same location.

Among the most scalable and storage efficient programs in its category, scheme is one of the most popular.

In this paper, we present four safe routing algorithms for HWSNs, which you can learn more about here.

The initial routing strategy in the HWSN takes advantage of the key management systems that are already in place. In HWSN, the first technique is appropriate for flat networks, but the second way is not. In the second scheme, we investigate the impact of the local and static relationship between SNs that are colocated on their performance. It is more resilient in terms of overall performance when the foundational key management is augmented by a local geographic link among the subnetwork nodes (SNs).

The second strategy takes into account the least squares approach in decreasing the volatility in the number of keys in linkages in order to minimize the number of keys in linkages. Optimal next hop selection is achieved on partially finished and currently being extended routes because it gives the least amount of volatility in terms of the running average number of keys while simultaneously being the most cost-effective option available. When more than 50% of the routes are taken, the variance (reduced) is better than it is in the case of the hypothetical situation.

The remaining sections of the paper are organized as follows. Section 1 included the relevant works of the data integration methods supplied by more than one author, as well as the data integration methodologies themselves. Section 2 covered the relevant works of the data integration methodologies themselves. Section 3 delves into the suggested data integration structure as well as the underlying ideas that guide it. Section 4 examines and analyzes the experiments, as well as the results, which were all reviewed and investigated in detail. Last but not the least, Section 5 of the text concludes the document.

2. Related Works

It has been a decade since the creation of technology for grid-based power generation was announced. Because there are so many different grid systems, enormous data integration between them has emerged as a major difficulty in recent years due to the multiplicity of grid systems. To address these issues, Lin Yue and colleagues [14] looked at a range of machine learning algorithms that may be used to data extraction, data reduction, and prediction challenges for a medical data platform. The medical diagnostic industry has created enormous volumes of unstructured and heterogeneous data, and this data will continue to rise in the future. It is recommended that this effort, which is motivated by the construction of a future deep learning model, investigates the characteristics of heterogeneous data, mortality rates, and electronic data records in more detail.

With the help of the semantic relations progression, the proposed integration model [15] describes how to create a theoretical perspective of shared knowledge by using the semantic relations progression. If the summary scheme model is used to create the levels of leadership in a wise system, the reformist relationships in CIM can be used to create the coordinating levels of leadership. This is an excellent example of how CIM concepts can be used as interoperable and normal concepts for application execution in a wise system. This results in a conventional reconciliation display, which is based on the essential notions of the system, being produced using the approach that has been proposed. It is true that this framework significantly decreases the projected limit in terms of taking care of the overall development in comparison to the previous one. We proposed and planned a MapReduce information integration and information combination design in this paper; after that, we set up a stable information preparation environment and data recovery interface for clients; and after that, we examined the MapReduce execution forms, administration forms, and the connection handle [16].

Wengang and colleagues developed an extractor-transform-load model, which is a multisource and asymmetric information integration approach for enormous data based on extensive data collection. Consider the data integration layer in the context of big information analytics, as an illustration of what I mean. Concentrate transform load is used in combination with change rules to handle massive volumes of data. Change rules are produced by a common information model and implemented in the entire dispatching and control framework. Upon further examination, it was shown that the coordinating model proposed here is capable of producing all-encompassing information and can adapt to diverse information sources by developing an information model that is compatible with the control framework [17]. A collaborative multisource deep network embedding (CDNE) approach was created by the authors in order to integrate the item structure with textual contents and information about the tags that were used. According to the proposed model, the asymmetric multisource network [14] receives the majority of the attention. Using a distributed learning technique, the authors [18] demonstrated how data gathered from distant detection estimations, like climate radars and satellites, could be coordinated. Because the structure provides for more accurate precipitation estimations in places where no downpour measure information is available [19], it may be used in situations when no downpour measure information is available. The method of predicting rainfall levels is divided into three primary phases:

information retrieval, data analytics, and the evaluation process. The quantity of rainwater that has fallen is classified using a deep neural network, which is trained specifically for this purpose. This framework makes use of a rectified linear unit with a batch normalization model in combination with a batch normalization model [20] in order to get the desired results.

In order to better understand what human mobility would imply in terms of car collision hazards, this information, as well as 1.6 million GPS data from consumers, was collected during the main stage. In order to better grasp the progressive component portrayal of human motion, Quanjun Chen, and colleagues built a complete model of "Stack denoised autoencoder" by mining this information. Furthermore, these features are utilized to provide reliable forecasts of the chance of an automotive accident occurring in a given situation [21].

3. Proposed Integration Framework

As the name implies, key pool generation is the process of creating all possible keys in K with the use of a set of GKs.

When it comes to cardinality, K equals the maximum network size that can be accommodated in the network, and G is the maximum network size that can be accommodated in the network [22].

In the key pool generation operation, the creation of GKs and the manufacture of KCs are the two components that must be completed. Additionally, in addition to creating GKs, BS generates a single network-wide key (), known as the master key [23].

The establishment of GKs is the responsibility of the BS. If the BS formula is applied to a randomly determined huge seed value, the result is an HBT. It is necessary to conduct a left shift operation on the tree node, followed by hashing, in order to get its left child. Right shift followed by hashing are two procedures that are used to determine which child is correct. A number of operations are carried out in order to produce HBT of an appropriate height for the application.

GKs are created from HBT leaves that were harvested at BS and dried off. BS and CHs are able to use the master key to produce an authentication key [24], but this is not recommended.

SNs are in charge of the creation of KCs at this point in the process. By using HBT, it is feasible to build a KC for each and every GK that already exists. The absence of common keys between any two KCs is due to the collision-free high fidelity of the algorithm used. A similar result is achieved by the employment of HBT in the creation of KCs by SNs. The root node of HBT is defined by the generation key values in set S; hence, a generation key in set S may serve as the root node of HBT. We must thus proceed to the basement in order to get the key in the HBT's key chain, which is anchored at the generating key [25], which is located there. In the same way as values and affectation of key sets are related, they too are connected. On the basis of their IDs, we investigate the assignment of GKs (S) to each SN from the pool of GKs (G) in this phase based on the assignment of S to each SN in the previous phase. In order to produce the node ids for a node (for both H-sensor and L-sensor nodes), a pseudo-random function is used to generate the node ids (PRF). Each L-sensor and sensor node is allocated and preloaded with a set S of GKs, which may be altered at any moment throughout the operation of the sensor network. It is necessary to seed a pseudo-random number generator (PRNG) with a large number of periods with the ID of the L-sensor node in order to create numbers for the L-sensor nodes, and this is done in the following way: These numbers in set G correspond to the places of GKs in their respective sets of numbers in the previous sets of numbers. SNs are granted to the GKs who have been assessed as correct or incorrect. The combination of these keys results in the key set S [26].

In addition, the authentication key for each L-sensor is preloaded; this key is generated by applying HF on the node ID to the node ID of the sensor. Each H-sensor node is preloaded with H GKs in the same manner as stated previously, resulting in the following configuration: In addition to the GKs, the master key has been encoded into the H-sensors as well as the GKs. Prior to preallocation, SNs are given the common setup key, which is used to identify them.

Figure 1 depicts the suggested data integration models for dealing with the various diverse health-care records of patients [27], which are shown in more detail below. The proposed approach is comprised of three separate learning models for processing heterogeneous data types such as videos, pictures, and signals, each of which has a different learning model.

3.1. Preliminary Overview of Algorithms. Recently, CNN is not simply a subset of deep learning models; it is also a member of the artificial neural networks (ANN) family, which has found uses in image preparation and video analysis. As shown in Figure 1, there is a standard CNN constructed in this manner. The CNN model has five layers, which are as follows: The information layer is made up of a lattice of standardized examples, and highlight maps are used to link contributions to the previous levels in the hierarchy of information. In pooling layers, the highlights obtained by the convolutional layer are used as contributions to the pooling layers. Almost all of the neurons in a single component map have a common piece of information and associated loads. Figure 2 gives basic classifier structure.

The following are the distinctive characteristics of the CNN model's basic assumptions:

(1) The basic properties of this system are unique in that they include local detecting region, weight sharing [], and down sampling

(2) Weight sharing is implemented, which reduces the preparation limits of the network as well as the number of tests that must be prepared.

(3) The model's structure ability and highlight measurement are both reduced as a result of down sampling operation. The CNN model is divided into three layers: the "input layer," the "hidden layer," and the "yield layer." There are two hidden layers: the convolution layer and the down sampling layer [28].

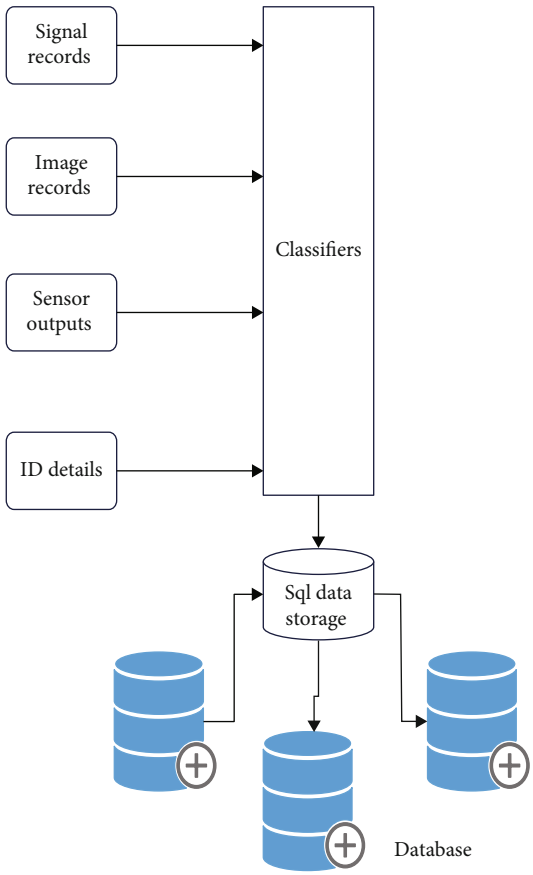

Figure 1: Architecture framework for the proposed hybrid deep learning data integration.

3.2. Boosted Long Short-Term Memory

3.2.1. LSTM: Long Short-Term Memory. The "RNN" and "LSTM" integrated framework is illustrated in Figure 2.

Figure 3 represents the LSTM network structure. Consider the following: given *xt*, the HL ("hidden layer") output is *ht* and its previous output is ht-1, the cell input state is *Ct*, the cell output state is *Gt*, and its former state is $Gt-1$, and the three gates' states are jt, Tf, and $T0$. This cell indicates that both the "*Gt*" and "*ht*" values are passed to the next neural network in RNN, according to the LSTM structure cell. When the preceding unit's output is combined with the current input state, this framework is used to update the memory. The FG and OG are employed to do this.

The following expressions are utilized to calculate the gates.

The IG is expressed as

$$j_t = \theta\left(G_l^i.O_t + G_h^i.e_{t-1} + s_i\right). \tag{1}$$

The FG is expressed as

$$T_f = \theta\left(G_l^f.O_t + G_h^f.e_{t-1} + s_f\right). \tag{2}$$

OG is expressed as

$$T_0 = \theta\left(G_l^0.O_t + G_h^o.e_{t-1} + s_o\right). \tag{3}$$

Cell input is expressed as

$$\widetilde{T_C} = \tanh\left(G_l^C.O_t + G_h^C.e_{t-1} + s_C\right). \tag{4}$$

where G_l^0, G_l^f, G_l^i, and G_l^C are the weight matrices connecting the IG to the output layers, whereas G_h^i, G_h^f, G_h^o, and G_h^C are the weight matrices connecting the gate inputs to the HL. Also s_i, s_f, s_o, and s_C are the bias vectors, and tanh is considered to be "hyperbolic function." Next, the cell output state is calculated, and it is represented as follows:

$$T_C = k_t * \widetilde{T_C} + T_f * T_{t-1}. \tag{5}$$

Also HL output is calculated which is then given as

$$e_t = T_o * \tanh\left(T_C\right). \tag{6}$$

LSTM is composed of a single organization layer that is shaped by a collection of units. A process is registered on one time list, and the yield is transferred to a subsequent LSTM unit by each unit. This results in the corruption of the display of the LSTM organization as the amount of image information increases from the broad measurements that are used to construct the layers of the LSTM organization.

3.3. ELM: Extreme Learning Machines—An Overview. It is advocated by G.B. Huang [21] that an organization employs a single secret layer, rapid and precise planning speed, remarkable theory/precision, and vast capacity guessing capabilities [29, 30]. This is a variation on the ELM concept. According to such a framework, whereas the "L" neurons in the secret layer are required to deal with actuation work that is immensely differentiable (for example, the sigmoid capacity), those in the yield layer are required to work with actuation work that is straight. Hidden layers in ELM should not be tuned on a mandatory basis. In ELM, the hidden layer is not required to be adjusted at all times. The hidden layer's piles are chosen by the secret layer's self-assertiveness (checking the bias loads). It is not the case that hidden hubs are irrelevant; nonetheless, they do not need to be adjusted, and the borders of secret neurons may be provided heedlessly even if they are not known beforehand. It should be noted that this is prior to dealing with the preparation set data. The framework yield for a single hidden layer ELM is given by the Equation (1)

$$f_L(x) = \sum_{i=1}^{L} \beta_i h_i(x) = h(x)\beta, \tag{7}$$

where x is input and β is the output weight vector and is represented as follows:

$$\beta = [\beta_1, \beta_2, \cdots \cdots \cdots \cdots ., \beta_L]^T, \tag{8}$$

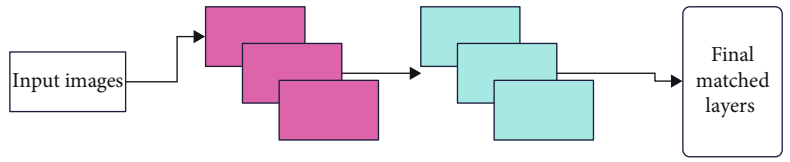

Figure 2: Block diagram for the traditional convolutional neural networks.

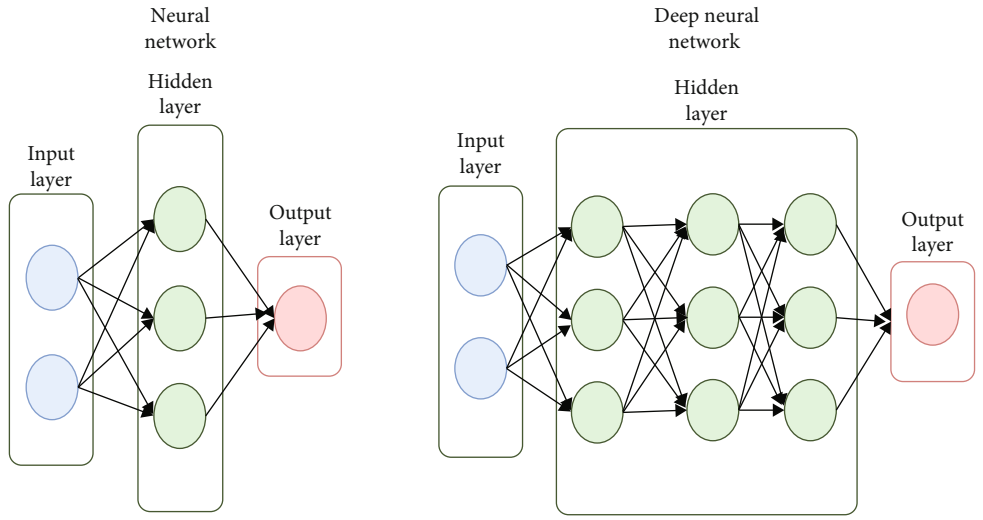

Figure 3: LSTM network.

where $H(x)$ is the output HL which is given by the following:

$$h(x) = [h_1(x), h_2(x), \cdots..h_L(x). \tag{9}$$

To find the output vector "O" known to be the TV (target vector), the HL are represented by Equation (9).

$$H = \begin{bmatrix} h(x_1) \\ h(x_2) \\ \vdots \\ h(x_N) \end{bmatrix}. \tag{10}$$

The ELM basic implementation utilizes the minimal "non-linear least square" methods given as follows:

$$\beta' = H^* O = H^T \left(HH^T\right)^{-1} O, \tag{11}$$

where $H*$ is the inverse of H known as "Moore–Penrose" generalized inverse.

The above equation can also be represented as follows:

$$\beta' = H^T \left(\frac{1}{C} HH^T\right)^{-1} O. \tag{12}$$

Hence, the output function can be found by using the above equation:

$$f_L(x) = h(x)\beta = h(x)H^T \left(\frac{1}{C} HH^T\right)^{-1} O, \tag{13}$$

ELM utilizes the portion capacity to yield great precision for better performance. The significant benefits of the ELM are insignificant in preparing blunder and better guess. Since ELM utilizes the auto-tuning of the weight predispositions and nonzero actuation capacities [31], ELM discovers its applications in arrangement and expectation esteems. The definite depiction of ELM's conditions can be found in [21, 22].

3.4. Proposed Multimodal Learning Models. In the proposed model, two hybrid models were used to train and test the patient's scan images and signal data. In the first tier, convolutional feature extractors are used to extract features, and boosted LSTM is used for predicting the outputs. As discussed in the section, LSTM suffers from the performance degradation as the input dimensions increase; hence, the model incorporates the new integration of the AdaBoost with LSTM to maintain the stability of the network even though the data increases [32].

The important steps which are involved in the boosted LSTM are given as follows

(1) Calculate the output LSTM classifier by using the Equation (12) and with input features obtained from CNN

(2) Set the threshold (using thumb rule)

(3) AdaBoost learning models which are integrated with LSTM check the accuracy with the threshold

(4) If classifiers' output is equivalent to the threshold, AdaBoost takes this as the final output

(5) If it is not equal, AdaBoost adjusts the weights of the LSTM classifier, until required output is obtained

This category of LSTM is employed in the paper to get the high accurate rate of recognition and tracking. As the second step, signal features are extracted by the convolutional learning, and prediction is done by the powerful kernelized extreme learning machines for predicting another classes of diseases. These two prediction results are then converted into single module by using major voting systems. The hyperparameters for constructing the networks are given in Tables 1 and 2.

Table 1: Hyperparameters used for the training the scanned image medical data.

Layers	Output_Layer	Filter-pool layer
Input_Layer	$48 \times 48 \times 1$	2×2
Convolution_1	$48 \times 48 \times 32$	2×2
Max_pooling	$24 \times 24 \times 32$	2×2
Convolution_2	$24 \times 24 \times 64$	2×2
Max_pooling	$12 \times 12 \times 64$	2×2
Convolution_3	$12 \times 12 \times 64$	2×2
Max_pooling	$6 \times 6 \times 128$	2×2
Fully_Connected	06	—
Classifier	Boosted LSTM	—
Activation	ReLU	—

4. Dataset Description

The experimentation is carried out with the two different databases such as fMRI images datasets which are downloaded from the open MRI datasets and ECG signal datasets. The proposed model has been implemented in the Django framework, and NOSQL databases were used for the storing the data and Python-OPENML libraries to implement the learning models over the data [33]. Figure 4 represents the storage framework. Figure 5 represents the application layer framework.

Our key management technique for the HWSN did not rely on using keys from a key pool, but rather on producing keys from scratch. In order to generate the keys, the strategy took use of a nonuniform predistribution of the available keys. It is possible to obtain high connection and a low compromise ratio by utilizing a nonuniform distribution of key generation keys, which is favorable due to the high likelihood of key sharing. It is necessary to employ the H-sensor, also known as CHs, in this instance, to guarantee conversions between a pair of low-end sensors (L-sensors). Using a binary tree called HBT to derive keys from generating keys, which we feel is more efficient [33], we proposed a new approach [29]. Calculating the computational complexity of the generation of any key may be expressed as follows: where and are the lengths of the chains, the impact of node compromise and replication has been significantly decreased to a large amount by using multirange broadcast from ANs to localize generating keys [29].

The approach circumvents the issue of limited storage by using a small number of generating keys in L-sensors to get the desired result. There is also provision for key revocation as well as the rekeying of keys, as well as the installation of more nodes [30] in the system.

An additional security solution known as LOCK is being considered for use with HWSN at this time. A fundamental feature of LOCK is that it takes use of location information to determine the keys that will be used for communication. A hierarchical topology with H-sensors serving as CHs may be achieved by using the LOCK function, as shown in the example below. It is the L-sensor that fulfills the role of a cluster member [34]. It is possible that each SN will get a part of the whole 112 broadcast because of the different transmission ranges of ANs. The subset that is received is determined by the location of the SN. LOCK is a key management approach that is based on the use of a matrix to organize information. Each SN stores just the diagonal of the key matrix as a backup, and no further information. When SNs receive broadcast from ANs, they use this information to determine the diagonal of the matrix. For the purpose of acquiring the whole key matrix, the HBT was enlarged into a dual skewed hash binary tree. The rows and columns of the matrix were taken out when they were needed. Due to the fact that only diagonal elements are kept in each SN, the method's storage needs are very low. Since all connections start or terminate at a compromised node are protected by pair-wise keys, the compromise of a node has an effect on all connections that originate or finish at the compromised node [34]. Given that SNs are only usable inside their cluster, replication and usage of SNs outside of their cluster are made ineffective. There are many different kinds of keys allowed by the scheme, which allows for the use of secure communication patterns.

Table 2: Hyperparameters used for the training the ECG signal records.

Layers	Output_Layer	Filter_Pool_layer
Input layer	$48 \times 48 \times 1$	2×2
Convolution_1	$48 \times 48 \times 32$	2×2
Max_pooling	$24 \times 24 \times 32$	2×2
Convolution_2	$24 \times 24 \times 64$	2×2
Max_pooling	$12 \times 12 \times 64$	2×2
Convolution_3	$12 \times 12 \times 64$	2×2
Max_pooling	$6 \times 6 \times 128$	2×2
Fully_Connected	06	—
Classifier	ELM	—
Activation	ReLU	—

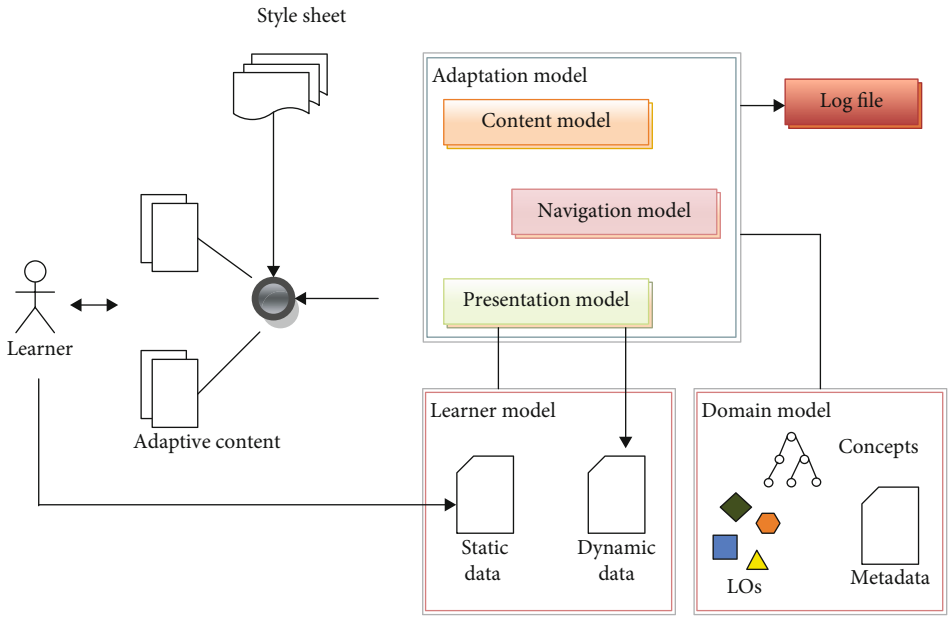

Figure 4: Developed Django framework for handing and storing the heterogeneous medical data.

ANs broadcast new data to the network, which serves to refresh the key. This is handled at the network level.

In the case of the HWSN, a unique variance aware safe routing protocol is now being considered for implementation. Using a nonuniform random key predistribution mechanism as the core key management system, as well as a variation aware next hop selection strategy, the protocol generates safe routes from every SN to every BS. In order to overcome poorer connections, the criteria for hop selection choose the next hop that is equally strong or robust as the partial route that is currently being formed. When using a scheme, it is possible to avoid major differences in the average number of keys on each route by following the rules. As additional hopes were added, we made sure that each link in the chain was as strong as the weakest link in the chain. There were just a few paths that had more hops [35], and one of them was the nonuniform keyed case. Sixty percent (60 percent) of the paths indicate an improvement in the average number of keys on their route as compared to a nonuniform keyed situation, with fifty-fifty percent (50 percent) of routes exhibiting a reduced variance in the average number of keys.

It has been proposed to use secure GPSR with uniform and nonuniform key predistribution to test the hypothesis of the influence of location on the average number of keys on secure routes in GPSR [36] in order to examine the influence of location on the average number of keys on secure routes in GPSR. It is important to note that the security characteristics that are taken into account while selecting the next hop in GPSR are influenced significantly by local cell-based interactions. Using local relationships in a uniform key distribution scenario to compare the average number of keys on the route, it was discovered that the average number of keys on the route rose by one hundred percent when compared to a simple uniform keyed scenario (100 percent). According to the same lines of reasoning, when considering the effect of local relationships in the nonuniform key distribution scenario, performance improvements ranging from 40 to 400 percent were seen. A higher level of resilience is indicated by the existence of extra keys in each connection.

Using secure data collection by mobile nodes, we recommended that the secure LEACH protocol in WSN be extended to incorporate mobile nodes as a component. Extended LEACH removes the requirement for distributed reclustering, which saves time and money.

A unique authentication technique called two-hop online authentication is used to authenticate mobile nodes, and it is used to perform this task (THA). When communicating inside a cluster, group keys are created using the congruent generator (Chinese remainder theorem) and then used to encrypt the communication between the members of the cluster. Between the CH and the members of the cluster, they both have access to the group key. A new group key is generated for each round at the beginning of the round [37]. The strategy was shown to be an energy-efficient and secure modification on the original clustering approach when compared to the original.

Multicast environments are generated by inducing multicast environments with the use of a randomly dispersed key that has been predistributed, which is described in detail in [38].

The approach [39] we described was novel in that it allowed us to pick a subset of one-hop neighbors in the direction of BS for further analysis. The routing approach offers a large number of channels to a destination that are all equally secure and have a high degree of resilience in their own right. Furthermore, both inquiries and replies are supported, and both are sent via separate channels. It is feasible to assess the strength of a protocol by using mathematical techniques [40].

The performance of the multimodel deep learning models is calculated as follows:

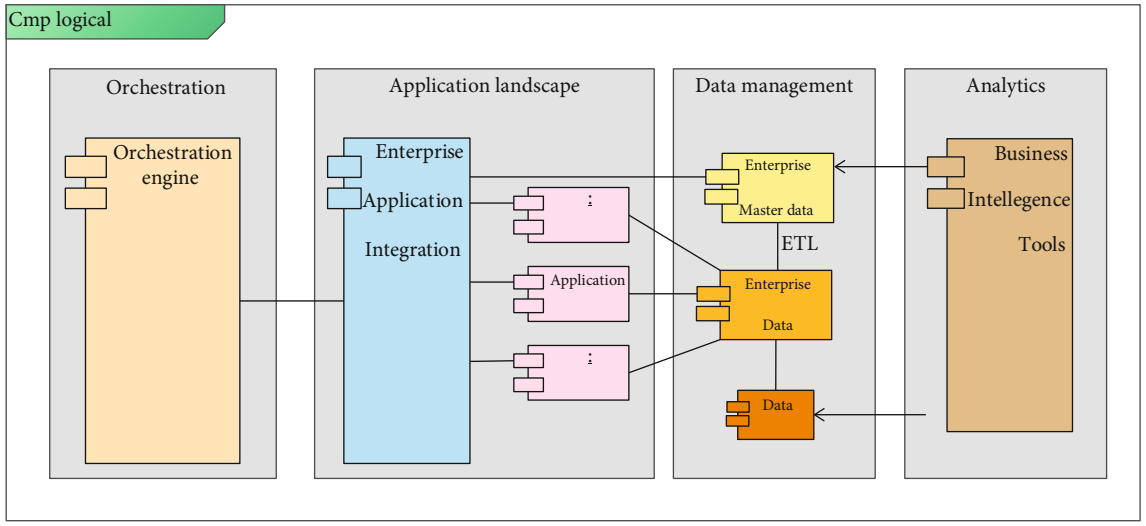

Figure 5: Developed Django framework for applying the hybrid deep learning models over the multiheterogonous data.

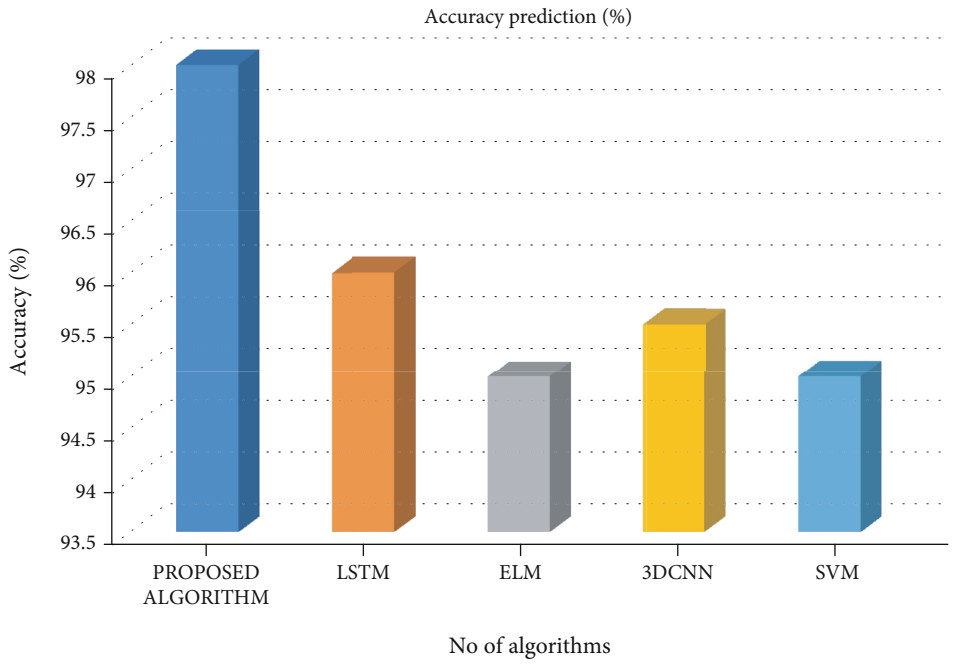

Figure 6: Accuracy Prediction for the different learning models used for the data integration process.

The parameters such as accuracy, specificity, and sensitivity were calculated by using the following expressions.

$$\text{Accuracy} = \frac{D.R}{T}, \tag{14}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{TN}}, \tag{15}$$

$$\text{Recall} = \frac{\text{TN}}{\text{TP} + \text{TN}}, \tag{16}$$

where TN is the true-negative values, TP is the true positive, DR is the number of detected results, and T is the total number of iterations.

The prediction performance has been given as follows.

Figure 6 represents the accuracy rate. Figure 7 represents the sensitivity rate, and Figure 8 represents the specificity rate of the proposed works.

A comparative analysis of numerous algorithms for the prediction of various arrhythmias following the data integration technique is shown in Figures 6, 7, and 8. The algorithms are based on performance metrics, and the results are shown in Figures 6, 7, and 8. Predictive performance of the recommended DL model following the "data integration technique" is shown to be better, as seen in the figures above.

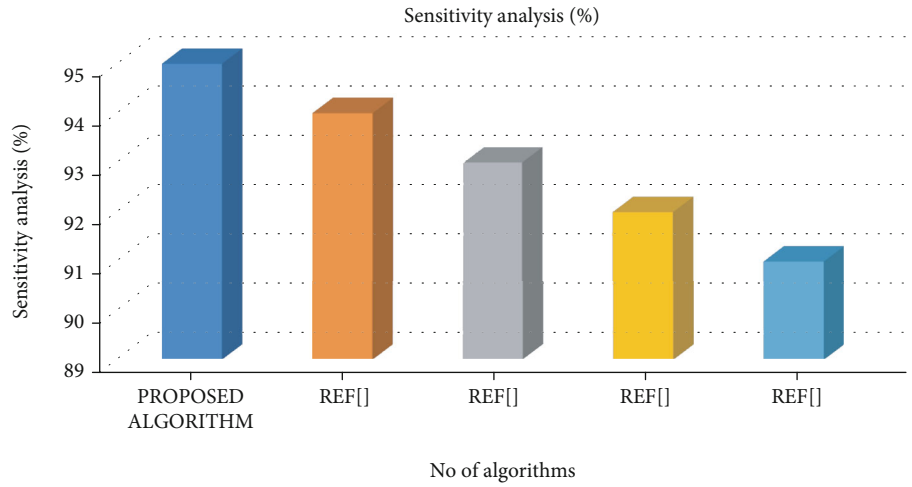

Figure 7: Sensitivity Analysis for the different learning models used for the data integration process.

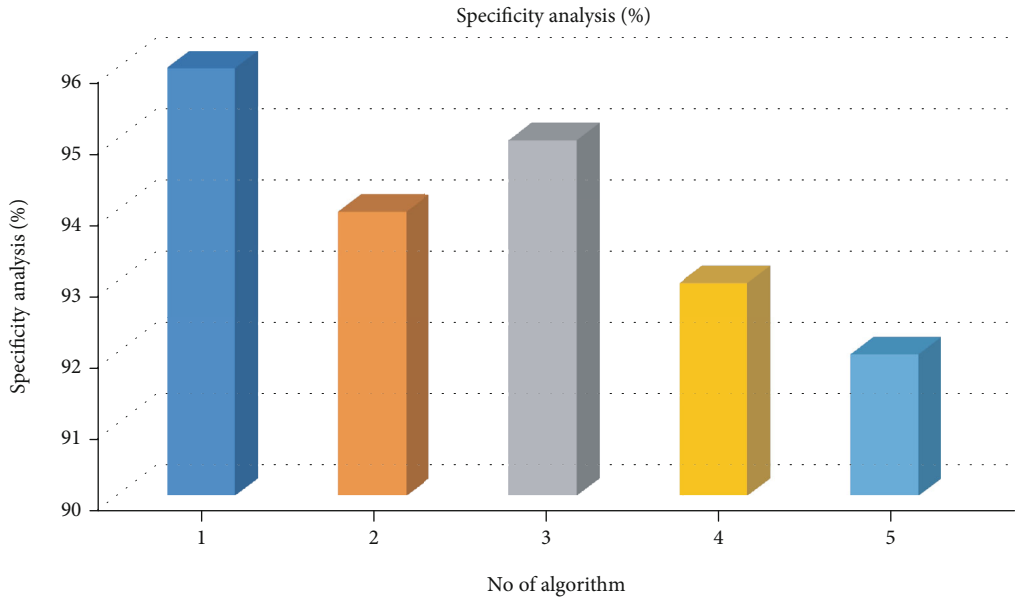

Figure 8: Specificity Analysis for the different learning models used for the data integration process.

This suggests that the data integration models presented here are more suited to the task of developing better prediction mechanisms than the models now in use [41].

Multipath routing in WSNs has been a long-standing priority in terms of security for quite some time. Many proposals for multipath routing have been proposed in ADHOC networks; however, when restricted to the predistributed keying environment, the vast majority of these solutions seem to be illiterate in comparison [42]. For WSNs to operate successfully, route security must be assured since crucial data is transmitted by SNs in the deployment area to their BS, which must be located in a secure location. When dealing with dynamic load and selective attacks, the availability of several safe routes is a blessing, since it increases the attacker's efforts by a factor of many [43]. Then, we design a subset of neighbors that will act as a front for us in the direction of the objective. As part of this procedure, we identified forwarders who might be contacted by base stations and asked for information. With regard to keeping the security credential and offering multiple channels, the front is intended to be as efficient as possible [44]. In this section, we provide our strategy, which consists of network components as well as a network modeling framework, for consideration. It is possible to employ query relays (QR) and data relays (DR) to ease the query and data routing concerns in our notion by implementing them (DR). QR routes the query from BS to a deployment area or a single SN for further processing [45], whereas DR uses data relays to route results back to BS from the deployment region. Using the same or different routes for inquiry and response ensures the least latency [46]. Using the same or different routes also ensures the smallest latency.

In [12], we proposed a list of forward SNs that may be used to choose SNs from one-hop neighbors that are traveling in the same direction in a certain destination. This is indeed the situation. WSN has just one destination, and that is the base station, which is where all communications take place. The HWSN is taken into account, and we have a specified transmission range in mind [47].

A circumstance such as the one shown in the figure serves as an illustration. The energy and security costs associated with each connection seen are shared by both the transmitter and the receiver. When working in an error-prone environment, each connection is subjected to a certain degree of failure.

5. Conclusion

Big health-care data has become feasible as a consequence of the exponential rise in the amount of health-care information being collected. In the health-care sector, a vast amount of data is provided, which may be used to accomplish a range of different goals and objectives. In recent years, the development of machine and deep learning algorithms has elevated the data integration process to a whole new level in terms of applicability, allowing for more precise prediction of different ailments. According to the suggested study, a unique hybrid deep learning model that is based on the concepts of convolutional neural networks, long short-term memory, and high-speed extreme learning machines, among other technologies, is offered. In order to determine which method was superior, different ECG record signals and cardiac picture datasets were used for data integration. Different performance characteristics such as sensitivity, accuracy, and specificity were measured and compared with the current algorithms in order to determine which method was superior. Consequently, when compared to existing methodologies, the new model has shown greater prediction of arrhythmias, and it has also been discovered to be well-suited for data integration while retaining high performance. However, as the datasets expand in size and the security of the data must be maintained throughout the storage and integration procedures, it becomes vital to alter these models to make them more accurate. It is thus necessary to enhance this strategy via the deployment of a more secure algorithm in order to preserve the privacy of the data, as well as the users.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

The authors wish to thank Prince Sattam Bin Abdulaziz University, Saudi Arabia, for its support partially in this proposed work.

References

[1] W. Kushniruk, T. Sahama, D. M. H. Kuo, K. Grunwell, and E. M. Borycki, "Health big data analytics: current perspectives, challenges and potential solutions," *International Journal of Big Data Intelligence*, vol. 1, no. 1/2, pp. 114–126, 2014.

[2] W. Raghupathi and V. Raghupathi, "Big data analytics in healthcare: promise and potential," *Health information science and systems*, vol. 2, no. 1, pp. 1–10, 2014.

[3] G. Khambra and P. Shukla, "Novel machine learning applications on fly ash based concrete: an overview," *Materials Today: Proceedings*, 2021.

[4] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based E-health care framework for green internet of things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, 2021.

[5] A. Sakalle, P. Tomar, H. Bhardwaj, D. Acharya, and A. Bhardwaj, "An analysis of machine learning algorithm for the classification of emotion recognition," in *Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing*, A. Tiwari, K. Ahuja, A. Yadav, J. C. Bansal, K. Deep, and A. K. Nagar, Eds., vol. 1393, Springer, Singapore, 2021.

[6] U. P. Rao, P. K. Shukla, C. Trivedi, S. Gupta, and Z. S. Shibeshi, *Blockchain for Information Security and Privacy*, Auerbach Publications, 1st edition, 2021.

[7] I. de la Torre Díez, H. M. Cosgaya, B. Garcia-Zapirain, and M. López-Coronado, "Big data in health: a literature review from the year 2005," *Journal of medical systems*, vol. 40, no. 9, p. 209, 2016.

[8] K. Verspoor and F. Martin-Sanchez, "Big data in medicine is driving big changes," *Yearbook of Medical Informatics*, vol. 23, no. 1, pp. 14–20, 2014.

[9] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[10] N. Perakakis, A. Yazdani, G. E. Karniadakis, and C. Mantzoros, "Omics, big data and machine learning as tools to propel understanding of biological mechanisms and to discover novel diagnostics and therapeutics," *Metabolism*, vol. 87, pp. A1–A9, 2018.

[11] N. Jain, S. Rathore, and P. K. Shukla, "Designing efficient optimum reduced order IIR filter for smoothening EEG motion artifacts signals," *Design Engineering*, vol. 2021, no. 6, pp. 5080–5101, 2021.

[12] R. K. Gupta, K. K. Almuzaini, R. K. Pateriya, K. Shah, P. K. Shukla, and R. Akwafo, "An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7291250, 14 pages, 2022.

[13] K. J. Karczewski and M. P. Snyder, "Integrative omics for health and disease," *Nature Reviews Genetics*, vol. 19, no. 5, pp. 299–310, 2018.

[14] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for internet of things," *Multimedia Tools and Applications*, 2022.

[15] A. Gupta, R. Ali, P. R. Kumar, A. Pratap Singh, H. Bhardwaj, and A. Bhardwaj, "An analysis on traffic signs identification model," in *2021 3rd International Conference on Advances in*

Computing, Communication Control and Networking (ICAC3N), pp. 527–530, Greater Noida, India, 2021.

[16] D. Zeevi, T. Korem, N. Zmora et al., "Personalized nutrition by prediction of glycemic responses," *Cell*, vol. 163, no. 5, pp. 1079–1094, 2015.

[17] B. Feldman, E. M. Martin, and T. Skotnes, *Big Data in Healthcare Hype and Hope*, 2015, http://ghdonline.org/uploads/big-data-in-healthcare_B_Kaplan_2012.pdf.

[18] D. Jain, P. K. Shukla, and S. Varma, "Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, 2022.

[19] H. Bhardwaj, P. Tomar, A. Sakalle, and A. Bhardwaj, "Classification of extraversion and introversion personality trait using electroencephalogram signals," in *Artificial Intelligence and Sustainable Computing for Smart City. AIS2C2 2021. Communications in Computer and Information Science*, A. Solanki, S. K. Sharma, S. Tarar, P. Tomar, S. Sharma, and A. Nayyar, Eds., vol. 1434, Springer, Cham, 2021.

[20] Twitter Usage Statistics–Internet Live StatsApril, 2019, http://www.internetlivestats.com/twitter-statistics/.

[21] F. Gesualdo, G. Stilo, E. Agricola et al., "Influenza-like illness surveillance on Twitter through automated learning of naïve language," *PLoS One*, vol. 8, no. 12, article e82489, 2013.

[22] A. Khare, R. Gupta, and P. K. Shukla, "Improving the protection of wireless sensor network using a black hole optimization algorithm (BHOA) on best feasible node capture attack," in *IoT and Analytics for Sensor Networks. Lecture Notes in Networks and Systems*, P. Nayak, S. Pal, and S. L. Peng, Eds., vol. 244, Springer, Singapore, 2022.

[23] M. Kanehisa, S. Goto, Y. Sato, M. Furumichi, and M. Tanabe, "KEGG for integration and interpretation of large-scale molecular data sets," *Nucleic Acids Research*, vol. 40, no. D1, pp. D109–D114, 2012.

[24] R. Bellazzi, "Big data and biomedical informatics: a challenging opportunity," *Yearbook of Medical Informatics*, vol. 23, no. 1, pp. 08–13, 2014.

[25] S. B. Goyal, N. Pradeep, P. K. Shukla, M. M. Ghonge, and R. V. Ravi, Eds., *Utilizing Blockchain Technologies in Manufacturing and Logistics Management*, IGI Global, 2022.

[26] R. Chisholm, J. Denny, and D. Fridsma, "Opportunities and challenges related to the use of electronic health records data for proposed work," National Institutes of Health, Bethesda, MD, USA, 2015, June, 2019, https://www.nih.gov/sites/default/files/proposedworktraining/initiatives/pmi/opportunities-challenges-electronic-healthrecords.pdf.

[27] L. Yue, D. Tian, W. Chen, X. Han, and M. Yin, Eds., "Deep learning for heterogeneous medical data analysis," Springer, 2020.

[28] F. In Al-Turjman, A. In Nayyar, A. In Devi, and P. K. In Shukla, "Intelligence of things: AI-IoT based critical-applications and innovations," Springer, 2021.

[29] W. Chen, R. Wang, R. Wu, L. Tang, and J. Fan, "Multi-source and heterogeneous data integration model for big data analytics in power DCS," in *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Chengdu, China, 2016.

[30] L. Gao, H. Yang, J. Wu, C. Zhou, W. Lu, and Y. Hu, "Recommendation with multi-source heterogeneous information," in *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18)*, Stockholm, Sweden, 2018.

[31] F. Sedighi and M. H. Moghadam, "Integration of heterogeneous data sources in smart grid based on summary schema model," in *2016 12th International Conference on Innovations in Information Technology*, Al Ain, United Arab Emirates, 2016.

[32] J.-m. Bao, T.-t. Hu, P. Lin, H. Xu, and H.-f. Hu, "Heterogeneous data integration and fusion system based on metadata conflict algorithms in USPIOT," in *2014 International Conference on Wireless Communication and Sensor Network*, Wuhan, China, 2014.

[33] T. D. Diwan, S. Choubey, H. S. Hota et al., "Feature entropy estimation (FEE) for malicious IoT traffic and detection using machine learning," *Mobile Information Systems*, vol. 2021, Article ID 8091363, 13 pages, 2021.

[34] D. Singh, J. Bhanipati, A. K. Biswal et al., "Approach for collision minimization and enhancement of power allocation in WSNs," *Journal of Sensors*, vol. 2021, Article ID 7059881, 11 pages, 2021.

[35] G. Folino, M. Guarascio, F. Chiaravalloti, and S. Gabriele, "A Deep Learning based architecture for rainfall estimation integrating heterogeneous data sources," in *IJCNN 2019. International Joint Conference on Neural Networks*, Budapest, Hungary, 2019.

[36] Q. Chen, X. Song, H. Yamada, and R. Shibasaki, "Learning deep representation from big and heterogeneous data for traffic accident inference," in *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16)*, Phoenix, Arizona, 2016.

[37] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: theory and applications," *Neurocomputing*, vol. 70, no. 1-3, pp. 489–501, 2006.

[38] B. Wang, S. Huang, J. Qiu, Y. Liu, and G. Wang, "Parallel online sequential extreme learning machine based on MapReduce," *Neurocomputing*, vol. 149, pp. 224–232, 2015.

[39] P. K. Shukla and K. R. Bhatele, "Security in ad-hoc networks (MANETS)," Lakhtaria, IGI Global, 2015.

[40] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. -N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.

[41] A. Purohit, A. Bhardwaj, A. Tiwari, and N. S. Choudhari, "Removing code bloating in crossover operation in genetic programming," in *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 1126–1130, Chennai, India, 2011.

[42] A. Sakalle, P. Tomar, H. Bhardwaj et al., "Genetic programming-based feature selection for emotion classification using EEG signal," *Journal of Healthcare Engineering*, vol. 2022, Article ID 8362091, 6 pages, 2022.

[43] M. Sathya, M. Jeyaselvi, L. Krishnasamy et al., "A novel, efficient, and secure anomaly detection technique using DWU-ODBN for IoT-enabled multimedia communication systems," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 4989410, 12 pages, 2021.

[44] H. Dhayne, R. Haque, R. Kilany, and Y. Taher, "In search of big medical data integration solutions-a comprehensive survey," *IEEE Access*, vol. 7, pp. 91265–91290, 2019.

[45] M. J. Paul and M. Dredze, "You are what you tweet: analyzing Twitter for public health," in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 20, pp. 265–272, Barcelona, Catalonia, Spain, 2011.

[46] N. K. Rathore, N. K. Jain, P. K. Shukla, U. S. Rawat, and R. Dubey, "Image forgery detection using singular value decomposition with some attacks," *National Academy Science Letters*, vol. 44, no. 4, pp. 331–338, 2021.

[47] P. K. Shukla, K. Gupta, S. Silakari, and A. S. Saxena, "An ethical way of encrypt data transfer in Bluetooth mobile using chaos based feedback technique," in *2009 Sixth International Conference on Information Technology: New Generations*, pp. 1583-1584, Las Vegas, NV, USA, 2009.