Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-021-06083-8

RESEARCH ARTICLE - SPECIAL ISSUE - FRONTIERS IN PARALLEL PROGRAMMING MODELS FOR FOG AND EDGE COMPUTING INFRASTRUCTURES

Internet of Things with Artificial Intelligence for Health Care Security

Taher M. Ghazal[1,2]

Received: 20 April 2021 / Accepted: 12 August 2021

Abstract
In recent years, health care facilities are moving towards technological advancements for precise patient monitoring and record management. Though it is technically advanced, the health care information and communication technology network's security is a significant challenge for health care. With the aid of standard algorithms, unstructured data existing outside organized databases (i.e., electronic documents and reports) is difficult to arrange and secure. The existing clustering method has a disadvantage of efficiency issues for recovering data transfer. This paper proposes the Internet of Things with Artificial Intelligence System (IoT-AIS) for health care security. Wireless sensor networks are developed by IoT technology. IoT network is used to bridge the physical and digital world. IoT-AIS is used to monitor the patient's data and encrypt them. The encrypted data are stored in the cloud to maintain the patient data to access remotely. The IoT-AIS dashboard provides an individualized user interface for individual patients to maintain their records individually with single-user access. The proposed paper's simulation analysis proved that the Patient Record of health care could be encrypted and provide individualized access. The experimental results of IoT-AIS achieve the highest data transmission rate to 98.14% and the highest delivery rate of (98.90%), high period of standard responses (93.79%), less delay estimation (10.76%), improved throughput (98.23%), effective bandwidth monitoring (83.14%) energy usage (8.56%) and highest performance rate (98.4%) when compared to other methods.

Keywords Technology · Wireless · Dashboard · Encrypted · Patient · Database · Artificial Intelligence

1 Overview of IoT with Artificial Intelligence for Health Care Security

The Internet of Things (IoT) is a creative framework that uses portable devices, sensors, and the cloud to communicate with a large group of objects and systems without human interaction [1]. The central point underlying IoT highlights the relationship between the physical environment and nature through the Internet [2]. In addition to meeting everyday life requirements, IoT offers various technologies, such as travel, farming, smart cities, emergency responders, and infrastructure [3]. The health care industry for Artificial intelligence applications is one of the most critical fields [4].

The integration of IoT and medical instruments contributes to promoting health care and clinical status reporting to those requiring regular, in-house surveillance and protection strategies [5]. IoT speeds up early identification and facilitates diagnosis and management, such as exercise services, chronic illnesses, and aged health care [6].

Security in health is the knowledge that one's well-being is stable; if not, then there are means to receive care to get back to a healthy state. A basic level of protection against illnesses and bad habits is the goal. Malnourishment and lack of access to health care, clean water, and other daily essentials make poor rural people more vulnerable to threats to health. For guaranteeing the health of people, health security comprises activities and procedures that transcend national boundaries. It is a developing concept within the areas of management affairs and strategic communications [7]. They argue that all states have a responsibility to preserve the health care and well-being of their citizens. According to its

✉ Taher M. Ghazal
Taher.ghazal@skylineuniversity.ac.ae

[1] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia

[2] School of Information Technology, Skyline University College, University City Sharjah, 1797 Sharjah, UAE

Published online: 23 August 2021

critics, health security has a detrimental effect on civil freedoms and the equitable allocation of expenditures. Health care equipment and facilities must deal with essential patient details, including specific data on health care applications, and alter or interact with the protocols adopted. In particular, such intelligent systems can be integrated into global communication technologies to link individuals anywhere, such that hackers can target the Web service field [8]. To promote the complete Internet acceptance of health care technology, IoT's distinguishing characteristics are efficient [9]. In the IoT platform, safety criteria and limitations, health care hazard templates, and detection systems must be defined and analyzed [10]. Network protection is essential for ensuring access to security and privacy risks following the vast growth of channels and telecommunications over the recent century, combined with advanced accessibility and the output of cyber threats [11]. Of course, these attempts negatively impact the channel's efficiency, where the defects and system interruption causes distress and lag [12].

A fundamental objective of any health care service is the expense of connectivity facilities via smooth and safeties between clients, clinics, and specific health care systems [13]. Chronic diseases, early treatment, actual surveillance, and critical services are supposed to be assisted by the most recent wireless connection in health care [14]. The technological developers, information portals play a significant role in developing health information to provide approved partners with health care systems on-demand [15]. Services of computers are linked, exchanged, and measured substantial data on IoT-based health care organizations.

In the health care sector, IoT applications are vulnerable to numerous cybercrimes [16]. The health sector is more likely to experience security challenges than any other sector and more vulnerable to identity theft [17]. IoT innovations help detect the automated system and follow-up the clinical surveillance that helps provide good health care [18]. IoT leads to cost savings and even decreases the staff's needs in most hospitals, leading to major problems [19]. Security and privacy of users are some of the main problems for such channels. Data protection is of significant significance in the health care system since the data on such applications are often the patients' confidential information. Therefore, IoT is crucial that security risks are mitigated, and large, stable nets built, taking the financial barriers into account. A structured evidence template for the confidentiality of the communication verifies security power. In addition to precise medical treatment and record-keeping, health care providers are progressing towards technical change. While it is technologically sophisticated, the protection of health information and communication technology network is a significant health care challenge. The standard algorithms are difficult to arrange and protect unstructured data from outside organized databases. The main contribution of IoT-AIS is described below.

IoT-AIS presents the Internet of Things for the Protection of Health Care technology in wireless sensor networks. IoT-AIS is used in the physical and digital world used to bridge, track and encrypt patient data. The IoT-AIS dashboard offers a customized user interface to hold records independently with single-user access.

This paper proposes the Internet of Things with Artificial Intelligence System (IoT-AIS) for health care security. Wireless sensor networks are developed by IoT technology. IoT network is used to bridge the physical and digital world. IoT-AIS is used to monitor the patient's data and encrypt them. The encrypted data are stored in the cloud to maintain the patient data to access remotely. The IoT-AIS dashboard provides an individualized user interface for individual patients to maintain their records individually with single-user access. The proposed paper's simulation analysis proved that the Patient Record of health care could be encrypted and provide individualized access.

The main contributions of the research section are:

- The research develops a system of Internet of Things with Artificial Intelligence System (IoT-AIS) for the health care unit.
- IoT network is used to monitor physical and numerical statistics.
- The encrypted data are deposited in the cloud system to access patient details distantly.

The remaining article is organized as follows: Sect. 2 comprises various background studies concerning the IoT for health care security. Section 3 elaborates the proposed IoT-AIS model to monitor the patient's data and encrypt the information available. Section 4 constitutes the results that validate the performance and predictability with the corresponding descriptions. Finally, the conclusion with future perspectives is discussed in Sect. 5.

2 Background Study on IoT for Health Care Security

This section discusses several works that various researchers have carried out; ÁineMacDermott et al. [20] developed Securing Things in the Health Care Internet of Things (ST-HIoT). Based on data from IoT issues, real-time tracking offers a broader summary of patient treatment, individual behaviors, and routines. The advantages of implementing ST-HIoT into health care are apparent; networks and device's fundamental security weaknesses cannot go unnoticed. ST-HIoT is set to have a significant effect on society, and with

hackers manipulating IoT by various means, the IoT is unavoidable as the most susceptible region for cybersecurity.

Lanjing Wang et al. [21] proposed Identified Security Attributes (ISA) framework. ISA introduces a proposal to test the Internet of Health Things-based devices' safety features in the health care environment through a Defined Protection Attribute system. The suggested system employs hybrid approaches, including the Analytical Hierarchical Process (AHP). ISA is a two-step framework: the parameters' measurements are extracted by the AHP method during the first stage. In contrast, the second phase, safety assessments of alternatives by AHP, are carried out regarding security parameters.

PriyanMalarvizhi Kumar et al. [22] discussed Intelligent face recognition and navigation system (IFR-NS). IFR-NS presents a new computer vision and orientation framework that offers reliable and fast voice signals for visual impairments to communicate directly. Neural learning methods with mapping techniques and testing components can be used for face recognition. Relatives and parents' photographs are saved on the user's mobile phone web page. If an individual comes before the blind, the application offers voice support to the server with the computer program's help. Relatively, using the Region of Curve study, the output of the proposed approach is evaluated.

GeethapriyaThamilarasu et al. [23] introduced An Intrusion Detection System (IDS). IDS introduces a new threat detection method focused on mobile nodes to protect interconnected health equipment infrastructure. The proposed framework is specifically centralized, adaptive, and uses computer vision, regressive techniques to identify interferences at the device level and sensor data abnormalities. IDS models the configuration of a medical group and conducts detailed tests for different Internet sites of medical products, namely wireless communication networks and other interconnected medical equipment. The simulation results indicate that IDS can obtain significant tracking precision with minimal additional resources.

HamedHaddadPajouh et al. [24] proposed an Artificial Intelligence-powered secure architecture for the IoT's edge layer (AI4SAFE-IoT). The proposed secure IoT infrastructure, Artificial Intelligence-powered secure architecture for the edge layer of the Internet of things Architecture, is designed into edge layer AI protection modules. Cyber threat assignment, cyber threat hunting, smart firewall, and Internet threat intelligence are the main modules suggested by the architecture. An attack life cycle stage based upon the cyber kill chain model can be identified, categorized, and further recognized in the proposed modules. The highest peer IoT level safety frameworks ranking for the suggested scheme was 84.7 out of 100.

PriyanMalarvizhi Kumar et al. [25] narrated CoAP (ChangeCipherSpec and Alert Protocol)-based authentication scheme. CoAP is developed for an intelligent portal authorized system to avoid and secure the more important clinical signals from attackers and malicious behavior to solve the authentication problem. To determine the efficiency of the improved DTLS, data transfer and interaction time are often measured.

Based on the survey, IoT-AIS ensures health care safety in IoT technology and develops wireless sensor networks. The IoT-AIS dashboard offers a personalized user experience to keep the records separately with fixed authentication.

3 The Proposed Internet of Things with Artificial Intelligence System (IoT-AIS)

This paper discussed the IoT-based secure patient data transmission and receiving using artificial intelligence. IoT provides a practical framework for safeguarding information security, confidentiality, and reliability on the Internet. The protection, confidentiality, and reliability of medical data are preserved in different health applications. However, IoT offers efficient protocols for managing information, attacking, and accessing health information, reducing the whole Internet health care system's privacy, safety, and reliability. This research incorporates deep learning to minimize malware attacks when handling health information and thus fix these issues. This approach explores medical knowledge in various layers by the AI concept, which reduces the intermediate attacks to the minimum.

Figure 1 demonstrates DNN-based Malware Detection. Initially, the IoT system is examined using a deep neural network that analyzes the user's authentication to remove the unwanted access and attacks in the IoT device. Each request traffic feature is removed from the database's request to analyze the malware activity after the authentication process. The quality value is examined from the extracted features using the characteristic status and related behavior to assess information qualitatively. The critical element is to preserve the protection of the IoT-based DNN method for medical data transactions.

The protocol analyzes incoming traffic requests for medical data, which are checked with the above authentication procedure. Following the authentication mechanism checking, an examination of the process is carried out concerning the IP address request, protocol transmission, file type sending, frame length, frame number, host post number. These traffic features eliminate the canal pulse's response, the signal received, the channel state's details, and the signal received from the query. Databases are trained by the specified AI method in networking to detect malware attacks during IoT health records.

Malware detection details are displayed in IoT health data in Fig. 1. Fig. 1 shows that the IoT-Health Data Detection

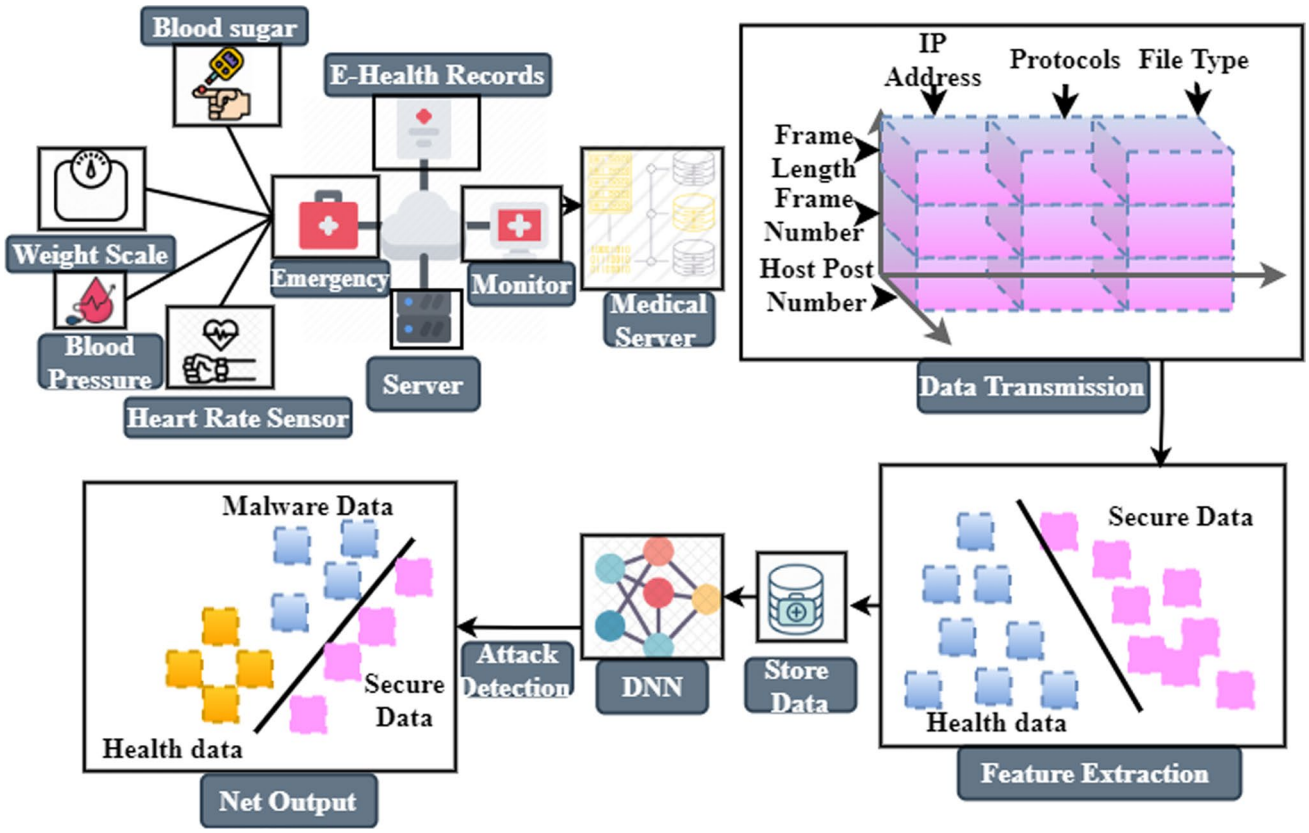

Fig. 1 DNN-based malware detection

Structure DNN-dependent security analysis helps preserve IoT health information effectively classifications affected malware data. The requested traffic data are collected in response to the abovementioned discussions; listing characteristics are obtained using the IoT-AIS-based data analysis from the security, privacy, and reliability analysis requests stored in the database.

Figure 2 illustrates the proposed IoT-AIS model-based data security. Information technology is used to retrieve, store, restore, analyze, and manage information and unify electronic health records to disseminate medical information. Distant surgeries and health care are often made possible with the use of smart e-health care tokens and other innovations. The goal is to improve contact with patients and improve health care services and the overall health care industry. Health care services and information are being digitized. E-health ensures that clients and physicians will accomplish everything digitally, ultimately leading to the lots of paperwork, such as documents and reports, that take up a big portion of medical centers. Health care will reap more rewards due to this, as it is under constant pressure to deliver health care services, continue to use them, and improve them. E-health systems are the key to achieving this. E-health data security refers to data protection measures against unwanted access and data manipulation during its life cycle. Data protection e-health requires data encryption, hacking, tokenization, and key data management activities that secure all apps and platforms. Medical data are commonly maintained in electronic health records where patients' ages, symptoms, procedures, and progress are systemically monitoring. Survey analysis permits researchers in a comparatively limited period to gather analytical evidence. According to the design and scope of surveys, data can be collected from a representative sample of people, primarily if samples are used randomized or intentionally unlikely.

All the real, behavioral, and demographic data obtained from its customers by marketing firms or departments are referred to in customer data or consumer data. Epidemiology is, by concept, the research in particular populations on the distribution and determinants of health conditions and events. The information systems in hospitals provide a shared source of health history information for patients. The device must hold data in a safe location and controls that can, in some instances, access the data. Pharmaceutical data are an essential aspect of the clinical data, providing the correct drug for the right patient, used at the right dosage; for direct patient treatment health data are a whole set of

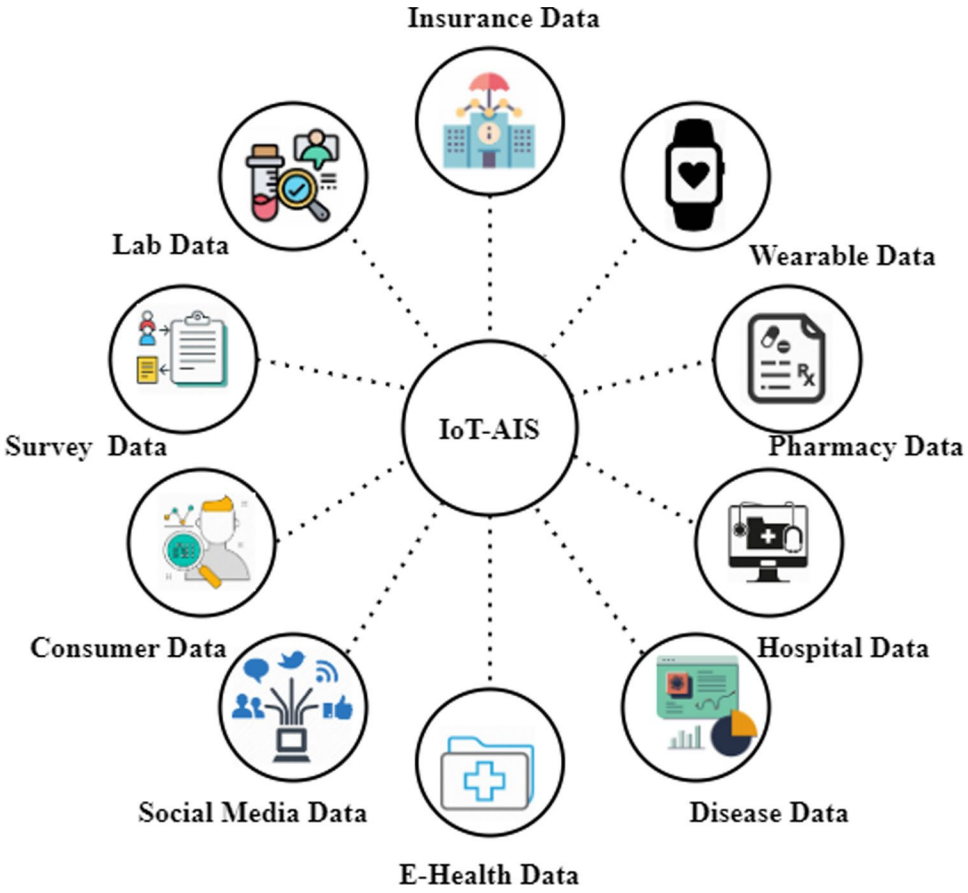

Fig. 2 Proposed IoT-AIS model-based data security

data for an individual or society related to health conditions, reproduction outcomes, causes of death, and quality of life.

Health data provided clinical indicators and knowledge related to health and well-being on the environment, socio-economic, and behavior. Social media provides health care with opportunities to exchange knowledge, address health policy problems and practice, encourage health behavior, communicate with the public, and inform and connect with patients, carers, students, and colleagues. Laboratory data are when a physician takes blood, urine, other bodily fluid, or body tissue sample for patient health information.

Another type of electronic record is claimed records, often referred to as administrative data. Claims databases compile information on millions of visits, bills, insurance records, and other correspondence from patient providers. It is a medical system community that enables IoT-AIS to store, display, update and share its health information. IoT-AIS center provides protected patient e-Health records for treating the disorder, testing and other uses, and safe storage and administration. Implement a centralized framework to store and update patients' health data within the e-health care system and track their data completely. Because patient's health records were stored in the cloud or other parties, there were large privacy concerns since third-party servers or unauthorized users might utilize patients' private health data. To protect patient privacy and improve protection, it is strongly recommended that patient data be encrypted before sourcing.

A single repository needs to collect health information from multiple sources and ensure interoperability with various stakeholders; aggregators can use different standards and protocols. Transit data encryption is the data encryption, network transmission, and cloud decoding process. It may have been a vital method since unauthorized eyes could access the path data, which created problems in data integrity. Transport layer security (TLS) is used to secure the interaction between web applications. TLS reserves an encrypted channel to send the cypher and transmit the key via a public encrypted file to negotiate between senders and recipients.

Figure 3 shows the sequence diagram for data transmission and receive. The article does not mention the use of a group node. Ultrasonic nodes and group nodes authentication failed to implement the IoT-AIS system. Nodes of ultrasonic are shuffled in multiple radiations to authenticate security. Group nodes make defined leveling sequence, yet combining ultrasonic and group cannot authenticate. It can accelerate data individually without the integration of channels. The IoT-AIS will send all the data to the server if sensor nodes directly send it to the Base Station. This

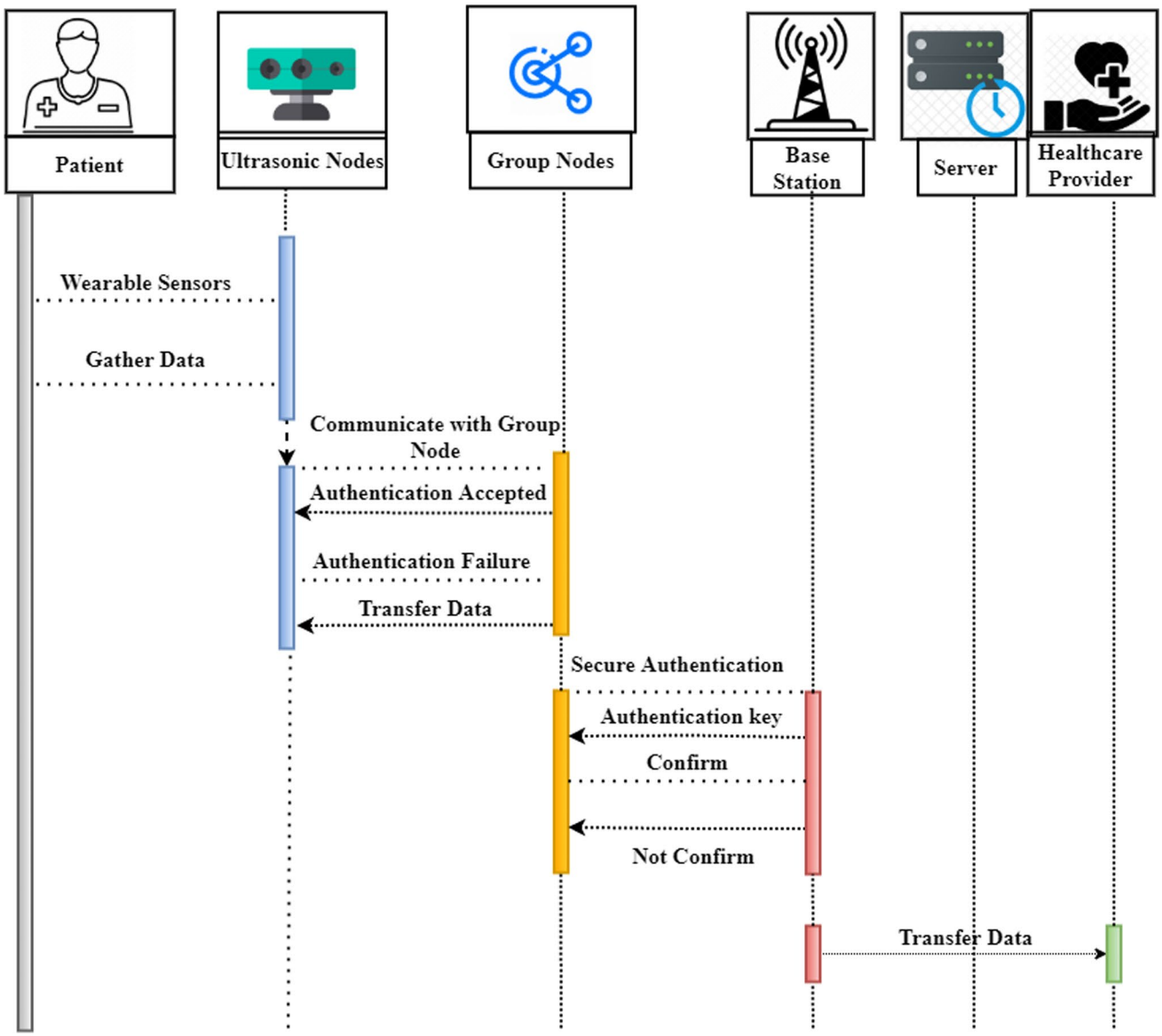

Fig. 3 Sequence diagram for data transmission and receive

produces more channels, because the base station is connected to every node and attacked by it. In addition, due to the distance from the sensor nodes to the base station, more energy is used, and the nodes' lifetime is reduced. The key authentication process extends; eight sensor nodes are used by the proposed one; eight authenticate the key for use by the server. This is addressed in our proposal by group nodes as interface and base stations (ultra-sensor). These sensor nodes send the collected data to the group node and the node to the server. The distance between sensor nodes and community nodes will then decrease. This decreases energy usage and increases the node's lifespan.

On the other hand, this improves protection since long distances do not exist and decrease an attack's chances. Furthermore, it will minimize the key authentication process since it authenticates the group node to obtain the server key. Our idea is to create and share the group node through crucial agreements with other ultra-sensor nodes. The Group node key shares all ultra-sensor nodes the same key agreement, and not each node needs to communicate individually to get the authentication key. They have a node group and eight nodes that scatter across the patient's body to capture general vital signs, including temperature, blood pressure, pulsation, and respiration. Collected information is sent to the group node and the group node to the server by the sensor nodes. Therefore, the group node would have limited mobility and a constant, wearable sense node and patient movement. Suppose the patient does not have the

status of mobility and body coordinates, then eight sensor nodes pass their values through the server to the group node and the base station. Eight sensors have been set in different coordination around the patient's body in patients with wheelchair mobility and are sent into the base station and server group node.

Until transacting from one place to another, the first step in the IoT medical health data transmission involves authentication. Due to the importance of confidential medical data, the established authentication assesses IoT networks and prevents intermedia attacks and unauthorized access. Restricted memory resources, batteries, and computations have been built in the IoT devices used to build Sybil attacks in the network. The physical layer uses different characteristics, such as channel pulses, signal strength indicators, channel status information, signal strength, and data privacy. However, this network functionality provides efficient security since creating IoT devices is resource-based and leads to less protection when transmitting health data. In this paper, deep learning neural networks (DNN) are implemented to maintain authentication, reducing data leakage, because they efficiently learn IoT features. Before using this system, the DNN system is implemented on the IoT device for medical data transactions. The IoT system must initially check its control range under the evaluation. A particular collection of authentication requests from the IoT system must be submitted to the IoT testing area due to the privacy verification of the health data transaction. Different signal features, including channel pulse response standard, battery status indicator, channel recorded data, and transmission power, are disabled when the authentication is needed. Depending on the extracted functionality, the parcel request and environmental radio signals are analyzed via DNN. First, the functionality extracted is trained to achieve the successful outcome of IoT-AIS authentication. It effectively trains the function even if there are few errors or noise in the extracted features. The training phase is carried out by the IoT system feature in Eq. (1):

Figure 4 shows the training feature of the IoT-AIS system that includes the pooling layer, feature extraction, training feature, and high recognition rate. Once the pooling layer parameter connects with the summation process, it adds to the training feature. The extraction feature filters the coordinate data and merges it to the summation value. These data are loaded into a training feature for recognition ideas. Therefore, the system classifies into three different methods as classification 1, classification 2, and classification L state.

$$E(y) = \sum_{i=1}^{i} \sigma_i g_i(y) \tag{1}$$

Figure 4 and Eq. 1 show the Training Feature. σ_i are the characteristics of the layer of pooling, g_i is a better-extracted feature. For authentication, training features are stored in the database. i is the neuron. The corresponding extracted signal functions are processed via a deep learning network, consisting of three layers: input, hidden, and output layer when the new authentication request enters the IoT system. These determined layers use the basic weights and biases in the measurement of the authentication-related result estimated in Eq. (2) as follows:

$$\text{Netoutput} = \sum_{j=1}^{M} Y_j * Z_j + a \tag{2}$$

Figure 5 and Eq. (2) deliberate the neural network output. Y_j is the authentication process input Z_j signifies the specific weights a is the bias value the network is further trained in a deep learning system that uses the weights and bias value defined as updating weights and the authentication performance estimation process in Eq. (3):

$$Y_{L+1} = Y_{L^-}\left[I^T I - \mu J\right]^{-1} I^T f \tag{3}$$

As initialized in Eq. (3) authentication performance estimation process has been evaluated. Y_{L+1} denotes the authentication performance with layer, Y_{L^-} expresses

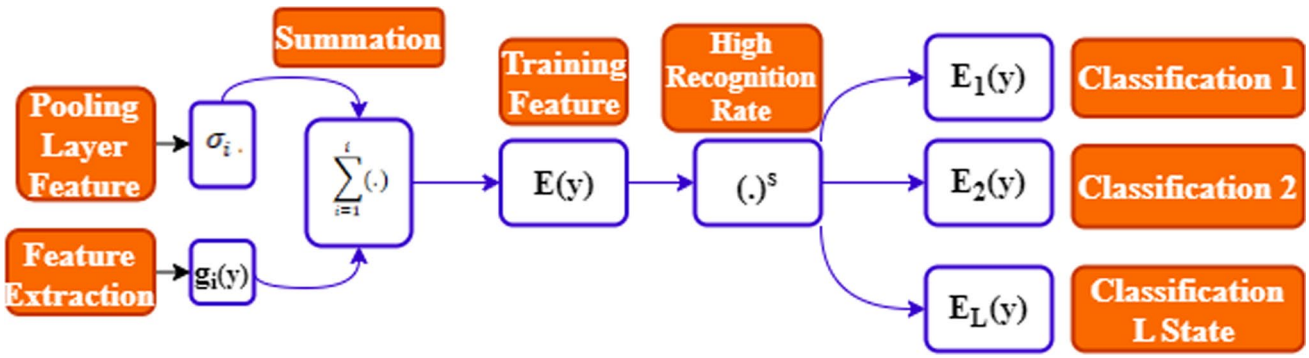

Fig. 4 Training feature

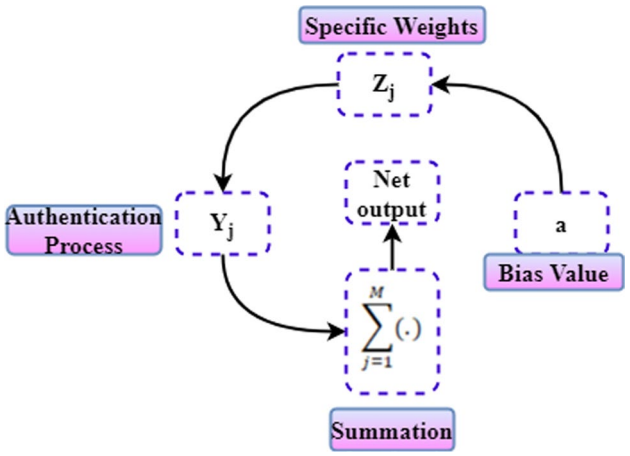

Fig. 5 Neural network output

the previous authentication with layer, I is explored the authentication request, f demonstrated the training function, T is a time, I^T denotes the authentication request with time transition, μ is updating weights, J denotes incoming authentication. Authentication on the authentication request is based on the above method to see if IoT device is authenticated, contrasted with the training feature. This authentication process is performed at a particular time to ensure that the transmission of health data is fast. This method of authentication removes intermediate attacks when IoT is used to transmit health information. An IoT access control is identified in the health data transaction and approved users effectively reach the IoT system using the authentication procedure. The health data transaction protection is further investigated using the IoT-AIS method based on learning after examining an IoT system authentication. To assess the data security, privacy, and durability of the data, the IoT-AIS approach implements the functionality suggested in the above discussions and the queries in a database. The medical transit information requested is retrieved. IoT-AIS is a powerful training tool that does not require an appropriate model to identify health information that is safe and malware identified. The Network uses Q values or quality functions at the time of this detection process to decide each state's action for the successful choice of particular data.

According to clustering, data or things with similar qualities are grouped into homogeneous subgroups, while variability is maximized within each cluster. Consequently, data or objects of interest are clustered together based on features that make them related, with the ultimate goal of separating them from other groupings. Cluster arrangements that are generally homogenous within each grouping, resulting in high intra-class similarity, are sought, while diversity between groups is maximized, resulting in low inter-class resemblance.

Furthermore, IoT-AIS often includes the set of T states; every state belongs to a particular B action, for which each action gives a special reward. In addition to the state, behavior and networks have special weights to determine the price and value of discounts. The reduction factor calculated is between 1 and 0. Then, every state's quality is calculated accordingly (4):

$$P : T * B \rightarrow Q + \left[I^T I - \mu J\right]^{-1} I^T f \tag{4}$$

As found in Eq. (4), every state's quality has been obtained. The Q value is defined as a fixed value chosen by the procedure before the method P is every state's quality. The new value is defined with the aid of the arbitrary value by action b_j state T_{s+1}, at a time s, that provides the reward value q_s. The value changes the current weighted average value in Eq. (5):

$$P^{\text{new}}\left(T_s, b_s\right) \leftarrow (1-\sigma).P\left(T_s, b_s\right) + \sigma\left(q_s + \beta.max_b P\left(T_{s+1}, b\right)\right) \tag{5}$$

In Eq. (5) current weighted average value has been evaluated. σ is a learning rate, q_s expresses the reward value, β denotes the discount factor, $\beta.max_b P\left(T_{s+1}, b\right)$ explores the optimal upcoming value,$\left(q_s + \beta.max_b P\left(T_{s+1}, b\right)\right)$ described the quality of learned value.

$P\left(T_s, b_s\right)$ is interpreted by each state as an old value; the process is continuously repeated until the quality values of each state and related activities are calculated, and the $T_e, P\left(T_s, b\right)$ is final, not modified, the rewards q and observed state T_e and $P\left(T_s, b\right)$ is considered to be 0. The characteristics state is checked, and data protection is checked effectively using qualitative metrics. In addition, the process of malware sensing is calculated by an extensive neural learning network that effectively classifies safe and malware-detected health data. For revised purpose using the weight and bias value , the classification process is further optimized in Eq. (6):

$$E(y) = \left(E_1(y), E_2(y), \ldots E_L(y)\right)^S \tag{6}$$

As obtained in Eq. (6), classification process optimization has been determined. $E(y)$ is the trained function classification process. $\left(E_1(y), E_2(y), \ldots E_L(y)\right)^S$ denotes the all-state trained function classification process with layer and overall time. The neural network's weight and bias value are modified based on that protocol to its previous value. In addition, the sigmoid function is used to train the extracted features to detect malware and highly recognized IoT health information. In the interests of security, safety, and data reliability, this method is constantly repeated.

The average response time is the time the Edge Server will send to the patients the information processed. The data rate, processing, and communications speed, number, and types of jobs submitted are factors that deteriorate the

answer time. The delivery percentage of packets (DPR) for packets is based on the number of packets sent, and the number of packets received successfully. The ratio of sent packets to the packet received is defined as calculated in Eq. (7):

$$\text{DeliveryPercentageofPackets} = \frac{\sum_{j=1}^{M} T_j}{\sum_{j=1}^{M} Q_j} \times 100 \tag{7}$$

As discussed in Eq. (7), the delivery percentage of packets has been determined, where T_j is the number of packets sent and Q_j is the number of packets received. The delay δ is the total time necessary to receive a packet successfully at the destination. In contrast, the average delay is the number of all delay samples, as measured in Eq. (8).

$$\delta = \tau - \mu \tag{8}$$

As shown in Eq. (8), a delay function has been found, where τ is when a packet is being transmitted, and μ the time packet reached its destination successfully. The packet transmission is traversed in the form of a bucket list to leveled destination. Thus, the packet with less delay confirms to perform more data transfer at a time. $F(\delta)$) is given the average delay in Eq. (9):

$$F(\delta) = \frac{\sum_{j=1}^{M} \delta_j}{M} + M - T_j \tag{9}$$

As described in Eq. (9), the average delay has been calculated. The network output is typically calculated per second in a bit (bps) or per second in packets (PPS). Network output is the sum of the data rates given to all network nodes. As in Eq, it is measured [4].

$$\rho = \frac{\sum_{j=1}^{M} Q_j}{\sum_{j=1}^{M} T_j} - \frac{E_1(y)}{S+1} + M \tag{10}$$

As deliberated in Eq. (10), throughput has been computed. ρ is throughput. Total Control Overhead is expressed. j is the IoT node M number of messages. The total number of controlling messages created by each network node is calculated according to the total number of packets received successfully. The first of these is in Eq. (11) as follows:

$$\upsilon = \frac{\sum_{j=1}^{M} D_j}{\sum_{j=1}^{M} P_j} + \frac{\rho}{\tau - \mu} \tag{11}$$

As initialized in Eq. (11), Total Control Overhead has been derived, where D_j is the number of control messages. The proposed IoT-AIS method provides reliable data transmission and data security which are achieved based on the five metrics, such as high period of standard responses, enhanced delivery percentage of packets, less delay estimation, improved throughput, and effective bandwidth monitoring.

The proposed system of IoT-AIS is created to consequence data transfer with the protection of less traffic formation. Therefore, the development system creates a processed formation of IoT sensor networks. The encryption and decryption of patient data are secured into a summing unit for admin access. Thus, the output access of patient security data to individual access is guaranteed.

4 Results and Discussion

The proposed IoT-AIS method provides reliable data security and receives data transmission securely which is evaluated based on the five metrics (1) Period of Standard Responses, (2) Delivery Percentage of Packets, (3) Delay estimation, (4) throughput, (5) Bandwidth Monitoring.

4.1 Period of Standard Responses

The estimated response duration is when the Edge Processor can transfer the data and transmit it back to clinicians. Data transmission rate and interaction rate, amount of jobs, and working experience presented are all factors which affect the reaction time. The device's database upload/download period for clinicians' data generation calculates the period of standard responses. The remaining period is the time needed for a job, and the duration to upload/download is the period to register. Likewise, the processing period is much less than the Central server for work on the Network devices. The period of standard responses is shown in Fig. 6.

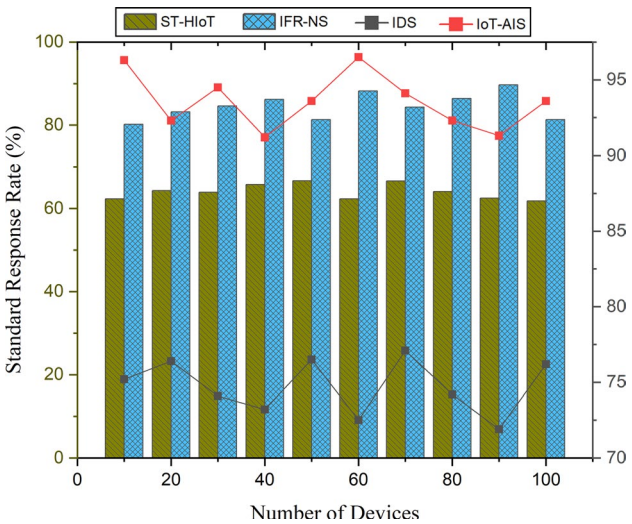

Fig. 6 The period of standard responses

4.2 Delivery Percentage of Packets

The delivery percentage of packets is determined by the number of packages delivered and the number of data packets obtained effectively. The percentage between sent and obtained packets is calculated as the delivery percentage of packets. The first possibilities represent packets' delivery in health care services with a conventional network, while the second or third illustrates the devices' data transfer. When the amount of data transmission people rises, the delivery percentage of packets increases. The delivery rate of packets is shown in Fig. 7.

4.3 Delay Estimation

The delay estimation is the maximum time needed to get the packet to its destination with completion, and the data rate amounts to a maximum of all defects separated by several delays are measured. The machine delay toward the percentage of participants is seen in these statistics. The late delivery, contact, uploading/downloading of patient data is worth notice. The delay is slight, and the IoT devices are high in processing. The processing on devices works together to support network management, load balance, and practical resource usage. The delay estimation is shown in Fig. 8.

4.4 Throughput

The system output is typically calculated in bytes. Network output reflects the number of transfer rates transmitted to all network devices. Edge cooperation, and effective use of Internet services, IoT devices have a higher throughput based on smart load balance decision, Edge cooperation. The Region detection network provides higher efficiency

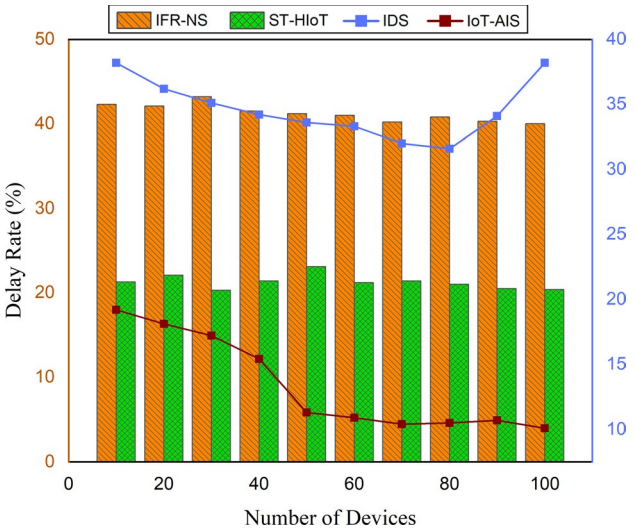

Fig. 8 The delay estimation of IoT-AIS

than conventional networks, although large amounts of data cannot be processed efficiently on standard IoT connected devices. The throughput of IoT-AIS is shown in Fig. 9.

4.5 Bandwidth Monitoring

Bandwidth monitoring represents each device's ratio in the total range of performance communications produced from the packet's output. The conventional system situation reduces overlap control because of few control packets. Simultaneously, the Edge nodes share additional control packets for node coordination and upload/download data, leading to greater overlap management. The bandwidth monitoring of IoT-AIS is shown in Fig. 10.

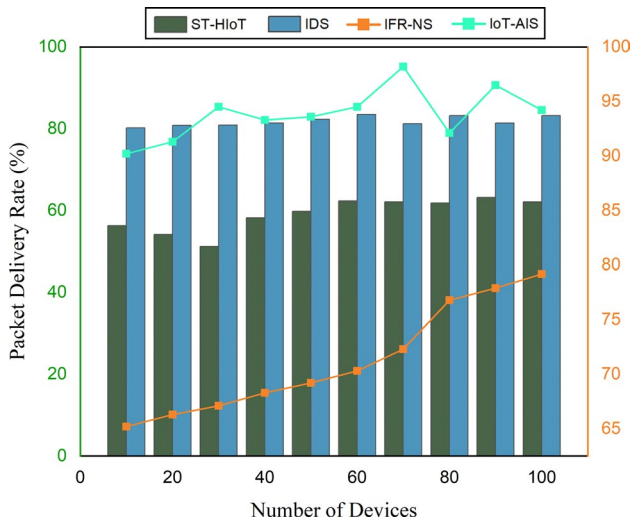

Fig. 7 The delivery rate of packets

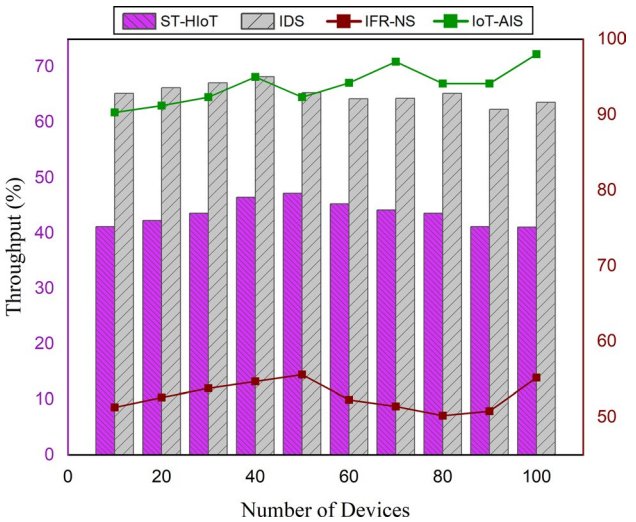

Fig. 9 The throughput rate of IoT-AIS

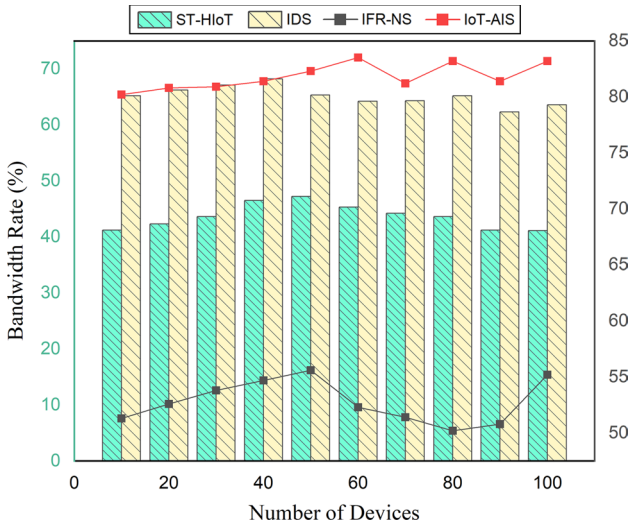

Fig. 10 The bandwidth rate of IoT-AIS

In line with the mathematical expression, access and transmission of data through IoT-health are accomplished using minimal network resources and effectively removing the intermediate malware attack**.** Despite the appropriate security of these networks, verification is less important during health data transmission than IoT devices' energy development. The transmission rate of IoT-AIS is shown in Table 1.

The network consistency is measured using IoT, system life, efficiency, threat identification performance, and threat error rate identification. There are many datasets taken for predicting performance on affecting the dataset size. This section imports the actions for evaluating the presentation part by increasing the output level. Whenever the dataset processing develops, the significance of measuring results will be influenced. The devices support a range of benefits for IoT implementations for effective interaction between IoT nodes, IoT applications in-vehicle networks, detector, and sensor networks. The energy usage between the IoT devices is evaluated based on the delay rate. The energy usage of IoT-AIS is shown in Table 2.

The proposed IoT-AIS method provides reliable data transmission and data security which is achieved based on the five metrics, such as high period of standard responses, enhanced delivery percentage of packets, less delay estimation, improved throughput, effective bandwidth monitoring when compared to other existing intrusion Detection Systems (IDS), Intelligent face recognition and navigation system (IFR-NS), Securing Things in the Health Care Internet of Things (ST-HIoT).

Thus, the approach of IoT-related patient data is traveled with security based on fundamental metrics. The data on period standard responses, delivery percentage packets, delay estimation, throughput, and bandwidth rate are identified. The tabulations over transmission rate and energy usage are significantly created for requiring outputs.

5 Conclusion and Future Works

This paper presents IoT-AIS for health care protection of data in the IoT platform. IoT technology is used to develop wireless sensor networks. The physical and digital worlds are linked with the IoT network. In an attempt to track and encrypt patient data, IoT-AIS is used. Encrypted data are recorded and stored for remote sharing of patient data. Besides individual patients keeping their records separately with a single access, the IoT-AIS dashboard offers a customized user interface. The mathematical expression proved that the health care medical record could be encrypted, and individual access can be provided. Health care providers are moving to technological development for accurate patient tracking and registration. The health care system's future aspects enable mobile application development for users of every standard people. The experimental results of IoT-AIS achieve the highest data transmission rate to 98.14% and

Table 1 The transmission rate of IoT-AIS

Number of devices	Transmission rate (%)
10	86.34
20	87.02
30	88.13
40	89.33
50	90.27
60	91.45
70	92.18
80	93.67
90	94.56
100	95.11

Table 2 The energy usage of IoT-AIS

Number of devices	Energy usage (%)
10	22.11
20	21.56
30	20.32
40	15.78
50	11.52
60	10.89
70	9.45
80	9.02
90	8.44
100	8.56

the highest delivery rate of (98.90%), high period of standard responses (93.79%), less delay estimation (10.76%), improved throughput (98.23%), effective bandwidth monitoring (83.14%) energy usage (8.56%), and highest performance rate (98.4%) when compared to other methods.

References

1. Thota, C.; Sundarasekar, R.; Manogaran, G.; Varatharajan, R.; Priyan, M.K.: Centralized fog computing security platform for IoT and cloud in the healthcare system. In Fog Computing: Breakthroughs in Research and Practice. IGI global, pp. 365–378 (2018)
2. Amin, R.; Kumar, N.; Biswas, G.P.; Iqbal, R.; Chang, V.: A lightweight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Gen. Comput. Syst. **78**, 1005–1019 (2018)
3. Amudha, G.; Jayasri, T.; Saipriya, K.; Shivani, A.; Praneetha, C.H.: Behavioural Based Online Comment Spammers in Social Media
4. Muthu, B.; Sivaparthipan, C.B.; Manogaran, G.; Sundarasekar, R.; Kadry, S.; Shanthini, A.; Dasel, A.:. IoT-based wearable sensor for diseases prediction and symptom analysis in the healthcare sector. Peer-to-peer networking and applications, 1–12 (2020)
5. Gao, J.; Wang, H.; Shen, H.: Smartly handling renewable energy instability in supporting a cloud datacenter. In: 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS). IEEE, pp. 769–778 (2020)
6. Ogudo, K.A.; Muwawa Jean Nestor, D.; Ibrahim Khalaf, O.; Daei-Kasmaei, H.: A device performance and data analytics concept for smartphones' IoT services and machine-type communication in cellular networks. Symmetry **11**(4), 593 (2019)
7. Liu, B.H.; Nguyen, N.T.: An efficient method for sweep coverage with the minimum mobile sensor. In: 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, pp. 289–292 (2014)
8. Gheisari, M.; Najafabadi, H.E.; Alzubi, J.A.; Gao, J.; Wang, G.; Abbasi, A.A.; Castiglione, A.: OBPP: an ontology-based framework for privacy-preserving in IoT-based smart city. Future Gen. Comput. Syst. **123**, 1–13 (2021)
9. Lakshmanaprabu, S.K.; Shankar, K.; Ilayaraja, M.; Nasir, A.W.; Vijayakumar, V.; Chilamkurti, N.: Random forest for big data classification in the Internet of things using optimal features. Int. J. Mach. Learn. Cybern. **10**(10), 2609–2618 (2019)
10. Amudha, G.; Narayanasamy, P.: Distributed location and trust-based replica detection in wireless sensor networks. Wirel. Pers. Commun. **102**(4), 3303–3321 (2018)
11. Kimani, K.; Oduol, V.; Langat, K.: Cybersecurity challenges for IoT-based smart grid networks. Int. J. Crit. Infrastruct. Prot. **25**, 36–49 (2019)
12. Nguyen, V.C.; Kostarakis, P.: The impact of green systems and signals on the health of green residences' habitants. Ann. Gen. Psychiatry **17**(1), A12 (2018)
13. Yang, P.; Yang, Y.; Wang, Y.; Gao, J.; Sui, N.; Chi, X.; Zou, L.; Zhang, H.Z.: Spontaneous emission of semiconductor quantum dots in inverse opal SiO_2 photonic crystals at different temperatures. Luminescence **31**(1), 4–7 (2016)
14. Alabdulatif, A.; Khalil, I.; Yi, X.; Guizani, M.: Secure edge of things for smart healthcare surveillance framework. IEEE Access **7**, 31010–31021 (2019)
15. Janarthanan, R.; Doss, S.; Baskar, S.: Optimized unsupervised Deep learning assisted reconstructed coder in the on-nodule wearable sensor for Human Activity Recognition. Measurement (2020). https://doi.org/10.1016/j.measurement.2020.108050
16. Tao, H.; Bhuiyan, M.Z.A.; Rahman, M.A.; Wang, G.; Wang, T.; Ahmed, M.M.; Li, J.: Economic perspective analysis of protecting big data security and privacy. Future Gen. Comput. Syst. **98**, 660–671 (2019)
17. Liu, B.H.; Pham, V.T.; Nguyen, N.T.: A virtual backbone construction heuristic for maximizing the lifetime of dual-radio wireless sensor networks. In: 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). IEEE, pp. 64–67 (2015)
18. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.Y.; Bashir, A.K.; Abd El-Latif, A.A.: DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access **8**, 111223–111238 (2020)
19. Kuthadi, V.M.; Selvaraj, R.; Baskar, S.; Shakeel, P.M.; Ranjan, A.: Optimized energy management model on data distributing framework of wireless sensor network in IoT system. Wirel. Pers. Commun. (2021). https://doi.org/10.1007/s11277-021-08583-0
20. MacDermott, Á.; Kendrick, P.; Idowu, I.; Ashall, M.; Shi, Q.: Securing things in the healthcare internet of things. In 2019 Global IoT Summit (GIoTS). IEEE, pp. 1–6 (2019)
21. Wang, L.; Ali, Y.; Nazir, S.; Niazi, M.: ISA evaluation framework for security of Internet of health things system using AHP-TOPSIS methods. IEEE Access **8**, 152316–152332 (2020)
22. Kumar, P.M.; Gandhi, U.; Varatharajan, R.; Manogaran, G.; Jidhesh, R.; Vadivel, T.: Intelligent face recognition and navigation system using neural learning for smart security in the Internet of Things. Clust. Comput. **22**(4), 7733–7744 (2019)
23. Thamilarasu, G.; Odesile, A.; Hoang, A.: An intrusion detection system for the Internet of medical things. IEEE Access **8**, 181560–181576 (2020)
24. HaddadPajouh, H.; Khayami, R.; Dehghantanha, A.; Choo, K.K.R.; Parizi, R.M.: AI4SAFE-IoT: an AI-powered secure architecture for edge layer of the Internet of things. Neural Comput. Appl. **32**(20), 16119–16133 (2020)
25. Kumar, P.M.; Gandhi, U.D.: Enhanced DTLS with CoAP-based authentication scheme for the Internet of things in healthcare application. J. Supercomput. **76**(6), 3963–3983 (2020)