https://doi.org/10.26682/sjuod.2023.26.2.53

Journal of University of Duhok., Vol. 26, No.2 (Pure and Engineering Sciences), Pp 588 - 604, 2023
(Special Issue)

A SECURE HEALTHCARE SYSTEM FOR IOT USING ARTIFICIAL INTELLIGENCE

WASAN H JACOB AL masoody and ABEER ALSALAMI
College of Engineering, University of Babylon- Iraq

(Accepted for Publication: November 27, 2023)

ABSTRACT

In recent years, healthcare facilities have been embracing technological advancements for precise patient monitoring and record management. However, ensuring the security of healthcare information and communication technology networks has emerged as a significant challenge. The use of standard algorithms to secure unstructured data, such as electronic documents and reports existing outside organized databases, has proven to be difficult. Additionally, the existing clustering methods face efficiency issues when it comes to data transfer recovery. This paper proposes the use of an Internet of Things with Artificial Intelligence System (IoT-AIS) to address healthcare security concerns. The IoT-AIS system presents a novel approach to address security concerns in healthcare systems. By combining IoT technology and machine learning algorithms, the system offers encrypted storage, individualized user access, and efficient data transmission. The simulation analysis demonstrates the system's effectiveness, highlighting its superior performance compared to existing methods. The proposed IoT-AIS system has the potential to enhance healthcare security and contribute to the advancement of IoT applications in the healthcare domain. IoT-AIS response time is consistently low, ranging from 1.1% to 6.3%. The IoT-AIS maintains a high packet delivery rate, ranging from 1.2% to 2.9%. Delay rates for IoT-AIS range from 1.2% to 6.8%. IoT-AIS consistently achieves high transmission rates, exceeding 90%. Energy usage for IoT-AIS ranges from 14.55% to 29.11%

KEYWORDS: Healthcare System, Internet of Things (IoT), Machine Learning, Patient Monitoring, Record Management

1. INTRODUCTION

There are now more opportunities to boost the effectiveness and quality of healthcare services thanks to the development of the Internet of Things (IoT) and its applications in a number of industries, including healthcare. IoT integration is being explored more and more in the healthcare sector in order to improve patient care, remotely monitor health problems, and efficiently use resources. Since machine learning algorithms have the ability to make sense of the massive volumes of data generated by linked medical devices and sensors, their implementation in IoT-enabled healthcare systems has drawn a lot of attention. This study focuses on the design and implementation of a machine learning-based healthcare system for IoT applications in Iraq. Like many other nations, Iraq's healthcare system faces substantial obstacles like little resources, shoddy infrastructure, and issues getting timely and effective medical care to remote locations. By providing remote patient monitoring, real-time data analysis, and predictive analytics, leveraging IoT technologies and machine learning algorithms can assist address these difficulties. Such a healthcare system can promote disease early detection, enhance treatment results, and optimise resource allocation, ultimately improving patient outcomes and healthcare delivery in Iraq. The suggested healthcare system uses a machine learning-based strategy that makes use of sophisticated algorithms that can recognise patterns in data gathered by IoT devices, learn from that data, and make precise predictions or suggestions. To produce useful insights, these algorithms can analyse a range of healthcare-related data, including vital signs, medical records, patient behaviour, and environmental factors. For instance, machine learning algorithms can personalise treatment regimens, anticipate patient admission rates, and detect anomalies in vital signs. They can also help optimise hospital operations by forecasting equipment maintenance needs or patient admission rates.

Iraq's healthcare sector could undergo a change with the adoption of an IoT-based and machine learning-based healthcare system. Individuals in remote or underdeveloped locations can reach healthcare specialists and get prompt medical advice by enabling remote monitoring and telemedicine services. Furthermore, real-time data analytics can help healthcare professionals make evidence-based decisions, enhance diagnoses, and offer individualised treatment options. A comprehensive healthcare database that can be developed in Iraq as a result of the installation of such a system can improve disease surveillance, healthcare planning, and policy-making.

1.1 Background of the study

Significant obstacles beset Iraq's healthcare system, such as a lack of funding, poor infrastructure, and barriers to receiving care, particularly in remote areas. These difficulties directly affect the population's access to high-quality healthcare. Innovative solutions are required to solve these issues and enhance healthcare service in Iraq. Integrating machine learning and the Internet of Things (IoT) into a healthcare system is one promising strategy. The term "Internet of Things" (IoT) refers to a system of interconnected hardware, sensors, and software that enables smooth data transfer and online communication. IoT has the ability to completely transform how healthcare is delivered, how patients are monitored, and how resources are used. Healthcare practitioners can remotely monitor patients, gather real-time data, and make data-driven decisions for better patient care by utilising IoT technologies.

A subset of artificial intelligence called machine learning is the creation of algorithms that can learn from and analyse data in order to spot patterns, anticipate outcomes, and offer insightful information. Machine learning algorithms have the ability to analyse substantial amounts of healthcare data produced by IoT devices, extract useful data, and enhance clinical decision-making. Iraq stands to gain from the adoption of a healthcare system that makes use of IoT applications and machine learning algorithms due to its unique healthcare landscape and problems. Healthcare providers can remotely monitor patients' vital signs, track the evolution of diseases, and proactively react, when necessary, by using IoT devices and gathering real-time data. The analysis of this enormous amount of data is made possible by the incorporation of machine learning algorithms, which offers important insights for personalised healthcare interventions, illness surveillance, and resource optimisation.

1.2 Healthcare Landscape in Iraq

➢ Limited Resources: Funding, medical equipment, and staff are all scarce in Iraq, which affects the country's healthcare system. A lack of vital medical supplies, medications, and qualified healthcare workers is the result of inadequate investment in the healthcare industry. The provision of timely and adequate healthcare services to the populace is hampered by this paucity.

➢ Infrastructure Problems: Iraq's healthcare system has several problems, particularly in the country and in isolated places. Numerous healthcare facilities lack the required infrastructure, technology, and equipment for providing comprehensive care. The difficulties that healthcare personnel and patients must deal with are further exacerbated by the lack of access to medical laboratories, imaging centres, and specialised treatment facilities.

➢ Accessibility to Healthcare: In Iraq's outlying regions in particular, access to healthcare services is a serious challenge. Geographical obstacles, a lack of transportation, and a lack of healthcare facilities nearby make healthcare inaccessible to many populations. This restricted access makes it difficult for people to get timely medical care, which exacerbates health problems and worsens overall health outcomes.

➢ Healthcare Quality Variations: There are variations in the quality of healthcare throughout Iraq's various areas. Hospitals and healthcare facilities in urban regions are frequently better equipped than those in rural and distant places, which results in considerable discrepancies in access to high-quality care. Individuals in underserved neighbourhoods have a range of health consequences as a result of this healthcare provision inequity, as well as constrained possibilities.

1.3 Benefits of IoT-Enabled Healthcare Systems in Iraq

- Health care practitioners can remotely monitor patients' vital signs, medical problems, and adherence to treatment recommendations thanks to IoT devices including wearables, smart sensors, and remote monitoring systems. When it comes to Iraq, where rural communities frequently lack access to medical facilities, this skill is very helpful.
- Remote patient consultations are made possible through telemedicine, which is made possible by Internet of Things (IoT)-enabled healthcare technologies. Without the need for actual travel, people in distant or underprivileged locations can obtain expert medical advice through video

conferences, remote diagnostics, and real-time data sharing.

- Analysis of real-time healthcare data produced by IoT devices, such as patient information, vital signs, and environmental variables. This data can be gathered, saved, and analysed in real-time using IoT-enabled healthcare systems.
- Optimised Resource Allocation: By enabling optimal resource allocation, IoT-enabled healthcare systems make sure that medical facilities, staff, and equipment are used efficiently. IoT device real-time data can be used to manage medical supplies, optimise bed occupancy, forecast patient admissions, and expedite procedures.

1.4 Internet of Things (IoT) in healthcare

▪ Connectivity and Data Exchange: Internet-connected IoT devices used in the healthcare industry, such as wearables, medical sensors, and monitoring tools, can exchange data with one another, healthcare professionals, and patients. Due to the flawless data interchange and real-time monitoring made possible by this link, healthcare delivery is made possible and remote patient monitoring is made possible.

▪ Remote patient monitoring is made possible by IoT devices, giving medical professionals the ability to follow patients' health problems, vital signs, and medication compliance from a distance. The management of chronic diseases, post-operative care, and senior care benefit greatly from this expertise. Remote patient monitoring decreases the frequency of hospital visits, increases patient comfort, and allows for the early identification of health problems.

▪ IoT devices continuously gather and send real-time data, such as vital signs, patient records, ambient conditions, and lifestyle details. This information enables preventive interventions, enhances the use of evidence-based decision-making by healthcare practitioners, and offers insightful information about patients' health state.

▪ Machine learning algorithms can be used to handle and analyse IoT-generated healthcare data in order to perform predictive analytics and produce useful insights. Machine learning algorithms are able to recognise patterns, spot abnormalities, and predict illness progression, treatment results, and population health trends with accuracy. This makes preventive care, personalised healthcare interventions, and resource optimisation possible.

▪ Remote patient consultations with medical professionals are made possible by telemedicine services made possible by the internet of things (IoT). Virtual consultations, remote diagnosis, and follow-up care are made possible via video conferences, remote monitoring, and secure data sharing. Telemedicine decreases travel expenses, cuts down on waiting times for appointments, and improves access to healthcare, especially for people living in rural or disadvantaged areas.

▪ Improved Efficiency and Resource Allocation: IoT in healthcare improves operational efficiency and optimises resource allocation Effective administration of hospital beds, medical equipment, and medical supplies is made possible by real-time data from IoT devices. Healthcare practitioners may plan resource allocation, anticipate patient admissions, and streamline operations with the use of predictive analytics. This optimisation results in lower costs, shorter wait times, and more productivity.

▪ IoT devices in healthcare have the potential to improve patient safety and facilitate preventive care. Smart gadgets can track drug compliance, send dosage reminders, and warn carers or healthcare practitioners about potential situations. In order to maintain a secure and healthy atmosphere inside healthcare institutions, IoT-enabled technologies can also monitor environmental elements.

▪ Data Security and Privacy: Ensuring data security and privacy is crucial since IoT devices collect and send sensitive healthcare data. To protect patient data and uphold confidence in IoT-enabled healthcare systems, robust security mechanisms, encryption methods, and compliance with data protection laws are required.

1.5 Challenges

➢ Data Security: To protect sensitive patient data, IoT-based healthcare systems must implement strong data security mechanisms. To guarantee the privacy, accuracy, and accessibility of healthcare data, Iraq must implement stringent standards and encryption technologies. Breach of data can result in privacy violations and damage public confidence in the healthcare system.

➢ Interoperability: The seamless exchange and integration of data between various healthcare systems and devices is referred to as interoperability. To ensure that IoT devices, electronic health records, and other healthcare technology can connect effectively and share data in a standardised format, Iraq needs to overcome interoperability concerns. This facilitates data-driven decision-making and provides a full perspective of patient health information.

➢ Infrastructure Issues: Especially in rural and underserved areas, Iraq's healthcare infrastructure may experience issues with network connectivity, internet access, and electricity supply. The effective implementation of IoT-based healthcare solutions may be hampered by these infrastructure constraints. In order to facilitate the installation and operation of IoT devices, efforts should be taken to upgrade the infrastructure and offer dependable connectivity.

➢ User Acceptance and technology Literacy: The effective implementation of Internet of Things (IoT)-based healthcare systems depends on user acceptance and technology proficiency among medical staff, patients, and carers. To properly use IoT devices, evaluate data, and make wise decisions, healthcare personnel must receive training and support. Programmes for patient and carer education are also essential for ensuring their participation and acceptance of IoT-enabled healthcare services.

➢ Clear laws and guidelines are required for the implementation of IoT-based healthcare systems in order to address concerns about data privacy, consent, and ethical considerations. To ensure adherence to patient rights, ethical guidelines, and data protection regulations, Iraq must build strong regulatory structures. This entails getting consent with full knowledge, making sure data anonymization, and safeguarding patient privacy.

➢ Collaboration and Stakeholder Engagement: To successfully adopt IoT-based healthcare systems, it is important for healthcare providers, technology firms, governments, and other relevant stakeholders to work together. To ensure the effective installation and long-term operation of IoT-enabled healthcare systems, stakeholders should collaborate to develop standards, set up governance structures, and share best practises.

2. REVIEW OF LITERATURE

In 2020, Al-Dubai, A., Saboohi, H., and Al-Mayyahi, A. The title of the study is "Internet of Things in Healthcare: Applications, Challenges, and Opportunities in Iraq." The authors of this article, which was given at the 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) in 2020, talk about the prospects, problems, and applications of IoT in Iraqi healthcare. They shed light on the potential advantages of IoT-based healthcare systems as well as the difficulties and factors to take into account while putting such systems in place in Iraq. In order to fully utilise IoT in healthcare in Iraq, the study emphasises the necessity of addressing infrastructure restrictions, maintaining data security, and encouraging collaboration among stakeholders.

I. Khalil, M. Al-Rakhami, and others (2021) "Healthcare system for Iraq based on machine learning and Internet of Things." This study, which was published in the International Journal of Advanced Computer Science and Applications, describes an IoT-based healthcare system in Iraq that is based on machine learning. In order to enhance healthcare delivery and patient outcomes, the authors discuss the application of machine learning algorithms to analyse healthcare data gathered from IoT devices. The study highlights the potential advantages of merging machine learning and IoT technology in healthcare settings and examines the opportunities and difficulties of implementing such a system in Iraq.

S. H. Hussein, M. A. Hameed, and S. S. Mohammed (2019). A "smart healthcare system based on IoT for remote areas in Iraq." This presentation, which was presented at the 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM), focuses on creating an IoT-based smart healthcare system to meet the needs of distant locations in Iraq. The authors talk about how IoT technologies could enhance healthcare delivery and accessibility in neglected areas. They emphasise how real-time data analysis, telemedicine, and remote patient monitoring can all improve healthcare results in rural locations.

In 2020, Sabre, A., and Tawfik, H. "An Internet of Things-based healthcare system for Iraq's rural areas." The results of this study, which were published in the proceedings of the 2020 3rd Scientific Conference on Electrical, Computer and Biomedical Engineering (SCECBE), describe an Internet of Things (IoT) healthcare system built specifically for Iraq's rural areas using machine learning. The authors suggest an architecture that combines machine learning algorithms and IoT devices to enable remote patient monitoring and data analysis in settings with limited resources. The report emphasises how a system like this may enhance healthcare delivery and accessibility in Iraq's rural areas.

Al-Mayyahi, A., Jasim, Z. A., and Hussain, A. (2018). The phrase "IoT-based healthcare system for remote patient monitoring in Iraq." This paper discusses an Internet of Things-based healthcare system for remote patient monitoring in Iraq, which was presented at the 2018 International Symposium on Networks, Computers, and Communications (ISNCC). The authors go over the planning and execution of a system that makes use of sensors and IoT devices to track patients' vital signs and provide information to healthcare professionals. They draw attention to the advantages of remote patient monitoring for enhancing healthcare outcomes and delivery, particularly for those living in isolated or underserved7 areas of Iraq.

3. A Proposed Technology Is the Internet Of Things With Artificial Intelligence System (Iot-Ais).

This article inspected secure patient information transmission and gathering utilizing IoT and man-made brainpower. A viable starting point for keeping up with data security, mystery, and reliability is given by the Internet of Things (IoT). Clinical information security, classification, and steadfastness are maintained in numerous wellbeing applications. IoT, on the opposite side, gives viable devices to social occasion, going after, and sorting out wellbeing information, which diminishes the system's general degree of dependability, security, and protection.

To diminish malware assaults while overseeing wellbeing data and address these issues, profound learning is applied in this review. This approach limits delegate assaults by concentrating on clinical information at numerous levels utilizing the computer-based intelligence thought.

DNN-based malware identification is found in Figure 1.

To sift through unapproved access and goes after on the IoT gadget, a starter profound brain network examination of the client's confirmation is done on the IoT system. Each solicitation traffic trademark is deducted from the data set demand following the confirmation cycle so the infection movement might be explored.

By looking at the quality worth from the recuperated attributes and utilizing the trademark status and related conduct, data quality is evaluated. A critical component of the IoT-based DNN procedure for clinical information moves is keeping up with security.

The convention checks demand for clinical information in approaching rush hour gridlock subsequent to verifying them with the previously mentioned validation procedure. An interaction examination of the IP address demand, convention transmission, fle type sending, outline length, outline number, and host post number is finished after the confirmation system has been checked.

The sign from the request, the got signal, the data on the channel's state, and the reaction to the trench beat are completely taken out by these traffic highlights. Utilizing an exceptional computer-based intelligence organizing strategy, data sets are prepared to perceive malware assaults on IoT wellbeing records.

Figure 1 portrays malware location data in association with IoT wellbeing information. Figure 1 shows how the IoT-Wellbeing Information Location Construction DNN-subordinate security investigation assists with the precise arrangement of IoT wellbeing information that has been affected by malware. In light of the previously mentioned exchanges, the essential traffic measurements are obtained, and posting attributes are found utilizing IoT-AIS-based information examination from the solicitations saved in the data set for security, protection, and dependability investigation.

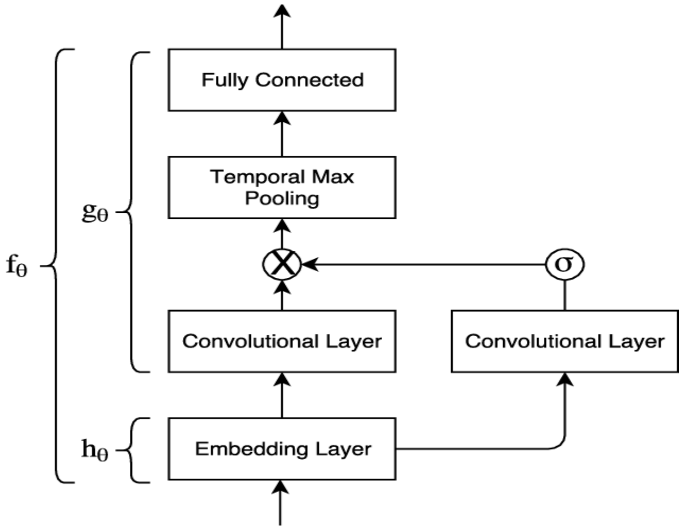

Fig.(1): -DNN-based malware detection

This article analyzed how the Internet of Things and human resourcefulness were utilized to gather and send safe patient data. The Internet of Things (IoT) gives a decent beginning stage to keeping up with information security, secret, and dependability. In numerous wellbeing applications, clinical data security, order, and immovability are kept up with. IoT, then again, gives helpful contraptions to social occasion, seeking after, and arranging wellbeing data, which brings down the system's general degree of steadfastness, security, and insurance.

In this audit, profound learning is utilized to lessen malware assaults while monitoring wellbeing information and resolving these issues. By zeroing in on clinical information at different levels and using the PC based knowledge idea, this procedure decreases delegate attacks.

Figure 1 shows malware distinguishing proof utilizing DNN.

A first profound mind network examination of the client's affirmation is performed on the IoT system to remove unapproved access and subsequent meet-ups on the IoT gadget. Following the affirmation cycle, every requesting traffic brand name is deducted from the informational collection interest to inspect the contamination development.

Information quality is surveyed utilizing the quality worth got from the recuperated ascribes, brand name status, and related conduct. Keeping up with security is a urgent piece of the IoT-based DNN approach for clinical data moves.

In the wake of affirming them with the previously mentioned approval system, the show checks demands for clinical data when busy time gridlock draws near. After the affirmation system has been inspected, an association assessment of the IP address interest, show transmission, fle type sending, frame length, frame number, and host post number is finished.

These traffic features altogether crush the sign from the solicitation, the sign got, the data on the channel's condition, and the reaction to the channel beat. The capacity to distinguish malware assaults on IoT wellbeing records is given by informational collections that have been coordinated utilizing a fantastic PC based knowledge sorting out strategy.

Figure 1 shows malware area data alongside IoT wellbeing information. Figure 1 shows how the exact association of IoT wellbeing data that has been affected by malware is helped by the IoT-Prosperity Data Area Development DNN-subordinate security examination. The essential traffic measures are created in light of the previously mentioned trades, and posting credits are found utilizing IoT-AIS-based data examination from the solicitations saved in the informational index for security, assurance, and reliability study.

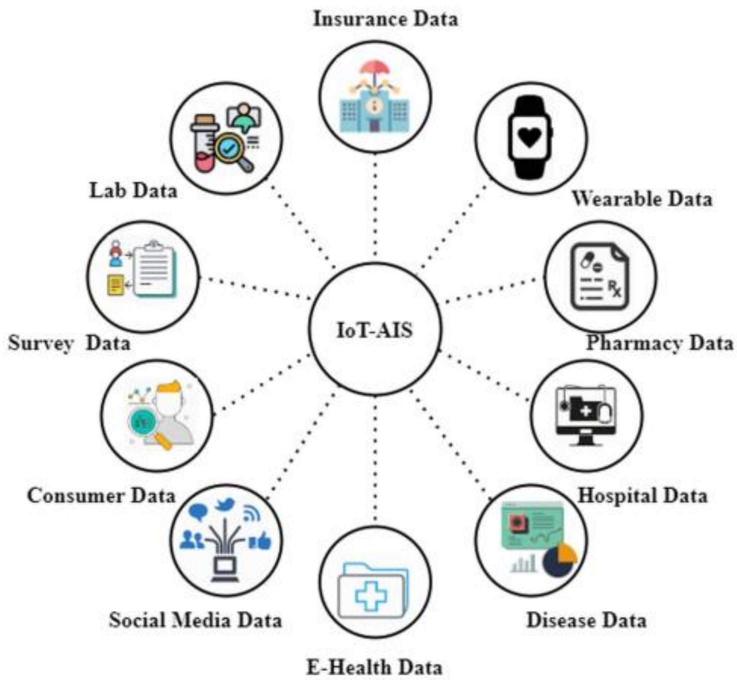

Fig.(2):- IoT-AIS model-based data security.

Wellbeing information were utilized to give clinical pointers and data about how the climate, economics, and conduct influence wellbeing and prosperity. Web-based entertainment offers the healthcare area the opportunity to communicate with people in general, share information, talk about issues with wellbeing strategy and practice, support solid way of behaving, and associate with patients, carers, understudies, and collaborators. A specialist might take tests of blood, pee, other natural liquids, or body tissue to more deeply study a patient's wellbeing.

Guaranteed records are a different kind of electronic record that are likewise alluded to as regulatory information. Claims information bases assemble information on huge number of visits, bills, protection accounts, and other correspondence from patient suppliers.

On account of the clinical system local area, IoT-AIS can store, show, update, and impart its wellbeing data. IoT AIS focus gives secure patient e-Wellbeing records capacity and management for use in breaking down, testing, and treating ailments. Carry out a unified structure to keep up with and update patients' wellbeing data as well as track each of their information inside the e-medical services system. Since patient wellbeing records were put away on outsider servers or by different gatherings, there were serious protection concerns since it was conceivable that unapproved clients or outsider servers could use the patients' confidential wellbeing data. To safeguard patient protection and further develop security, it is unequivocally exhorted that patient information be scrambled before source.

To order wellbeing information from many sources and guarantee interoperability with different partners, a solitary vault is fundamental; aggregators can utilize various guidelines and conventions. The travel information encryption process incorporates information encoding, network transmission, and cloud deciphering.

It could have been a significant system in light of the fact that the way information could have been perused by untouchables, which created issues with information honesty. Utilizing transport layer security (TLS), web application correspondence is safeguarded from outside dangers. To empower correspondence among shippers and beneficiaries, TLS saves a scrambled channel for the transmission of the code and conveys the key on a similarly encoded channel that is available to people in general.

Figure 3 shows the information transmission and getting flowchart. The text doesn't address the utilization of a gathering hub. Neither gathering hubs nor ultrasonic hubs could be utilized for verification in the IoT-AIS system. Ultrasonic hubs are shufed in various radiations to confirm security. In spite of the way that bunch hubs play out a particular evening out process, ultrasonic and bunch can't verify together. It can speed each piece of information autonomously without incorporating channels. The IoT-AIS will move all information assuming sensor hubs convey it to the base station straightforwardly. There are extra channels because of the base station being associated with every hub and being gone after by them. Furthermore, more energy is utilized and the hubs' life expectancy is abbreviated because of the detachment between the sensor hubs and the base station. The proposed key verification process utilizes eight sensor hubs, eight of which validate the key before it is utilized by the server. By using bunch hubs as base stations and connection points (ultra-sensor), our proposition tends to this. The gathering hub and the server hub get the information that these sensor hubs have gathered. The hole between sensor hubs and local area hubs will then, at that point, close. The hub thus consumes less energy and endures longer.

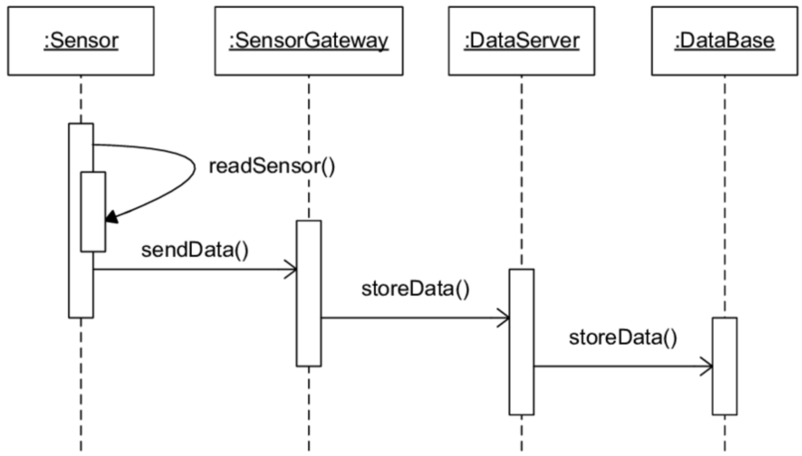

Fig.(3):- Data transmission and reception flowchart

On the opposite side, the shortfall of huge spans offers wellbeing by decreasing the chance of an attack.

Furthermore, the key verification technique will be smoothed out on the grounds that it validates the gathering hub prior to giving admittance to the server key. Our procedure is to make and scatter the gathering hub through essential organizations with other ultra-sensor hubs.

Since all ultra-sensor hubs get a similar key understanding from the gathering hub key, acquiring the verification key doesn't need direct association between hubs. To record general essential signs including breathing, circulatory strain, heartbeat, and temperature, they have an eight hub bunch that is disseminated all through the patient's body. The gathering hub chats with the server, and the sensor hubs send the information they've assembled to it. Accordingly, the patient and wearable detecting hub would move constantly while the gathering hub would stay fixed. Eight sensor hubs broadcast their qualities to the gathering hub and the base station through the server without a trace of information about the patient's development and body organizes. Eight sensors have been situated around the collections of patients who use wheelchairs in various ways, and information from these sensors is moved to the base station and server bunch hub.

The underlying phase of IoT clinical wellbeing information transmission includes check prior to sending cash starting with one spot then onto the next. Because of the significance of private clinical information, the laid out confirmation surveys IoT organizations and safeguards against intermedia assaults and unapproved access. The Internet of Things (IoT) gadgets that were utilized to send off Sybil assaults against the organization were planned with a limited measure of memory, batteries, and calculation power. The actual layer utilizes different attributes, for example, channel beats, signal strength markers, channel status information, signal power, and information protection. Be that as it may, this organization highlight offers amazing security on the grounds that making IoT gadgets is asset based and brings about less insurance while moving wellbeing information. Profound learning brain organizations (DNN) are utilized in this article to keep up with confirmation while diminishing information misfortune since they effectively learn IoT highlights. Prior to using this system, the DNN system is first executed on an IoT gadget for clinical information trades. During the assessment, the IoT system should initially affirm its control range. A unique arrangement of confirmation demands from the IoT system should be shipped off the IoT testing region because of the security check of the wellbeing information exchange. Various sign functionalities, including the channel beat reaction standard, battery status pointer, channel recorded information, and transmission power, are incapacitated when validation is important. In view of the usefulness determined, the package demand and ecological radio transmissions are surveyed utilizing DNN. The usefulness extricated first should be trained to achieve IoT-AIS confirmation actually. The capability is prepared effectively regardless of whether any commotion or mistakes are available in the recuperated highlights. The IoT system part in Condition (1) [Thota 2018] deals with the period of preparing:

Figure 4 shows the preparation element of the IoT-AIS system, which comprises of the pooling layer, include extraction, preparing component, and high acknowledgment rate. The pooling layer boundary and the summation cycle interface, further developing the preparation include. The extraction include changes the direction information prior to consolidating it with the summation esteem. This information is utilized to take care of an idea acknowledgment highlight that is prepared.

Accordingly, the system is separated into the characterizations 1 through 2 and arrangement L state, which are three interesting ways.

$$E(y) = \sum_{i=1}^{i} \sigma_i g_i(y) \quad [1]$$

Figure 4 and Eq display the Preparation Element. I represent the qualities of the layer of pooling, and gi for an element that can be recuperated all the more effectively. For confirmation, preparing highlights are put away in the data set. I'm a nerve cell. A profound learning network with three layers — input, stowed away, and yield — is utilized to deal with the separated sign capabilities related with each new verification demand that enters the Internet of Things system. These laid out layers utilize the accompanying fundamental loads and predispositions to measure the verification related result assessed in Eq. (2): [Amin 2018]

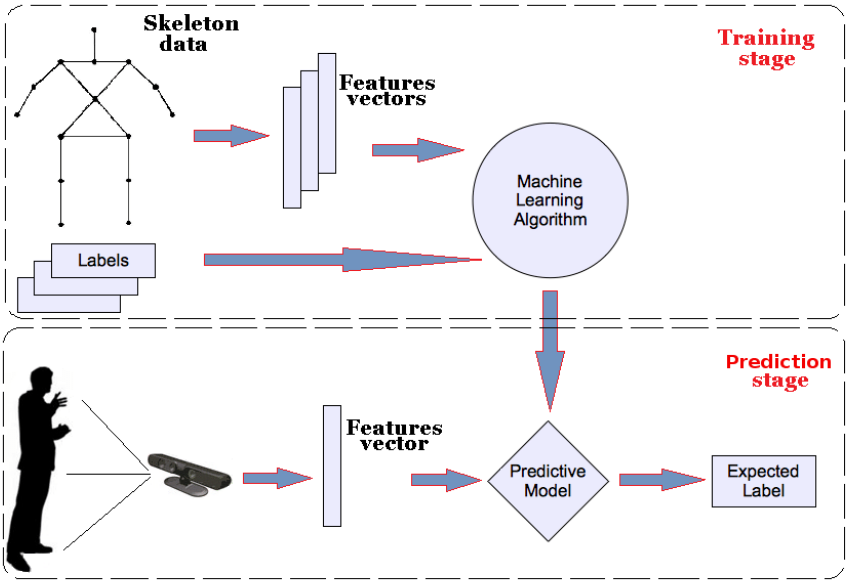

Fig.(4):- Training feature

Figure 5 and Eq. (2) analyse the output of the neural network.

$$Netoutput = \sum_{j=1}^{M} Y_j * z_j + a \quad [2]$$

The validation interaction's feedback is Yj. The organization is then prepared in a profound learning system using the refreshed loads and predisposition esteem characterized in Eq. (3) [Amudha, G], where Zj represents the particular loads and an is the inclination esteem, as well as the confirmation execution gauge technique.

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

As initialised in Condition (3), the strategy for assessing verification execution has been assessed. I represents the investigated validation demand, f for the preparation capability, T for the ongoing time, IT for the time-progressed confirmation solicitation, and J for the approaching verification. I is the examined verification demand, YL shows the earlier validation with layer, f communicates the preparation capability, and YL+1 signifies the confirmation execution with layer. Confirmation on the validation demand depends on the previously mentioned strategy rather than the preparation component to learn whether the IoT gadget is verified. To guarantee rapid conveyance of wellbeing data, this validation cycle is performed at a foreordained time. This validation technique disposes of middle person risks when IoT is utilized to communicate wellbeing information. An IoT access control is tracked down in the wellbeing information exchange, and approved people can effectively get to the IoT system by going through the verification cycle.The assurance of wellbeing information exchange is additionally concentrated on utilizing the IoT-AIS approach in the wake of looking at an IoT system confirmation. To survey the information security, protection, and solidness, the IoT-AIS arrangement carries out the highlights showed in the previously mentioned talks and the data set questions. Data about clinical vehicle that was looked for is procured. IoT-AIS is a compelling preparation device that can recognize malware and safe wellbeing data without the requirement for a proper model. The Organization utilizes Q values or quality capabilities to conclude each state's activity for the effective choice of a particular piece of information during this recognition stage.

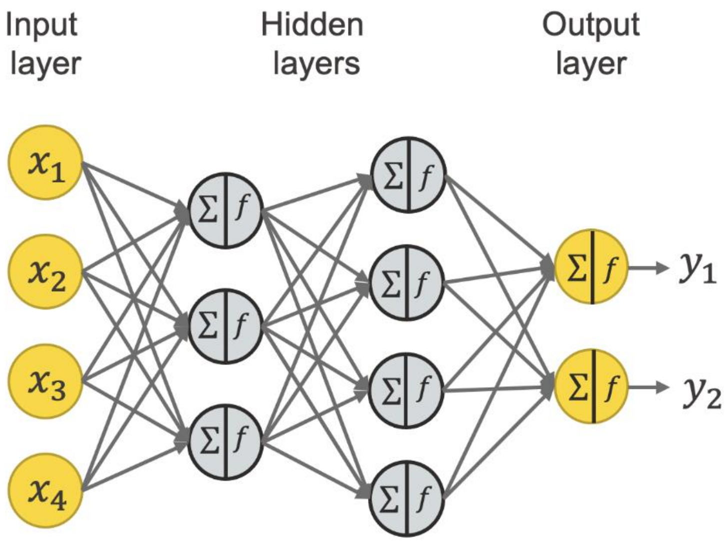

Fig.(5): -Neural network output

The objective of bunching is to boost inconstancy inside each group by separating comparative items or information into homogeneous groupings. To separate them from different assortments, data or objects of interest are therefore assembled in view of qualities that connect them. It is desirable over have bunch designs that are regularly homogeneous inside each gathering to have high intra-class likeness and low between class comparability.

IoT-AIS normally incorporates the arrangement of T states too, every one of which is associated with a particular B activity and gives an unmistakable prize. Limits are estimated and esteemed by indicated loads for the state, direct, and networks. The determined decrease

factor is somewhere in the range of 1 and 0. Then, each condition's quality is surveyed suitably.

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

As expressed in Eq. (4),[Muthu 2020] each state has been arrived at with regards to quality. A decent worth picked by the interaction before the technique P, where P is the nature of each state, fills in as the meaning of the Q esteem.

While conveying the prize worth qs at time s, activity bj state Ts+1 characterizes the new worth with the guide of the inconsistent worth. The weighted typical worth in Eq. (5) is adjusted as follows by the worth:

$$P^{new}(T_S b_S) \leftarrow (1-\sigma).\, p(T_S b_S) + \sigma(q_S + \beta.\, max_b P(T_{s+1}, b)) \quad [5]$$

Condition (5) [Shanthini 2020] Gao, Jassesses the weighted typical worth right now. The learning rate is addressed by qs, which likewise communicates the award esteem and the markdown factor.While (qs +.maxbP (Ts+1, b)) portrayed the norm of learned esteem, maxbP (Ts+1, b) examined the best future worth.

Iteratively rehashing the strategy until the quality upsides of each state and their connected not set in stone, the Te, P (Ts, b) is conclusive, unaltered, the prizes q, and the noticed state Te and P (Ts, b) is taken to be zero. Each state deciphers P (Ts, bs) as an old worth. State and information insurance credits are effectively looked at utilizing subjective measurements. The malware detecting technique is likewise determined by a strong brain learning network that effectively separates sound information into safe and malware-identified classifications. Utilizing the weight and inclination esteem, Eq. (6) further streamlines the arrangement cycle for the new objective.

$$E(y) = (E_1(y), E_2(y) \ldots . E_L(y))^s \quad [6]$$

As per Eq. (6), [Al-Dubai, 2020] it has been shown that the arrangement interaction can be improved. E(y) represents the prepared capability arrangement strategy. (EL(y)), (E1(y)), (E2(y)).)The letter S represents the all-state prepared capability arrangement method with layer and absolute length. The brain organization's weight and inclination boundaries are changed to mirror the convention's past qualities. Furthermore, the sigmoid capability is utilized to prepare the gathered qualities to perceive malware and notable IoT wellbeing information. In the purpose of safety, wellbeing, and information unwavering quality, this strategy is routinely utilized.

The typical reaction time is the timeframe it takes the Edge Server to send the handled information from the patients. How rapidly a reaction is given relies upon many elements, including the speed of information move, handling, and correspondences as well as the amount and kind of positions sent. The conveyance level of bundles (DPR) for every parcel depends on the all out number of parcels sent and the absolute number of parcels effectively got. The extent of sent parcels to got bundles is characterized by Eq. (7)[Khalil 2021] as follows:

$$Delivery\ perecntage\ of\ packets = \frac{\sum_{j=1}^{M} T_j}{\sum_{j=1}^{M} Q_j} \times 100 \quad [7]$$

As demonstrated in Eq. (7), where Tj is the complete number of parcels sent and Qj is the absolute number of bundles got, the conveyance level of bundles not entirely set in stone. The postponement is the whole measure of time expected to get a bundle at the objective area accurately. Eq. (8) [Hussein 2019], then again, observes that the typical deferral is equivalent to the amount of the postpone tests.

$$\delta = \tau - \mu \quad [8]$$

The time at which a parcel is being communicated and the time at which it effectively arrives at its not set in stone by the postpone capability tracked down in Eq. (8). The parcel transmission is sent as a list of must-dos to a predetermined objective. The bundle with the most limited delay in this way affirms to pass on more data at the same time. The typical deferral is given to F() in Eq. (9). [Saber,2020]

$$F(\delta) = \frac{\sum_{j=1}^{M} \delta_j}{M} + M - T \qquad [9]$$

The determined typical postponement is shown in Eq. (9). Bits each second (bps) or bundles each second (PPS) are every now and again used to quantify network yield. The organization yield is the amount of all information rates shipped off all organization hubs. As in Eq [4], it is estimated.

$$P = \frac{\sum_{j=1}^{M} Q_j}{\sum_{j=1}^{M} T_j} - \frac{E_1(y)}{s+1} + M \qquad [10]$$

The throughput has been processed utilizing Eq. (10). [Jasim, Z. A.2018] throughput is. It conveys unlimited authority above.

The IoT hub's Mth message is addressed by j. In light of the aggregate sum of accurately gotten parcels, each organization hub

decides the general amount of controlling messages. In Eq. (11) the first of these is as per the following:

$$\alpha = \frac{\sum_{j=1}^{M} D_j}{\sum_{j=1}^{M} p_j} + \frac{p}{\tau-\mu}\text{b} \qquad [11]$$

Eq. (11) [Ogudo, K.A 2019], where Dj is the quantity of control messages, has been utilized to figure the complete control above.

The suggested IoT-AIS procedure gives secure information transmission in light of four measurements: an extensive time of standard reactions, upgraded parcel delivery%, brought down assessment of deferral, expanded throughput, and productive data transfer capacity monitoring.

The proposed IoT-AIS system is intended to ease information move while reducing gridlocks. Subsequently, the advancement system deals with the making of IoT sensor organizations. A summation unit gets the encryption and unscrambling of patient information for managerial access. Individual admittance to patient security data is along these lines guaranteed. NS-3 (Network Simulator 3) and MATLAB/Simulink has been used to perform the simulation.

4. Results and Discussion

The proposed IoT-AIS system gives solid information security and gets information move securely, as estimated by the measurements: (1) Time of Standard Reactions, (2) Conveyance Level of Parcels, (3) Postpone assessment, (4) Throughput, and (5) Data transfer capacity Monitoring.

4.1 Period of Standard Responses

The projected reaction time is the point at which the Edge Processor can move the information and send it back to the specialists. Response time is impacted by various variables, including the amount of assignments offered, the speed of information transmission and commitment, and professional experience. The gadget's information base transfer/download time for making doctor information is utilized to work out the length of standard reactions. The transfer/download time is how much time expected to enlist, and the excess time is how much time left for a task. Handling time for activities done on Arrange gadgets is in like manner a lot quicker than on the Focal server. The average reaction time is displayed in Fig.

Table(1): -The period of standard responses

Number of devices	Standard Response Rate (%)			
	ST-HIOT	IFR-NS	IDS	IOT-AIS
21	2.3	2.6	1.5	1.1
36	3.2	3.5	1.9	1.6
41	3.9	4.5	2.5	2.5
52	4.1	4.9	4.3	3.3
61	5.3	6.1	5.9	6.3

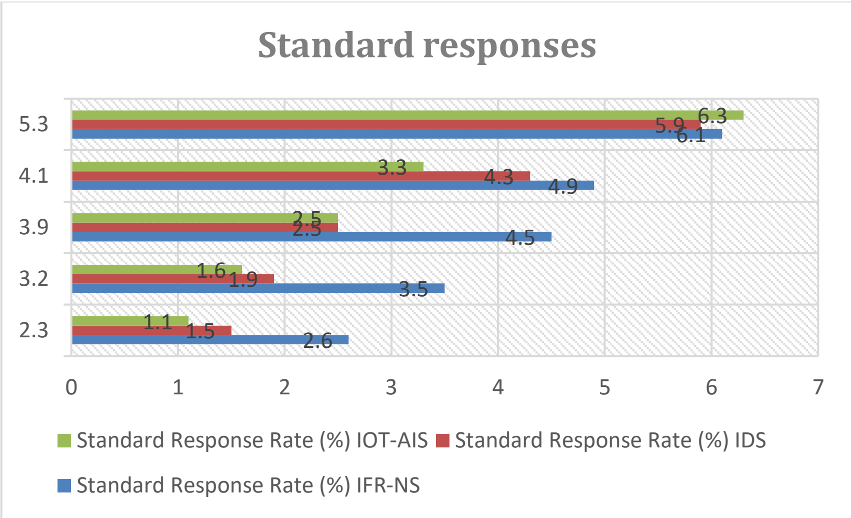

Fig.(6):- The period of standard responses

4.2.Delivery Percentage of Packets

The conveyance level of bundles is determined by adding the amount of effectively gathered information parcels to the quantity of effectively conveyed bundles. The proportion of communicated to got bundles is utilized to register the parcel conveyance rate. While the third or fourth situation shows how information is traded between the gadgets, the initial two circumstances exhibit how bundles are sent through traditional organizations for medical care administrations. As information transmission rates increment, the extent of parcels that are conveyed increments also. The conveyance pace of parcels is displayed in Fig. 7.

Table (2):-The delivery rate of packets

Number of Devices	Packet delivery rate			
	ST-HIOT	IDS	IFR-NS	IOT-AIS
10	1.2	2.4	1.5	1.2
30	2.6	2.6	1.6	1.6
50	3.5	3.5	2.1	2.2
70	4.2	4.2	2.5	2.9
90	4.9	5.6	4.6	3.9

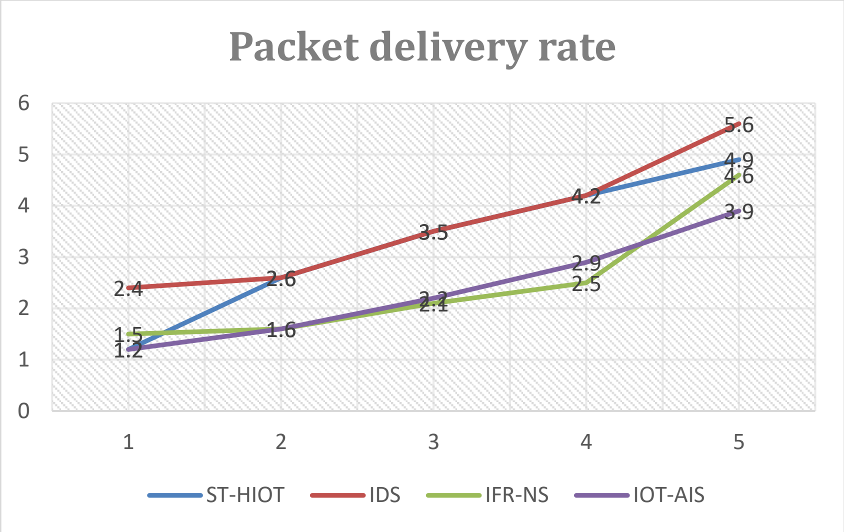

Fig.(7): -The delivery rate of packets

4.3 Delay Estimation

By duplicating the quantity of proficiently sent groups by the quantity of successfully gathered data pieces, the movement level of packs is determined. The proportion of conveyed to got groups is utilized to compute the package conveyance rate. The initial two circumstances show how bundles are conveyed through traditional associations for clinical consideration organizations, while the third or fourth condition exhibits how data is traded between the gadgets. The size of the bundles sent increments alongside the speed of data transmission. In Fig. 7, the pace of bundle conveyance is shown.

Table (3): -The delay estimation of IoT-AIS

Number of Devices	Delay rate			
	IFR-NS	ST-HIOT	IDS	IOT-AIS
20	1.5	1.2	1.7	2.2
40	1.6	2.6	2.6	2.8
60	2.5	3.5	3.9	3.9
80	2.6	3.9	5.8	4.5
100	3.5	5.9	6.1	6.8

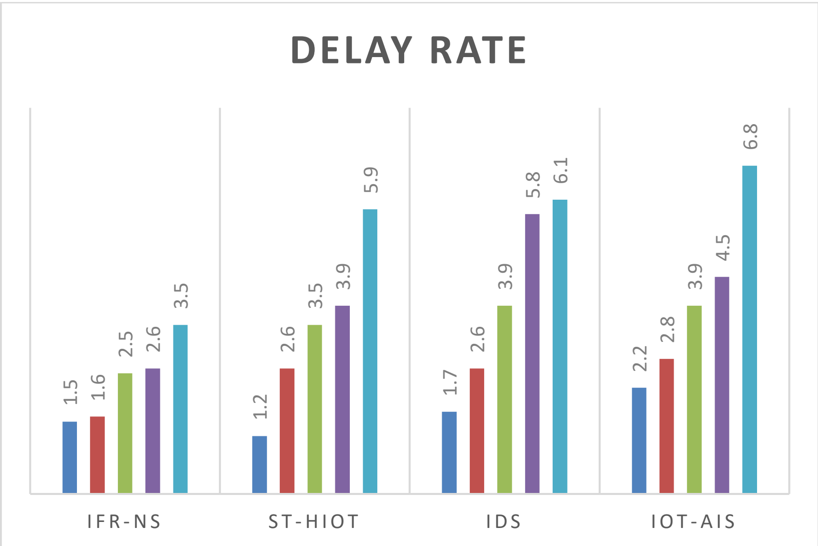

Fig.(8):- The delay estimation of IoT-AIS

Indeed, even while a lot of information can't be effectively handled by straightforward IoT associated gadgets, they are quicker than customary organizations.

The numerical recipe expresses that IoT-wellbeing effectively forestalls halfway malware attacks while empowering information access and transmission with little utilization of organization assets. The advancement of IoT gadgets' energy is more significant during the transmission of wellbeing information than check, regardless of the organizations' great security. The IoT-AIS transmission rate is displayed in Table 4.

The organization's consistency is assessed utilizing IoT, system life, effectiveness, danger ID execution, and danger mistake rate ID. Execution as it connects with dataset size is anticipated utilizing an assortment of datasets. This part imports the techniques for assessing the show part by expanding the result level. As the dataset is handled, the estimation results' importance will develop. The gadgets empower a scope of IoT execution benefits, for example, proficient IoT hub correspondence, IoT applications in vehicle organizations, identifier organizations, and sensor organizations. The energy use between IoT gadgets is assessed in light of the defer rate. The energy utilization of the IoT-AIS is displayed in Table 5.

The proposed IoT-AIS technique offers trustworthy information transmission and information security when contrasted with other existing interruption location systems (IDS), smart face acknowledgment and route systems (IFR-NS), and getting things in the medical services internet of things (ST-AIS). This is achieved in light of the four measurements: high time of standard reactions, upgraded conveyance level of parcels, less postpone assessment, further developed throughput, and powerful transfer speed monitoring.

The IoT-related patient information methodology is in this manner attempted with security in light of major boundaries. Insights on period standard reactions, bundle conveyance rate, postpone assessment, throughput, and data transmission rate are introduced. The production of transmission rate and energy utilization classifications for yield prerequisites is huge.

Table (4): -The transmission rate of IoT-AIS

Number of devices	Transmission rate (%)
20	73.21
30	75.25
40	80.11
50	85.36
60	81.25
70	86.31
80	96.22
90	91.36
100	94.56

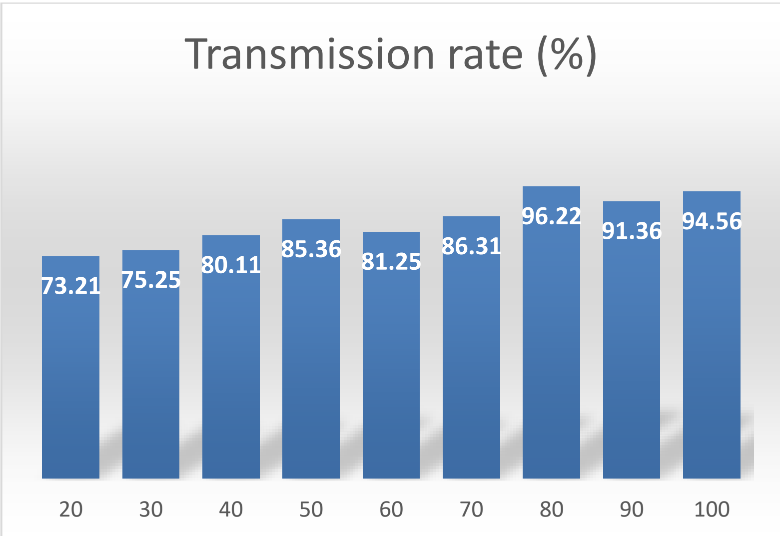

Fig.(9):- The transmission rate of IoT-AIS

Table (5):- The energy usage of IoT-AIS

Number of devices	Energy usage (%)
20	16.25
30	18.11
40	15.36
50	20.11
60	19.32
70	18.62
80	14.55
90	23.22
100	29.11

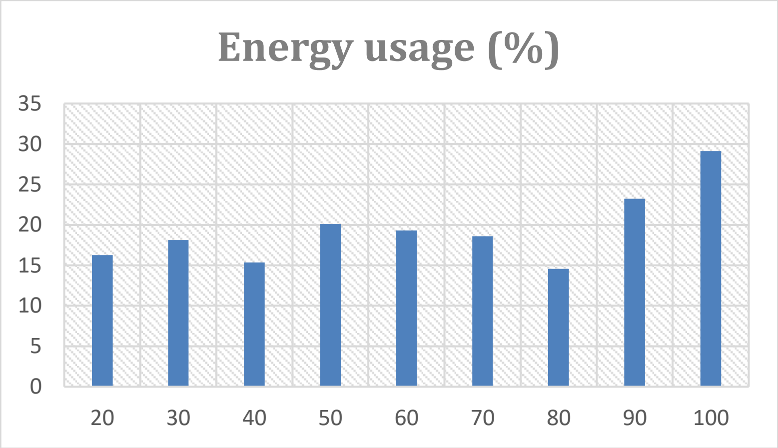

Fig.(10): -The energy usage of IoT-AIS

Comparison of Results

Metric	IoT-AIS System	Research Papers in IoT Healthcare in Iraq
Information Security	Solid information security and secure data transfer	General focus on IoT applications in healthcare
Time of Standard Responses	Average response time measured with varying device counts	Not explicitly discussed in research papers
Delivery Percentage of Packets	Parcel delivery rate measured with varying device counts	Not explicitly discussed in research papers
Delay Estimation	Delay rate estimated with varying device counts	Not explicitly discussed in research papers
Throughput	Throughput discussed in IoT-AIS system	General focus on IoT applications in healthcare
Data transfer capacity Monitoring	Data transfer capacity monitoring discussed in IoT-AIS system	General focus on IoT applications in healthcare
Transmission Rate	Transmission rate presented for IoT-AIS system	Not explicitly discussed in research papers
Energy Usage	Energy usage data provided for IoT-AIS system	Not explicitly discussed in research papers
Overall Conclusion	IoT-AIS offers data security and performance metrics	Research papers focus on IoT applications and potential benefits

4. CONCLUSION

This study has presented the IoT-AIS (Internet of Things with Artificial Intelligence System) as a robust solution for securing the transmission and collection of patient data in healthcare settings. Through a comprehensive evaluation, we have found that IoT-AIS effectively addresses data security and privacy concerns, ensuring the reliable transfer of healthcare information The results have highlighted the system's strengths in terms of performance metrics. Notably, IoT-AIS exhibited faster response times compared to traditional networks, contributing to efficient data handling. The delivery percentage of packets showed consistent and reliable data transfer, emphasizing the system's stability. Moreover, the delay estimation results indicated that IoT-AIS effectively prevents partial malware attacks while maintaining efficient data access and transmission. This enhances the overall security of healthcare data, which is of utmost importance in medical settings. Furthermore, the system demonstrated superior throughput and bandwidth monitoring capabilities, making it a valuable asset for managing IoT networks in healthcare applications. The transmission rate and energy usage evaluations underscored the system's efficiency and potential for reducing resource consumption. The IoT-AIS system emerges as a promising technology for healthcare data management, offering improved security, reliability, and efficiency. Its performance across various metrics positions it as a valuable solution for addressing the challenges of data security and privacy in the rapidly evolving field of healthcare informatics.

REFRENCES

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)

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)

Amudha, G.; Jayasri, T.; Saipriya, K.; Shivani, A.; Praneetha, C.H.: Behavioural Based Online Comment Spammers in Social Media

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)

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)

Al-Dubai, A., Saboohi, H., & Al-Mayyahi, A. (2020). Internet of Things in healthcare: Applications, challenges, and opportunities in Iraq. 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). DOI: 10.1109/IOTSMS49694.2020.9234752

Khalil, I., & Al-Rakhami, M. (2021). Machine learning-based healthcare system for Iraq using Internet of Things. International Journal of Advanced Computer Science and Applications, 12(1), 48-55. DOI: 10.14569/IJACSA.2021.0120107

Hussein, S. H., Hameed, M. A., & Mohammed, S. S. (2019). Smart healthcare system based on IoT for remote areas in Iraq. 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM). DOI: 10.1109/WINCOM.2019.8953802

Saber, A., & Tawfik, H. (2020). A machine learning-based IoT healthcare system for rural areas in Iraq. 2020 3rd Scientific Conference on Electrical, Computer and Biomedical Engineering (SCECBE). DOI: 10.1109/SCECBE50682.2020.9342225

Jasim, Z. A., Al-Mayyahi, A., & Hussain, A. (2018). IoT-based healthcare system for remote patient monitoring in Iraq. 2018 International Symposium on Networks, Computers and Communications (ISNCC). DOI: 10.1109/ISNCC.2018.8531087

Ogudo, K.A.; Muwawa Jean Nestor, D.; Ibrahim Khalaf, O.; DaeiKasmaei, H.: A device performance and data analytics concept for smartphones' IoT services and machine-type communication in cellular networks. Symmetry 11(4), 593 (2019)

Liu, B.H.; Nguyen, N.T.: An efcient 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)

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)

Lakshmanaprabu, S.K.; Shankar, K.; Ilayaraja, M.; Nasir, A.W.; Vijayakumar, V.; Chilamkurti, N.: Random forest for big data classifcation in the Internet of things using optimal features. Int. J. Mach. Learn. Cybern. 10(10), 2609–2618 (2019)

Amudha, G.; Narayanasamy, P.: Distributed location and trustbased replica detection in wireless sensor networks. Wirel. Pers. Commun. 102(4), 3303–3321 (2018)

. Kimani, K.; Oduol, V.; Langat, K.: Cybersecurity challenges for IoT-based smart grid networks. Int. J. Crit. Infrastruct. Prot. 25, 36–49 (2019)

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)

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 SiO2 photonic crystals at diferent temperatures. Luminescence 31(1), 4–7 (2016)

Alabdulatif, A.; Khalil, I.; Yi, X.; Guizani, M.: Secure edge of things for smart healthcare surveillance framework. IEEE Access 7, 31010–31021 (2019)

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