Original Research Article

INTERNATIONAL JOURNAL OF ENGINEERING BUSINESS MANAGEMENT

International Journal of Engineering Business Management
Volume 17: 1–14

DOI: 10.1177/18479790251315317
journals.sagepub.com/home/enb
Sage

Wireless body area network: Architecture and security mechanism for healthcare using internet of things

Arun Kumar[1], Ritu Dewan[1], Wisam Subhi Al-Dayyeni[2], Bharat Bhushan[3], Jayant Giri[4], Sardar MN Islam[5] and Ahmed Elaraby[6,7]

Abstract

Internet of Things (IoT) enabled wireless body area network (WBAN) is a novel technology that combines medical, wireless, and non-medical devices for healthcare management applications. Indoor healthcare institutions, such as hospitals, may employ IoT devices to manage medical equipment, maintain inventory, and monitor patients. In addition to monitoring temperature, humidity, and air quality, IoT sensors may help prevent the spread of sickness. The data generated by small sensor devices need strong security methods for secure transmission over a public network. Security of the data sent from source to destination is handled by transport layer security (TLS) protocol and prevent message loss or reordering. The most difficult component of TLS is determining how to handle reliability. Low-power wireless networks employ the Datagram Transport Layer Security (DTLS) protocol to solve this problem. But if the Server is exposed to a malicious attack (i.e., flooded with ClientHello messages, the DTLS protocol may no longer serve the purpose) as it may lead to Denial-of-Service (DoS). The paper proposes an intelligent gateway-based verification and approval system to protect health data from IoT wearable devices, a key worldwide data security risk. Paper used Contiki Network Simulator for designing an advanced smart gateway-based constrained application Improved DTLS (CoAP I-DTLS) security protocol. To assess the effectiveness of the proposed work, the packet loss ratio is computed for the CoAP, CoAP-DTLS, and CoAP I-DTLS protocols. To assess the effectiveness of the improved CoAP I-DTLS, calculations are also made for data transfer and handshake time. Paper will also look at ways to increase security by integrating the CoAP I-DTLS protocol with the Secure Hash Algorithm (SHA-256) and utilizing Certificate Authority (CA) improvements. Evaluation parameters such as Packet loss ratio, Data transmission time, and Energy consumption average are considered and detailed simulation results have been presented.

Keywords

IoT, DoS, security, CoAP, healthcare

Date received: 15 January 2024; accepted: 2 January 2025

[1]Galgotias College of Engineering and Technology, Greater Noida, India
[2]School of Information Technologies and Engineering, ADA University, Baku, Azerbaijan
[3]Sharda University, Greater Noida, India
[4]Department of Mechanical Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, India
[5]ISILC& Decision Sciences and Modelling Program, Victoria University, Melbourne, VIC, Australia
[6]Department of Cybersecurity, College of Engineering and Information Technology, Buraydah Private Colleges, Buraydah, Kingdom of Saudi Arabia
[7]Department of Computer Science, Faculty of Computers and Information, South Valley University, Qena, Egypt

Corresponding author:
Wisam Subhi Al-Dayyeni, School of Information Technologies and Engineering, ADA University, Ahmadbey Aghaoghlu Str. 61, Baku AZ1008, Azerbaijan.
Email: wdayyeni@ada.edu.az

Introduction

A vital aspect of living is access to healthcare. Regretfully, the increasing age of the population and the corresponding increase in chronic illnesses are putting a great deal of stress on contemporary healthcare systems, since hospital beds, physicians, and nurses are in high demand. It appears that a solution is needed to lessen the burden on healthcare systems while still offering at-risk individuals high-quality care. The potential of Internet of Things (IoT) technology to relieve the burden on healthcare systems brought on by an aging population and an increase in chronic sickness has garnered significant attention in recent years. Since standardization is a major barrier to advancement in this field, this article suggests a standard model that will be used in IoT healthcare systems in the future. A big transition is necessary in healthcare to more scalable and cost-effective alternatives. The solutions to these issues involve redesigning healthcare systems to actively manage wellness rather than illness and putting an emphasis on early disease identification and prevention.[1] In order to deal with the rising costs of healthcare, the Internet of Things in healthcare applications has drawn the attention of numerous researchers in recent years.

Collecting physiological parameters like the heartbeat and body temperature is a crucial duty for such a system. One of the best technologies for creating discrete, scalable, and reliable IoT healthcare systems is WBAN. Sensor nodes that are structured make up a WBAN.[2] These sensors can be inserted beneath the skin, on the body, or in clothing. There is a wireless interface on the sensors. Body sensors gather data about the environment (the human body), which is then correlated for monitoring and/or actuation purposes, similarly to conventional wireless sensor networks. IoT advances are expanding quickly, having turned into an achievement progression in the computerized medical services area.[3] As indicated by,[4] today 50 million clinical gadgets are being used, and it is expected that by 2025 there will be more than 161 million of them associated around the world. This enormous extension of the IoT clinical gadgets market is because of the development of high-velocity organizing advances, and the expanding reception of wearable gadgets, cell phones, and other versatile stages in medical services. Notwithstanding, these gadgets are regularly portrayed by a serious level of heterogeneity, creating tremendous measures of wellbeing and wellness information in heterogeneous configurations.[5]

These days, scalability is a topic that must be covered while talking about IoT healthcare systems. Vernon Turner, senior vice president of enterprise systems at IDC, claims to know. By 2025, there will be 152,000 smart gadgets online per minute.[6] IoT solutions must expand significantly in order to accommodate this enormous number of linked devices. To put it another way, scalability is a crucial factor to consider when selecting an IoT solution supplier. Scalability guarantees that, as your company expands, your deployment will continue to be viable and secure. When growing IoT systems, there are a few basic obstacles to overcome. In addition to ensuring that your IoT solution can expand without problems, you also need to think about connection, device management, security, necessary certifications, and the availability of IoT devices. Data security and privacy are the primary concerns when deploying IoT in logistics and supply chains since many IoT device makers disregard even the most basic security standards for IoT systems.[7]

Many medical care associations bargain regularly with challenges in removing information from various types of clinical gadgets, influencing both patient consideration and clinical exploration.[8] By and by, this load of medical services associations is confronting numerous troubles in dealing with this load of colossal measures of information, mostly inadequate with regards to an incorporated information trade framework.[9] To trade in-formation with however many associations as would be prudent, interoperability is the main way for allowing frameworks to connect,[10] being considered as a need in the electronic medical care frameworks for settling in-formation heterogeneity issues. Major applications of IoT in healthcare are shown in Figure 1.

A key is a series of pieces that are utilized by the encoding calculation or calculations during the method involved with encoding and unscrambling the information.[11] A cryptographic key resembles a key for a lock; just with the right key would you be able to open the lock.[2] When sending scrambled information, TLS regularly utilizes a cryptographic hash capacity to guarantee information honesty.[12] The hash work keeps Charlie from altering information that Alice ships off Bob. A cryptographic hash is like a checksum. The smallest change to the message normally rolls out an enormous improvement in the subsequent hash. A cryptographic key doesn't require cryptographic hash work.[13]

Interoperability in the healthcare industry refers to an electronic health system's capacity to interact with other computers or software systems from different hospitals or healthcare providers in an easy and smooth manner. It permits the sharing and openness of health information across pharmacies, laboratories, clinics, hospitals, and hospices, going beyond simple interconnection. A strategic strategy with detailed steps is needed to ensure that healthcare information systems can cooperate effectively, improve data interchange, and ultimately improve patient care. WBANs use wireless sensor nodes attached to a human body to track various physiological parameters like BP, temperature and sugar levels. This is being done to make it easier for patients to have remote health monitoring. Both implanted and wearable versions of these WBANs are available. WBANs aim to provide medical personnel with

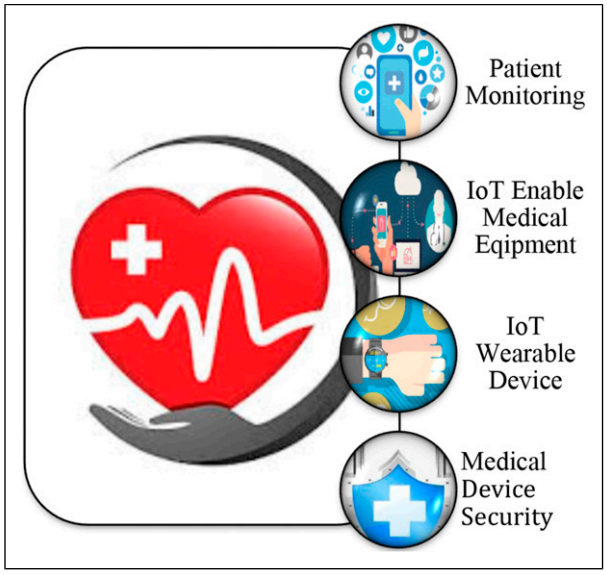

Figure 1. Applications areas of internet of things in healthcare domain.

insights into a patient's health status by strategically positioning sensors on the body to transfer bodily information to data servers, ultimately aiming to protect human well-being.[14]

These technologies greatly benefit both medical boards and individuals during emergencies by providing functions such as monitoring, dispensing health information, enhancing data administration, managing home appliances, and transferring information. In the context of WBANs, this study paper attempts to examine different options that might extend the network's lifespan, reduce node energy consumption, and increase security and safety at the same time.[15] To put it another way, the paragraph underlines the significance of addressing both security and energy consumption concerns.[16] WBAN is a confined network that operates within, on, or around the human body. Sensor advancements, Micro-Electro-Mechanical Systems (MEMS), and wireless communication have all contributed significantly to WBAN advances. WBANs have proven invaluable in healthcare monitoring, medical, sports, and multimedia communication. However, the small size of the sensors and actuators necessitates significant energy consumption levels. WBANs provide the secure storage and delivery of patient information to healthcare providers while reducing the risk of data loss.[17,18]

Objectives, motivation, and contributions

The primary objective of paper is to strengthen the DTLS protocol's defense against Denial-of-service attacks. Put the suggested technique into reality using the Cooja simulator for Contiki OS to demonstrate its practicality. The recommended DTLS's performance was assessed and contrasted with that of the conventional DTLS protocol in terms of DTLS Handshake Run-Time and energy consumption. To assess the success of the proposed task, the packet loss ratio is computed for CoAP, CoAP-DTLS, and CoAP I-DTLS. Data transit and handshake timings are also monitored to gauge how well the upgraded DTLS performs. The success of IoT devices in providing low power consumption, secure information, and cost-effective solutions to IoT networks for smart healthcare systems in emergency scenarios provided the inspiration for this contribution. Important contributions made by this article are:

a. It discusses the latest papers investigating the intermingling of smart healthcare with various IoT applications.
b. CoAP, CoAP-DTLS, and CoAP I-DTLS have been used for performance comparison and analysis.
c. To increase security, it suggests using a CoAP I-DTLS smart gateway system.
d. Evaluation parameters such as Packet loss ratio, Data transmission time, and Energy consumption average are considered and detailed simulation results have been presented.
e. To integrate the CoAP I-DTLS protocol with SHA-256 using optimizations from the CA to improve security.

The rest of the paper is organized as follows: Section 1 discusses how IoT works in the healthcare sector. In Section 2, a review of the literature is presented, and in Section 3, IoT healthcare architecture is covered. The suggested strategy or solution is presented in Section 4, and the findings and analysis are expanded upon in Section 5. Section 6 concludes the paper.

Literature review

Many researchers have developed IoT-enabled healthcare solutions. The main problem with IoT-based healthcare research is that it has been applied in a very limited context to connect a particular group of medical devices, like sensors and wearables, while ignoring many non-medical items, like those found in the transportation and security sectors, which are undoubtedly used in healthcare organizations.[19] Even if some crucial healthcare devices might not be able to connect to the Internet, communication between healthcare system nodes is exclusively relied on the Internet. It's possible that internet signals are unavailable in many isolated areas. The monitoring, security, and hardware design industries account for the majority of related work.[20]

Since an IoT-based wellness system gathers all of the weak person's information and transmits it to the network, which is accessible both locally and worldwide, a framework was created to address the main problems with the

structured engineering of the system.[21] It attempted to use the Contiki continuing working framework in this paradigm. The model included three levels, each of which had a certain capacity; in any case, the system came up short on the security foundation to consolidate the current managerial undertakings. The framework upholds a proficient person to examine the wellbeing data, even in the absence of the patient.[22] A few arrangements offer key situations for e-wellbeing applications. All things considered, this examination has given a vigorous strategy to consolidate undisclosed sharing plans and associating personalities to shape gatherings of people of patients experiencing a comparable infection.[23]

The gatherings are isolated into independent blocks, and the block division helps the square chief gather point-by-point data from patients' cell phones. Albeit the framework does not answer noxious trespassers, these intruders are not malignantly influencing the patients; all things considered, it helps the patients in antagonistic circumstances by sharing some delicate data about their security.[24] WBAN frameworks currently have advancements defeating limitations like force, handling, versatility, overseeing, and figuring by taking on distributed computing innovation. The fusion of WBANs with distributed systems upholds the medical services climate through continuous patient following and early infection recognition.[25]

Notwithstanding, this needs standard design, strategy consistency, regular information assortment, patient conduct on the board, medicinally coded passwords, information sharing, information exposure, information for the executives, and different information associations.[26] Reliable information correspondence assumes a fundamental part in IoT for solid information combination, information mining, setting mindful-based administrations, and client protection.[27] A method of talking about these worries is to hypothetically virtualize the IoT climate across the cloud and afterward interface every gadget with at least one cloud specialist.[28] To do this, an algorithm known as CoTAG (Cloud of Things Agent Grouping algorithm) was developed to group agents based on information about their dependability and reputation gathered by them. To test the efficiency and usefulness of this method, certain experiments were conducted in a simulated environment.[29]

In Ref. 30, two important characteristics are examined for the optimum next hop selection while routing medical data packets to the BS. Each on-body sensor has its own link quality and energy usage rate determined. The next hop is a sensor with good connection quality and residual energy. The limitations of this technique include restricted criteria for determining the next hop and a lack of suitability for transmitting sensitive data. An improved health monitoring mechanism was implemented in Ref. 31. This work includes cluster members, cluster chiefs, and core networks. In this study, the cluster head is selected by introducing three optimization algorithms: ant colony optimization, multi-objective particle swarm optimization, and the complete learning particle algorithm. The chosen cluster head serves as a link between the core network and the clusters. This work uses a cluster head as a gateway between the core network and members in clusters, which influences the QoS limitations in terms of latency and throughput.

A secure healthcare monitoring strategy[32] is used to monitor and operate the smart healthcare system. To create a safe technique, the authors combined two AI algorithms: a fuzzy system and neural network classifiers. It determines the data's priority level depending on the information obtained from the sensor. The GSM module sends sensor data obtained from the patient's body to the Azure IoT hub. Ref. 33 presents a safe certificateless biometric authentication method for WBAN that includes group key management. However, the coordinator node is critical in gathering medical data since it serves as the personal controller for each WBAN. The biometric component utilized for authentication is electrocardiogram (ECG) recordings. Then, group key management is carried out for all verified sensor nodes in the WBAN. The lack of security and privacy caused by ECC and the one-way hash function make it unsuitable for resource-constrained IoT devices.

Ref. 34 presents a two-level lightweight technique for identifying anomaly data from huge sensor readings. First, the game theory technique is used to identify the spatial correlation of sensor data and the dynamic changes in the WBAN. Second, the Mahalanobis distance is shown in the local processing unit (LPU), which provides a global perspective on the multivariate analysis. Overall confidence in sensors is quite low, and defect detection consumes more energy.

The authors of[35] proposed a secure architecture for WBAN-IoT in healthcare systems. This work employs five layers, namely, the collection of the data layer from the WBAN sensors to the gateway agent, the second layer is responsible for data routing to the local gateway server from the gateway agent, the third layer is responsible for data routing to the distant server, and the fourth layer is responsible for data routing to the fog layer, where controllers are deployed to provide data security and classify the data as critical and noncritical. Finally, all data is kept in a private cloud. This work secures the data in the fog layer; nevertheless, the authenticity of the users was not addressed, resulting in security issues and numerous assaults in the networks. The authors of[36] demonstrated a WBAN design with dual sink nodes. Clusters were established based on LoS and NLoS, followed by the placement of two sinks. The primary goal of this article was to reduce the energy usage of the network. After the data is sensed, essential data is transmitted immediately to the sink, while periodic data is routed to the subsequent forwarders. All sensors put on a patient are given equal time periods, which must be slotted

based on the node priority. The intermediary cooperates with the client from one viewpoint and with the administrations on the other.[37]

Data security, pricing, memory, scalability, trust, and openness amongst platforms are all concerns that the smart health architecture must address.[38] Since user identification is uncertain in the open internet environment, it is essential to manage data integrity and privacy. An assembly of electronic medical devices and software that can enhance patient care is known as the Internet of Medical Things (IoMT).[39] The project's objective is to make remote patient data collection utilizing the CoAP more secure. Different techniques may be used to protect these sensor networks. For communication between multiple IoMT devices and a remote server, the secure CoAP is compatible with the DTLS protocol for establishing a secure session utilizing current techniques like lightweight establishment of secure session. However, there are concerns with key control, session establishment, and multicast message exchange with the DTLS layer of CoAP. These networking protocols are very vulnerable to intrusion. The authors argue that the distributed approach, in which IoT devices employ powerful gateways attached to them, may not be sufficient, and that the controller's access control decisions make the security of CoAP messages more efficient and can help prevent DDoS attacks. Subsequently, auhos implemented a software-defined networking scheme to authorize the messages over the CoAP protocol.[40]

Many studies have been done to find solutions to these security problems in various IoT sectors. Using two popular IoT protocols, CoAP and MQTTT, his paper offers a security architecture for real-time health monitoring systems that ensures the privacy, accuracy, and reliability of data. As sensor data is continuously communicated through the layers, this security framework uses HTTPs to shield it from security issues. As a result, it offers an extremely low-risk defense against the breach.[41] Numerous studies evaluate the CoAP protocol's performance and security on the commonly used Raspberry Pi 4 as an Internet of Things endpoint. The research used strict performance criteria, such as CPU, memory, and latency, in conjunction with a comprehensive security analysis that concentrated on vulnerabilities at the network level. Theoretical and practical methods are employed to arrive at conclusions.

The study's conclusions shed light on whether CoAP is appropriate for Internet of Things installations on Raspberry Pi 4s and make suggestions for improving security and functionality.[42] The careful examination of putting CoAP into practice revealed that, while employing several threads to move data via sockets can even boost the total throughput of some known systems, it also limits the potential of others, as demonstrated by the Micro benchmarks. The server may select the right number of thread-lines for a fixed platform by wrapping the receiving and sending operations into their own distinct stage, all without significantly influencing the other stages. Moreover, it operates on top of the UDP or DTLS protocols when security mode is enabled, and it employs a brand-new, ultra-sleek binary number format. It even permits multicasting connectivity and communication.

Replica flow identification and dependable digital message delivery are provided by the sub-layer of the digital messaging level.[43] The Datagram Transport Layer Security (DTLS) protocol is used to secure CoAP communication. The DTLS implements a handshake procedure to create a secure connection and negotiate the same cipher suites before initiating a secure transmission. On the other hand, DTLS is susceptible to DoS assaults. The DTLS cookie exchange procedure was unable to manage the DoS assaults during the handshake mechanism. This study proposed an improved DTLS Handshake authentication technique that lessens the vulnerability to denial-of-service attacks. The outcomes were assessed in relation to elapsed time, energy efficiency, and handshake time. In order to simulate the proposed mechanism, simulation is performed using the Cooja simulator and Contiki-NG operating system.

The literature review covers relevant work based on factors such as efficiency, environmental surveillance, secure transmission, speed, and service quality (QoS). All of the solutions discussed above are designed with certain features in mind. As a result, this article focuses on the CoAP I-DTLS protocol for smart healthcare, which will provide the greatest security, less packet loss ratio and less energy consumption.

Proposed architecture

The upgraded smart gateway-based CoAP I-DTLS is shown in Figure 2. The suggested approach is expanded with the use of typical Datagram TLS. Authentication and authorization are often initiated between the client and server. However, it is possible that an attacker or malicious user will send a number client greeting message in order to compromise the server and get access to important health data. To address this issue, a variety of smart gateways are employed in improved CoAP I-DTLS to establish a connection between the client and server. Traditional CoAP I-DTLS is done between the client and gateway rather than the client and server. After successful login and authorization, a session update is utilized to connect to Gateway. This suggested work focuses on preserving ongoing monitoring of an individual's physiological circumstances, such as healthcare data on heart rate, perspiration, ECG, breathing rate, skin temperature, blood pressure, and heart sound. The IoT wearable devices in this architecture continuously provide clinical data to doctors. When physiological indicators such as heart rate, ECG, respiration rate, perspiration, skin temperature, blood pressure, and heart sound exceed normal levels, IoT devices transmit a clinically relevant alarm message to other caregivers and doctors.

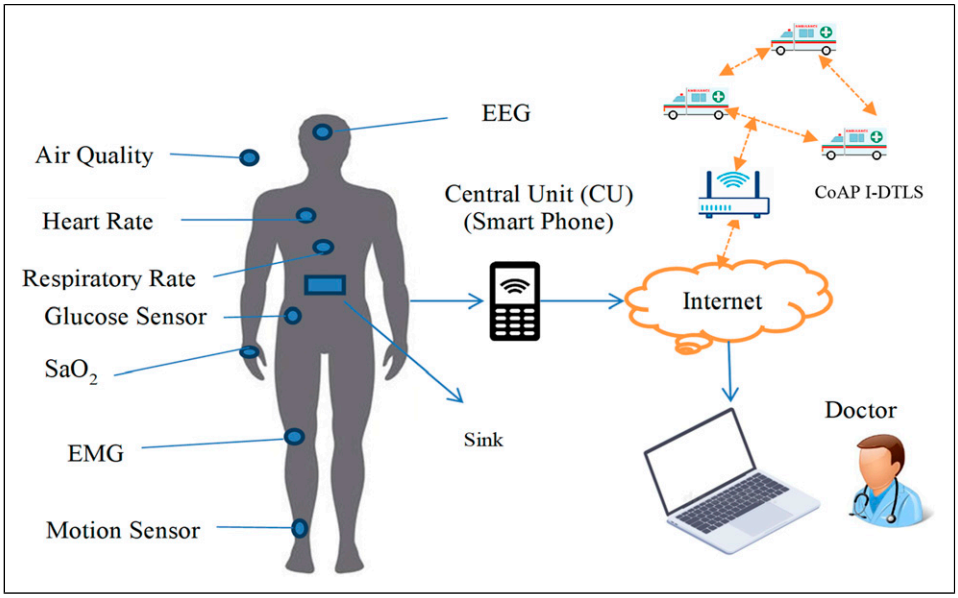

Figure 2. Architecture for health care using the internet of things.

WBAN innovation has been progressively utilized in medical care. Various clinical gadgets are utilized or embedded and coordinated into the WBAN to screen patient wellbeing and treat patients with robotized treatments, and that's just the beginning. These frameworks should ensure information during assortment, transmission, preparing, and putting away]. A WBAN gadget is comprised of keen, low-controlled sensor hubs. WBAN is a remote organization made out of associated sensors equipped for ascertaining and assembling information on a client's wellbeing circumstance. The sensors can be worn on various parts of the body and held beneath the skin by the patients.[44] Sensors placed in distant body region organizations can monitor a patient's mental state, and the data gathered by these sensors is subsequently communicated to doctors and medical clinics.[45] The interchange of health-related data between human body sensors and the medical services monitoring system must be encoded for the patient's vital data to remain safe and private while being transmitted over the network.

Sensors collect data from the environment and then transmit it to a company or the cloud, where it is analyzed and important decisions are made. In the field of medical services, even the smallest advancement in a patient's data might result in passing or real outcomes. Actual security and virtual security are two more comprehensive divisions of security. Real IoT security controls cutting-edge technology like equipment and sensor devices. It is interesting how virtual security controls a person's virtual adversary across a wired or remote connection. It is challenging to adjust to the second type of safety because attackers or sniffers seek to modify the information while they are sitting on the communication channel. Due to the identical functionality of all Internet-connected devices, it is crucial to boost system security and offer end-to-end protection, whether this is accomplished by installing sensors at entryways, opening doors to the cloud, or tying the cloud to healthcare providers. Electrocardiogram (ECG) of a wild-type (WT) man derived from DII, displaying measurements of wave amplitudes and durations transferred to WBAN cloud.

IsoDAM8 amplifiers from WPI, Aston, UK, were used to amplify DII derivation recordings with a bandwidth of 1–500 Hz, and a Gould oscilloscope (20 MHz, model 1421) was used to continually examine the results.[46] Both patients and medical professionals greatly benefit from WBAN. This network may be used to monitor the patient's condition remotely. Each node in a WBAN is independent and equipped to find an appropriate path for data transmission at a distant site. The WBAN node may link to the internet for data transfer. The healthcare sector is becoming more effective and technologically sophisticated thanks to the usage of information technology. WBAN was developed with consideration for medical systems and emergency situations. The network's small sensor nodes in these situations gather crucial data from the body and transmit it to the hospital's medical server. A doctor or medical professional at the hospital then examines this material to determine the diagnosis. Communication in the WBAN is secure because this network employs physiological values (PVs), which are private pieces of human data.[47–52]

Methodology

Contiki is a low-power operating system for the Internet of Things. Cooja is a knockoff of a Contiki firm. Contiki is a

memory-required, well-structured operating platform for low-power distant Internet of Things clients. Road lighting systems, delicate structural sound control, radiation monitoring, and warnings all make use of Contiki. Additionally, a simulation environment may be used to construct the remainder of the framework in the future. CoAP I-DTLS is a protocol designed for usage by IoT nodes in resource-constrained internet networks. CoAP is designed to automatically transition to HTTP for ease network integration while maintaining particular characteristics such as multicasting, minimal overhead, and usability CoAP I-DTLS communicates in two ways: requests and answers, using a basic binary base header format. Options in an appropriate Type-Length-Value format can be sent to the base header. CoAP I-DTLS is designed to be coupled to UDP and, optionally, DTLS, ensuring a high level of communication security. Now the simulation begins, and ping may be conducted in a fresh terminal for each node address in the network.

Table 1 lists the simulation parameters. In this paper, the suggested model, as shown in Figure 3, consists of five sensor motes, four of which serve as sensors (in yellow) and one of which serves as a border router (in green). There is some distance between all sensors, like the distance between sensor 1 (border router) and sensor 5 is 45 cm. Then, via an IPv4 or IPv6 connection, the border router sends this information to the internet, where anybody may read the value of the Contiki Operating System (OS) sensor using any digital device such as a mobile phone (M) or a computer. The recommended simulation uses the OS and its integrations in smart healthcare systems to collect and provide information. The CoAP I-DTLS protocol is used in this suggested model to simulate the network and collect data from network nodes. In some scientific archives, this data can also be saved for later research. Massive volumes of data are processed using it as well.

Ongoing use of the Cooja simulator system is made to display the suggested design. Another essential tool is the power tracer, which is accessible from the Tools menu under the heading duty cycle of motes. This technique allows us to gauge the amount of force used both collectively by all Sky motes and individually by each mote within the organization. These estimations are shown in the subsequent Table 2. We learn about the force applied to each hub, the force applied to each mote's transmission cycle (Tx), receiving cycle (Rx), and the typical yield. Sky Mote is powered by a Texas Instruments MSP430 low-power microcontroller with an 8 MHz clock speed, 10 KB of RAM, and 48 KB of flash memory. In addition to sensors for humidity, temperature, and light, it contains a Chipcon Wireless Transceiver with 250 Kbps, 2.4 GHz, IEEE 802.15.4, 16-pin expansion capability, and an optional antenna connector. Integrated onboard antenna used with the 50-m range in the sensor device.

Table 1. Simulation Contiki settings.

Item	Description
DTLS library	TinyDTLS0.8.1
Simulator	COOJA
Computer	RAM 8 GB
Data size	21 bytes (GET/.well-known/core)
Simulator	Cooja (MSPSim)
OS of sensor	Contiki 2.7
Network feature	RPL/IPv6/UDP
Measuring function	msp430-gcc (in ubuntu)
Sensor device	5 sky motes
Networking environment	Mesh
Node distribution	Randomly

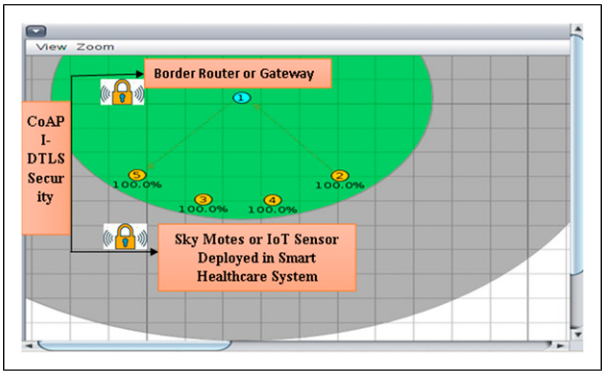

Figure 3. Proposed simulation scenario in Contiki Cooja.

The basic CoAP I-DTLS features include a Real-Time Publishing Subscription (RTPS) service. The CoAP I-DTLS architecture is decentralized to offer a high degree of stability and low-latency data access for essential IoT applications. The RTPS protocol employs discovery module data readers, data authors, and themes to reveal preconfigured QoS and security protocols, as well as current domain participant information. A domain member is newly created. Definitions can also be omitted when network or system services are restricted from exploration announcements (see Figure 4).

Length of bit size in SHA-1 is 160 bit and in SHA-256-bit size is 256. Because of its smaller bit size, SHA1 is more vulnerable to attacks and SHA1 has been deprecated due to security flaws. SHA256, which is more secure and reliable, uses a Public Key Infrastructure (PKI) where X.509 v3 certificates, signed by a trustworthy shared Certificate Authority (CA), are authenticated by communicating parties. DTLS uses approvals and governance manuals defining the right of access within the entire Domain to specific themes and general security policies. Thus, the IoT technology's SHA-256 Cryptographic Hash Algorithm generates hashes for secure access, which are

Table 2. Power tracing of Tx and Rx anteena.

Motes	Radio Tx (%)	Radio on (%)	Radio Rx (%)
Sky mote 1 (border router)	0.55	94.62	0.28
Sky mote 2	0.31	1.17	0.04
Sky mote 3	0.56	1.70	0.03
Sky mote 4	0.29	1.15	0.04
Sky mote 5	0.04	0.82	0.03

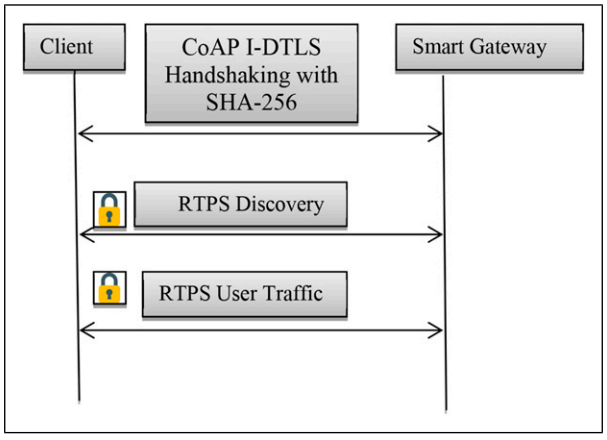

Figure 4. CoAP I-DTLS handshaking real-time publishing subscription.

primarily used for verifying data and message integrity during transactions, session time, data identification, and password verification.

A Sleeping End Point (SEP) is a special form of the system allowed by CoAP I-DTLS that spends a significant portion of its lifespan disconnected from the network, largely to conserve energy, or simply because it does not store the energy needed for its service. Nonetheless, in the same restricted RESTfull environment, it owns and hosts a collection of services and wants to make them accessible to the other participants. In this respect, the processes that allow it to operate within its limitations must be built and enforced, and its services must be accessible as if it were an ordinary, always linked, CoAP I-DTLS server. The Central Smart Gateway (SG) is the second related CoAP I-DTLS mechanism. Mirror servers can often be used on behalf of mobile devices for mirror services, which, due to their flexibility, often alter their Internet endpoint. Figure 5 demonstrates the configuration of a mirror server. SEP will start by registering it's to be mirrored resources with the mirror server via a POST request. From then on, sleeping endpoints will serve as clients of the CoAP I-DTLS. They upgrade their services to the mirror server via CoAP I-DTLS PUT requests and can request updates to the mirror server via CoAP I-DTLS POST requests.

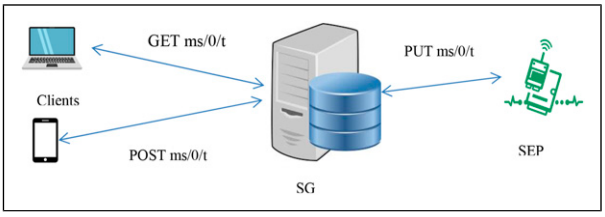

Figure 5. CoAP I-DTLS mirror server: clients and G.

Data aggregation methods at border routers have a significant optimization goal of reducing energy consumption, which may be accomplished by reducing the mandatory communication burden of routing. Applying data aggregation is an effective technique to boost the energy efficiency of smart healthcare networks as both the number of IoT sensor devices and the volume of transmitted data grow.[53] Using a mathematical model, consider how information is obtained in the system here in line with the guiding convention. Reinforcement Signal (RS) is the total number of data packets received at border router (node j) throughout time t.

$$R_{ateip_j} = P_{AN} + P_{AM} \tag{1}$$

R_{ateip_j} is the rate of input packets, while P_{AN} is the total amount of data packets that the preceding nodes gathered along the routing process. P_{AM} is used to represent the number of data packets that are not combined from earlier nodes along the routing process.

$$RS = 1 - \frac{1}{R_{ateip_j}} \tag{2}$$

PA_{gg} probability of aggregated by IoT nodes) varies as

$$PA_{gg} = PA_{gg} + \alpha \times \left(1 - PA_{gg}\right) \tag{3}$$

Where α is the action of Automata and if a bonus is received by the node, PA_{gg} will be as

$$PA_{gg} = (1 - \beta(1 - R))PA_{gg} \tag{4}$$

Here, penalty coefficient is β (input set of automata), Packets obtained at node j over time t is

$$N_{APack_j} = \sum \mathrm{i} = 1 \mathrm{degree}\, N_{PK_i} \tag{5}$$

$$T = 1 - \frac{1}{N_{AP_j}} \quad (6)$$

For the processing of data from many network sources, data aggregation is a crucial component of wireless routing. It gathers data from the sensor, reducing the amount of delivered data and removing data redundancy. As a result, it preserves the IoT sensor nodes' strength.

Contiki cooja tool activates the shrewdness of the energy utilization with data transmission for packet loss calculation throughout the reception, the transmission, the CPU cycles, and in the low power mode, based on time spent in the modes t_{RX}, t_{TX}, t_{CPU} and t_{LMP} respectively, as:

$$E = UI_{RX}t_{RX} + U\mathrm{t}_{TX}\,t_{TX} + UI_{CPU}t_{CPU} + UI_{LMP}t_{LMP} \quad (7)$$

Where the voltage (U) and values of the currents (I) in various modes are acquired from the specialized determinations by summarizing the current of the microcontroller.

The t_{CPU} Value was determined by monitoring CPU use time for various t values and then with basic linear regression to determine the value that corresponded to the communication session alone. Finally, the time spent in low-power mode was estimated to be as follows:

$$t_{LMP} = \mathrm{t} - t_{CPU} \quad (8)$$

The handshake procedure for CoAP I-DTLS is shown in the illustration in Figure 6. Multiple CoAP I-DTLS messages can be combined into a single set of messages to simplify network packet utilisation. In the diagram, the horizontal arrows represent these groups of messages. The process is started by the CoAP I-DTLS client by sending the ClientHello message, to which the server replies with a HelloVerifyRequest message. A stateless cookie created for DoS risk mitigation is contained in the HelloVerifyRequest message, and the client is required to repeat this cookie in its following ClientHello message. The ServerHello message is sent after the server successfully validates the cookie. These messages help the client and server communicate while developing security enhancing features. All the following are established: cypher suite, compression mechanism, protocol version, and session ID (used for session restart). Additionally, two random values—one for the client and one for the server are generated and exchanged.

The agreed-upon improvements in security capabilities determine the order of handshake communications. The diagram's messages marked with an asterisk (*) are either optional or reliant on the context. The graphic depiction shows the message exchange for a certificate-based encryption scheme. Messages like Certificate, ServerKeyExchange, CertificateRequest, and ServerHelloDone are included in the server's reply. When the cypher suite requires server authentication, the server transmits its X.509 certificate via the Certificate message. A

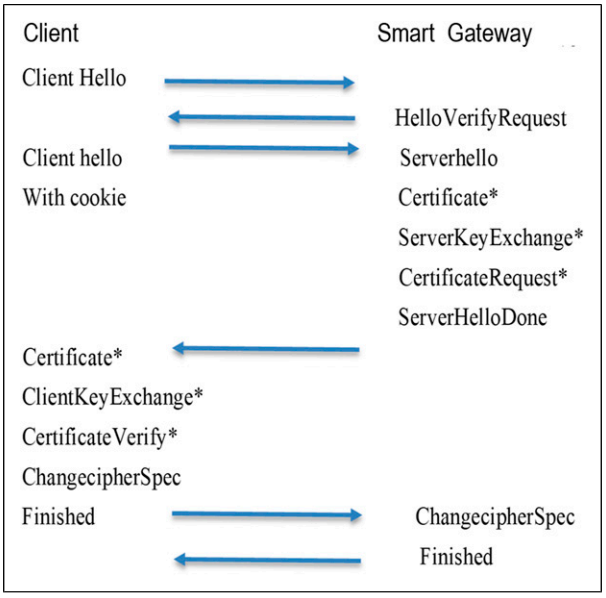

Figure 6. The full CoAP I-DTLS handshake.

ServerKeyExchange message could be sent if the key exchange skips using a server certificate. The server could alter-natively send a CertificateRequest message to the client to start the certificate acquisition process. The server then sends a ServerHelloDone message to end the hello-message portion of the handshake.

Smart e-health gateways include a local database that enables them to temporarily store medical sensor data, do local processing, and obtain clearance as an embedded server, in contrast to standard gateways and delegation servers. The verification and approval tasks of a centralized server can be made decentralized and controlled by intelligent e-health gateways by utilizing the properties of these gateways.[54] With this strategy, individual smart e-health gateways can manage remote endpoint authentication and authorization across various smart medical environments' sub-domains or rooms. The potential impact of a DoS attack or compromised smart e-health gateway is restricted to the medical sub-domain.[55] In this paper, initially intend to reuse existing security protocols in order to offer authentication and authorization across many network domains in the proposed architecture. Second, paper strive to give medical devices with limited hardware resources the security context they require to properly connect with a distant healthcare institution.[56–59]

One more attack, A sophisticated, ongoing cyberattack known as an advanced persistent threat (APT) occurs when an attacker sneaks into a network and remains there for an extended amount of time with the goal of stealing confidential information. APT attacks are meticulously prepared and intended to sneak inside a particular company, circumvent security protocols, and go unnoticed.

Unfortunately, a company cannot be adequately protected against an APT assault by typical security measures like firewalls, defense-in-depth, and antivirus software. To thwart any assaults, sophisticated persistent threat detection systems must be employed, utilizing the most recent threat signatures and threat methods on the manipulating threat actors.

As seen in Figure 7, a full handshake starts with a ClientHello message that contains the connection's credentials. During the handshake, this message is used to calculate the pre-master secret key. On Flight 3, a ClientHelloVerify cookie is present. The ServerHello message, the first message in Flight 4, contains the agreed-upon cypher suite. It also includes the random value generated by the smart gateway during the handshake, which is utilized to create the master secret key. The supported cypher suites of the end user provide the foundation for the mutually agreed-upon cypher suite. For Flight 4, the message ServerHelloDone signifies the end of communication. The end certificate is the first message of flight 5 if mutual authentication is utilized. The master secret key is calculated in ClientKeyExchange using the user-provided additional parameters. Throughout flight 6, gateway transmits its own ChangeCipherSpec and Finished signals. The final communications are used by both peers to send and receive data from apps that are correctly encrypted. Contrarily, the smart e-health gateway uses certificates or an application-level password to authenticate with the remote endpoint following the DTLS handshake.

Results and discussion

IoT has a favorable effect on healthcare, enhancing millions of people's lives. It finds illness and conducts a thorough analysis of the healthcare system. It offers personalized attention to each person for their benefit. IoT de-vices may remind patients about appointments, activity checks, calorie counts, blood pressure, disease states, and much more when employed in medical crises. The Internet of Things (IoT), which is supported by cutting-edge technology, has a surprising capacity to produce better results. Innovative concepts that improve patient care and allow for precise surgical interventions are put into practice when they lead to significant improvements in the field of medicine. Even in the face of the ongoing pandemic's difficulties, complex situations can be smoothly managed and digitally supervised. IoT helps to build first-rate support services for medical professionals, such as doctors, surgeons, and patients, by solving new issues in the medical field.

The traditional I-DTLS is performed between the customer and entryway rather than customer and server. Small DTLS 0.8.1 was picked for library capacities, and Contiki 2.7 is picked to demonstrate the complete work. By and large, MSPSim is additionally named as Cooja test system.

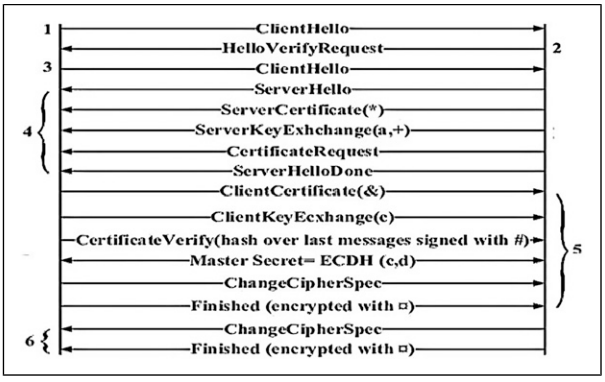

Figure 7. Full handshake between CoAP I-DTLS server and client.

The bundle misfortune proportion is determined for the CoAP, CoAP-DTLS, and CoAP I-DTLS. Similar outcomes are shown in Figures 8–10 with Packet loss ratio at a time out of 20 s, 40 s, and 60 s respectively.

Data is routed along the shortest path, which increases network capacity and promotes a longer network lifetime. Equation (9) gives the estimated PDR as

$$PDR = \frac{Packet\ Received\ (\mathrm{Pr})}{Total\ Packet\ Sent\ (Pts)} \times 100\% \qquad (9)$$

Furthermore, data transmission is computed to assess I-DTLS efficiency. When compared to other security protocols such as CoAP and CoAP-DTLS, the CoAP I-DTLS protocol performed better, as demonstrated in Figure 11.

Figure 12 shows the energy consumption rates of the three protocols such as CoAP and CoAP-DTLS and CoAP-DTLS. The energy spent by sensing, communication, and processing activities is utilized to estimate the average node energy consumption. The simulation duration and average energy consumption rates are shown by the x- and y-axes, respectively. The suggested IoT-enabled healthcare architecture's energy usage is lower than that of traditional healthcare architecture.

Healthcare has been greatly impacted by IoT, which improved the infrastructure and information system during the COVID-19 Pandemic. It enhances hospital administration and medical procedure digitization. New medical applications are made available as more gadgets and instruments are connected to the internet. Several inter-net-connected patient devices are being introduced in an effort to monitor patient health more effectively. It alerts the public to problems with public health by monitoring climate change. The hospital can function efficiently during the COVID-19 Pandemic because to this technology. It offers verifiable information, which greatly aids in drug monitoring. This result can be explained by the availability of alternative coverage technologies that enable interactivity

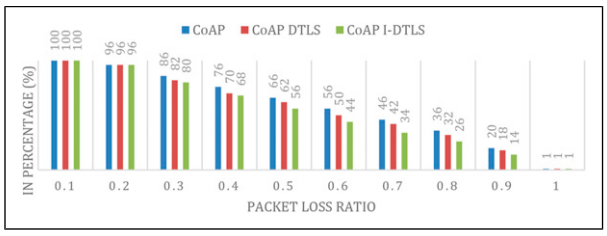

Figure 8. Packet loss ratio at a time out 20 s.

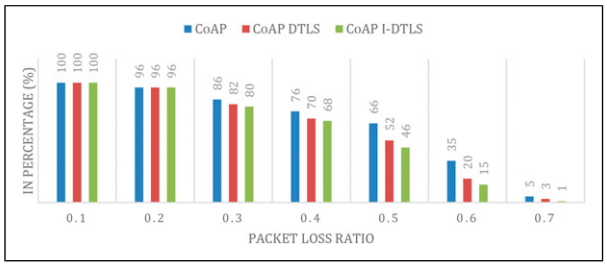

Figure 9. Packet loss ratio at a time out 40 s.

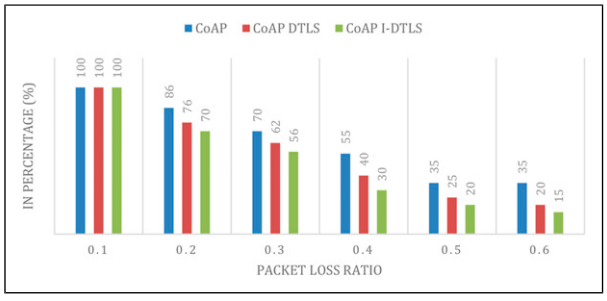

Figure 10. Packet loss ratio at a time out 60 s.

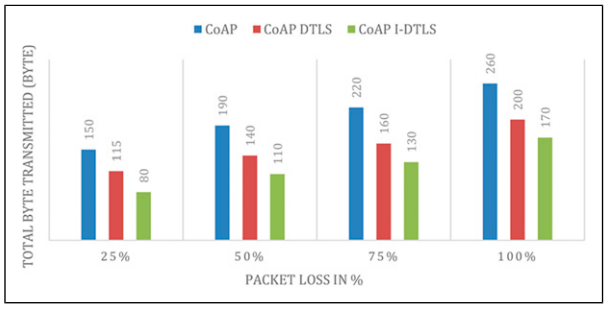

Figure 11. Data transmission.

amongst all medical equipment in an IoT-enabled healthcare architecture. As a result, compared to traditional design, the transmitted data is dispersed among a larger number of devices. As a result, the amount of each device's sent data is reduced, resulting in lower energy consumption rates. Furthermore, the prioritized component's ability to reduce

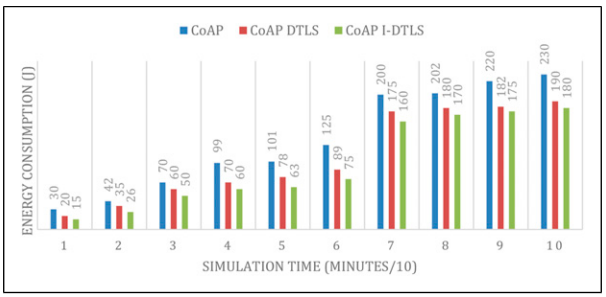

Figure 12. Energy consumption average.

the quantity of processed data is an essential aspect that has a beneficial impact on energy consumption rates. Because of the growing data processing requirements, the energy consumption rates for both healthcare systems have grown over time.

An IoT healthcare system prototype was detailed in this study. The CoAP I-DTLS routing protocol was proposed in the paper. The neighbor discovery procedure gathers and stores the movement and energy data of the neighbor Coordinators. To choose the most appropriate neighbor to forward the data to, CoAP I-DTLS forwarding is used. According to the simulation results, in comparison to the other three routing protocols, the suggested protocol performs better. With the aid of the data gathered and monitored by the sensors, the CoAP I-DTLS protocol, which offers a high level of communication security in our proposed work, will be employed to help achieve energy efficiency. In contrast to other studies, the proposed protocol has developed a system that uses IoT sensors to monitor physiological metrics like respiration rate, sweat, skin temperature etc. The user of the system we are developing will have direct access to sensor data and will also need to follow the device guidelines in order to take any actions.

Conclusion

This paper describes how IoT technology can be utilized to build smart healthcare systems and smart systems that will boost as well as maximize the accuracy of expected results. As a result, the Internet of Things and sensor networks have enormous potential to free up doctors and improve disease detection. In recent years, security and privacy in healthcare have emerged as major concerns. Several academics have created a variety of authentication and authorization techniques to avoid and secure sensitive data obtained using wearable IoT devices. However, end-to-end security solutions are required to prevent and regulate access to health data. TLS is a well-known protocol for reliably transferring data from source to destination. The primary function of this protocol is to ensure that no messages are lost or reordered. The challenge with this protocol is to accept unreliability. To

address this issue, the DTLS protocol is commonly used in current wireless networks. The technical issue with the DTLS protocol is that an attacker might send multiple ClientHello messages to a server. As a result, there is a chance of causing a DOS attack on the server. To address this issue, we suggested a smart gateway-based authentication and authorization solution that prevents and protects health data acquired from IoT wearable devices. In this study, smart gateway-based improved DTLS is shown using a Contiki-based network simulator. The performance of the upgraded DTLS protocol is compared to other security protocols as CoAP, HIP, and CoAP-DTLS. Based on extensive simulation testing, the proposed CoAP I-DTLS protocol beats earlier work by attaining the highest security and the best throughput with respect to consumption of energy. As future work perspective, work can be done to develop a more effective routing protocol that increases network efficiency rather than continuously moving the smart gateway location to add more nodes covering a larger area.

Author contributions

All authors contributed equally to the conceptualization, formal analysis, investigation, methodology, and writing and editing of the original draft. All authors have read and agreed to the published version of the manuscript.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Wisam Subhi Al-Dayyeni https://orcid.org/0000-0002-1859-9504

References

1. Atadoga A, Omaghomi TT, Elufioye OA, et al. Internet of Things (IoT) in healthcare: a systematic review of use cases and benefits. *Int J Sci Res Arch* 2024; 11(1): 1511–1517.
2. Nissar G, Khan RA, Mushtaq S, et al. IoT in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends. *Multimed Tool Appl* 2024; 83(33): 1–62.
3. Raj A and Prakash S. A privacy-preserving authentic healthcare monitoring system using blockchain. *Int J Software Sci Comput Intell* 2022; 14(1): 1–23.
4. Nguyen GN, Viet NHL, Elhoseny M, et al. Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with ResNet model. *J Parallel Distr Comput* 2021; 153: 150–160.
5. Arya V, Kumari M and Rana AK. Historical development of passive optical network (PON): a review. *J Opt Commun*. 2024; 9: 1–15.
6. Vats T, Singh SK, Kumar S, et al. Explainable context-aware IoT framework using human digital twin for healthcare. *Multimed Tool Appl* 2023; 83: 1–25.
7. Kumar M, Goyal N, Singh AK, et al. Analysis and performance evaluation of computation models for node localization in deep sea using UWSN. *Int J Commun Syst* 2024; 37(11): e5798.
8. Singh H, Rana AK, Giri J, et al. Automatic machine learning model for enhanced partition and identification of breast disorders in breast MRI scan. *Comput Methods Biomech Biomed Eng: Imaging & Visualization* 2024; 12(1): 2378734.
9. Dhawan S, Rana AK, Rana SK, et al. Internet of medical things devices: a review. In: *Convergence of deep learning and artificial intelligence in internet of things*. Boca Raton, FL: CRC Press, 2022, pp. 135–148.
10. Dewan R, Nagpal T and Rana AK. IoT based efficient and secure building architecture with constrained application protocol (CoAP). *Jes* 2024; 20(7s): 1456–1467.
11. Rana S, Bhuyan M, Kumar R, et al. Effect of nuclear deformation and orientation about the symmetry axis of the target nucleus on heavy-ion fusion dynamics. *Phys Rev C* 2024; 110(2): 024601.
12. Puri V, Kataria A and Sharma V. Artificial intelligence-powered decentralized framework for internet of things in healthcare 4.0. *Trans Emerging Tel Tech* 2024; 35(4): e4245.
13. Shen S, Huang L, Zhou H, et al. Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks. *IEEE Internet Things J* 2018; 5: 1043–1054.
14. Rezaeibagha F, Mu Y, Huang X, et al. Fully secure lightweight certificateless signature scheme for IIoT. *IEEE Access* 2019; 7: 144433.
15. Thumbur G, Rao GS, Reddy PV, et al. Efficient pairingfree certificateless signature scheme for secure communication in resource-constrained devices. *IEEE Commun Lett* 2020; 24(8): 1641–1645.
16. Zhou C, Zhao Z, Zhou W, et al. Certificateless key-insulated generalized signcryption scheme without bilinear pairings. *Secur Commun Network* 2017; 2017: 1–17.
17. Tripathy SS, Bebortta S, Mohammed MA, et al. An SDN-enabled fog computing framework for wban applications in the healthcare sector. *Internet of Things*. 2024; 26: 101150.
18. Prathaban BP, Subash R, Sathesh M, et al. Unleashing the leap toward secured IoMT environment in WBAN: a comprehensive review. In: *Security, Privacy, and Trust in WBANs and E-Healthcare*. Boca Raton, FL: CRC Press, 2024, 148–165.
19. Jha S, Nkenyereye L, Joshi GP, et al. Mitigating and monitoring smart city using internet of things. *Comput Mater Continua (CMC)* 2020; 65: 1059–1079.

20. Singh SK, Cha J, Kim TW, et al. Machine learning based distributed big data analysis framework for next generation web in IoT. *Comput Sci Inf Syst* 2020; 8: 105–119.
21. Nanayakkara M, Halgamuge M and Syed A. Security and privacy of internet of medical things (IoMT) based healthcare applications: a review. In: Proceedings of the international conference on advances in business management and information technology, Istanbul, Turkey, 24–25 May 2019.
22. Mohammed KI, Zaidan AA, Zaidan BB, et al. Real-TimeRemote-health monitoring systems: a review on patients prioritisation for multiple-chronic diseases, taxonomy analysis, concerns and solution procedure. *J Med Syst* 2019; 43: 223–237.
23. Sun Y. *Securing body sensor networks and pervasive healthcare systems*. Ph.D. Thesis, Imperial College London, London, UK, 2019.
24. Selvaraj P and Doraikannan S. Privacy and security issues on wireless body area and IoT for remote healthcare monitoring. *Intell Pervasive Comput Syst Smarter Healthcare* 2019; 40: 227–253.
25. Masood I, Wang Y, Daud A, et al. Towards smart healthcare: patient data privacy and security insensor-cloud infrastructure. *Wireless Commun Mobile Comput* 2020; 15: 1012–1023.
26. Ali T, Yasin S, Draz U, et al. Motif detection in cellular tumor p53 antigen protein sequences byusing bioinformatics big data analytical techniques. *Int J Adv Comput Sci Appl* 2018; 9: 330–338.
27. Choi J, In Y, Park C, et al. Secure IoT framework and 2D architecture for end-to-end security. *J Supercomput* 2018; 74: 3521–3535.
28. Yan Z, Zhang P and Vasilakos AV. A survey on trust management for internet of things. *J Netw Comput* 2014; 42: 120–134.
29. Fortino G, Messina F, Rosaci A, et al. Using trust and local reputation for group formation in the cloud of things. *Futur Gener Comput Syst* 2018; 89: 804–815.
30. Qureshi KN, Din S, Jeon G, et al. Link quality and energy utilization based preferable next hop selection routing for wireless body area networks. *Comput Commun* 2020; 149: 382–392.
31. Aadil F, Mehmood B, Ul Hasan N, et al. Remote health monitoring using IoT-based smart wireless body area network. *CMC-Comput Mater Contin* 2021; 68: 2499–2513.
32. El Zouka HA and Hosni MM. Secure IoT communications for smart healthcare monitoring system. *Internet Things* 2019; 13: 100036.
33. Tan H and Chung I. Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. *IEEE Access* 2019; 7: 151459–151474.
34. Arfaoui A, Kribeche A, Senouci SM, et al. Game-based adaptive anomaly detection in wireless body area networks. *Comput Network* 2019; 163: 106870.
35. Balakrishnan A, Kadiyala R, Dhiman G, et al. A personalized eccentric cyber-physical system architecture for smart healthcare. *Secur Commun Network* 2021; 2021: 1–36.
36. Ullah Z, Ahmed I, Razzaq K, et al. DSCB: dual sink approach using clustering in body area network. *Peer-to-Peer Netw Appl* 2019; 12: 357–370.
37. Huang H, Gong T, Ye N, et al. Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Trans Ind Inf* 2017; 13: 1227–1237.
38. Farooq SM, Hussain SMS, Kiran S, et al. Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5. *Electronics* 2018; 7: 370–377.
39. Tahir M, Sardaraz M, Muhammad S, et al. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. *Sustainability* 2020; 12: 6960–6969.
40. Alzahrani B and Fotiou N. Enhancing internet of things security using software-defined networking. *J Syst Architect* 2020; 110: 101779.
41. Dhanvijay MM and Patil SC. Optimized mobility management protocol for the IoT based WBAN with an enhanced security. *Wireless Network* 2021; 27(1): 537–555.
42. Biersteker S. *Evaluating security and performance of CoAP protocol on Raspberry Pi 4 for IoT applications*. Bachelor's Thesis, University of Twente, Enschede, Netherlands, 2024.
43. Arfeen NU, Iqbal Bangash J, Ahmed S, et al. Enhanced Datagram transport layer security protocol for IoT environment. In: Proceedings of 1st international conference on computing technologies, tools and applications, Peshawar, Pakistan, 9–11 May 2024, pp. 44–62.
44. Niu Y, Zhao K, Zhang X, et al. Review on DNA cryptography. In: International conference on bio-inspired computing: theories and applications, Zhengzhou, China, 22–25 November 2019, pp. 134–148. Springer.
45. Wang Z, Ren X, Ji Z, et al. A novel bio-heuristic computing algorithm to solve the capacitated vehicle routing problem based on Adleman–Lipton model. *Biosystems* 2019; 184(1): 1–9.
46. Erlache F and Dressler F. On high-speed flow-based intrusion detection using snort-compatible signatures. *IEEE Trans Dependable Secure Comput* 2020; 19: 1–12.
47. Chai X, Bi J, Gan Z, et al. Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Process* 2020; 176: 107684.
48. Mansouri A and Wang X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. *Inf Sci* 2020; 520: 46–62.
49. Bravo-Zanoguera M, Cuevas-González D, Vazquez JPG, et al. Portable ECG system design using the AD8232 microchip and open-source platform. *Multidisciplinary Digital Publishing Institute Proceedings*, 2019, vol 42, p. 49.
50. Rana AK and Sharma S. Contiki Cooja Security Solution (CCSS) with IPv6 routing protocol for low-power and lossy networks (RPL) in Internet of Things applications. In: *Mobile*

radio communications and 5G networks. Berlin, Germany: Springer, 2021, pp. 251–259.
51. Dhawan S, Gupta R, Rana AK, et al. Internet of medical things (IoMT) & secured using steganography for development of smart society 5.0. In: *Internet of medical things (IoMT) & secured using steganography for development of smart society 5.0*. Singapore: Springer, 2022, pp. 173–189.
52. Kumar A, Sharma S, Goyal N, et al. Secure and energy-efficient smart building architecture with emerging technology IoT. *Comput Commun* 2021; 176: 207–217.
53. Rana SK, Rana SK, Nisar K, et al. Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare. *Sustainability* 2022; 14(15): 9471.
54. Homaei MH, Salwana E and Shamshirband S. An enhanced distributed data aggregation method in the Internet of Things. *Sensors* 2019; 19(14): 3173.
55. Rana SK, Rana AK, Rana SK, et al. Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain. *IEEE Access* 2023; 11: 83289–83300.
56. Memon SK, Nisar K, Hijazi MHA, et al. A survey on 802.11 MAC industrial standards, architecture, security & supporting emergency traffic: future directions. *J of Industrial Inf Int* 2021; 24: 100225.
57. Rana SK, Kim HC, Pani SK, et al. Blockchain-based model to improve the performance of the next-generation digital supply chain. *Sustainability* 2021; 13(18): 10008.
58. Subashini S, Kamalam GK and Vanitha P. A survey of IoT in healthcare: technologies, applications, and challenges. *Artificial Intelligence and Machine Learning*. 2024; 22: 136–144.
59. Sharma N and Jindal N. Emerging artificial intelligence applications: metaverse, IoT, cybersecurity, healthcare-an overview. *Multimed Tool Appl* 2024; 83(19): 57317–57345.