A secured internet of robotic things (IoRT) for long-term care services in a smart building

Shih-Hao Chang1 · Chih-Hsien Hsia2,3 · Wei-Zhi Hong4

Accepted: 19 September 2022 / Published online: 13 October 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022, corrected publication 2022

Abstract
Long-term care refers to any support, both medical and non-medical, provided to the elderly with a chronic illness or disability due to physical or mental conditions. Since the cost of long-term care insurance is not inexpensive, low-cost devices and sensors can be used to create medical assistance systems to reduce human maintenance costs. The requirement of security and privacy under healthcare information protection is a critical issue for internet of medical things (IoMT) data transmission. In this paper, we designed an IoMT security robot for a long-term care system. The goal of this IoMT security robot is to provide secure transmission of the residents’ private information. It is composed of three layers, namely, collection, encryption, and transmission. The function of the IoMT security robot is to first collect data from the patient or the elderly, then provide efficient data encryption, and deliver secured data transmission mechanisms to send the valuable data to the cloud. This IoMT security robot also has a server authentication mechanism, and a support IoT and IoMT devices inspection function. Our evaluation results showed that even when we utilized a low power consumption device like Raspberry Pi, AES algorithm achieved an encrypt and decrypt of 100–100 K bytes under 9 ms, which is a lot better than ECC, which takes about 104 ms. Further, we found that the AES only takes 0.00015 s to decrypt 100 Bytes data, which is way faster than the ECC algorithm, which takes 0.09 s.
Keywords  Cybersecurity · Internet of medical things · Internet of robotic things · Long-term care · Smart building

1 Introduction

The global coronavirus pandemic, which started in 2019, otherwise known as COVID-19, took a great toll and has crashed the medical system worldwide [1]. COVID-19 outbreaks in long-term care (LTC) facilities resulted in devastating effects on the health and well-being of residents. The emergence of the pandemic created a huge need for even more hasty changes, which ushered in an era more akin to “revolution”. Due to the alarming growth of COVID-19 infection across the globe, conventional medical practices and technologies had to undergo drastic and immediate upgrading to battle and contain the pandemic. The internet of medical things (IoMT) has empowered remote resident consideration, improved clinic and pharmaceutical processes, and sped up information transmission.

The use of IoMT as a health monitoring system provides real-time observation through the use of smart health-sensing devices, artificial intelligence (AI), body area networks (BAN), and cloud technologies. IoMT operates by establishing a connection between physical, network, and application layers; and connects the infrastructure of medical devices, software applications, and health systems and services [2]. This enables the patient to transfer medical data through the internet, which helps reduce hospital visits, resulting in a patient-centric approach. The physical layer consists of the sensors and/or actuators used to collect vital health information from the patient via smart devices like watches and rings. It is a very helpful tool that serves as an early warning system to control the spread of infection by taking advantage of the IoMT functional components like data collection, storage, transfer, and analytics. IoMT is changing the way providers deliver care and how individuals can take control of their health at home to stop the spread of COVID-19.

Recent statistics showed that by 2050, the number of elderly people above the age of 60 will exceed 2 billion. Thus, there will be an even higher demand for nurse-aides in the future. Maintaining a healthy lifestyle at an advanced age is easier with external support from humans and devices. Smart building is one of the solutions to our lack of nursing homes, in which patients can be monitored and remain healthy while retaining a feeling of independence. A smart building may use a wide range of existing technologies and can be designed or retrofitted in a way that allows for the integration of future technological developments [3]. As shown in Fig. 1, IoMT sensors, building management systems, AI, and augmented reality are some of the mechanisms and robotics that may be used in a smart building to control and optimize its performance.

Many researchers have proposed long-term care monitoring systems that adopt existing equipment and technology. A previous study [4] suggested using RFID and WLAN to transmit data to mobile phones and record data. These wireless techniques integrated smart devices and internet and mobile applications, resulting in the emerging use of telemedicine and telehealth through IoMT. In another
study [5], the interconnections were improved to communicate effectively with controllers and network protocols. The application layer first takes the information from the physical layer, which is retrieved via the network layer, and then performs specified tasks accordingly. However, IoMT also has inherent drawbacks due to restrictive factors, such as device pairing and connection distance.

Within the conceptual framework and inherent drawback of IoMT, the internet of robotic things (IoRT) is concerned with the integration of smart space capabilities and autonomous agents (robots). IoRT operates by establishing a connection between the physical environment, internetworking, and application layers. The physical layer consists of sensors and/or actuators that collect vital health information from the patient via smart devices like smartwatches and rings. The robot can then connect to the internet and cloud from the IoMT sensors or actuators. IoRT is the enabler of collaborative robot and IoMT devices; as can be seen in a recent study [6], the authors have proposed IoRT-based architectural concepts to connect, share, and disseminate distributed computational resources, business activities, context information, and environmental data. However, issues such as optimization and security are challenges that are yet to be solved.

Since IoRT can be connected to long-term care or the cloud through the internet, insecure communication between users and robots could lead to cyber-attacks. Hackers can easily hack into an insecure communication link in no time. According to the 2020 CyberMDX report [7], nearly half of IoMT devices are vulnerable to exploits. Healthcare data’s average cost is 50 times more than credit card information, making them highly valuable on the black market [8]. The healthcare data involved in IoRT should be protected at various stages, including data collection, transmission, and storage. This, coupled with the fact that most IoRT applications often rely on diverse technologies with different embedded properties, each of which often has its own set of security issues, eventually led to many widespread IoT protocols missing basic security mechanisms [9, 10].
Security will always be a concern because the IoRT application area is evolving vastly and devices and services are vulnerable to attacks; thus, protecting the security of IoRT and healthcare systems has become a major concern. Meanwhile, IoT protocols are mainly designed to be energy efficient and capable of effectively handling node connectivity in complex ad-hoc environments where security comes as a major issue. Therefore, in this paper, the proposed IoRT system differs from other IoRT systems since it can affect patients’ lives and impose privacy concerns if patients’ identities are revealed. We envisioned a trusted IoRT security architecture that can provide an overarching guarantee that the correct security protections are always applied to each IoRT. We used this aforementioned definition of trust throughout this work. Our architecture aims to provide robust trust properties to a broad range of hardware platforms utilizing existing hardware and open-source software with reasonable performance overhead. Main cyber-security problems in IoRT arise due to some of the following reasons below:

- Confidentiality: Information is encoded and can only be accessed or decrypted by an authorized user with the correct encryption key. The lack of proper encryption on the side of the user can expose private and sensitive data to potential hackers.
- Integrity: This is described as data accuracy and consistency over the system’s entire life cycle and is a critical aspect of the design. Maintenance of the integrity of data in the IoMT network and IoRT mobile robots are vital and intruders that can get access to the programmable features and change them must be prevented at all cost.
- Authentication: Failure in guarding against unauthorized access can easily allow hackers to enter the robot and IoMT systems and use their functions from remote locations without using any valid username and password.

In this scenario, incorporating security modules in the design will definitely impact the performance. Therefore, the challenge is to overcome the issue of designing an efficient security module that should have high performance, be power efficient, and provide memory optimization. The remainder of this paper is organized as follows: a brief review of the background and related works is presented in Section II. The implementation issues for a long-term care setting are discussed in Section III. The IoMT-aided robotic system architecture is described in Section IV. The experiment testbed and evaluation results are explained in Section IV. Finally, conclusions and future work is presented in Section V.

2 Background and related works

Many researchers have proposed many interesting and implementable ideas to improve and adapt the traditional medical ecosystem into an IoMT ecosystem. These improvements were applied across the board- application, architecture, technology, communication, and security components [11]. The medical ecosystem framework is generally referred to as the open systems interconnection (OSI) model but with
relevant modifications made to incorporate IoT communication and technology. The technology in IoMT includes the hardware (firmware), middleware, and cloud platform (software). The medical ecosystem communication is the protocol used to interconnect IoT devices, either through short-range communication or long-range communication [12]. The medical ecosystem security involves vulnerability, attack, defense, and mitigation that highlights the advances in IoMT technologies, architectures, applications, and security. The previous works [13, 14] also incorporated security features, including security requirements, threat models, attacks, and risk management.

Past research [15] proposed a DiasNet Mobile, which is a personalized advisory service targeting telehealth. Telehealth is described as the use of data communication and information technologies, such as IoT and mobile devices, to access healthcare services remotely. They implemented this DiasNet by utilizing Bluetooth technology, which enabled a blood glucose meter through a mobile phone. This service allowed the estimation of a patient’s blood glucose level based on three factors: insulin, carbohydrate intake, and BMI (body mass index) measurements. Based on the estimated blood pressure, glucose, BMI, and waist circumference, the patient’s blood pressure classification and risk for diabetes and obesity can be approximated. Table 1 presents the classification of blood pressure and the risk for diabetes and obesity based on the measurement values for blood pressure, blood glucose, BMI, and waist circumference.

In a long-term care setting, the IoMT system involves the development, integration, and utilization of IoMT and communication infrastructure. The developed data acquisition system utilizes low-cost computers, sensor modules, developed software agents, and the existing Wi-Fi network. Data frameworks that can provide integrated and comprehensive residents’ data for long-term care environment applications are yet to be developed. Extensive studies on the facility information logistics, the right information, at the right time, at the right place, and in the right form are needed to generate associated real-time data by connecting multiple facility databases and to enable advanced data analytics for enhancing smart built environments [16, 17].

Due to their inherent complexity and diversity, IoMT networks cannot adopt a single network protocol for all possible implementations. Different medical environments have different needs in processing, communication, and device connectivity. Nevertheless, data confidentiality is of utmost importance when it comes to

| Risk factors       | Normal | Pre stage | Stage 1   | Stage 2  | Stage 3   |
|--------------------|--------|-----------|-----------|----------|-----------|
| Blood pressure     | SBP    | <120      | 120–139   | 140–159  | ≥ 160     |
|                    | DBP    | <80       | 80–89     | 90–99    | ≥ 160     |
| Glucose            | FPG    | <100      | 100–125   | ≥126     |
|                    | 2h-PG  | <140      | 140–199   | ≥200     |
| BMI                |        | 18.5–24.9 | 25.0–29.9 | 30.0–34.9| 35.0–39.9 | ≥40
| Waist circumference|        | ≤40, ≤35  | ≥40, >35  |          |           |

FPG fasting plasma glucose, 2h-PG hours plasma glucose, BMI body mass index
protecting medical services. As such, the use of a horizontal rule when encrypting data in the IoMT is mandatory. This is something that should also be addressed at a legal level, where possible extensions or an explanatory circular on the general data protection regulation (GDPR) [18] can specifically be used to address encryption schemes for modern medical networks. The EU GDPR, which began to be enforced across all EU member states on 25 May 2018, is a landmark in the evolution of the European privacy framework. In addition, an IoMT development framework is needed to provide integration of sensors and healthcare systems to the platform; it is extensible in terms of sensors and communication protocols. Furthermore, its abstraction layer can be extended to meet the specific requirements of these components.

Since various communication protocols are being used in IoT/IoMT devices, these devices must be able to provide data-sharing services. Therefore, we integrated multiple IoMT communication protocols in our IoRT security robot including, message queuing telemetry transport (MQTT), constrained application (CoAP), and representational state transfer over HTTP (REST HTTP). Data-sharing parts such as those developed by the health level 7 [19] (HL7) standard, enable data-sharing among various health systems and applications. However, the EHR data must be first translated to HL7-compatible resources. Applications focusing on knowledge extraction that works with a large volume of data require more than an API to prevent latency. The platforms must provide mechanisms for the application of data mining and data warehousing techniques that could help physicians through clinical decision support systems (DSS).

In a previous study [20], the IoRT was presented as a new concept that describes the integration of robotics technologies in IoT scenarios. The two research fields, robotics and IoT technologies started to interact, linking research communities. The authors intended to make further steps in joining the two communities and broaden the discussion on the development of this interdisciplinary field. Also, further analysis and discussion of the challenges and possible solutions for the IoRT were considered, examining the issues of its architecture, integration of smart spaces, and robotic applications. Moreover, they mentioned the cybersecurity problem in IoRT which affects big data processing and cloud computing due to access to program libraries, datasets arrangement, etc., and cloud operations associated with access to parallel grid computing using on-demand statistical analysis [21]. The same problem was also outlined in similar research [22], which discussed existing bugs and vulnerabilities that predispose robots to be hacked remotely, as well as applications that require security and privacy that need to be implemented in the field of robotics. Cybersecurity is also relevant for robots and automation systems that rely on data and software code from the network to maintain their functionality. IoT-based applications for robotics require solving some problems, developing methodologies, and choosing architectural solutions [23].

Cybersecurity in robots, including household robots, is related to data transfer and processing with communication protocols; therefore, such communications must be encrypted, although in most cases, it does not occur [24]. In human–robot interactions, there is a potential danger of interfering in such communications, leading to changes in commands to robots. If there is no encryption or authentication
mechanism that controls such an interface, the system becomes prone to man-in-the-middle attacks. In the next decade, it is expected that every house will have robots, e.g., home assistants in daily chores. They may contain microphones, cameras, and sensors that will collect datasets, including personal information about the house and even people’s health status. Insufficient care about the protection of confidential information may result in an unauthorized entity gaining control of such service robots and accessing confidential data. Cybersecurity of IoT systems using cloud computing is another challenging problem since IoMT devices can be connected through a cloud, providing cloud computing and data collection. In this case, protection against DDoS attacks becomes an important element of the system’s security [25].

3 Design algorithms inside IoRT and IoMT

Owing to the continued growth of the aging population, elderly care and long-term care facilities often struggle to provide the best possible care to patients and their families. Many research or business projects have undertaken long-term care programs to develop coordinated systems of community-based and in-home care services for the elderly and other functionally dependent persons. The coordination and integration of medical services in this type of setting is a relatively recent phenomenon; nevertheless, access to medical services is still a problem in many areas of the country. Not only are the services fragmented among many providers, but the eligibility for utilization of the services under publicly funded programs also varies on multiple dimensions; both factors present a difficult navigational problem to those needing the services.

The structure of the current system of long-term care providers is being stressed to its limits; it is functioning inadequately with serious problems in cost and financing, quality of care, and access to services. Moreover, systematic information on the quality of formally provided community-based and in-home care services is also not readily available and is more difficult to assess at present than institutional care. As noted previously, these services have to include not only assistance in everyday living activities, but medical, nursing, educational, rehabilitative, or other specialized skilled services. Considering the need for demanding and accurate long-term care services, smart buildings could provide a platform for providers to become more agile and accessible, giving a wide range of benefits in many aspects of service provision.

The IoMT communication protocols support the interaction of near-patient medical devices with other medical-related information technology (IT) systems. IoMT devices may utilize sensors and/or actuators to monitor and treat patients in real time. Sensors may acquire data from patients using some IoT communication technology at the perception layer. Then, the network layer communication protocols may transmit this information to IT systems after they have transformed it into a form suitable for a particular medical application. This information could then trigger real-time patient treatment. On the other hand, actuators connected to patients could support the real-time provisioning of medical treatment. IoMT devices may
process the information received from presumably trusted communication channels to modify medicine treatment protocols (e.g., modify the dosage to be injected).

In a long-term care environment, a robot serves as a bridge between the external network and the internal IoMT network. The IoRT robot could connect several sensors or actuators to form a multi-IoMT network. In the network layer, the interconnections are improved to communicate effectively with controllers and network protocols. The application layer then retrieves the information from the physical layer via the network layer and performs specified tasks accordingly. The IoRT long-term care environment crosses multiple professional fields including medical equipment, architectural engineering, and information technology. However, the robot in IoMT long-term care environment will also face multiple attacks and have the potential to un-discover vulnerabilities as it can be used as a defense in information security to protect customer data and shield against all types of network attacks.

As shown in Fig. 2, our IoRT robot serves as a mobile gateway between the external network and the internal IoMT network, it requires a server authentication mechanism to support IoMT devices inspection function. This IoRT robot functions like a mobile gateway; the hardware platform needs to have high performance, be power efficient, and be able to provide memory optimization. Hence, its software system and embedded application program could not be too complicated. If its application process consumes resources excessively, it will lead to performance decay and transmission delay. In addition, since each IoMT device may not have a fixed IP address, e.g., Arduino, NB-IoT device, they are not able to provide chip number authentication as well as Internet transmission process authentication.

For instance, after the robot and server are authenticated, the robot can start sending the received IoMT device messages to the server. The first information that an IoMT device will send to the server should be a message requesting a key as the first step in two-part authentication. The authentication steps are discussed in detail below. During the authentication process, a predetermined key and a predetermined message are employed. These are written in the code and are not randomly generated; the predetermined contents are all IoT devices and servers. The authentication process is presented in Fig. 3 and the process is as follows:

![Fig. 2 IoMT long-term care infrastructure](image-url)
Step 1: The IoMT device sends a request key command to the server.
Step 2: After receiving the key request command, the server randomly generates a 16 Bytes key and records it.
Step 3: The server uses the predetermined key to encrypt the randomly generated key, and then sends it to the IoMT device.
Step 4: After receiving the encrypted key, the IoMT device uses the default key to identify the real key.
Step 5: The IoMT device uses the real key to encrypt a predetermined message and sends it to the server.
Step 6: The server uses the real key of the IoMT device to decode the received message. If the extracted content is a predetermined message, the authentication is completed. Otherwise, the server ignores the message other than the key requested by the IoMT device.
Step 7: If the authentication is completed, the server notifies the authentication completion message to the IoMT device. The server and the IoMT device can use the real key for encrypted transmission.

This process is similar to the authentication between the robot and the server. It does not explicitly send the entire real key, and it needs to calculate the real key and encrypt the message to the server to obtain real authorization. Although the real key needs to be calculated, it can prevent the encrypted information from being read after the key is transmitted by a malicious device.

As IoRT robot is a mobile gateway between the IoMT network and the Internet, it plays an important role in information security. After all, connecting to the internet also increases the risk of information being stolen. The main purpose of the IoRT security robot is to initially filter messages and transmit messages from IoMT devices to the cloud server, or to receive messages from the cloud server and then forward them to the IoMT devices. But before that, the IoRT robot and the cloud server must have a set of authentication procedures after the connection to let the server know that the gateway is safe; otherwise, there will be malicious hackers outside the system who would want to steal private information from the cloud server. It is required that the residents’ information with its authentication be unique, such as a fixed IP or the chip number of the device like a physical unclonable function (PUF) technology. If the gateway takes the TCP/IP route and has a fixed IP with the chip number of the device like a PUF itself that is unique, it is preeminent to cooperate with the server and the database to register those two kinds of information to achieve the construction effect.

The IoMT devices and IoRT robot identification have to be unique and cannot be duplicated. If the server has a message to be transmitted to the IoT device through the gateway, the ID search can avoid misrepresentation and the problem of fake stations. From the perspective of the cloud server, a timeout mechanism design should be considered. As long as the client has no authentication information and can connect to the air, it will be at risk of disconnecting with the client. In such a situation, the authentication code mechanism can be used to determine whether the code of the gateway is designed by a system. In this paper, we propose to utilize a randomly generated key with AES encryption to generate a 4 Bytes authentication code for the server to validate with the gateway, and the number of transmitted content bytes is lesser to improve the authentication speed as shown in Fig. 4.

4 Experiment and evaluation results

The basic process of this experiment involved the mentioned two-part authentication plus the two-way encrypted transmission of the IoT device and the Server. We used two sets of Arduino and ZigBee as IoT devices A and B, and one set of Raspberry Pi and ZigBee as robots; then, a PC was utilized as a server. Since this test used the broadcast mode of the ZigBee module, only two IoMT devices were used to avoid interference caused by the frequent transmission of messages. To facilitate
screenshots and observations, IoT Device A was connected to the computer to open the Arduino dedicated IDE to watch the Log, the Raspberry Pi was used as a robot and connected to the TV through HDMI, and the Pi terminal was turned on to watch the Log. The set-up is shown in Fig. 5.

During the implementation, the device-robot-server basic structure was used to simulate the actual IoMT connection communication, to test the impact of the transmitted data plus the encryption and decryption process on each device, and to summarize various test results. The development of IoMT was mostly due to hardware
limitations and the initial rush of products to the market. Security By design was not the main security consideration; therefore, it was more feasible to add anti-theft mechanisms at the application layer. The “identity recognition” and “transmission” were included in the practical application. In terms of “encryption and decryption”, "access control", etc., adding the encryption and decryption process to the transmission content was not a difficult technology to obtain; however, some performance issues were considered. As shown in Figs. 6 and 7, we utilized AES and ECC encryption and decryption algorithms on Raspberry Pi 3 model B. There is no significant performance degradation in Raspberry Pi, so it is a feasible and worthwhile method to encrypt and decrypt messages in IoT. The analysis result showed the average time required to encrypt and decrypt messages with AES and ECC encryption algorithms. The X-axis represents the number of message bytes, and the Y-axis is the required time in milliseconds.

Since the time consumed by ECC decryption was much longer than that of the AES decryption algorithm, and the original code steps of ECC decryption were numerous, the time required for confirmation of the time function was added to each step. As shown in Figs. 8 and 9, the time required for ECC decryption was much longer than AES decryption. Using ECC to decrypt 100Bytes of data took 0.09 s,
while AES only needed 0.00015 s. What is more special is that the time required for ECC to decrypt information that is less than 10,000 Bytes was almost the same. Overall, using OpenSSL’s AES encryption and decryption resulted in a way better performance.

5 Conclusion and future works

A smart building is an emerging application of IoMT, where devices communicate, and long-term care services will contain confidential information. Security always is a critical component for IoMT data transmission, and it affects the adoption rate of smart nation applications. In this paper, we designed a novel IoMT security robot for long-term care management system. Different from previous works, the propose IoMT security robot will securely collect residents’ data as well as surrounding environmental information and provide security transmission for residents’ privacy information. Moreover, this IoMT security robot include a
server authentication mechanism, and support IoMT devices inspection function. The evaluation results show the AES and ECC encrypt and decrypt 100–100 K bytes average time consumption. The result shows that even utilize low power consumption device like Raspberry Pi, AES algorithm still can achieve encrypt and decrypt 100–100 K bytes under 9 ms. And ECC algorithm encrypt and decrypt 100–100 K bytes take 104 ms. On the contrary, ECC algorithm decrypt 100Bytes data will takes 0.09 s, while AES only takes 0.00015 s. In the future, we will continuously evaluate and compare with other light weight encryption algorithm and cooperate with architectural engineering for real work estimation.

**Funding** This work was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C. under Grant No. MOST 111-2221-E-197-020-MY3.

**Data availability** Data generated during the current study are available from the corresponding author on reasonable request.

**Declarations**

**Conflict of interest** The authors declare no conflict of interest.

**References**

1. COVID-19 infection prevention and control: preparedness checklist for long-term care facilities [https://iris.wpro.who.int/handle/10665.1/14569]. Accessed 6 May 2021
2. Wu F, Qiu C, Wu T, Yuce MR (2021) Edge-based hybrid system implementation for long-range safety and healthcare IoT applications. IEEE Internet Things J 8(12):9970–9980
3. Mir U, Abbasi U, Mir T, Kanwal S, Alamri S (2021) Energy management in long-term care environments and homes: current approaches to a hypothetical solution and open issues and challenges. IEEE Access 9:94132–94148
4. How the Internet of Medical Things Is Transforming Healthcare, Kajeet, Bethesda, MD, USA. Accessed 18 Nov 2020
5. 2020 Vision: A Review of Major IT & Cyber Security Issues Affecting Healthcare. CyberMDX, New York, NY, USA. Accessed 18 Nov 2020
6. Maddox W. Why Medical Data Is 50 Times More Valuable Than a Credit Card. Accessed 18 Nov 2020
7. Information Assurance, United States Naval Acad., Annapolis, MD, USA. Accessed 18 Nov 2020
8. Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2020) Securing internet of medical things systems: limitations, issues and recommendations. Future Gener Comput Syst 105(C):581–606
9. Vyas A, Pal S (2020) Preventing security and privacy attacks in WBAN. Handbook of Computer Networks and Cyber Security, Springer, pp 201–225
10. Pesapane F, Suter MB, Codari M, Patella F, Volonté C, Sardanelli F (2020) Chapter 52—Regulatory issues for artificial intelligence in radiology. Precision Medicine for Investigators, Practitioners and Providers. Academic, London, pp 533–543
11. Aman AHM, Yadegaridehkordi E, Attarbashi ZS, Hassan R, Park Y-J (2020) A survey on trend and classification of internet of things reviews. IEEE Access 8:111763–111782
12. Sheng T-J (2020) An internet of things based smart waste management system using LoRa and tensorflow deep learning model. IEEE Access 8:148793–148811
13. Sadhukhan D, Ray S, Biswas GP, Khan MK, Dasgupta M (2021) A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. J Supercomput 77:1114–1151
14. Touqeer H, Zaman S, Amin R, Hussain M, Al-Turjman F, Bilal M (2021) Smart home security: challenges, issues and solutions at different IoT layers. J Supercomput 77:14053–14089
15. Jensen KL, Pedersen CF, Larsen LB (2007) Diasnet mobile—a personalized mobile diabetes management and advisory service. In: Afhandling præsenteret på second international workshop on personalisation for e-health in conjunction with user modelling
16. Sengupta J, Ruj S, Bit SD (2020) A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 149:1–20
17. Prasetyo H, Hsia C-H (2019) Lossless progressive secret sharing for grayscale and color images. Multimed Tools Appl 78(17):24837–24862
18. Data protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. Accessed 6 May 2020
19. HL7. Standard: Refinement, Constraint and Localization, Release 2. http://www.hl7.org/implement/standards/ansiapproved.cfm. Accessed 5 May 2019
20. Afanasyev I, Mazzara M, Chakraborty S, Zhuchkov N, Maksatbek A, Yesildirek A, Kassab M, Distefano S (2019) Towards the internet of robotic things: analysis architecture components and challenges. In: IEEE International Conference on Developments in Eystems Engineering, pp 3–8
21. Kehoe B, Patil S, Abbeel P, Goldberg K (2015) A survey of research on cloud robotics and automation. IEEE Trans Autom Sci Eng 12(2):398–409
22. Dragoni N, Giaretta A, Mazzara M (2016) The internet of hackable things. In: International Conference in Software Engineering for De-Fence Applications, pp 129–140
23. Grieco LA, Rizzo A, Colucci S, Sicari S, Piro G, Paola DD, Boggia G (2014) Iot-aided robotics applications: technological implications, target domains and open issues. Comput Commun 54:32–47
24. Hu G, Tay WP, Wen Y (2012) Cloud robotics: architecture, challenges and applications. IEEE Network 26(3):21–28
25. Donno MD, Giaretta A, Dragoni N, Bucchiarone A, Mazzara M (2019) Cyber-storms come from clouds: Security of cloud computing in the iot era. Future Internet 11(6):127

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.