http://jhmi.sums.ac.ir
Health Man & Info Sci 2021, 8(3), 200–209

HMIS
Health Management and Information Science

Original Article

Security in Telemedicine-based IoT

Fatemeh Rabeifar[1], **Reza Radfar**[2]*, **Abbas Toloie Eshlaghy**[3]

[1]PhD candidate, Department of Information Technology Management, Science and Research branch, Islamic Azad University, Tehran, Iran
[2]Professor, Department of Technology Management, Science and Research branch, Islamic Azad University, Tehran, Iran
[3]Professor, Department of Information Technology Management, Science and Research branch, Islamic Azad University, Tehran, Iran

Abstract

Introduction: Internet of Things is an extensive network of interconnected objects across the world, in which each thing has a unique address. IoT is considered as the future innovation in the field of wireless technologies, which would be used in certain areas such as healthcare services, medical operations, etc. Hence, security requirements are very essential in these technologies. This study aims at finding the most effective model of IoT to improve Security for managing telemedicine. Following its widespread applicability, security have attracted a lot of attention and also have brought about some new challenges over security, confidence, and privacy areas.

Methods: In this study, previous literature on how to improve the security in various layers of IoT protocol and resistance against the certain attacks in any layer for the telemedicine have been considered. Relying on previous studies made on the field of research, The Recommended Architecture of IoT for Telemedicine is the three-layer: perception, network, and application.

Results: Data Security along with how data are received completely in receivers with a minimum delay, which can influence the network, is a vital challenge one may find in telemedicine. The recommended method was RPL protocol in which telemedicine systems are used.

Conclusion: We need to pay more attention to the connection points employed to transfer data among all things, cloud and networks over the telemedicine and make them secure as much as possible.

Keywords: Internet of things, Medical informatics, Mobile health, Telehealth, Telemedicine

Article History:
Received: 19 July 2021
Accepted: 18 September 2021

Please cite this paper as:
Rabeifar F, Radfar R, Toloie Eshlaghy A. Security in Telemedicine-based IoT. Health Man & Info Sci. 2021; 8(3): 200-209. doi: 10.30476jhmi.2022.92061.1091.

***Correspondence to:**
Reza Radfar,
Professor, Department of Technology Management, Science and Research Branch, Islamic Azad University, Tehran, Iran
Tel: +98 9123897600
Email: Radfar@gmail.com

Introduction

The Internet of things is a visage of the modern technology which covers millions of people, things with the sensory processing capability and services with the capability of interaction, which will be able to communicate with other machines using the communication protocols, in the sensory uses, and to communicate with each other.

Emergence of IoT and other similar networks has developed electronical communications among patients, doctors, and other providers of healthcare services. As a set of medical, management, financial, and technological information and knowledge, telemedicine is an appropriate strategy used to meet the healthcare goals, free from all temporal and spatial constraints, as well as have easier and better learning. Relying on electronic systems, it tries to minimize costs, save time, and reduce city traffic load. Telemedicine does not mean just having a website, but it has many applications. Owning backup information and supporting infrastructures are necessary to implement such applications.

The communication between the following infrastructures is imperative to launch telemedicine: people, marketing and advertisement, support services, business partners (1).

In fact, many websites are designed to facilitate communications between doctors to each other and to patients. There are companies who have formed their websites to communicate with hospitals and clinics to supply their required medical equipment.

Telemedicine project is designed to organize the followings items: (2, 3)

- Increasing accessibility to healthcare and medical services and improving quality of healthcare and medical services.
- Declining the necessity of being admitted in hospitals and reducing transportation costs for

patients, doctors, and hospital staff.

- Improving the accessibility to patients' medical files and pursuing their treatment process.
- Helping specialists in the rural and remote areas to send healthcare and medical services to their patients in a quicker way.

The positive effect of Information technology (IT) efficiency in projects causes the organizations to use this technology (4); as a result, the attitude of working with IT facilitates the project's activities (5), increases the income, and decreases the costs (6). Also, it is clear cut that in the modern world, medicinal organizations, institutes and companies increasingly try to organize their activities and products (7). They use different methods to direct, coordinate and control these. Therefore, for developing and expanding IoT in the telemedicine, considering the concept of security in IoT to prevent any delay and to enhance data sending rate is necessary. Thus, the necessity of paying attention to this issue prompted the author to deal with development of security in IoT for telemedicine in this study.

Methods

The Recommended Architecture of IoT for Telemedicine

There is no consensus about the architecture of IoT in the world. Researchers have proposed many structures. The most basic architecture, based on the previous studies, is the three-layer structure. The three layers in this structure are perception, network and application:

A) Perception Layer (8, 9)

It is a physical layer which has sensors to feel and collect information about the environment. This layer senses some physical parameters or determines other intelligent things in the environment.

B) Network Layer (8, 9)

This layer accounts for making connection between intelligent things, network tools, and servers. It also is used to transfer and process the sensory data.

C) Application Layer (8, 9)

This layer facilitates provision of special application services to users. It defines different applications in which IoT can be installed for telemedicine (Figure 1).

Security of the Internet of Things (IoT)

Within recent years, advancements in the field of information technologies have accelerated the virtual world development. On the one hand, web-based technologies, such as network processing, service-oriented processing, and cloud computing, have made the network world not only a research/servicing platform, but also an arena for world-class cooperation and communications among various virtual societies, communities, and organizations. (10)

In the IoT, data submission process is so that a certain device is given a unique ID and an IP by which the necessary data are sent to the relevant database. The data which are sent through different devices including smart phones, computers, and tablets can be observed. Data are sent automatically and based on the default setting and at specific times.

Security for IoT covers definition of approaches which can bring about basic security properties including confidentiality, accuracy, and authentication; it also include secure implementations for different devices with limited resources and must be able to meet the high-level requirements of IoT over the telemedicine system. The requirements are as follows: (11-14)

Authentication of medical data: The identity of retrieved address and information of things must be authenticated.

Controlling users' accessibility: Data suppliers must be able to facilitate the accessibility control for the supplied data.

Patient's safe electronic file: It includes keeping confidentiality and maintaining the accuracy of the sensitive data stored in the patient's electronic file system.

Privacy of client, who can be either a patient or a doctor: Some measures must be taken, according to which only data suppliers are allowed to analyze the users' personal information based on the system's graphs.

Authentication and management of user's identity: The users' identity must be authenticated before using system.

One of management widespread fields is authentication of people/things in a system and controlling their access to the internal resources of system.

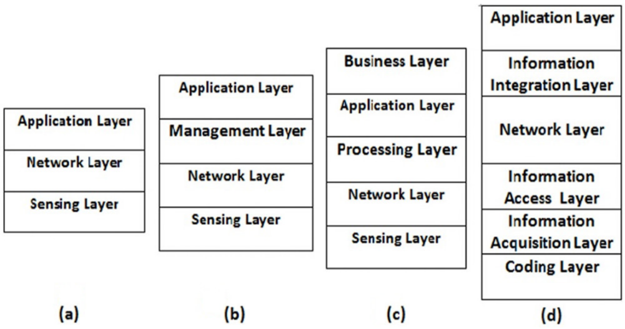


Figure 1: Layered Architecture (a) Three (b) Four (c) Five (d) Six (8)

Secure communications of medical data: It includes existence authentication of both parties, i.e. physician and patient, making sure about the confidentiality and accuracy of the exchanged data, and preventing any denial of a communicative transaction.

Accessibility: It means that illegal systems or people should not be able to block accessibility or use of the legal ones.

Secure environment of Telemedicine: It refers to the safe and managed environment which is protected against the malicious programs. The system should not have the unique breaking point, and it needs to be equipped with the self-regulating property in the case of node failure. It also refers to both maintaining and keeping alive the security requirements, even when the system is controlled by attackers and may be misused either physically or logically.

IoT Communication Protocol

The Internet is one of the important communication platforms for telemedicine projects; hence, healthcare depends on major factors, i.e. manpower and technology as no one is able to use its full potential without the other one (15). Using medical documents, medical equipment, and communication technologies, specialists of medical sciences diagnose the disease and minimize the medical errors. A standard communication protocol stack for IoT is shown in Figure 2. One of the basic properties of Internet architecture is that packs can pass the interconnected networks using heterogeneous technologies of connection layers. The necessary conformities and mechanisms to pass the IP packs are defined and identified in the proper descriptions over the special connection layer. The related technologies of IoT, and its main ingredients, are radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Low-Power Wireless Personal Area Networks (LoWPAN), smart phones, tablets, and personal computers (16-18).

Based on a similar purpose, in 2007 a work group was formed to work on IPV6 over 6LOWPAN. Its mission was producing descriptions by which IPV6 packs can be passed over low-power IEEEE802.15.4 and wireless environments. Given the network condition such as network speed and traffic, authenticating and categorizing the available devices in the IoT optimize the tracking level and also unweigh the data overload (19). Although it is possible to develop a system which is successful technically, it would be unsuccessful organizationally. Therefore, apart from how well the data systems are developed or what technology, devices and techniques are used in them, users may not welcome the new data systems. Paying equal attention to both technical and management aspects of the telemedicine projects is necessary for delivering a successful project. A precise look at success and failure records of such projects over the world shows how important the management of such projects is. The main reservoir of healthcare information in a healthcare and medical organization is the patient's medical file. Besides a new communication system, Internet network indicates a database for gathering, storing, and retrieving healthcare and medical information about a certain person since their birth to their death in an information system (20, 21).

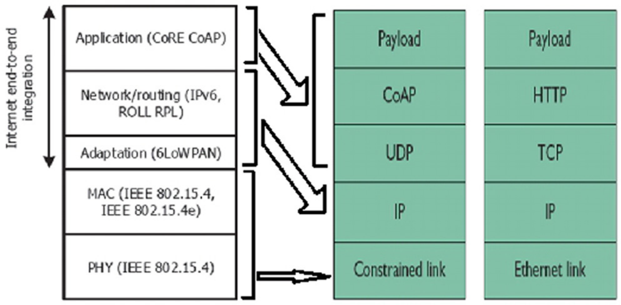


Figure 2: Internet of Things Layered Architecture

Results

Security in the Perception Layer of IoT for Telemedicine

Network disruption, lack of timely availability of resources, temporal failure of information systems, failure to make a backup of one's files, low efficiency of software, and long intervals between searching for medical data and receiving them are among the drawbacks which can bring about serious risks. However, their probability and effectiveness in the telemedicine projects can be estimated through identifying and predicting them.

For providing security services in this part, standard IEEE802.15.4 will support different modes in the MAC sub-layer. It is due to supporting hardware-based symmetric cryptography, which is carried out over sensor levels. The security defined by this standard is optional; it means that an applied program can decide about security or lack of security in other protocol stack layers. 128-bit buttons are used to provide backup. Using some fields in the security header in this standard, it is possible for the sender to bring about the necessary support to apply protection against the message redistribution attacks in all standard security modes. This standard also brings about manual control capability, by which the sensor machine will be able to use origin and destination addresses of the frame and in this way begins to search and interpret data on security and information necessary for maintaining the message security (22, 23).

Sensors

IoT plays a vital and fundamental role through placing sensors or medicines in the body in order to monitor the patients' mood and provide clinical cares, because by using the patients' information, it can gather and analyze their information and then send the analyzed information to the processing center for taking proper decisions. A smart thing includes microprocessor, a communication set, and a sensor. Networks developed by such things are called low-power networks. RPL routing protocol, which is compatible with the IPV6 protocol stack is used to design such networks. Sensors are used to determine the patient's mood and condition. Their performance range covers both outpatients and inpatients. In a wireless network, composed of several other wireless networks which work with each other, it monitors biological signals received from patients based on the remote access.

The idea of connecting systems to each other has resulted in construction of giant telemedicine systems based on the Internet of things. A three-layered architecture is used to implement such systems which consider the IoT as a network of interconnected devices; in them, by using wireless connections, data are connected to a central processor in a cloud and are shared there. In a wireless network, composed of several other wireless networks which work with each other, it makes the biological signals received from patients from the healthcare system effective and makes the scientific environment possible (Table 1).

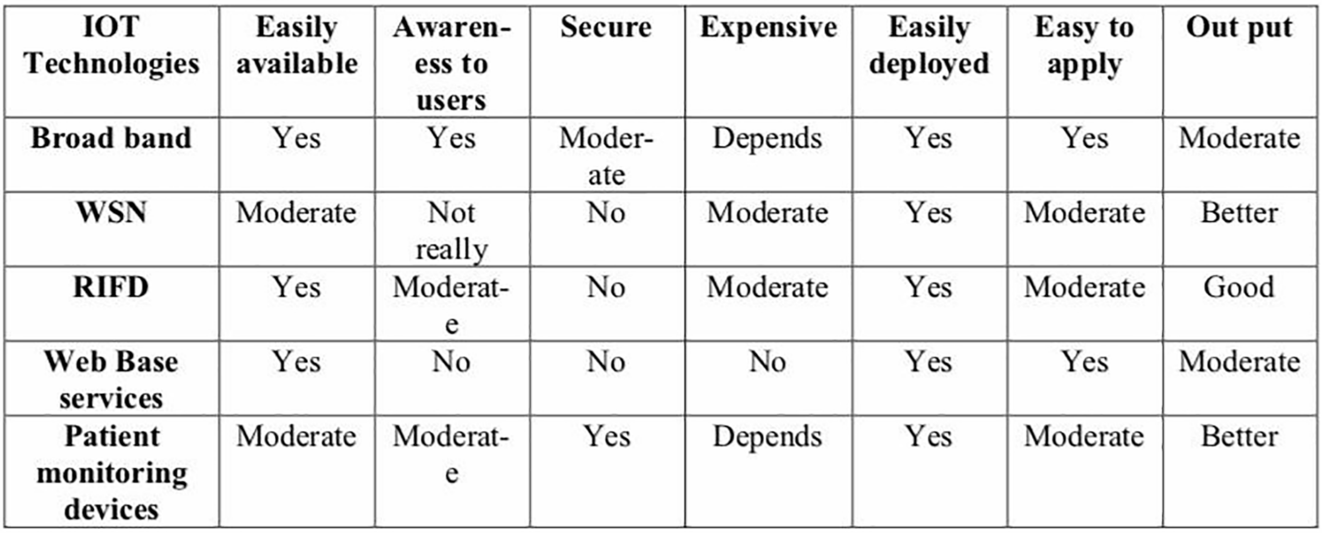
Security in the Network Layer of IoT for Telemedicine

Sensor network consists of many small nodes. There are a number of sensors in each node which interact with the physical environment and sense certain qualities such as temperature, pressure, moisture, etc. Such sensors are used to take information from the environment and send them to the central node. Each node has memory and processing capability, and its connection is wireless (24).

The wireless sensor networks are employed for removing spatial distance and minimizing the time and doctors' fee. For instance, a continuous glucose monitor (CGM) can provide you with an online monitoring anytime, anywhere. It also very critical in treating nervous diseases (25); given the numerous utilities of telemedicine, we need to create a proper platform and structure to provide medical services effectively as much as possible so, taking advantage of both information technology properly and management process will let us start designing and implementing such systems. Wireless devices must be able to act independently from the Internet. Particularly, there might be intervals during which there is no connection between the wireless device and Internet. During these timespans, the wireless devices must be able to act stably, while their connection to the remaining structure has been cut. Especially, they must be able to develop local case networks using their internal protocols. Therefore, certain issues such as identity confirmation and synchronization of the device status must be done precisely and with the minimum delay (26, 27).

The current nomenclature system in the Internet is very difficult and inflexible, which is proper for hierarchical and static topologies. In order to support movement of nodes and routing, IOT needs to find a

Table 1: The Performance of different Internet of Things technologies for Telemedicine (7)



IOT Technologies	Easily available	Awaren-ess to users	Secure	Expensive	Easily deployed	Easy to apply	Out put
Broad band	Yes	Yes	Moder-ate	Depends	Yes	Yes	Moderate
WSN	Moderate	Not really	No	Moderate	Yes	Moderate	Better
RIFD	Yes	Moderat-e	No	Moderate	Yes	Moderate	Good
Web Base services	Yes	No	No	No	Yes	Yes	Moderate
Patient monitoring devices	Moderate	Moderat-e	Yes	Depends	Yes	Moderate	Better

way by which the network elements will be found easier than by just having connection points. Therefore, a clear and transparent structural separation between routable names and addresses is a vital requirement for IOT (28, 29). Based on IPV6 address space allocation, the issue of IoT and a network of smart devices has been offered. IOT is a set of smart things which are interconnected to each other and send the data through certain intervals. Such information is sent by RPL routing protocol, which is effective in routing nodes. RPL routing protocol in low-power networks is used for different usages and is compatible with the IPV6 stack. For communications of this protocol, there are various sorts of attacks based on fragmentation process, which are generally based on weak points of IP protocol implementing, which are introduced in (29, 30). In the small segments attacks through many protocol implementations, there is a possibility by which an extraordinary small size is announced for the output packs. If the size of the segment is too small that some fields of TCP package are protruded in the next segment, then the filtering codes which determine the patterns will not work for these fields any more. If the filtering implementation has not forced a minimum size, an impermissible pack can pass the Gateway because it has not been compatible with the filter. In a router, it is possible to implement security through applying certain limits for the segments which may pass; it means that the first segments need to be large enough. Authors in (31) have proposed a plot in which each segment is coded separately and there is no cryptographic dependence between the segments of a pack. Any segment, upon receiving, is processed and there is a possibility to process out-of-order segments in the suggested plots and redundant segments will be thrown away immediately. Properties and descriptions of safe versions of RPL protocol introduce controlling messages of various routes and three basic security modes. (32). Security requirements and access points, through which security would be endangered, were studied in the security reference model 2 (ISO7498-2(1988)) (33). Using this standard, routing protocol of ROLL (34) has introduced such threats which include identity confirmation, data accuracy, non-denial, and accessibility. This model enables us to categorize and discuss about certain threats and attacks related to confidentially and accessibility in the exchange of routing messages in the field of this protocol. Recently, topological attacks have been recognized as a risk factor in the routing protocols such as RPL; we will announce some ways to fight against such attacks. Authors in (10) have suggested a method in which the node of the graph root sends a message alternatively to other nodes and asks them to respond to this message. It seems that the node which does not respond is the attacker one and will be removed from the network. In a study (32), it was suggested that digital signature must be used in order to fight against the attack to the node rank. They also have offered implementation of topological general tests in order to analyze the accuracy of RPL routing structure. In the method suggested in (35), HASH chaining quantities are used to fight against the mentioned attacks; also, in the fighting method proposed in (36), according to the status quo of the network, nodes adapt themselves dynamically to fight against the topological attack. In this method, nodes dynamically compute a threshold limit and then according to that threshold limit will throw away packs including detrimental information.

The findings suggest that application of telemedicine is centered on mobile technology. This shows that despite the huge benefits of telemedicine to healthcare delivery and health outcome (37), the technology has concentrated on telephone communication over the years with a rather limited application in other aspects of technology (1, 38).

Most smart devices are mobile. Their changing location makes it difficult to communicate with the cloud data center, which is due to changing network condition in various locations. To solve the mobility problem, researchers have proposed the mobile cloud computing, although there are still problems. (39, 40) Mobile cloud computing also suffers from mobility problems, including frequent changing network condition, which is due to removal of the signals. As a solution for storage resource problems, we provide calculation for the network, known as Fog. Fog can be considered as cloud which is close to the earth. Data can be analyzed, stored, filtered, and processed in this network edge, before being sent to the cloud through costly media (41).

Fog is computed based on the following considerations: (42-44)

1. There is less time to access the reserve resources and computing across the fog nodes.

2. As the fog is in the network edge, it knows the location of the software and their field. It is aware of the important property of IoT software and is useful.

3. Unlike the cloud nodes, fog nodes are published in a centralized fashion.

4. Fog nodes can interact with the cloud and only pass the data, which must be sent to the cloud (Figure 3).

In one incident, multiple IoT devices were used to start a distributed Denial-of-Service (DDoS) attack

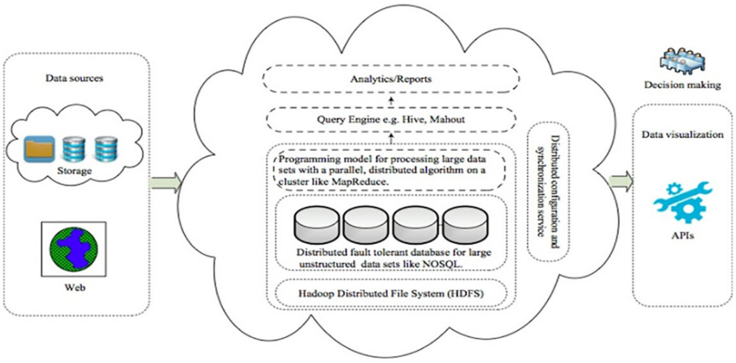

Data sources
Storage
Web
Analytics/Reports
Query Engine e.g. Hive, Mahout
Programming model for processing large data sets with a parallel, distributed algorithm on a cluster like MapReduce.
Distributed fault tolerant database for large unstructured data sets like NOSQL.
Hadoop Distributed File System (HDFS)
Distributed configuration and synchronization service
Decision making
Data visualization
APIs

Figure 3: Usage of cloud computing in Big Data (45)

on an American Internet services company that made it impossible for many customers to access certain Internet services (46). Bakhsh et al. proposed adaptive intrusion detection and prevention system for the IoT devices utilizing agent technology to support portability, rigidness, and self-started attributes (47).

Security in the Application Layer of IoT for Telemedicine

As smart devices gather a great deal of sensory data, computing and storing resources for analysis, storage and process of data are required. The most common computation and storage resources are based on clouds because cloud makes us able to control data, scalability, and flexibility.

Cloud computing has provided modern capabilities to carry out big data processing and analysis within the organizations and various businesses such as Telemedicine (48). Cloud computing used big data for the purpose of analyzing it and providing proposed solutions to various digital problems in various fields such as social sciences, business, industrial and other fields (49). The growth of Big Data, particularly its adoption by organizations and industry, increases the meaning/content of Big Data (49). Varieties of big data coming from different sources are handled with elasticity, resources pooling, and self-service advantages (50).

Protocol of datagram transport layer security (DTLS), which uses COAP protocol to support security in the utility layer, has been considered. Utility layer connections, supported by COAP protocol, are being designed. This protocol has defined some limitations to secure COAP message by a few configurations which are proper for the environments with limitations (51). To guarantee security in this layer, authors in (52) used public-key cryptography to design an identity confirmation protocol and key agreement in the wireless sensory networks and in the same year, the authors in (53) used bilinear map and designed an efficient identity confirmation protocol for the mobile factors in the client-server environments. Although the proposed protocols are secure, because they had not used digital signature properties, they fail to provide non-denial property. An identity confirmation protocol using both smart card and finger-print has been suggested in (54), which was improved by the study made in (55) in order to be able to be resistant against the spoofing attack. Using a biometric authentication and smart card, authors in (56) proposed a user identity confirmation plot, which brings about anonymity; also, they proved that the mentioned plot was resistive against the recognized attacks. Similar works have been proposed in (57-59), but since they don't use biometric authentication, they are vulnerable against certain attacks such as spoofing or card theft or smart machines, so they are not proper for the telemedicine systems. For providing security in the utility layer through confirmation of the user's identity, an identity confirmation protocol, which has enabled mutual authentication through curve cryptography and HASH Function, is proposed in (60). Technically, our starting point is the formal specification language IoT-LySa, a process calculus recently proposed for describing IoT systems (61-64). Designers can model the architecture of a system, the algorithmic behaviour fits smart objects and their interactions through theIoT-LySaprimitives. Furthermore, IoT-LySa enables them to reason about qualitative properties as system correctness and robustness by using a static analysis, namely Control Flow2 Analysis (CFA).

Discussion

The Internet of Things is a part of modern technology that consists of millions of people, objects with sense-process ability and services with the ability to interact. That will be able to connect with other machines by communicative protocols in the field of sense functions and each other. Therefore, the Secure connection mechanism is an essential factor of the Internet of Things, and in order to strengthen current users and future users, it should be considered in Telemedicine. Telehealth monitoring service integrates health care resources to extend the coverage of health care institutions, which can essentially be understood as a telemedicine for communities (65) and provide timely medical and health protection (66). Telemedicine based IoT is an important branch of IoT and the change of the development of the health service industry (67, 68). The Mobile health monitoring application integrates sensors, wireless communication technology, and cloud computing, overturning the traditional health monitoring model and becoming an important branch of Telehealth (69). Wireless sensor networks are used to eliminate location and reduce the time and cost of physician visits. For example, there is a remote blood sugar control system (24) and this network can provide online monitoring at any time. As telemedicine systems work in public networks, privacy preservation issue of sensitive and private transmitted information is important. (70). Due to the numerous applications of the remote medical system, we need to create a suitable platform and structure to provide efficient and effective medical services, which can be designed and implemented by using the correct information technology and using the management processes. As it was seen, the main focus of each item discussed in this study was on one of layers of communication protocol stack, and architecture of three layers of internet as well as approaches for networks with limited resources such as IoT and wireless sensory networks which are proper for a better performance of telemedicine.

Conclusion

A smart thing includes microprocessor, a communication set and a sensor. Networks which are developed by such things are called low-power networks. RPL routing protocol, which is compatible with the IPV6 protocol stack, is used to design such networks. Sensors are used to determine the patient's mood and condition. Thus, this study dealt with some approaches that would be used to guarantee security in three layers of IoT architecture in telemedicine. Certain criteria including low energy consumption, necessary bandwidth, and resistance against certain attacks in any layer were considered. Cooperation between IT engineers and physicians in this regard will guarantee more successful and more secure use of telemedicine services.

Conflict of Interest: None declared.

References

1. Tuckson RV, Edmunds M, Hodgkins ML. Telehealth. *N Engl J Med*. 2017;377(16):1585-92. doi: 10.1056/NEJMsr1503323.
2. Qureshi A, Shih E, Fan I, Carlisle J, Brezinski D, Kleinman M, et al. Improving patient care by unshackling telemedicine: adaptively aggregating wireless networks to facilitate continuous collaboration. *AMIA Annu Symp Proc*. 2010;2010:662-6.
3. Dhanvijay MM, Patil SC. Internet of Things: A survey of enabling technologies in healthcare and its applications. *Computer Networks*. 2019;153:113-31. doi: 10.1016/j.comnet.2019.03.006.
4. Johns ML. The CIO and IRM (information resources management) alliance: maneuvering for the competitive edge in hospital information management. *Top Health Rec Manage*. 1990;11(1):1-7.
5. Friedman C, Wyatt J. Evaluation methods in medical informatics. New York: Springer; 1997.
6. Choi H, Park IH, Yoon HG, Lee HM. Wireless patient monitoring system for patients with nasal obstruction. *Telemed J E Health*. 2011;17(1):46-9. doi: 10.1089/tmj.2010.0105.
7. Shams R, KHAN FH, SALEEM F. Internet of things in telemedicine: a discussion regarding to several implementation. *Journal of Information Communication Technologies and Robotic Applications*. 2018:17-26.
8. Sheikh A, Ambhaikar A. Quality of Services Parameters for Architectural Patterns of IoT. *Journal of Information Technology Management*. 2021;13:36-53.
9. Qi J, Yang P, Min G, Amft O, Dong F, Xu L. Advanced internet of things for personalised healthcare systems: A survey. *Pervasive and Mobile Computing*. 2017;41:132-49. doi: 10.1016/j.pmcj.2017.06.018.
10. Wallgren L, Raza S, Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks*. 2013;9(8):794326. doi: 10.1155/2013/794326.
11. Hassanalieragh M, Page A, Soyata T, Sharma G, Aktas M, Mateos G, et al., editors. Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. June 27-July 2, 2015. New York: IEEE International Conference on Services Computing. doi: 10.1109/SCC.2015.47.
12. Alami H, Gagnon M-P, Fortin J-P. Telehealth in

light of cloud computing: clinical, technological, regulatory and policy issues. *Journal of the International Society for Telemedicine and eHealth*. 2016;4:e5.

13. Lee JD, Yoon TS, Chung SH, Cha HS. Service-Oriented Security Framework for Remote Medical Services in the Internet of Things Environment. *Healthc Inform Res*. 2015;21(4):271-82. doi: 10.4258/hir.2015.21.4.271.
14. Masood I, Wang Y, Daud A, Aljohani NR, Dawood H. Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. *Wireless Communications and Mobile Computing*. 2018;2018. doi: 10.1155/2018/2143897.
15. Dubey H, Monteiro A, Mahler L, Akbar U, Sun Y, Yang Q, et al. FogCare: fog-assisted internet of things for smart telemedicine. *Future Generation Computer Systems*. 2016.
16. Patel KK, Patel SM. Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*. 2016;6(5):6122-31.
17. Aman MN, Sikdar B, Chua KC, Ali A. Low power data integrity in IoT systems. *IEEE Internet of Things Journal*. 2018;5(4):3102-13. doi: 10.1109/JIOT.2018.2833206.
18. Madakam S. Internet of things: smart things. *International journal of future computer and communication*. 2015;4(4):250. doi: 10.7763/IJFCC.2015.V4.395.
19. Collins K, Bowns I, Walters S. General practitioners' perceptions of asynchronous telemedicine in a randomized controlled trial of teledermatology. *J Telemed Telecare*. 2004;10(2):94-8. doi: 10.1258/135763304773391530.
20. Abdelhak M. Health information: management of a strategic resource. 2nd Ed. Philadelphia: Saunders; 2001.
21. Salunke P, Nerkar R. IoT driven healthcare system for remote monitoring of patients. *International journal for modern trends in science and technology*. 2017;3(6):100-3.
22. IEEE Standard for Local and metropolitan area networks. Part 15.4. Low-Rate Wireless Personal Area Networks (LRWPANs 802.15 standard), 2011.
23. IEEE Standard for Local and metropolitan area networks. Part 15.4. Low-Rate Wireless Personal Area Networks (LR-WPANs 802.15.4e standard); 2012.
24. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer networks*. 2002;38(4):393-422. doi: 10.1016/S1389-1286(01)00302-4.
25. Carmo JP, Dias NS, Silva HR, Mendes PM, Couto C, Correia JH. A 2.4-GHz low-power/low-voltage wireless plug-and-play module for EEG applications. *IEEE Sensors Journal*. 2007;7(11):1524-31. doi: 10.1109/JSEN.2007.908238.
26. Hu YC, Wang HJ. Location Privacy in Wireless Networks. Hong Kong: ACM SIGCOMM Asia Workshop; 2015. p. 1-5.
27. Adjie-Winoto W, Schwartz E, Balakrishnan H, Lilley J, editors. The design and implementation of an intentional naming system. New York: Proceedings of the seventeenth ACM symposium on Operating systems principles; 1999. p. 186-201. doi: 10.1145/319344.319164.
28. Seskar I, Nagaraja K, Nelson S, Raychaudhuri D. MobilityFirst future internet architecture project. New York: Proceedings of the 7th Asian Internet Engineering Conference; Bangkok, Thailand: Association for Computing Machinery; 2011. p. 1–3. doi: 10.1145/2089016.2089017.
29. Ziemba G, Reed D, Traina P. Security considerations for IP fragment filtering. 1995;RFC 1858:1-10. doi: 10.17487/rfc1858.
30. Ptacek TH, Newsham TN. Insertion, evasion, and denial of service: Eluding network intrusion detection. Alberta: Secure Networks INC Calgary, 1998.
31. Hummen R, Hiller J, Wirtz H, Henze M, Shafagh H, Wehrle K, editors. 6LoWPAN fragmentation attacks and mitigation mechanisms. Budapest: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec 2013); 2013. p. 55-66. doi: 10.1145/2462096.2462107.
32. Winter T. RPL: IPv6 routing protocol for low power and lossy networks. *RFC6550*. 2012.
33. International Organization for Standardization, Information Processing Systems. Open Systems Interconnection Reference Model. Security Architecture, ISO Standard 7498-2, 1988.
34. Tsao T, Alexander R, Dohler M, Daza V, Lozano A. A Security Threat Analysis for Routing over Low-Power and Lossy Networks. Internet-Draft–work in progress 03, IETF, 2013. doi: 10.17487/rfc7416.
35. Dvir A, Buttyan L, editors. VeRA-version number and rank authentication in RPL. 17-22 Oct. 2011. Valencia: IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems; 2011. p. 709-14. doi: 10.1109/MASS.2011.76.

36. Mayzaud A, Sehgal A, Badonnel R, Chrisment I, Schönwälder J. Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks. *International Journal of Network Management*. 2015;25(5):320-39. doi: 10.1002/nem.1898.
37. O'Connor M, Asdornwised U, Dempsey ML, Huffenberger A, Jost S, Flynn D, et al. Using Telehealth to Reduce All-Cause 30-Day Hospital Readmissions among Heart Failure Patients Receiving Skilled Home Health Services. *Appl Clin Inform*. 2016;7(2):238-47. doi: 10.4338/ACI-2015-11-SOA-0157.
38. Harvey JB, Valenta S, Simpson K, Lyles M, McElligott J. Utilization of Outpatient Telehealth Services in Parity and Nonparity States 2010-2015. *Telemed J E Health*. 2019;25(2):132-6. doi: 10.1089/tmj.2017.0265.
39. Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU. The rise of "big data" on cloud computing: Review and open research issues. *Information systems*. 2015;47:98-115. doi: 10.1016/j.is.2014.07.006.
40. Voruganti S. Map Reduce a Programming Model for Cloud Computing Based On Hadoop Ecosystem. *International Journal of Computer Science and Information Technologies*. 2014.
41. Alyass A, Turcotte M, Meyre D. From big data analysis to personalized medicine for all: challenges and opportunities. *BMC Med Genomics*. 2015;8:33. doi: 10.1186/s12920-015-0108-y.
42. Zhu H, Yuan Y, Chen Y, Zha Y, Xi W, Jia B, et al. A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. *IEEE Access*. 2019;7:90036-44. doi: 10.1109/ACCESS.2019.2924486.
43. Verma H, Chahal K, editors. A review on security problems and measures of Internet of Things. 15-16 June 2017. Madurai: 2017 International Conference on Intelligent Computing and Control Systems (ICICCS); 2017. p. 71-6. doi: 10.1109/ICCONS.2017.8250560.
44. Suciu G, Suciu V, Martian A, Craciunescu R, Vulpe A, Marcu I, et al. Big Data, Internet of Things and Cloud Convergence--An Architecture for Secure E-Health Applications. *J Med Syst*. 2015;39(11):141. doi: 10.1007/s10916-015-0327-y.
45. Khan S, Shakil KA, Alam M. Cloud-based big data analytics—a survey of current research and future directions. *Big data analytics*. 2018:595-604. doi: 10.1007/978-981-10-6620-7_57.
46. Khan ZA, Herrmann P. Recent advancements in intrusion detection systems for the Internet of Things. *Security and Communication Networks*. 2019;2019. doi: 10.1155/2019/4301409.
47. Bakhsh ST, Alghamdi S, Alsemmeari RA, Hassan SR. An adaptive intrusion detection and prevention system for Internet of Things. *International Journal of Distributed Sensor Networks*. 2019;15(11):1550147719888109. doi: 10.1177/1550147719888109.
48. Sokiyna MY, J Aqel M, Naqshbandi OA. Cloud computing technology algorithms capabilities in managing and processing big data in business organizations: Mapreduce, hadoop, parallel programming. *Journal of Information Technology Management*. 2020;12(3):100-13.
49. Yang C, Huang Q, Li Z, Liu K, Hu F. Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*. 2017;10(1):13-53. doi: 10.1080/17538947.2016.1239771.
50. Noraziah A, Fakherldin MAI, Adam K, Majid MA. Big Data Processing in Cloud Computing Environments. *Advanced Science Letters*. 2017;23(11):11092-5. doi: 10.1166/asl.2017.10227.
51. Bormann C, Castellani AP, Shelby Z. Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing*. 2012;16(2):62-7. doi: 10.1109/MIC.2012.29.
52. Luo M, Zhao H. An authentication and key agreement mechanism for multi-domain wireless networks using certificateless public-key cryptography. *Wireless Personal Communications*. 2015;81(2):779-98. doi: 10.1007/s11277-014-2157-5.
53. Tsai J-L, Lo N-W. Provably secure and efficient anonymous ID-based authentication protocol for mobile devices using bilinear pairings. *Wireless Personal Communications*. 2015;83(2):1273-86. doi: 10.1007/s11277-015-2449-4.
54. Lee C, Zappaterra L, Choi K, Choi H-A, editors. Securing smart home: Technologies, security challenges, and security requirements. San Francisco: 2014 IEEE Conference on Communications and Network Security; 2014. doi: 10.1109/CNS.2014.6997467.
55. Lin CH, Lai YY. A flexible biometrics remote user authentication scheme. *Computer Standards & Interfaces*. 2004;27(1):19-23. doi: 10.1016/j.csi.2004.03.003.
56. Das AK, Goswami A. A robust anonymous biometric-based remote user authentication scheme using smart cards. *Journal of King Saud University-Computer and Information Sciences*.

2015;27(2):193-210. doi: 10.1145/1031154.1031165.

57. Huang X, Xiang Y, Chonka A, Zhou J, Deng RH. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*. 2010;22(8):1390-7. doi: 10.1109/TPDS.2010.206.
58. Jiang Q, Kumar N, Ma J, Shen J, He D, Chilamkurti N. A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. *International Journal of Network Management*. 2017;27(3):e1937. doi: 10.1002/nem.1937.
59. Kothmayr T, Schmitt C, Hu W, Brünig M, Carle G, editors. A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. Clearwater: 37th Annual IEEE Conference on Local Computer Networks-Workshops; 2012. doi: 10.1109/LCNW.2012.6424088.
60. Guanglei Z, editor. A novel mutual authentication scheme for Internet of Things. Modeling, Identification9 and Control (ICMIC), Proceedings of 2011 International Conference on IEEE; 2011.
61. Bodei C, Degano P, Ferrari G-L, Galletta L. Tracing where IoT data are collected and aggregated. *arXiv preprint arXiv:161008419*. 2016;13(3). doi: 10.23638/LMCS-13(3:5)2017.
62. Bodei C, Degano P, Ferrari G-L, Galletta L. Sustainable precision agriculture from a process algebraic perspective: A smart vineyard. *IRIS*. 2018;125(4):39–44. doi: 10.2424/ASTSN.M.2018.6.
63. Bodei C, Galletta L, editors. Tracking sensitive and untrustworthy data in IoT. Venice: 2017 The Italian Conference on Cybersecurity (ITASEC17).
64. Bodei C, Degano P, Galletta L, Tuosto E. Tool supported analysis of IoT. *arXiv preprint arXiv:171111210*. 2017;261:37-56. doi: 10.4204/EPTCS.261.6.
65. Wright SP, Hall Brown TS, Collier SR, Sandberg K. How consumer physical activity monitors could transform human physiology research. *Am J Physiol Regul Integr Comp Physiol*. 2017;312(3):R358-R67. doi: 10.1152/ajpregu.00349.2016.
66. Muneer A, Fati SM, Fuddah S. Smart health monitoring system using IoT based smart fitness mirror. *Telkomnika*. 2020;18(1):317-31. doi: 10.12928/telkomnika.v18i1.12434.
67. Vanrenterghem J, Nedergaard NJ, Robinson MA, Drust B. Training Load Monitoring in Team Sports: A Novel Framework Separating Physiological and Biomechanical Load-Adaptation Pathways. *Sports Med*. 2017;47(11):2135-42. doi: 10.1007/s40279-017-0714-2.
68. Triloka J, Senanayake SA, Lai D. Neural computing for walking gait pattern identification based on multi-sensor data fusion of lower limb muscles. *Neural Computing and Applications*. 2017;28(1):65-77. doi: 10.1007/s00521-016-2312-x.
69. Guo M, Wang Z, Yang N, Li Z, An T. A multisensor multiclassifier hierarchical fusion model based on entropy weight for human activity recognition using wearable inertial sensors. *IEEE Transactions on Human-Machine Systems*. 2018;49(1):105-11. doi: 10.1109/THMS.2018.2884717.
70. Garai Á, Péntek I, Adamkó A. Revolutionizing healthcare with IoT and cognitive, cloud-based telemedicine. *Acta Polytechnica Hungarica*. 2019;16(2):163-81. doi: 10.12700/APH.16.2.2019.2.10.