Article

Security Framework for IoT Based Real-Time Health Applications

Aamir Hussain ¹ , Tariq Ali ² , Faisal Althobiani ³, Umar Draz ^{4,*} , Muhammad Irfan ^{5,*} , Sana Yasin ⁶, Saher Shafiq ¹, Zanab Safdar ⁴, Adam Glowacz ^{7,*} , Grzegorz Nowakowski ⁸ , Muhammad Salman Khan ⁹ and Samar Alqhtani ¹⁰

- ¹ Department of Computer Sciences, MNS-University of Agriculture Multan, Multan 60000, Pakistan; aamir.hussain@mnsuam.edu.pk (A.H.); saher.shafiq43@gmail.com (S.S.)
- ² Department of Computer Science, Sahiwal Campus, COMSATS University Islamabad, Sahiwal 57000, Pakistan; tariqali@cuisahiwal.edu.pk
- ³ Faculty of Maritime Studies, King Abdulaziz University, P.O. Box 80401, Jeddah, Saudi Arabia; falthobiani@kau.edu.sa
- ⁴ Department of Computer Science, University of Sahiwal, Sahiwal 57000, Pakistan; zanabsafdar@uosahiwal.edu.pk
- ⁵ Electrical Engineering Department, College of Engineering, Najran University, Najran 61441, Saudi Arabia
- ⁶ Department of Computer Science, University of Okara, Okara 56130, Pakistan; sanayaseen42@yahoo.com
- ⁷ Department of Automatic Control and Robotics, Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering, AGH University of Science and Technology, al. A. Mickiewicza 30, 30-059 Krakow, Poland
- ⁸ Faculty of Electrical and Computer Engineering, Cracow University of Technology, Warszawska 24 Str., 31-155 Cracow, Poland; gnowakowski@pk.edu.pl
- ⁹ Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Lahore 54000, Pakistan; mskhan@cuilahore.edu.pk
- ¹⁰ College of Computer Science and Information Systems, Najran University Saudi Arabia, Najran 61441, Saudi Arabia; smalqhtani@nu.edu.sa
- * Correspondence: sheikhumar520@gmail.com (U.D.); miditta@nu.edu.sa (M.I.); adglow@agh.edu.pl (A.G.)

Citation: Hussain, A.; Ali, T.; Althobiani, F.; Draz, U.; Irfan, M.; Yasin, S.; Shafiq, S.; Safdar, Z.; Glowacz, A.; Nowakowski, G.; et al. Security Framework for IoT Based Real-Time Health Applications. *Electronics* **2021**, *10*, 719. <https://doi.org/10.3390/electronics10060719>

Academic Editor: Kenji Suzuki

Received: 22 February 2021

Accepted: 13 March 2021

Published: 18 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: The amazing fusion of the internet of things (IoT) into traditional health monitoring systems has produced remarkable advances in the field of e-health. Different wireless body area network devices and sensors are providing real-time health monitoring services. As the number of IoT devices is rapidly booming, technological and security challenges are also rising day by day. The data generated from sensor-based devices need confidentiality, integrity, authenticity, and end-to-end security for safe communication over the public network. IoT-based health monitoring systems work in a layered manner, comprising a perception layer, a network layer, and an application layer. Each layer has some security, and privacy concerns that need to be addressed accordingly. A lot of research has been conducted to resolve these security issues in different domains of IoT. Several frameworks for the security of IoT-based e-health systems have also been developed. This paper introduces a security framework for real-time health monitoring systems to ensure data confidentiality, integrity, and authenticity by using two common IoT protocols, namely constrained application protocol (CoAP) and message query telemetry transports (MQTT). This security framework aims to defend sensor data against the security loopholes while it is continuously transmitting over the layers and uses hypertext transfer protocols (HTTPs) for this purpose. As a result, it shields from the breach with a very low ratio of risk. The methodology of this paper focuses on how the security framework of IoT-based real-time health systems is protected under the tiers of CoAP and HTTPs. CoAP works alongside HTTPs and is responsible for providing end-to-end security solutions.

Keywords: e-health; IoT and data privacy; IoT layered architecture; CoAP

1. Introduction

The internet of things is a network of physical technologies that you can access online, such as devices, vehicles, buildings, and hospitals [1]. With emerging advancements in the internet and computing devices, new technologies are being developed to help advance healthcare's existing structure [2]. Healthcare is a technique of medical services that are used for informational and audiovisual coordination, and records processing. The incorporation of IoT in health monitoring systems is quite challenging because the data are generated in massive amounts, and it requires security to save the private data of the patients from hackers [3]. With the help of internet of things (IoT) devices, patients are being monitored 24/7 in this era [4]. These devices are small but have the power to monitor the patients who carry these devices with them. In emergency times, the patient can be monitored remotely, and necessary measures can also be taken. As these devices are continuously connected to the internet, they can detect abnormalities, and provide emergency services simultaneously [5]. Healthcare covers various topics, including medical healthcare, diagnostic assessment, and cure health awareness among people [6]. In developing countries, it is still a big challenge to monitor chronic patients in real-time environments due to the poor adaption of technology. According to the World Health Organization (WHO), the rapid increase of deaths worldwide is due to cardiovascular diseases (CVDs). According to an estimate, the annual number of deaths due to heart failure and heart stroke may increase to 23.3 million by 2030 [7]. Due to their busy lifestyles, most people do not have much time to take care of their health. IoT-based health monitoring systems can help people monitor their own health and remain informed about the health of other chronic disease patients, the elderly, and disabled people staying at their home. A system has also been proposed to improve the existing health care services to allow the practitioners to effectively treat those cardiac patients who are living alone in their homes [8,9].

People living in rural areas are deprived of advanced healthcare systems due to the unavailability of technology and doctors [10]. To cope with this situation, the real-time monitoring of the patient's health, location and medication is vital. However, any hostile person's interference can reveal and alter a patient's critical data by any means which can lead to harmful consequences, even death [11]. For instance, let us say an asthmatic patient with a severe cough is being monitored by the health care system in real-time and, suddenly, an adversary alters the data by spoofing the data communication medium, and provides the wrong dosage to the patient [12]. Moreover, Covid-19 has become a pandemic that has affected the whole world, and we can limit its spread through the continuous monitoring of the affected patients [13]. A WBAN (wireless body area network) can be used to monitor the environmental conditions around people. These wearable sensory nodes are attached to the human body to monitor respiration rate, heart rate, pulse rate, and body temperature [14]. With the sensory nodes' help, useful information can be gained about the patient for a comprehensive understanding of the disease. Thus, such systems should be implemented in rural areas to provide instant aid in case of emergency [15,16].

1.1. Health Care in IoT

The healthcare industry has been transformed by the advent of IoT. Many wearable devices have been built and are being used in healthcare to monitor the patient's status in a real-time environment. In the domain of healthcare, sensors generate the data in bulk. It is quite hard to handle this type of data as it requires confidentiality, integrity, and authenticity of every single bit. Although these devices support health monitoring, the data that is being sensed and conveyed to the cloud require greater protection and security.

Security is the primary concern of this era. From home privacy to health safety, everything demands security and protection. It is a crucial part of our lives. Indeed, people are more conscious about their personal data privacy, whether it is regarding money, vehicles, or health [17]. They do not want to discuss things that are not necessary to share with a third person. Confidentiality, integrity and availability are the primary requirements

of data security. Confidentiality ensures that the machine or network must be accessed by the authorized entity, whereas integrity ensures that only the legal and authorized user can modify the data with their permission. Furthermore, the availability requirement means that the data should be available for the legal entity at the time of need without any interruptions and limitations [18].

1.2. Security and Privacy

In e-health, security, and privacy stand for two different terms according to the context. The security of the patient's essential data refers to the availability, validity, and integrity of data, whereas privacy ensures that the data can only be approached and perceived by the legal owner. Several devices work in a real-time health monitoring system that builds a communication medium between physicians, and patients. This communication medium requires the security of the data which are being exchanged between the health monitoring systems and patients.

This paper presents a security framework for IoT-based real-time health monitoring applications through the IoT layered architecture. We have defined multiple sections to ensure end-to-end security with communication, and security protocols of constrained application protocol (CoAP) and hypertext transfer protocols (HTTPs). Section 2 describes the related work. Section 3 elaborates the IoT layered architecture, and Section 4 explains the methodology. Implementation is discussed in Section 5 while Section 6 illuminates the conclusion and future direction.

2. Background and Related Work

The indoor and outdoor patients are responsible for their data safety by enhancing their security awareness regarding cyber-attacks. Meanwhile, facility workers, and vendors are accountable for delivering improved hardware devices to defend indoor and outdoor patient data [19]. As IoT is in the developing phase, it lacks security morals. The data interchanging with the patient's real-time health monitoring systems would be secured in the sense of authenticity, integrity, and confidentiality. The current safety conditions require co-operative academic efforts to overcome the security challenges in the telemedicine and real-time health monitoring systems [20].

IoT is the blend of different technologies, and data is exchanged between devices by different communication levels. Each communication level requires different security activities. Many scientists have recommended biometric safety arrangements because they deal with individuals' unique actions to provide scalable security solutions. Biometric systems are becoming very popular among the masses because of their use for identity verification and authentication. However, many challenges are being faced by these systems, such as cost, real-time implementation, hardware maintenance, cyber-attacks like Denial of Services [21], eavesdropping, and data manipulation. Man in the middle attacks, spoofing, and brute force attacks occur on the perception layer in biometric systems from where the individuals enter their data into the biometric systems. These attacks create problems in the system for decision-making.

A framework was developed to address key issues in the layered architecture of an IoT-based health system as it collects the complete data of the patients and sends it to the cloud which is accessed locally and globally [22]. The proposed model was tested using the Contiki real-time operating system. The model consisted of three layers in which each layer had a specific function; however, the framework lacked the security infrastructure to combine the current administrative tasks.

The Mobicare plan was recommended for mobile healthcare applications. This system gives the patients access to a nursing and tracing system about the current and accurate monitoring of their health status. The system supports professional staff to analyze the current health information while the patient is not present [23]. Technological change is a continuous process; thus, Mobicare has some challenging research issues,

including body sensor network security, reliable and protected sensor code updates, and potential opportunities.

Some solutions offer key scenarios for e-health applications. Instead, this research has provided a robust methodology for combining undisclosed sharing schemes and connecting identities to form social groups of patients suffering from a similar disease [24].

mHealth provided a social network. The groups are divided into separate blocks, and the block department helps the block director collect detailed information from patients' mobile devices. Although the system does not provide a solution to malicious invaders, these invaders are not maliciously affecting the patients; instead, it helps the patients in adverse situations by sharing some sensitive information about their safety [25].

Wireless body area networks (WBANs) systems now have technologies overcoming restrictions such as power, processing, scalability, managing, and computing, by adopting cloud computing technology. The unification of WBANs and cloud-computing as a sensor cloud infrastructure (SC-I) supports the healthcare environment by real-time patient tracking, and early disease detection [26]. However, this lacks standard architecture, policy compliance, typical data collection, patient behavior management, medically coded passwords, data sharing, data disclosure, data management, and multiple data organization [27]. Likewise, the SC-I needs to pay particular attention to friendly applications, network security, real-time implementation, access control, and better-quality patient data access [28].

Reliable data communication plays a vital role in IoT for reliable data fusion, data mining, context-aware based services, and user privacy [29]. A way of addressing these concerns is to theoretically virtualize the IoT environment across the cloud, which is known as the Cloud-of-Things (CoT), and then connect each device with one or more cloud agents [6,30] that have developed a CoTAG (CoT agent grouping), algorithm to shape agent groups based on the reliability details and credibility obtained by agents. They carry out the tests in a simulated scenario to check this algorithm's reliability and efficacy. The findings show the possible benefits of plan acceptance.

An IoT framework and two-dimensional IoT architecture were developed to provide end-to-end security and resolve the problem of limiting HTTP-CoAP proxies. They proposed a new HTTP-CoAP security model. The easiest way was to encrypt the HTTP payload to provide end-to-end security with HTTP and CoAP compatibility [31].

The Reliable IoT-based Security System Architecture is the first scholarly summary-based proposal. To conclude, this research addresses the concrete realization of the trusted IoT-based security architecture, which consists of secure device modules, reliable perception modules, secure terminal modules, reliable network modules, and advisor modules. Furthermore, it is important to study how to resolve IoT security problems due to accessibility, and incomplete IoT growth [32].

A survey was conducted to analyze IoT safety from three perspectives: three-layered network architecture, security issues at each level, and security countermeasures.

Another survey was conducted to expose some IoT security issues through a layer in the network structure and find solutions to the problems mentioned above and key technologies. Such safety measures include those described in the climate layer, including key management and algorithm, security routing protocol, data fusion software, authentication, and access control [33,34].

A study was conducted to improve the sensor-based attacks and mechanisms in mHealth to ensure patient data privacy. A multilayered taxonomy was undertaken to achieve the goal. Around 3064 papers were collected which were later categorized into surveys on telemedicine, three tiered architectures of telemedicine, sensor-based smartphones orientations for user authentication, and other articles. They focused on the second layer in smartphones based on sensors to enhance the authentication in mHealth.

Continuous monitoring of patient health store and submit status, and updated records of data need a high-end system. To access patient information in real-time, a secure cloud

server allows authenticated users to consult remote medical specialists. Different policy management rules are applied to enhance data privacy and security [35].

Using IoT, multimedia allows meaningful and better communication between the patients and the experts to implement remotely and offers the sector vast innovations. The research in [36] stated that a wireless body area network (WBAN)-based overall three-tier pervasive telemedicine system enables continuous real-time surveillance of health care.

To confirm that the private data collected are used solely to support official services by authorized providers, solutions have been proposed that are usually based on a system, called a privacy broker. The proxy interacts with the user on the one hand, and with the services on the other.

A balanced solution was proposed between security and feasibility; with the help of a DTH-P2P social network and cryptographic protocol, the system guaranteed the security requirements without the complicated features of the current e-voting system [37].

Suppose a Wireless Sensor Network (WSN) is to be thoroughly combined into the IoT. In that case, various security challenges need to be considered, such as creating a secure channel between an internet host and a sensor node. To create such a network, key management mechanisms must be provided that allow two remote devices to negotiate specific security credentials (e.g., secret keys) to protect the information flow [38].

Complete semantic interoperability can be provided to the different IoT platforms and vendors through the VICINITY framework. It aims to resolve privacy and security problems and offers a robust solution to IoT issues. A decentralized architecture that consists of nodes is used to secure peer-to-peer communication by using the legal principles [39].

Trust is the primary factor of intelligent agent technology because trust enhances the reputation of the smart objects in the community. To reduce the security problems and take full advantage of wearables, a study offers a secure model and architectural mechanism of different IoT e-health areas that help to send and receive e-health patients' data. They present brief research showing how many patients' data can be dealt with the IoT e-health applications [40].

A certificate-based Datagram Transport Layer Security (DTLS) uses a handshake protocol to provide security between the end-users and the IoT-based e-health gateways due to the limited resources of constrained devices to implement the cryptographic technique [41].

RSA keys, DTLS and clasp authentication techniques are used for verification and deployment of this mechanism [42]. They provide an algorithm based on public-key cryptography using TSA features and modules so that security can depend on these features. It has been learned after replacing DTLS with this proposed protocol, that the slight difference seen at the platform of the hardware is entirely compatible with IoT. This protocol provides the integrity of the SMS end-to-end throughput minimum power consumption privacy and authentication. Ultimately it is concluded that IoT is the appropriate option for the use of DTLS [43].

The abovementioned works have done a lot for the security of real-time health monitoring systems regarding data confidentiality, authenticity, and integrity. Different research studies are being conducted on the safety of real-time data. Growing technology is attracting hackers, and cyber threats are increasing day by day [44]. The IoT-based monitoring systems services are different from the services we access over the public network [45]. No standard of security is developed to secure real-time health monitoring data properly and lacks protection. However, different frameworks and security algorithms have been designed to cope with security challenges. Our work aims to develop a security framework with the help of application layer security protocols (CoAP and HTTPS) to secure real-time data of the patients being transferred from a constrained environment to the web, according to the need of time. The system will shield the data in a layered manner from the sensor layer to the application layer. CoAP and HTTPS will provide end-to-end security to the patients' essential data generated in the real-time scenario.

3. IoT Layered Architecture

According to many studies, the IoT works in three layers: perception, network, and application layers. The flow of data through these layers is shown in Figure 1. In [46], each layer has some security problems like confidentiality, integrity, and authenticity due to human involvement. The involvement of humans has increased the sensitivity; that is why collected data from the individuals and patients requires the system's permission to access the records. Such a privacy concern limits the users in getting the full advantage of the system. The security of healthcare data is paramount; thus, to secure the authenticity, integrity, and confidentiality of data, we need to develop a security framework for the real-time health monitoring system. There are many security frameworks and devices already in use by health technicians and paramedics. These systems, however, become absurd over time. Moreover, our previous efforts in this regard also support our words (see [42–50]).

Figure 1. Flow of data from the patient to healthcare systems.

As mentioned above, IoT works in layered manners, and each layer has security loopholes that are needed to resolve strong security concerns. The first layer is the physical layer, also known as the perception layer. Data is sensed from the surroundings in terms of temperature, humidity, location, etc., through the sensor devices transmitted to the network layer.

The network layer's data is routed and transmitted to different IoT hubs and devices using some emerging technologies, e.g., Wi-Fi, Bluetooth, ZigBee, and 4G LTE. The communication between other platforms like cloud computing and gateways routers has been done due to these technologies. Gateways serve as middleware between two or more different IoT nodes of the network to transmit the data.

The application layer ensures the security triad confidentiality integrity and authenticity of the data through this layer. All the applications that have been deployed with IoT are defined on the application layer. The application layer provides an interface between the end devices and the network. This layer provides the services to the applications; the services may vary for each application due to the sensors' information.

In recent years, WBAN technology has been increasingly used in healthcare. Numerous medical devices can be used or implanted and integrated into the WBAN to monitor patient health, treat patients with automated therapies, and more. The traditional architecture of e-health with IoT can be seen in Figure 2. These systems must protect data during collection, transmission, processing, and storing. A WBAN device is made up of smart, low-powered sensor nodes. WBAN is a wireless network composed of connected sensors capable of calculating and gathering data on a user's health situation. The patients can wear the sensors on different parts of the body and keep this under the skin.

Figure 2. Traditional internet of things (IoT) architecture.

The patient's psychological condition can be monitored through the sensors embedded in wireless body area networks, and the information gathered through these sensors is then forwarded to the physicians and hospitals. The transfer of health-related information between sensors of the human body and the healthcare monitoring system must be encrypted so that the patient's vital information that is being exchanged over the network remains secure and private.

An IoT-based healthcare domain consists of portable WBAN sensors and devices that the patient carries with them all time, as showed in Figure 2. Sensors get the data from the surroundings and then send them to the network or cloud, where the data is analyzed, and significant decisions are taken. In the healthcare domain, a single bit of change in a patient's data can lead to serious consequences or even death. Security can be divided into two broader terms: physical security and virtual security.

Physical security in the IoT deals with technological equipment like hardware and sensor devices. In contrast, virtual security deals with someone's virtual adversary through some wired or wireless medium. To cope with the second type of security is difficult because attackers or sniffers sit on the communication medium and try to alter the data.

All the devices connected through the mediums operate collectively, so there is a need to make our systems more secure and provide end-to-end security, whether this is from sensors to gateway, or gateways to cloud, and cloud to healthcare providers.

4. Methodology

By studying several kinds of research, we concluded that there have been proposed many different frameworks for the security of real-time health monitoring systems. In [47], the authors proposed a framework in which they used two application layered protocols to CoAP and HTTP to provide end security by encrypting the HTTP payload. However, there is still a need to resolve the security conflicts in the IoT environment. The vital part of this paper presents a particular layer base framework for secure communication between patients and doctors.

In our work, we have proposed a framework for solving the security and privacy problems in electronic health care systems with the help of two application layer protocols, namely, CoAP and HTTPs. Unlike HTTP, CoAP uses the client/server model to establish the connection when client sends the request to the server to respond.

Further data are moved to the network layer: this layer is known as infrastructure. This layer consists of many communication protocols such as IP, REST, 6LowPAN, Bluetooth, Wi-Fi, ZigBee, and QoS. This layer is responsible for sending data over the network by using different routers and switches. Data are coming into this layer from the sensors, so the transmission of data from the sensor layer to the network layer of the IoT gateway plays a crucial role. It works as an intermediate to connect two different environments;

moreover, to develop gateways ARM Corte-M3 and M4 which are the finest selections in the IoT environment. On the network layer, data are packed in packets with a header and generate the frames. These patients' frames or information then transmit on the cloud for storage, analysis, and decision-making, and they move towards the application layer. As healthcare data are needed to analyze in real-time, the loss or delay of any packet can be hazardous.

In a heterogeneous environment, communication protocols have higher importance for the interaction of devices. To meet the IoT requirements, hundreds of messaging protocols have been developed to address the application's base collection of data in a constrained environment, e.g., CoAP and message query telemetry transports (MQTT). Meanwhile, HTTP and CoAP have been designed for web applications that require communication over the internet. It is clearly proven that a single protocol is not sufficient to deal with the entire IoT system. It also indicates that the coming years of the technology revolution rely on several messaging protocols to communicate over the internet. In Figures 3 and 4, three application layer protocols are chosen to secure the peer-to-peer and end-to-end security: RESTful HTTPs [48], CoAP and MQTT.

Figure 3. Security framework for IoT-based real-time health application.

Figure 4. Proposed system of block diagram.

5. Evaluation and Implementation

To return to our proposed model, we will implement some prototype of our proposed framework. In our proposed framework, we used HTTPS and the CoAP protocol for secure data communication from the patient to cloud storage and environment. As it is known that in the cloud environment and for internal structure, HTTP is more appropriate and well known, it is an application layer protocol and works at the backend. HTTPs is connection-oriented and helpful in the transport layer as it collaborates with TCP. Figure 5 shows the initialization or handshaking process and end-to-end security mechanism with CoAP and HTTPS.

Figure 5. Process initialization and end-to-end secure methodology with Hypertext Transfer Protocols (HTTPS).

GET and PUT methods are used to access resources to provide end-to-end secure commutation and send inputs to the servers. POST, DELETE, READ, and WRITE commands are also useful to show the communication competency between e-health clients and servers [49].

All these methods of posting and retrieving data depict the working environment of our proposed methodology. We have used a predefined set of codes like XML, HTML and simple JSON code to represent the responses while using the resources.

Results of Contiki Cooja Simulation

For the real-time simulation, we have used the Contiki operating system 2.7 with a Cooja simulation environment as shown in Figure 6, which provides the results of different framework modules using different parameters. These parameters help judge the secure packet transmission, time to live (TTL) maximum time, and minimum time using CoAP in a real-time e-health environment from the sensor layer to the network layer. CoAP works in a client-server environment. To support CoAP in Cooja, a Copper extension is used and operated on Mozilla Firefox. CoAP also supports GET, PUT, POST, and DELETE methods [50,51] as the sensor devices are limited in power, processing, and memory. This works under the 6LoWPAN network: a border router is used to connect a regular IP with the RPL 6LoWPAN network. In the Contiki–Cooja simulation environment, the border router is present at the edge of the border of a network. The border router is also working as a gateway to connect two different networks: one is a wireless sensor network, and the other is Wi-Fi, Bluetooth, etc. When conducting tests for Cooja, two main points we need to concentrate on are:

Figure 6. Deep client and server communication using sky mote.

- Border router, which allows access to the internet.
- Web-server, which gives internet access to the border router. Through the following steps, the Cooja simulation for a border router is done.

The following are the steps to create the sky motes (shown in Figure 6) as a client and server:

- For creating the server mote: Go to motes > Create mote > Select the mote type > Browse > Go to example folder > Select IPV6 > Rpl-border router > Border-router.c > Open > Compile > Create > Add motes > Add only 1 mote to make it server > View > Select the interfaces for the network.

After creating the server mote, mote one goes to the mote connectivity of all the client motes. By default, client motes are always active to communicate with each other, but they wait for the connection response from the CoAP server. The following Figure 7 shows the process of getting the IPV6 address from the server. After getting the IPV6 connection, we can communicate securely via a Copper extension for the CoAP in Mozilla Firefox.

```

user@instant-contiki: ~/contiki/examples/ipv6/rpl-border-router
File Edit View Search Terminal Help

inet addr:127.0.1.1 P-t-P:127.0.1.1 Mask:255.255.255.255
inet6 addr: fe80::1/64 Scope:Link
inet6 addr: aaaa::1/64 Scope:Global
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

Rime started with address 0.18.116.1.0.1.1.1
MAC 00:12:74:01:00:01:01:01 Contiki-2.6-900-ga6227e1 started. Node id is set to 1.
CSMA ContikiMAC, channel check rate 8 Hz, radio channel 26, CCA threshold -45
Tentative link-local IPv6 address fe80:0000:0000:0000:0212:7401:0001:0101
Starting 'Border router process' 'Web server'
*** Address:aaaa::1 => aaaa:0000:0000:0000
Got configuration message of type P
Setting prefix aaaa::
Server IPv6 addresses:
aaaa::212:7401:1:101
fe80::212:7401:1:101

```

Figure 7. Server IPv6 address.

After getting the IPV6 of the server, it enables us to communicate successfully using the IDs of client motes and server motes. These mote IDs are used to show the neighboring and connecting routes, which can be seen in Figure 8. Moreover, the paths in which these packets are moving can be detected.

```

Applications Places
ContikiRPL - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ContikiRPL [aaaa::212:7401:1:101/]
[aaaa::212:7401:1:101] Google

Neighbors
fe80::212:7407:7:707
fe80::212:7402:2:202
fe80::212:7408:8:808
fe80::212:7403:3:303

Routes
aaaa::212:7407:7:707/128 (via fe80::212:7407:7:707) 16711423s
aaaa::212:7406:6:606/128 (via fe80::212:7407:7:707) 16711415s
aaaa::212:7402:2:202/128 (via fe80::212:7402:2:202) 16711423s
aaaa::212:7408:8:808/128 (via fe80::212:7408:8:808) 16711423s
aaaa::212:7404:4:404/128 (via fe80::212:7403:3:303) 16711415s
aaaa::212:7403:3:303/128 (via fe80::212:7403:3:303) 16711420s

```

Figure 8. Neighbors and routes of the client mote.

The following Figure 9 shows the ping statistic for mote four having ID `aaaa::212:7404:4:404`. The statistics show that we have selected five packets to transmit over the network through the border router working on the motes' edge. All the packets are transmitted towards the receiving end, and the given transmission shows zero packet loss. Hence, we can say that the packets are securely and successfully transmitted.

```

user@instant-contiki: ~/contiki/tools
File Edit View Search Terminal Help
user@instant-contiki:~$ cd contiki
user@instant-contiki:~/contiki$ cd tools
user@instant-contiki:~/contiki/tools$ ping6 -c 5 -s 8 aaaa::212:7404:4:404
PING aaaa::212:7404:4:404(aaaa::212:7404:4:404) 8 data bytes
16 bytes from aaaa::212:7404:4:404: icmp_seq=1 ttl=62 time=73.8 ms
16 bytes from aaaa::212:7404:4:404: icmp_seq=2 ttl=62 time=163 ms
16 bytes from aaaa::212:7404:4:404: icmp_seq=3 ttl=62 time=117 ms
16 bytes from aaaa::212:7404:4:404: icmp_seq=4 ttl=62 time=128 ms
16 bytes from aaaa::212:7404:4:404: icmp_seq=5 ttl=62 time=42.8 ms

--- aaaa::212:7404:4:404 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 42.815/105.478/163.833/42.505 ms
user@instant-contiki:~/contiki/tools$

```

Figure 9. Ping statistics for mote eight.

Figure 9 shows that our developed security framework for the real-time health monitoring system's privacy is implemented in the Contiki-Cooja simulation environment. Thus, to prove the results, we have implemented one module of the framework; this module covers the network layer.

The network layer covers how the devices are interconnected and communicating in the end-to-end secure environment successfully. Furthermore, the rest of the framework can also be implemented by using a simulation environment in the future. Our results ensure that the framework is successfully running and can be deployed quickly in the future.

6. Conclusions

In the present era, wearable smart devices have become an essential part of our lives. Human lifestyle has been changed by the development of IoT-based smart systems. This paper presents a security framework constructed on layered architecture to ensure the privacy of real-time health monitoring systems. Two lightweight protocols of the application layer, namely, CoAP and MQTT, have been used in this framework to provide peer-to-peer security in a constrained environment whereas RESTful HTTPs have been used to provide security in the internet environment. CoAP and RESTful HTTPs are collectively used in this framework by using some proxies to secure end-to-end communication. Our proposed model can be used easily on a Cooja simulation and can be implemented on any OS separately using different defined framework modules. All these modules can be separately implemented to work properly and provide security. Operational simulations are another important aspect that can be performed easily while using sensors to provide the best work. We cannot say everything comes up with perfection, but we do hope to have extended the boundaries of the area of interest for the researchers and practitioners in e-healthcare systems.

Author Contributions: A.H. and T.A. have proposed the research conceptualization and methodology. The technical and theoretical framework is prepared by F.A., M.I. and S.S. The technical review and improvement have been performed by S.Y. and Z.S. The overall technical support, guidance, and project administration are done by U.D., A.G., S.Y., M.S.K. and G.N. The editing and proofreading is done by A.H., U.D., S.A. and G.N. All authors have read and agreed to the published version of the manuscript.

Funding: The research was conducted at the Faculty of Electrical and Computer Engineering, Cracow University of Technology and was financially supported by the Ministry of Science and Higher Education, Republic of Poland (grant no. E-3/2021).

Acknowledgments: The authors acknowledge the support from the Deanship of Scientific Research, Najran University, Kingdom of Saudi Arabia.

Conflicts of Interest: The authors declare there is no conflict of interest.

References

1. Pasha, M.; Shah, S.M.W. Framework for e-health systems in IoT-based environments. *Wirel. Commun. Mob. Comput.* **2018**, *2018*. [CrossRef]
2. Swaroop, K.N.; Chandu, K.; Gorreputu, R.; Deb, S. A health monitoring system for vital signs using IoT. *Internet Things* **2019**, *5*, 116–129. [CrossRef]
3. Hussain, A.; Draz, U.; Ali, T.; Tariq, S.; Irfan, M.; Glowacz, A.; Daviu, J.A.A.; Yasin, S.; Rahman, S. Waste Management and Prediction of Air Pollutants Using IoT and Machine Learning Approach. *Energies* **2020**, *13*, 3930. [CrossRef]
4. Ali, T.; Noureen, J.; Draz, U.; Shaf, A.; Yasin, S.; Ayaz, M. Participants Ranking Algorithm for Crowdsensing in Mobile Communication. *ICST Trans. Scalable Inf. Syst.* **2018**, *5*. [CrossRef]
5. Rahaman, A.; Islam, M.M.; Islam, M.R.; Sadi, M.S.; Nooruddin, S. Developing IoT Based Smart Health Monitoring Systems: A Review. *Rev. D'intelligence Artif.* **2019**, *33*, 435–440. [CrossRef]
6. Chattopadhyay, A.K.; Nag, A.; Ghosh, D.; Chanda, K. A Secure Framework for IoT-Based Healthcare System. In *Proceedings of International Ethical Hacking Conference 2018*; Springer: Singapore, 2018.
7. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* **2017**, *18*, 113–122. [CrossRef]
8. Hussain, A.; Wenbi, R.; da Silva, A.L.; Nadher, M.; Mudhish, M. Health and emergency-care platform for the elderly and disabled people in the Smart City. *J. Syst. Softw.* **2015**, *110*, 253–263. [CrossRef]
9. Hussain, A.; Rao, W.; Zheng, X.; Wang, H.; Aristides, L.D.S. Personal Home Healthcare System for the Cardiac Patient of Smart City Using Fuzzy Logic. *J. Adv. Inf. Technol.* **2016**, *7*, 58–64. [CrossRef]
10. Yew, H.T.; Ng, M.F.; Ping, S.Z.; Chung, S.K.; Chekima, A.; Dargham, J.A. IoT Based Real-Time Remote Patient Monitoring System. In *Proceedings of the 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, Langkawi, MA, USA, 28–29 February 2020; pp. 176–179.
11. Kim, D.-W.; Choi, J.-Y.; Han, K.-H. Medical Device Safety Management Using Cybersecurity Risk Analysis. *IEEE Access* **2020**, *8*, 115370–115382. [CrossRef]
12. Abouelmehdi, K.; Beni-Hssane, A.; Khaloufi, H.; Saadi, M. Big data security and privacy in healthcare: A Review. *Procedia Comput. Sci.* **2017**, *113*, 73–80. [CrossRef]
13. Islam, S.; Lloret, J.; Zikria, Y.B. Internet of Things (IoT)-Based Wireless Health: Enabling Technologies and Applications. *Electronics* **2021**, *10*, 148. [CrossRef]
14. Draz, U.; Ali, T.; Yasin, S.; Waqas, U.; Zahra, S.B.; Shoukat, M.A.; Gul, S. A Pattern Detection Technique of L-MYC for Lungs Cancer Oncogene in Bioinformatics Big Data. In *Proceedings of the 2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan, 14–18 January 2020; pp. 218–223.
15. Ali, G.; Ali, T.; Irfan, M.; Draz, U.; Sohail, M.; Glowacz, A.; Sulowicz, M.; Mielnik, R.; Bin Faheem, Z.; Martis, C. IoT Based Smart Parking System Using Deep Long Short Memory Network. *Electronics* **2020**, *9*, 1696. [CrossRef]
16. Wu, F.; Wu, T.; Yuce, M.R. An Internet-of-Things (IoT) Network System for Connected Safety and Health Monitoring Applications. *Sensors* **2018**, *19*, 21. [CrossRef]
17. Kavitha, S.; Alphonse, P.J.A.; Reddy, Y.V. An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System. *J. Med. Syst.* **2019**, *43*, 260. [CrossRef]
18. Carta, S.; Podda, A.S.; Recupero, D.R.; Saia, R. A Local Feature Engineering Strategy to Improve Network Anomaly Detection. *Futur. Internet* **2020**, *12*, 177. [CrossRef]
19. Almahdi, E.M.; Zaidan, A.A.; Zaidan, B.B.; AlSalem, M.A.; Albahri, O.S.; Albahri, A.S. Mobile Patient Monitoring Systems from a Benchmarking Aspect: Challenges, Open Issues and Recommended Solutions. *J. Med. Syst.* **2019**, *43*, 207. [CrossRef]
20. Shah, S.T.U.; Badshah, F.; Dad, F.; Amin, N.; Jan, M.A. Cloud-assisted IoT-based smart respiratory monitoring system for asthma patients. In *Applications of Intelligent Technologies in Healthcare*; Springer: Cham, Switzerland, 2019; pp. 77–86.

21. Rahmani, A.-M.; Thanigaivelan, N.K.; Gia, T.N.; Granados, J.; Negash, B.; Liljeberg, P.; Tenhunen, H. Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2015; pp. 826–834.
22. Nanayakkara, M.; Halgamuge, M.; 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, 6–7 November 2019.
23. Mohammed, K.I.; Zaidan, A.A.; Zaidan, B.B.; Albahri, O.S.; AlSalem, M.A.; Hadi, A.; Hashim, M.; Albahri, A.S. Real-Time Remote-Health Monitoring Systems: A Review on Patients Prioritisation for Multiple-Chronic Diseases, Taxonomy Analysis, Concerns and Solution Procedure. *J. Med. Syst.* **2019**, *43*, 223. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Sun, Y. Securing Body Sensor Networks and Pervasive Healthcare Systems. Ph.D. Thesis, Imperial College London, London, UK, 2019.
25. Selvaraj, P.; Doraikannan, S. Privacy and Security Issues on Wireless Body Area and IoT for Remote Healthcare Monitoring. *Intell. Pervasive Comput. Syst. Smarter Healthc.* **2019**, 227–253. [\[CrossRef\]](#)
26. Masood, I.; Wang, Y.; Daud, A.; Aljohani, N.R.; Dawood, H. Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. *Wirel. Commun. Mob. Comput.* **2018**, 2018. [\[CrossRef\]](#)
27. Ali, T.; Yasin, S.; Draz, U.; Ayaz, M.; Tariq, T.; Javaid, S. Motif Detection in Cellular Tumor p53 Antigen Protein Sequences by using Bioinformatics Big Data Analytical Techniques. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 330–338. [\[CrossRef\]](#)
28. Choi, J.; In, Y.; Park, C.; Seok, S.; Seo, H.; Kim, H. Secure IoT framework and 2D architecture for End-To-End security. *J. Supercomput.* **2018**, *74*, 3521–3535. [\[CrossRef\]](#)
29. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [\[CrossRef\]](#)
30. Fortino, G.; Messina, F.; Rosaci, D.; Sarné, G.L. Using trust and local reputation for group formation in the Cloud of Things. *Futur. Gener. Comput. Syst.* **2018**, *89*, 804–815. [\[CrossRef\]](#)
31. Li, X.; Xuan, Z.; Wen, L. Research on the Architecture of Trusted Security System Based on the Internet of Things. In Proceedings of the 2011 Fourth International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, 28–29 March 2011; Volume 2, pp. 1172–1175.
32. Qi, J.; Yang, P.; Min, G.; Amft, O.; Dong, F.; Xu, L. Advanced internet of things for personalised healthcare systems: A survey. *Pervasive Mob. Comput.* **2017**, *41*, 132–149. [\[CrossRef\]](#)
33. Yasin, S.; Ali, T.; Draz, U.; Jung, L.T.; Arshad, M.A. Formal Analysis of Coherent Non-Redundant Partition-based Motif Detection Algorithm for Data Visual Analytics. *J. Appl. Environ. Biol. Sci.* **2018**, *8*, 23–30.
34. Mohapatra, S.; Rekha, K.S. Sensor-Cloud: A Hybrid Framework for Remote Patient Monitoring. *Int. J. Comput. Appl.* **2012**, *55*, 7–11. [\[CrossRef\]](#)
35. Hamrioui, S.; Díez, I.D.L.T.; Garcia-Zapirain, B.; Saleem, K.; Rodrigues, J.J.P.C. A Systematic Review of Security Mechanisms for Big Data in Health and New Alternatives for Hospitals. *Wirel. Commun. Mob. Comput.* **2017**, 2017, 1–6. [\[CrossRef\]](#)
36. Logambal, M.; Thiagarasu, V. Healthcare Monitoring Systems: A WBAN Approach for Patient Monitoring. *Int. J. Future Revolut. Comput. Sci. Commun. Eng.* **2017**, *3*, 26–31.
37. Buccafurri, F.; Fotia, L.; Lax, G. Privacy-preserving resource evaluation in social networks. In Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust, Paris, France, 16–18 July 2012; pp. 51–58.
38. Huang, H.; Gong, T.; Ye, N.; Wang, R.; Dou, Y. Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System. *IEEE Trans. Ind. Inform.* **2017**, *13*, 1227–1237. [\[CrossRef\]](#)
39. Farooq, S.M.; Hussain, S.M.S.; Kiran, S.; Ustun, T.S. Certificate Based Authentication Mechanism for PMU Communication Networks Based on IEC 61850-90-5. *Electronics* **2018**, *7*, 370. [\[CrossRef\]](#)
40. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4. *Comput. Commun.* **2020**, *153*, 311–335. [\[CrossRef\]](#)
41. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 457–464.
42. Ali, T.; Masood, K.; Irfan, M.; Draz, U.; Nagra, A.; Asif, M.; Alshehri, B.; Glowacz, A.; Tadeusiewicz, R.; Mahnashi, M.; et al. Multistage Segmentation of Prostate Cancer Tissues Using Sample Entropy Texture Analysis. *Entropy* **2020**, *22*, 1370. [\[CrossRef\]](#) [\[PubMed\]](#)
43. Tewari, A.; Verma, P. Security and Privacy in E-Healthcare Monitoring with WBAN: A Critical Review. *Int. J. Comput. Appl.* **2016**, *136*, 37–42. [\[CrossRef\]](#)
44. Draz, U.; Ali, T.; Yasin, S. Towards Pattern Detection of Proprotein Convertase Subtilisin/kexin type 9 (PCSK9) Gene in Bioinformatics Big Data. *NFC IEFER J. Eng. Sci. Res.* **2018**, *6*, 160–165.
45. Al-Qaseemi, S.A.; Almulhim, H.A.; Almulhim, M.F.; Chaudhry, S.R. IoT architecture challenges and issues: Lack of standardization. In Proceedings of the 2016 Future Technologies Conference (FTC), San Francisco, CA, USA, 6–7 December 2016; pp. 731–738.

-
46. Caviness, J.A. Wireless Sensing for Healthcare Solutions. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 923–927.
 47. Pandey, I.; Dutta, H.S.; Banerjee, J.S. WBAN: A Smart Approach to Next Generation e-healthcare System. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 344–349.
 48. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [[CrossRef](#)]
 49. Shuwandy, M.L.; Zaidan, B.B.; Zaidan, A.A.; Albahri, A.S. Sensor-Based mHealth Authentication for Real-Time Remote Healthcare Monitoring System: A Multilayer Systematic Review. *J. Med. Syst.* **2019**, *43*, 33. [[CrossRef](#)]
 50. Nowakowski, G. REST API safety assurance by means of HMAC mechanism. *Inf. Syst. Manag.* **2016**, *5*, 358–369.
 51. Niksaz, P.; Branch, M. Wireless body area networks: Attacks and countermeasures. *Int. J. Sci. Eng. Res.* **2015**, *6*, 556–568.