Smart Secure and Energy Efficient Scheme for E-Health Applications using IoT: A Review

Mamoona Humayun
Department of Information Systems
College of Computer and Information Sciences
Jouf University
Al-Jouf, KSA
mahumayun@ju.edu.sa

NZ Jhanjhi
School of Computer Science and Engineering (SCE), Taylor's University, Malaysia
noorzaman.jhanjhi@taylors.edu.my

Malak Z Alamri
Department of Information Systems
College of Computer and Information Sciences
Jouf University
Al-Jouf, KSA
mzalamri@ju.edu.sa

Abstract
IoT devices have gained rapid growth by providing the interconnection of heterogeneous objects such as Sensors, smart devices, wearable, etc. IoT revolutions touch all areas of our daily life, mainly the health domain with better health surveillance and monitoring. However, they are extremely vulnerable and exploitable at the same time, which increases the consciousness of a patient's life. It is evident that the IoT devices are resource constraints, which results in increased challenges to address security in conventional ways. A good number of schemes have been proposed by several researchers to address these issues. However, most of them are providing a partial solution, with less or almost no mobility of the patient, where the distance from the base station may vary, as well as the possibility of the handover of base stations. This brings ease and opens the endless doors for a network to be compromised easily. This research focused to shorten the distance by adopting a multi-group node concept for communicating with the base station, which leads to the energy-efficient scheme with enhanced security, with patient's mobility support. Our proposed model will address the raised issues by curbing the communication distance during data transfer from patient to the base station, as well the iterations of key exchange communication where the base station does not require to communicate with each individual node, but with the group nodes. These research findings will help IoT practitioners and researchers by providing them with a secure and efficient scheme of data transmission. The proposed model will be validated using a survey and expert opinion, while future validation of the model will be done using simulation.

Keywords: *Security; Efficiency; Healthcare; IoT; Sensors; Energy-efficiency; Base Station*

1. Introduction

In recent decades, a new paradigm Internet of Things (IoT) has been observed in the field of the wireless sensor network. IoT is the interconnectivity of heterogeneous devices such as sensors, smartphones, wearable, etc. IoT has made all the daily used objects (human, home appliances, vehicles, etc.) addressable and locatable on the internet. IoT-enabled devices and smart sensors are helping us in almost all fields of life by providing us with air and water cleaning, smart cities, smart agriculture, cutting food and energy waste and most importantly fighting various illnesses by connecting patients to the doctor. Almost every field of modern life is affected by IoT, but healthcare is considered as one of the important applications of IoT [1-4]. Modern IoT-Enabled healthcare system also known as the e-health system is an interconnected wireless network that is composed of wearable sensors interconnected with one or more base stations. Wearable sensors attached to the human body are used to collect patients' information e.g. blood pressure, heart rate, sugar, etc. and send it to the nearby base station. Then the data from the base station is sent to the main server of the hospital for further decision making. Hence, we can say that IoT enables the healthcare system to provide continuous patient monitoring and thus help in providing emergency care to the patient [5-7]. However, the other side of the coin is that IoT devices are vulnerable to various security attacks due to the use of a wireless medium of communication. Besides, the key characteristics of IoT devices such as low capability in terms of energy and computing make it difficult to implement complex security schemes, therefore, they become an ideal target for attackers [2, 7, 8].

Manuscript received April 5, 2020
Manuscript revised April 20, 2020

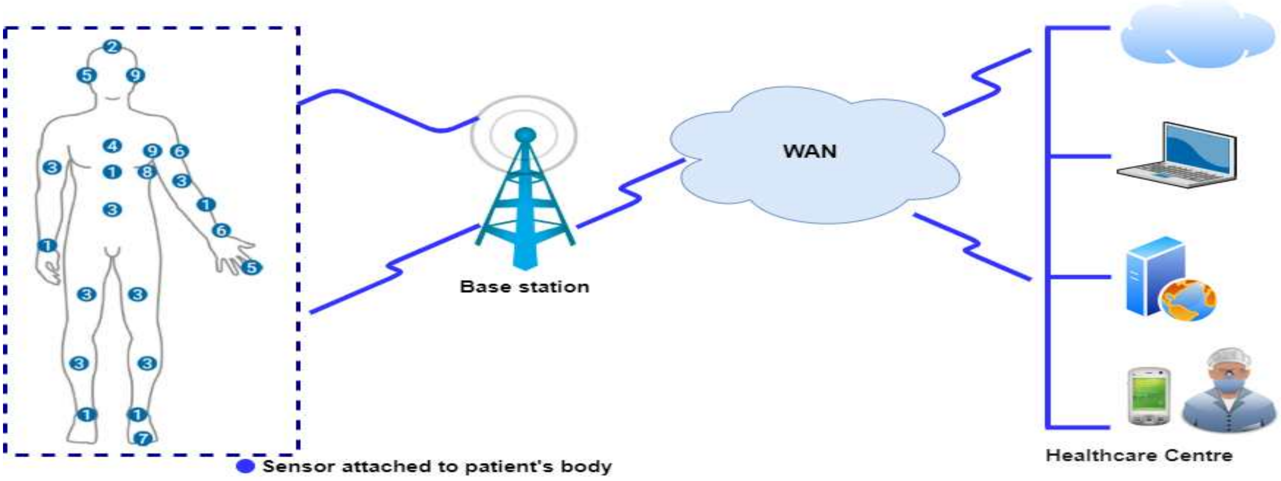


Fig.1. How IoT-enabled E health system work

Figure 1 shows the basic structure of IoT enabled health system, where various sensors are attached to the human body and are forming a wireless body area network (WBAN) for monitoring the vital health conditions. This WBAN is connected to a base station that can be any smart device, e.g. smartphone, laptop, PDA, etc. that captures the data from these individual nodes/sensors and send this data to the healthcare center through the internet. The idea in the picture seems very simple and easy to implement but the reality is somehow different. WBAN solutions promise various benefits but still, they are facing several issues that need to be tackled to make them efficient and reliable [9-11]. The sensors in WBAN are continuously monitoring patient's health conditions due to which its battery power is depleted and sometimes it is not able to send patients' vital health information to the base station. Further, these low powered IoT enabled devices are vulnerable to various security attacks. A lot of research efforts have been done to address the issue of security and efficiency of data transmission. Still, the transmission of data from a wearable sensor to the base station securely and efficiently is an important issue that needs to be addressed. Further, the distance between the base station and the wearable sensor also increases in the case of a patient's mobility. Some more issues include the distance of wearable sensors from each other and communication overhead in case of simultaneous data transmission from sensors to the base station [12-14].

The aforementioned issues are very important and researchers and practitioners working in this area need awareness about the security problems faced. This research aims to provide a solution for some key challenges that are faced by IoT based healthcare system. The main contribution of the paper involves: providing secure and efficient data transmission from wearable sensors to base station. Secondly, the proposed solution is energy efficient, portable, scalable, and reliable with mobility support. The proposed framework has been tested using the Delphi technique, and the results are positive against the determined threshold value.

This research paper consists of six mains sections; sections 1 is an introduction that provides an overview of IoT-enabled health care applications and the challenges faced. Section 2 defines key terminologies that are necessary to understand the proposed scheme. Section 3 provides a detailed literature review which includes existing work in the area done so far and their comparison. Section 4 includes our proposed system model followed by section 5 that provides the discussion of survey results. Finally, Section 6 summaries the article and provide insights into future work.

2. Background

Before proceeding towards the discussion of existing work, we briefly define some important terminologies that are necessary to understand the area under study

2.1. Internet of things

IoT is a concept of connecting anything/object to the internet and other connected devices. These connected IoT devices have a unique identifier and they possess the ability to transfer data over the network. Although IoT has impacted almost every field of life, however; it has impacted the healthcare system a lot beyond its traditional boundaries. IoT has revolutionized the healthcare industry by providing a myriad number of devices [15-18].

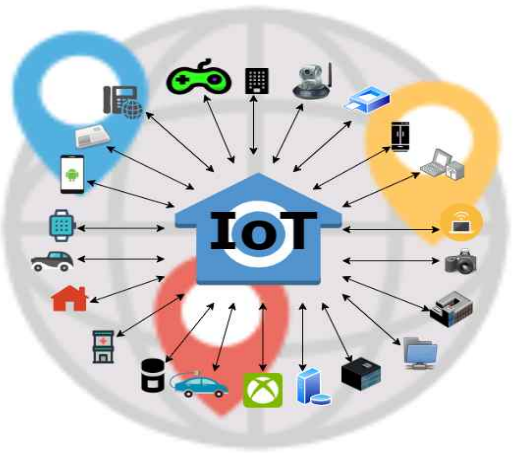


Fig.2. Internet of Things

IoT devices are either attached to the human body or are implanted for gathering vital patient information such as temperature sensing, BP sensing, ECG, Glucose level, etc. These devices aim to provide timely medical services to patients. The use of IoT devices in the field of healthcare is tremendously growing due to the benefits associated with it. These benefits include disease management, remote monitoring, test automation, preventive care, reducing cost, etc. [19-24].

2.2. WPAN

The e-healthcare system, also known as an m-healthcare system include wireless personal area network(WPAN) in which sensor nodes are attached to the human body and are connected to each other at a small scale. This WPAN gathers vital biological information about the patient and reports this information to the nearby base station. WPAN is a wireless network technology used for communicating over a short distance and in case of low powered devices. Its range usually vary from a few centimeters to few meters [25-28].

Fig. 3. Wireless Personal Area Network

2.3. WBAN

WBAN also referred to as BAN (body area network) or MBAN (medical body area network) or BSN (body sensor network). It is a wireless network consisting of wearable computing devices. WBAN devices can be implanted, embedded inside the human body, mounted on the human body at a fix position or maybe devices that humans can carry with them in different positions by hand or in pockets/bags [29]. WBAN technology started around 1995 with the idea of using WPAN for communicating near or around the human body. However, now the term WBAN refers to the system where communication is totally within the human body or in a very close proximity of it. WBAN can use WPAN as a gateway for connecting wearable devices to the internet. In this way, the healthcare system can access patients' information online and independent of patient's location [25,30-33].

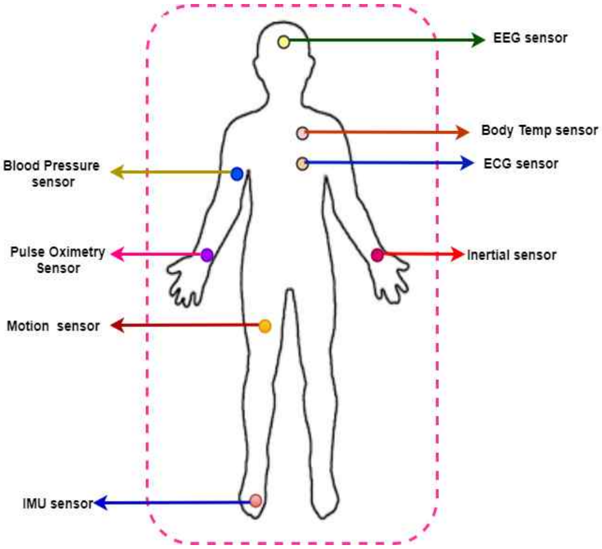


Fig.4. Wireless Body Area Network

2.4. WLAN

The term WLAN in e-health refers to the network that connects two or more devices within a limited area using wireless devices. It provides the ability to the patient for moving around the hospital in the range of a network. WLAN can be connected to the internet using gateway [34, 35]. Figure 5 shows the basic architecture of WLAN

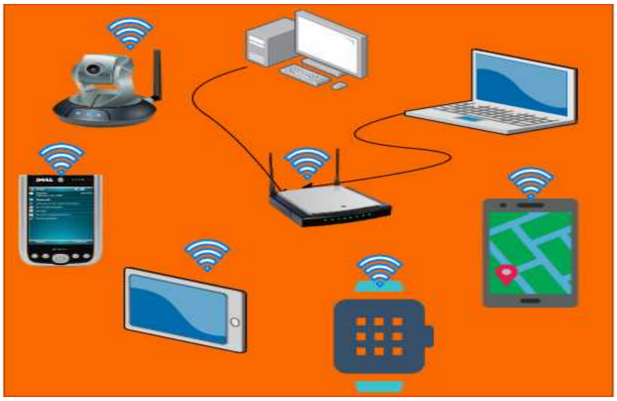


Fig.5. Wireless Local Area Network

2.5. RPL

In WBAN, wearable sensors are attached to the human body that collects the patient's biological information and send it to the nearby base station. These sensors are resource-constrained, therefore RPL protocol is preferably used for data transmission [36,37]. RPL is a standard routing protocol for IoT, it is used for low power and lossy network where devices are resource-constrained and we need the energy-efficient transmission of data. RPL protocol was designed by the RoLL working group and IETF defined it as a standard protocol to be used for low power and lossy networks (LLNs) [38]. This routing protocol uses a tree-based proactive routing structure in which an acyclic graph is created for data exchange among nodes. In RPL protocol, the network topology is in the form of a destination-oriented graph (DAG), that is usually composed of one or more destination-oriented directed acyclic graphs (DODAG). Where each DODAG represents a tree that consists of a root node also called a sink node. RPL protocol uses objective function (OF) for constructing DODAG, this OF adopt routing metrics for calculating the best path between leave nodes and the root node [39-41].

2.6. HOW RPL WORK

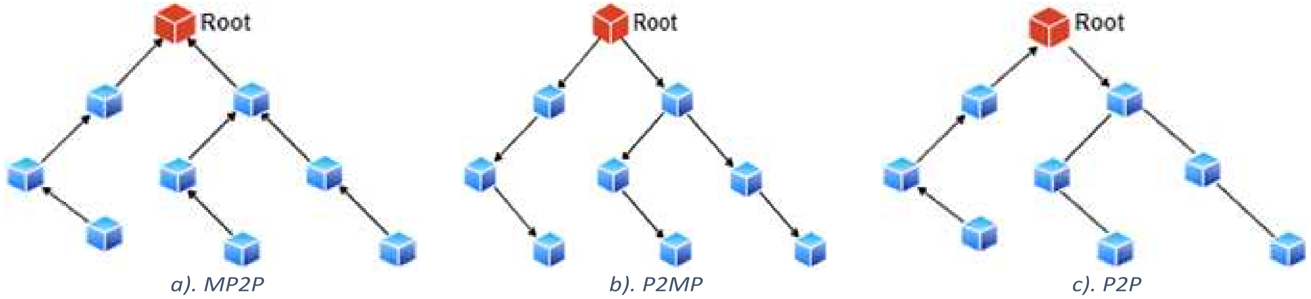


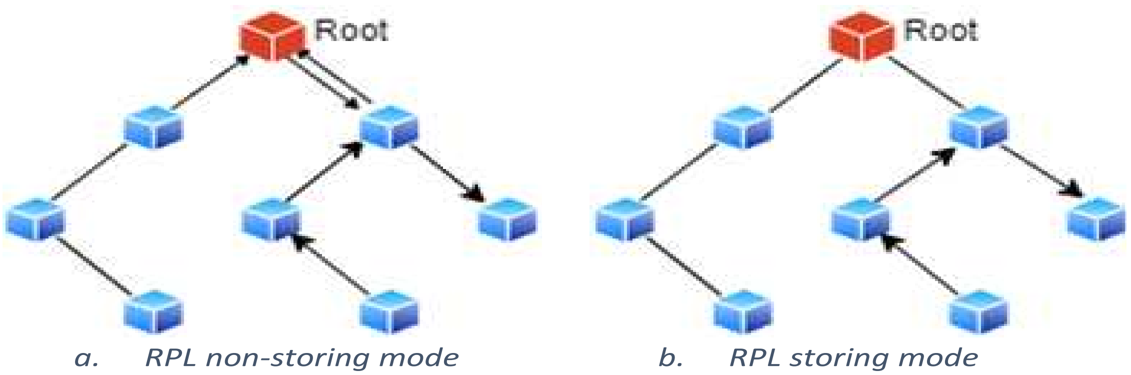
Fig.6. Traffic Patterns Supported by RPL

The first step in RPL operation is DODAG creation that is usually created by the root node, the root that constructs DODAG send the DIO (DODAG information object) message to its neighboring nodes. This DIO consists of various information such as node rank, OF, mode of operation (MOP) and metrics. All the nodes that receive DIO message must process it to decide whether they want to join DODAG or not, this decision is made based on OF used. Once a node decides to join the DODAG, an upward path is created from that node to the root node. At this stage, the rank of a node is computed by refreshing its neighbor table and by choosing the preferred parent based on the lowest rank computed using OF. Some routes are configured in such a way that they serve as a router by providing routes to other nodes. Router node must update the data table and should resend the DIO message to its neighboring nodes otherwise it will be considered as a leaf node in the routing tree. The node that receives a DIO message is responsible for processing it and to continue the operation until all network nodes may be traversed. RPL allows any new node to join the network by using DIS (DODAG information solicitation) message for requesting DIO message of already incorporated nodes in DODAG. Once the DIO message is received, the new node chooses its preferred parent according to OF. DIO message is also used for DODAG maintenance as it is periodically sent for maintaining network stability [42-44].

RPL supports both upward and downward routes. Upward routes are created during the process of DIO sending while downward routes need to handle DAO (Destination advertisement object) messages. This DAO message is processed according to RPL MOPs. DAO message also needs the acknowledgment receipt that is usually done by using DAO-ACK messages. RPL is preferably designed for multipoint-to-point (MP2P) traffic pattern, however; it also supports point-to-point (P2P) and point-to-multipoint (P2MP) [39,42, 45]. In MP2P, the data message is sent to the root node by creating an upward flow as shown in Figure 6a.In P2MP also known as multicasting, root node send the message to other nodes by producing a downward flow as shown in Figure 6b. In P2P, a nod can send the messages to another non-root node thus both upward and downward flow is required as shown in Figure 6c

2.7. RPL MODE OF OPERATIONS (MOPS)

RPL protocol defines four MOPs that might be chosen while considering the traffic pattern, the choice of traffic pattern depend on the application and the nodes' computational capacity. The first RPL MOP is MOP 0, MOP o only maintains the upward route and does not provide support for downward routes, therefore; only MP2P traffic is enabled. The second MOP of RPL is MOP 1 also called non-storing MOP, it only supports downward routed, therefore, both P2P and MP2P traffic patterns can be used. However; in MOP 1, downward routes are maintained via root node which means that all the downward traffic should be sent to root node and root node will forward it to the destination as shown in Figure 7a. The third MOP named as MOP 2 or storing without multicast supports downward routes. Unlike MOP1, in MOP 2 nodes maintain a routing table individually to provide downward traffic support. This routing table is constructed using DAO messages. Hence, downward traffic in MOP2 occurs without involving root nodes as shown in Figure 7b. The last MOP defined by RPL protocol is MOP3 also known as storing with multicast MOP, It’s functioning is similar to MOP2 plus multicast data sending is also possible in it. In this transmission mode, the non-root node is allowed to send messages to a group of nodes that is formed using multicast DAOs [39-42,46].



a. RPL non-storing mode

b. RPL storing mode

Fig.7. P2P message forwarding using MOP1 and MOP 2

2.8. RPL ATTACKS

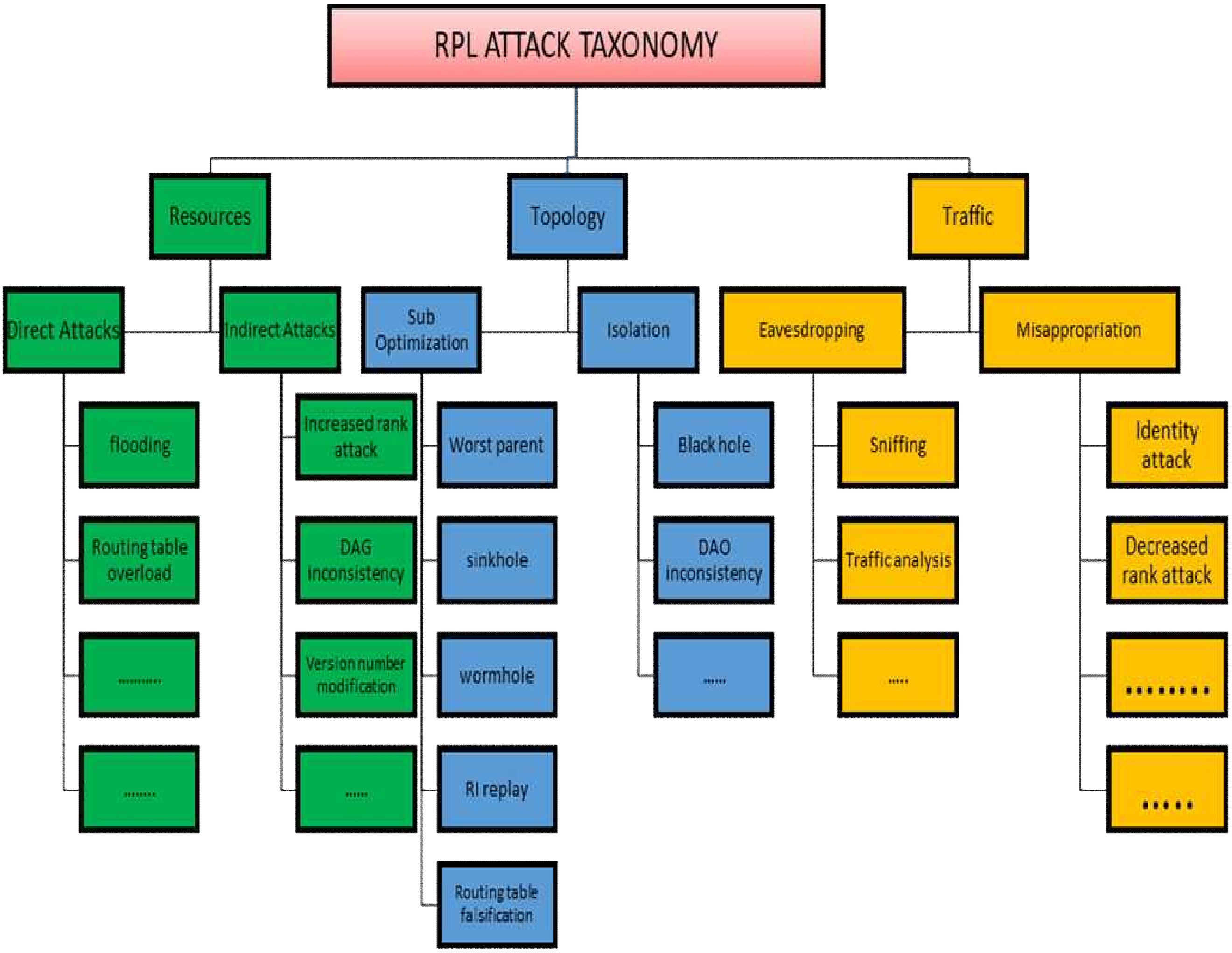


Fig.8. RPL Attack Taxonomy

In the current era, IoT has become a mainstream topic for practitioners and researchers and the world is embracing it at a rapidly growing speed due to its potential benefits and it is expected that in 2020 about 50 billion devices will be connected to the internet [47]. Although IoT has impacted almost every field of life, one of its potential and a significant role is in the field of healthcare where it has brought tremendous changes such as real-time monitoring, data collection and analysis, time to time tracking and alerts, remote medical assistance and better and affordable connectivity. According to iotfrall.com, the IoT healthcare market is expected to reach 14,660 million US dollars by 2022. This tremendously increasing growth of interconnected devices has shifted the paradigm from IPv4 to IPv6 as IPv4 only supports 4.2 billion possible addresses. IPv6 has several advantages over IPv4 such as support for large IoT networks by providing plenty of addresses, helping in preserving battery lifetime of IoT devices and reducing maintenance and administrative load [48-50].

The increasing cost of healthcare and the growth of chronic diseases around the world highly demand the transformation from traditional healthcare systems towards a person-centered environment. This transformation demands that a secure and efficient IoT network needs to be considered more actively. IoT network for healthcare deals with personal data collected through resource-constrained wearable sensors, therefore; it might be vulnerable to various security threats. In IoT-bases healthcare system, patient data privacy and security is a major concern due to some key challenges such as wireless communication between devices, direct human involvement and resource constraints of IoT sensors. Existing security solutions including existing security protocols, cryptographic methods, and privacy assurance techniques are not suitable for IoT networks due to the above-mentioned challenges. Keeping in view the challenge of resource-constrained IoT devices, Internet Engineering Task Force (IETF) has standardized RPL as the routing protocol to be used for low power and lossy networks (LLNS) and ECC has been proposed as an effective cryptographic technique for LLNs due to its shortest key length [51-55].

The above discussion shows that secure communication in IoT based healthcare network is a challenge despite the use of preferred cryptographic techniques and standardized protocol for LLNs. Although RPL is a standardized protocol for LLNs and it has self-healing capability, still it is vulnerable to various security threats as depicted in the RPL attack taxonomy shown in Figure8. RPL attacks are mainly categorized into three areas namely; resources, topology, and traffic [56-62]as shown in Figure 8.

2.9. Elliptic curve cryptography (ECC)

WBAN has been known as one of the promising wireless sensor technologies in the field of healthcare for real-time patient monitoring and real-time information exchange. However, the lack of proper security measures while exchanging patient data may lead to disaster. Therefore, sending patient data to the concerned person safely and securely is a big challenge that needs to be addressed. There exist a lot of data protection techniques, one of the commonly used techniques of encryption is ECCC. ECC is one of the best known asymmetric cryptographic algorithms which have attracted a lot of attention along with other asymmetric cryptographic algorithms such as RSA. The reason for getting this much attention from researchers and practitioners is its shortest key length as compared with RSA especially in the case of WBAN sensors technologies where sensors have limited computational power. ECC 160 bit key provides equivalent security level as provided by RSA using a 1024 bit key [6, 7, 63-66].

3. Literature Review

The role of IoT in healthcare is remarkable and a lot of research is going on to improve the healthcare system using IoT. However, a security attack on IoT based healthcare systems is a great challenge due to the low computational power of the attached IoT devices. In this section, we will discuss various cybersecurity attacks targeting IoT based healthcare system along with the existing solution to overcome these attacks.

[17] has provided a comprehensive survey to explore diverse aspects of IoT-based healthcare technologies by presenting different network architectures that facilitate IoT-based healthcare system. This paper has discussed that how IoT has played its role in various dimensions of healthcare, it also discusses industrial trends and enabling technologies to show that how advancement in IoT devices have motivated the healthcare industry to expand IoT-based healthcare services cost-effectively. The paper also focuses on the security dimension of IoT-based healthcare system and provides various security issues and challenges and propose a model for mitigation of these problems. Further, it also presents IoT rules and regulations for helping stakeholders who are interested in the assessment of IoT-based healthcare technologies. To conclude, this paper is helpful for researchers and practitioners who are working in IoT and healthcare technologies.

[20] has proposed a model for the secure transmission of medical data in the IoT environment. This model is composed of four steps which include (1) data encryption in which the patient's data encrypted using a hybrid encryption scheme that is based on two well-known algorithms AES and RSA. (2) Next, the encrypted data is concealed into a cover image and a stego image of this data is produced. (3) In this step, data is extracted and finally, in (4) step data is decrypted to retrieve the original image. The proposed model was evaluated with the help of an experiment. The results of the experiment show that the proposed model is capable of concealing confidential data of patients into a cover image and there is minimal deterioration in stego-image received.

[21] have investigated the privacy issue in IoT based healthcare systems and tried to find the possible attacks that make the patient data vulnerable and inaccessible. Some of the challenges and attacks identified in this study include data breaches, eavesdropping, impersonation, data integrity, and collusion. The authors in this paper have proposed a

framework named PrivacyProtector for secure storage and transmission of patients' data. This framework is based on four schemes like traditional IoT infrastructure for healthcare applications. These schemes include IoT network, medical sensors, storage system, and patient data access control system (PDAC). However, the proposed framework only considers the last two schemes, namely the storage system and PDAC. Therefore the main focus of the paper is on security in communication aspects. The mechanisms proposed to secure data from internal and external attacks are key cryptosystem and secret sharing. The scheme presented for secret sharing is SW-SSS (Slepian- Wolf-coding-based secret sharing). The proposed scheme helps to optimize the size of the secret share and also provide the share repairs. The author suggests to keep patients' data on multiple cloud servers to avoid data loss, these multiple servers collaborate for providing patients' data to healthcare providers without revealing its contents.

[24] has proposed a lightweight and secure authentication scheme for transmitting patient data safely from attached sensors to the base station. The proposed architecture in this study consists of wearable sensors, a base station, and a group node. The data of wearable sensors is received by the group node and is forwarded to the base station. This scheme is different from the existing scheme in the sense that it introduces the concept of group node, this group node plays the role of leader and distributes the authentication key among all wearable sensors. Further, the group node is less constrained in terms of computational power and energy as compared to other wearable sensor nodes. The communication overhead decrease on low powered wearable sensors due to group node therefore this scheme is energy efficient. Further, wearable devices are attached to various parts of the human body and thus they are far from each other. This distance between wearable sensor effect data transmission as these sensors are low powered but the group node solves this problem by reducing the distance. The proposed scheme was tested using the Contiki simulator and achieved results show that the proposed scheme is energy efficient and secure.

According to [67], sensors used in IoT-based healthcare are constrained devices therefore it is not feasible to use conventional cryptographic techniques at sensors level. However, a gateway in the existing IoT based system just serves as a connection point between IoT devices and cloud servers. This paper proposes a secure and efficient authentication architecture for IoT-based healthcare system in which gateway share the burden of resource-constrained IoT sensors by providing the services of authentication and cryptography. The proposed system architecture is composed of four main components: 1) Medical sensor network that include implantable or wearable sensors which collect patient's data 2) Smart e-health gateway that provides the services of protocol conversion, data aggregation and filtering 3) Back-end system that consists of remaining components including cloud computing platform, hospital database, and other devices. In the proposed architecture, the gateway performs authentication of remote end-users securely on behalf of medical sensors. This reduces the overhead on sensors without degrading security. The results of the study claim that proposed architecture reduces communication overhead by 26 % and communication latency from a smart gateway to end-users by 16 % as compared to existing approaches.

[68] have defined the layered architecture of IoT and discussed various cybersecurity attacks targeting different layers of IoT. According to this paper, some key attacks targeting the network layer of IoT include DoS (denial of service) attack, eavesdropping (including Man-in-the-Middle attack), spoofing and Sybil attack. On the other hand, the middleware also known as the support layer is the target of tampering data attack. The application layer of IoT is a target of harmful code injection and sniffing attacks. This paper has categorized Cyber-attacks on IoT based healthcare systems into two categories namely internal attacks and external attacks. Internal attacks include Trojan horses, password sniffing and data tampering while external attacks include DoS attack, Brute force attack and Man-in-the-middle attack. The authors of this paper have also discussed some key challenges that need to be considered while designing the IoT infrastructure of healthcare application and also suggested some solutions to overcome these challenges. The authors further emphasize an integrated security solution for IoT based healthcare systems instead of addressing security at the individual layer level.

A lightweight authentication scheme for IoT based healthcare applications is proposed in [69]. This scheme uses masked identity, nonces and key hashes authentication messages (HMAC) for ensuring the integrity of exchanged messages. According to this paper, IoT based healthcare system involves two types of devices namely constrained devices that are sensor nodes attached to or implanted on the human body and non-constrained device that is a base station in their case. In this scheme, patient data is collected via sensors planted in or on his body and this data is then transmitted to the base station using wireless technology. The authors in this paper prefer to use smartphones as a base station to provide mobility. The base station transmits the received data to the caregiver using the internet. This scheme is helpful in transmitting data safely in an insecure environment and provide resistance against eavesdropping and replay attacks. According to authors, there is no chance to impersonate a sensor node due to masking its identity, data integrity is maintained through HMAC code verification, mutual authentication, no replayed messages due to timestamps, the session key is used to ensure secure communication and the proposed model is also scalable as new nodes can join the system.

[70] have reviewed recent security attacks reported in Electronic healthcare applications and discussed possible solutions. The authors also discuss the security challenges that need to be considered while designing e-health systems. Various categories of attacks discussed in this paper include masquerade attacks (in which fake identity is used to get access) and the solution provided for this attack is mutual authentication between user and gateway. Next, the attacks on wearable and implantable devices are discussed, one common attack on these devices is a replay attack that can be

avoided through strong encryption and rolling code technique. Further, the author discusses some other attacks such as accountability and revocability attacks, data injection attack, internal and external cloud attack and the corresponding solutions as discussed in the existing literature.

[71] has discussed the importance of BSN (body sensor network) technology in healthcare applications. The authors have highlighted the major security requirements of the BSN based healthcare system and proposed a secure solution named BSN-care for it. The key security requirements in IoT- based healthcare systems using BSN discussed in this study include; data privacy, data integrity, data freshness, authentication, anonymity, and secure localization. The paper also discusses some popular IoT based healthcare projects that used BSN which include CodeBlue that was developed in the Harvard sensor network lab Alarm-net developed in the University of Virginia, UbiMon proposed in imperial college London and Median designed at Johns Hopkins University. All these projects mainly focus on reliability, power consumption, and cost-effectiveness and do not consider all security requirements. To address the above-mentioned issue, BSN-Care is proposed, BSN-Care architecture is composed of implantable and wearable sensors integrated with biosensors. These sensors collect the patient's information and forward it to the coordinator known as a local processing unit (LPU). This LPU is a portable device such as a smartphone or PDA that works as a router between BSN and the central server. If any abnormality is detected by LPU, an immediate alarm is sent to the person wearing bio-sensors. The proposed system efficiently addresses the maximum security requirements of the BSN based healthcare systems.

[72] have analyzed the current security schemes prevailing in the domain of IoT based healthcare systems and tried to identify the fundamental security requirements for proposing a robust security solution. According to this paper, the key security requirements for designing an efficient security solution for IoT based healthcare are 1) secure key generation 2) secure authentication and authorization and 3) secure end to end communication. The authors argue that IoT devices in healthcare are tiny and resource-constrained therefore they are vulnerable to various security threats and existing solutions do not apply to these resource-constrained devices. Based on the identified security requirements, a security model for IoT based healthcare systems has been proposed in this study. This model consists of three layers namely: device layer consisting of physical devices such as wearable sensors for collecting medical data; fog layer or the middleware that is the network of the interconnected gateway and a cloud layer that is responsible for sending data to the healthcare database server. To address the end-to-end security of data; three solutions have been provided in this study. These solutions include; Feature-Based Cryptographic Key Generation for sensor devices, mutual authentication of IoT components and mobility-based end-to-end communication. The proposed scheme was implemented by generating ECG-based cryptographic keys for all medical sensors attached, the communication between gateway and end-user was authenticated using certificate-based DTLS and session resumption technique was used for secure communication between medical sensors and end-users. The proposed model was evaluated using two different scenarios: in-home and hospital rooms. The results of the experiment show that the proposed scheme reduces communication overhead, communication latency and improve performance and energy efficiency.

[73]claims that IoT technologies have brought drastic changes in the healthcare industry, however; these resources constrained IoT devices are vulnerable to various security and privacy attacks. Some common security attacks discussed in this study include loss of data privacy, data hijacking and modification, location privacy, unpretentious authentication on medical/clinical procedure and attacks on Server Security. To save the IoT based healthcare system from the above-mentioned security risks, a model has been proposed in this study. This model is based on privacy, security and risk factors that were identified using a comprehensive analysis of the healthcare sector and practitioners. The authors claim that the proposed model serves as a base principle for the safe use of IoT in healthcare.

According to [74], conventional security solutions often provide security to patient's health data during communication. However, the attacks that target data at the time of cipher conversion and after cipher transmission are not adequately addressed yet. To overcome this issue, this paper proposes a scheme for IoT based healthcare security named SecureData to handle security concerns as mentioned before. The proposed scheme is based on 4 layer architecture which includes: 1) IoT sensor/Network devices layer that is responsible for collecting patient's health information and transmitting it. 2) Fog-layer that is responsible for forwarding patient's data towards a cloud data server 3) Cloud computing layer that summarizes and stores patient's data obtained as secret cipher shares by the IoT devices through Fog layer 4) healthcare provider layer that gets patient's information in a meaningful format. The proposed model only covers the first three layers of the proposed architecture. To ensure security at first two layers the model proposes two techniques, namely: lightweight field programmable array (FPGA) and hardware-based cipher algorithm by implementing the KATAN algorithm and, secret cipher share algorithm for protecting patient's data privacy. The cloud layer is protected using distributed database techniques. The key attack discussed in this study includes collusion attack, eavesdropping, impersonation, and patient data leakage and destruction. The performance of the proposed solution was validated using simulation and the results show that the proposed scheme is helpful in protecting security risks in IoT

TABLE 1: SUMMARY OF LITERATURE REVIEW

Ref	Paper Type	Research Method used	Main features or research contribution of the paper	Research Gap	Evaluation parameters
17	Survey	Comprehensive Survey	Provided comprehensive survey and analytics	Just explored existing Literature without any novel contribution	N/A
20	Technical Paper	Simulation	Proposes a hybrid security model for securing the diagnostic text data in medical images The proposed model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image	The security and efficiency of data transmission is not evaluated and compared with the state of the art	Security Performance
21	Exploratory study	General review provided	Proposed a practical framework called Privacy-Protector with the objective of preventing threats and attacks. Privacy-Protector includes a new idea of secret sharing and share repairing (in case of data loss or compromise) for patients' data privacy	The paper does not consider privacy in the data acquisition stage and the communication service provider stage	N/A
24	Technical paper	Simulation	proposed an efficient secured group-based lightweight authentication scheme for IoT based E-health applications	All transmission is dependent on the group node. The failure of the Group node will affect overall data transmission.	Energy efficiency Security Communication overhead
67	Conference Paper	Experiment	Proposed a secure and efficient authentication and authorization architecture for IoT-based healthcare using distributed smart e-health gateways called SEA	Do not address the patient's mobility Do not address system reliability and availability	Communication overhead Communication latency Scalability Reliability
68	Conference Paper	Review	Presented Overview of different IoT applications and their cyber vulnerabilities	General review provided, No novel contribution	N/A
69	Conference paper	Prototype development and evaluation	Proposed light-weight authentication scheme for an e-health application The proposed scheme allows both sensors and the Base Station (BS) to authenticate each other to secure the collection of health-related data	Do not address the patient's mobility Do not address system reliability and availability	Energy Performance Security Adaptability
70	Review Paper	Review	Provided general review about security attacks on e-healthcare along with their mitigation techniques	General review provided, No novel contribution	N/A
71	Technical Paper	Prototype development and evaluation	proposed a secure IoT-based healthcare system using BSN Identified various dimensions of healthcare data security	The paper only focus on security dimensions Some key parameters such as patient's mobility, system reliability, availability, scalability, communication overhead, and energy efficiency have not been discussed	Data Privacy Data Integrity Data Freshness Authentication Anonymity Security
72	Conference paper	Prototype development and evaluation	Proposed an end-to-end security scheme that was designed by generating ECG-based cryptographic keys for medical sensor devices, certificate-based DTLS handshake between end-users and smart gateways as well as employing the session resumption technique for the communications between medical sensor devices and end-users	The paper mainly focusses on security. However, the other factors including efficiency, throughput, and latency are not considered.	Energy Communication overhead Communication latency
73	Technical paper	Case Study	Proposed framework for IoT risk management in the healthcare industry	Model evaluation is missing	Security Privacy Risk
74	Technical paper	Simulation	Identified security challenges for e-healthcare	This paper mainly focuses on data security during conversion into cipher	Hardware frequency

			Proposed a scheme named as SecureData for data security and privacy in IoT-based healthcare.	and after cipher transmission. Some key parameters such as patient's mobility, system reliability, availability, and scalability have not been discussed	Energy cost Computation time

The above discussion is summarized in Table 1. It shows that IoT technologies have brought a great revolution in the field of healthcare especially patient monitoring through wearable sensors. However, secure and efficient transmission of data in IoT is a big challenge due to the limitation of resource constraints IoT devices. Various solutions have been provided to address the issue of security and efficiency in general. One of the main issues in IoT-based healthcare system is secure and efficient data transmission between wearable sensors and base station. It is an important concern because, in the whole IoT-based healthcare system, it is the most critical part due to the resource constraint nature of IoT devices attached to the human body that often lose signal and storage capacity while transferring data to the base station. The transmission of data from the base station to the main server is also important but is less crucial and vulnerable due to the good computational and storage capacity of devices involved. To address the above-mentioned issue, in this paper we will provide a model that is helpful in transmitting patient data securely and efficiently from wearable/attached sensors to the base station.

4. Proposed system model

IoT technologies have brought many positive changes in the field of healthcare, however, the issue of secure and efficient data transmission from IoT sensor nodes to the base station is still an issue that needs to be addressed. To do so, we have proposed a four-layered framework as shown in figure 9. The proposed framework is aimed to pass the sensory data in a more efficient and secure way, by reducing the communication iterations of the sensor nodes to the base station by involving the concept of multiple group nodes.

Framework Layer 1 consists of WBAN in which various IoT based sensors are attached to the patient body for monitoring his health. These sensors send the sensed data to the nearby group node, which is not resource-constrained and is responsible for key authentication/certificate sharing and data transfer to the base station. In this case, Individual nodes (resource-constrained) are not required to communicate with the base station directly, this improves the energy overhead and also increase the security level by reducing the communication iterations and distance. Layer 2 consists of the base station; group nodes recognize all the nodes in its network and vice versa. These group nodes are connected to the base station. Communication between the base station and the group node is secured using ECC and RPL. The patient's data collected from the group nodes is transmitted to the server via the base station. Layer 3 is the primary source of the internet cloud where data can be further processed and stored for the next use. Further, this layer is connected through a secure connection with layer 4. Layer 4 is the final destination of the data to be stored, examined and used for the patients' benefit. This layer provides authorized access of data to the concerned authorities including related Doctors, caretakers, and Hospital management.

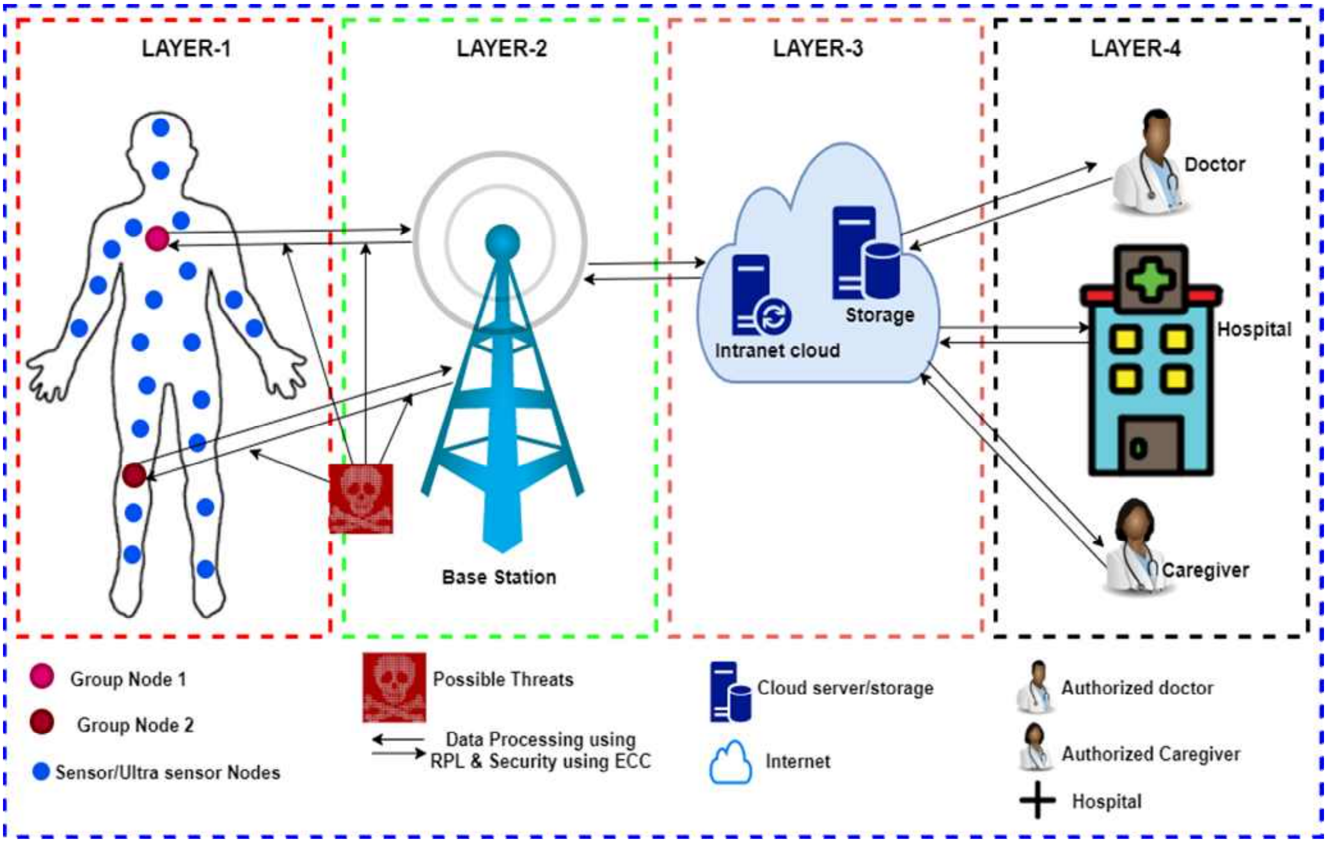


Fig.9. Proposed Model for secure and efficient data transmission between IoT sensors and base station

To evaluate the proposed framework, we identified the key parameters that are important for IoT based healthcare solutions. These factors/parameters include security, latency, mobility, patient data privacy, portability, scalability, communication overhead, reliability and efficient use of energy. These parameters were identified from literature in IoT based healthcare systems [75-78]. Based on identified parameters from literature, an online survey was prepared to gather experts' opinion about the validity of the proposed framework

The survey consists of two parts: part 1 was related to the demographic information of respondents and part two consists of respondents' opinion to know that whether the proposed framework adequately addresses the desired features or not.

The answer to each question in part two was on a Likert scale of 1-5, where 1 means strongly agree and 5 means strongly disagree. The threshold value was set to 70 %. This means if 70% of responses are strongly agree or agree in favor of any parameter, this means that the proposed framework adequately addresses that parameter.

5. Results and Discussion

As discussed above, an online survey was prepared using Google form and a survey link was sent to various researchers and practitioners in the field of IoT-based healthcare system. Table 2 shows the demographic information of respondents.

TABLE 2: DEMOGRAPHIC INFORMATION OF RESPONDENTS

Variables	Category	Total participant	Participant Percentage
Gender	Male	12	60%
	Female	8	40%
Age	20-29 years	1	5%
	30-39years	9	45%
	>=40years	10	50%
Education	Graduation	0	0
	Masters	5	25%
	PhD	9	45%
	Post Doc	6	30%
Role in IoT based Healthcare	Researcher	11	55%
	Practitioner	9	45%
Experience of research in IoT based healthcare	1-3 years	3	15%
	4-6years	5	25%
	>6years	12	60%
IoT-based healthcare usage experience	1-3Years	3	15%
	3-6 Years	5	25%
	>=6 Years	12	60%

Now we discuss the results against each parameter that were used to evaluate the proposed framework.

5.1. Security

IoT sensors also known as ultraviolet sensors are resource-constrained devices, therefore, they lose data during transmission and are easily vulnerable to various security attacks. We introduced the concept of multiple group nodes that are non resource-constrained devices, these group nodes collect all the data from trusted sensor nodes and send it to the base station. These group nodes are also responsible for authentication/certificate sharing. Further, traditional security mechanism does not apply to resource-constrained IoT sensors, Group nodes solve this problem as well. Thus we can say that the proposed model provides secure data transmission between sensor nodes and base station via group nodes. Below is the respondents' agreement regarding the security of the proposed framework/model.

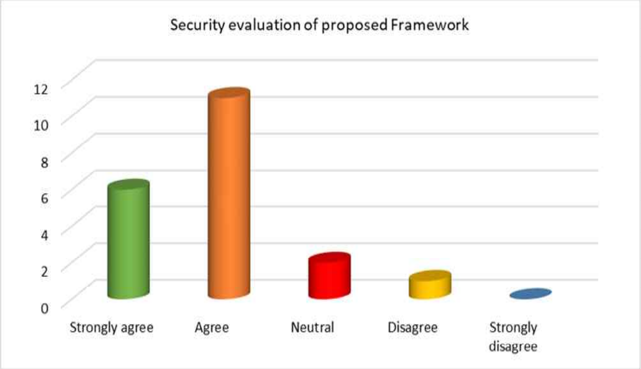


Fig.10. Security Evaluation of Proposed Framework

According to figure 10, 30% of respondents (6 out of 20) are strongly agree about the statement that the proposed scheme is more secure while 55 % (11 out of 20) are agree about it. On the other hand, 10 % (2 out of 20) respondents are neutral about it and 5 % (1 out of 20) were not agree. However, the good thing is that no one was totally disagree about it. The total percentage of agree and strongly agree was 85 % that is greater than the threshold value of 70%. This shows that proposed model adequately address security feature while transmitting patient's data.

5.2. Improved latency

Latency refers to the time interval between stimulation and response. The proposed scheme has introduced two group nodes that are resource sufficient and all the time available for data transmission and reception between sensor nodes and base station. Thus latency is improved in proposed scheme by reducing delay in communication. Figure 11 shows the respondents' view about the proposed scheme latency

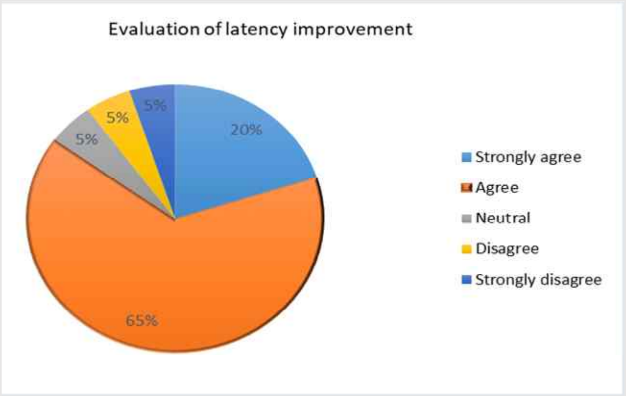


Fig.11. Latency improvement of Proposed Framework

According to Figure 11, 20 % of respondents (4 out of 20) were strongly agree that the proposed scheme improves latency by reducing delay in communication through resource sufficient group nodes. 65 %(13 out of 20) respondents agreed about it and 5 % (1 out of 20) were neutral, agree and disagree respectively. The total percentage of agree and strongly agree was 85 % that is greater than the threshold value of 70%. This shows that the proposed model improves latency while transmitting patient's data.

5.3. Mobility

Patient mobility inside the premises of the hospital is very important to get benefit from IoT devices. The other reason for mobility is limited resources available in healthcare centres. For example, healthcare centres have limited number of ICUs therefore the patient with less severity can be shifted to the ward if mobility is possible. The problem with IoT sensors is that they lose connection with the base station during mobility due to constrained resources. Group nodes can resolve this issue and thus make the patient's mobility possible. Figure 12 shows respondents view about mobility feature of the proposed framework

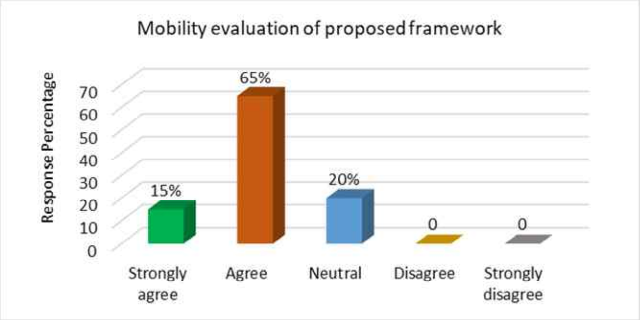


Fig.12. Mobility Evaluation of Proposed Framework

The results of Figure 12 shows that 15 %(3 out 0f 20) respondents strongly agreed with the statement that the proposed framework provides patient's mobility in the premises of the hospital, while 65 %(13 out of 20) respondents agreed with this. 20 %(4 out of 20) respondents were neutral about this but no one was disagree or strongly disagree about it. The total percentage of agree and strongly agree was 80 % that is greater than the threshold value of

70%. This shows that the proposed model support patient's mobility.

5.4. Patient data privacy

Healthcare data is very sensitive data and its privacy is very important. Leakages of this data to unauthorized users sometimes cause great loss or even death. Therefore, the privacy of patient data is very important. The proposed scheme uses a secure cryptography technique using ECC and RPL protocol for keeping the confidentiality and integrity of transmitted data. Figure 13 shows the respondents view about the privacy feature of the proposed framework

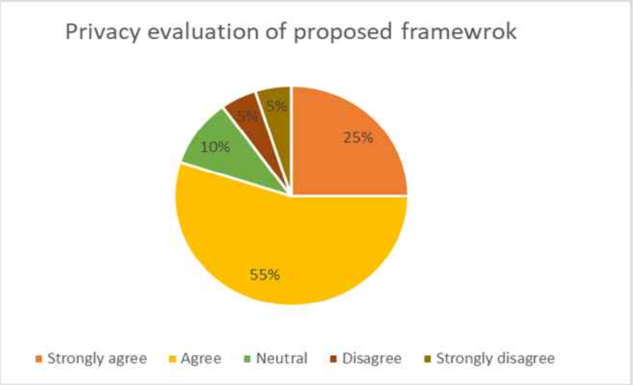


Fig.13. Privacy Evaluation of Proposed Framework

According to figure 13, 25% (5 out of 20) respondents strongly agreed that the proposed system provides patient's data privacy while 55% (11 out of 20) respondents agreed over it. However, 10% (2 out of 20) respondents were having no opinion about this. On the other hand, 5 % (1 out 0f 20) respondents disagreed and the same was the percentage of strongly disagree. The total percentage of agree and strongly agree was 80 % that is greater than the threshold value of 70%. This shows that the proposed model adequately address patient's data privacy.

5.5. Scalability

This feature is very important for all kinds of the network but especially useful in case of IoT based healthcare networks where any time new nodes need to be added or an old node might be deleted. This feature makes the network more flexible. The proposed framework provides the feature of scalability as a group node is responsible for nodes authentication and data transmission between sensor nodes and base stations. Figure 14 shows respondents' view about the support of scalability feature in the proposed framework

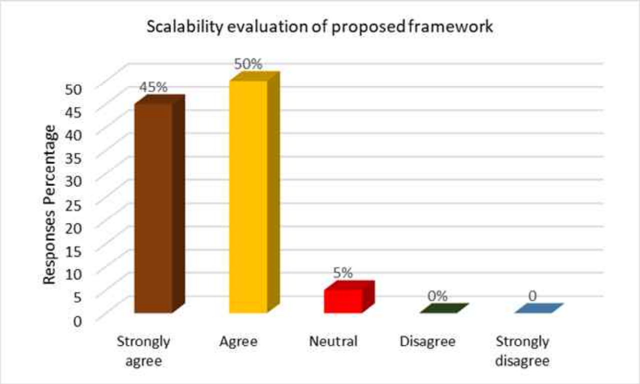


Fig.14. Scalability Evaluation of Proposed Framework

The graph of figure 14 shows that 45 % (9 out of 20) respondents were strongly agree about the scalability feature of the proposed framework while 50% (10 out of 20) respondents agreed over it. On the other hand, only 5 % (1 out of 20) respondents were not sure about it therefore the response from their side was neutral. Still, the agreement level is good as no one disagree or strongly disagree about it. The total percentage of agree and strongly agree was 95 % that is greater than the threshold value of 70%. This shows that the proposed model is scalable and new nodes can be added easily.

5.6. Communication overhead

WBAN is usually equipped with a lot of resource-constrained ultraviolet sensor nodes, these nodes need to communicate with the base station for data transmission. Transmission of data from multiple sensor nodes simultaneously increase communication overhead. The proposed scheme uses two group nodes that are resource sufficient. These group nodes collect data from nearby sensors and send it to the base station. This reduces communication overhead as only two group nodes need to communicate with the base station instead of multiple sensor nodes. Graph of figure 15 shows the respondents view about low communication overhead in the proposed framework

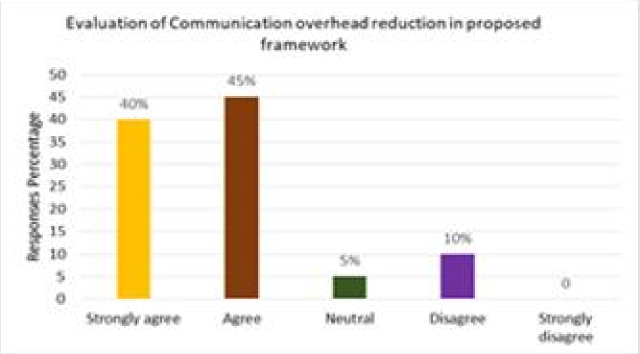


Fig.15. Communication overhead of Proposed Framework

The graph of figure 15 shows the respondents' agreement percentage about reducing communication overhead in data transmission. According to this, 40 % (8 out of 20) respondents strongly agreed that proposed framework reduces communication overhead of data transmission between sensor nodes and base stations by introducing two resource sufficient group nodes. 45 %(9 out of 20) respondents agreed about it while 5 %(1 out of 20) respondents were neutral over it. On the other hand, 10 % (2 out of 20) disagreed about it and no one strongly disagreed about the statement that the proposed framework reduces communication overhead of data transmission between sensor nodes and base station. The total percentage of agree and strongly agree was 85 % that is greater than the threshold value of 70%. This shows that the proposed model reduces communication overhead.

5.7. Reliability

In IoT based healthcare system, the timely transmission of patient's data is very important. The delay in transmission sometimes leads to a fatal disaster. However, IoT sensor nodes are not so reliable due to constraints of computing and storage resources. The proposed scheme is more reliable because in this case group nodes are not resource-constrained and they are responsible for timely data gathering from sensor nodes and transmitting it to the base station. Further, the proposed scheme gives the option of two group nodes, where one group node can share the burden of other group node. In this case, even if one group node fails due to some reasons the second group node continues data gathering and transmission. Figure 16 shows the respondents' view about the reliability of the proposed framework

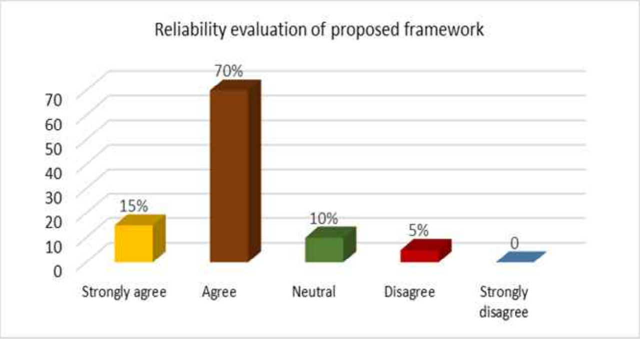


Fig.16. Reliability Evaluation of Proposed Framework

The graph of figure 16 shows that 15 %(3 out of 20) respondents were strongly agree about this statement that proposed framework provides reliable data transmission between sensor nodes and base station while 70 % (14 out of 20) respondents were agree about it. On the other hand, 10 % (2 out of 20) respondents were not sure about it so they chose to be neutral. Only 5 % (1 out of 20) respondents were not agree about the reliability feature of proposed scheme, however, no one was strongly disagree about it. The total percentage of agree and strongly agree was 85 % that is greater than the threshold value of 70%. This shows that proposed model is reliable.

5.8. Energy efficiency

Energy is one of the important concerns in IoT based healthcare technologies as most of the IoT devices are low powered and their energy degrade while transmitting data. The proposed framework is energy efficient as according to this framework, individual sensor nodes do not need to communicate with a base station that is at a distance from them ,rather they need to communicate with the group nodes only. Group nodes are responsible for collecting data from sensor nodes and transmitting it to the base station. Further, the nodes in the network will communicate with the nearest possible group nodes (from two group nodes). This will also reduce energy consumption. Figure 17 shows respondents' view about energy-efficient feature of the proposed framework

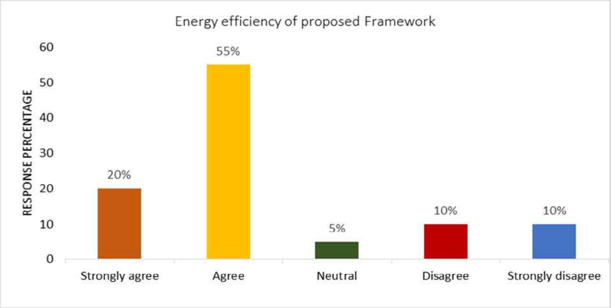


Fig.17. Energy Efficiency Evaluation of Proposed

According to the graph of figure 17, 20% (4 out of 20) respondents strongly agreed that the proposed scheme provides energy-efficient data transmission between sensor nodes and base station while 55% (11 out of 20) respondents agreed about it. 5 % (1 out of 20) respondent didn't give their opinion about it and chose neutral. 10 % of respondents (2 out of 20) were disagree and the same percentage was for strongly disagree. The total percentage of agree and strongly agree was 75 % that is greater than the threshold value of 70%. This shows that the proposed model consumes less energy and is suitable for resource constraints IoT devices.

5.9. Availability

Healthcare systems are considered critical systems as they deal with patients. Therefore, these systems must be 24/7 available so that the patient could get timely treatment in case of any emergency. However, an issue with these IoT based healthcare system is that the sensors attached to the human body which are responsible for sending patient information to the doctor are resource-constrained. Due to these constraints, these ultraviolet sensors are sometimes not able to transmit data. To overcome this problem, the proposed scheme has introduced two resource sufficient group nodes that are responsible for sending data between sensor nodes and base station. These group nodes are 24/7 available for data transmission and reception. Figure 18 shows the respondents'' view about the availability feature of the proposed framework

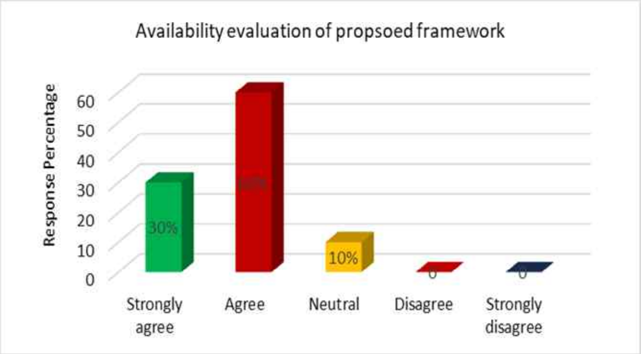


Fig.18. Availability Evaluation of Proposed

According to graph of figure 18, 30 % (6 out of 20) respondents strongly agreed about the existence of a 24/7 availability feature in the proposed framework while 60% (12 out of 20) respondents were agreed about it. On the other hand, 10 % (2 out of 20) respondents were not sure about their answer so they chose the option of neutral. However, none of the respondents was disagree or strongly disagree about the 24/7 availability of proposed framework architecture. The total percentage of agree and strongly agree was 90 % that is greater than the threshold value of 70%. This shows that the proposed model possess availability feature.

6. Conclusion and Future work

IoT devices have gained a rapid growth by providing interconnection of heterogeneous objects such as sensors, smart devices, wearable, etc. IoT revolutions touch all areas of our daily life, mainly the health domain with better health surveillance and monitoring. However, they are extremely vulnerable and exploitable at the same time, which increases the consciousness of patient's life. These resource-constrained devices are vulnerable to various security threats. Patient data security is one of the important concerns in the field of healthcare, as unauthorized access of this data can create many problems. To address these problems, this research has proposed a layered framework. This framework introduces two resource-sufficient group nodes that are responsible for collecting data from nearby ultraviolet sensors and sending it to the base station. Communication between the group nodes and the base station is secured using ECC through RPL. The proposed framework provides security as individual resource-constraint nodes not need to send data to the base station. In addition, the proposed scheme reduces the communication overhead, supports patient's mobility, and possesses the feature of scalability, availability, and reliability.

The proposed scheme was tested using the Delphi technique, in which a panel of expert was selected for evaluation of the proposed solution. We identified key parameters that affect tpatient's data transmission. Based on these parameters, an online survey was prepared. The survey link was sent to the panel of experts for evaluation. The results of the survey show that the proposed technique provides secure and efficient data transmission between ultraviolet sensor nodes and base station.

In the future, we are planning to validate the proposed scheme using simulation to get more insight into the proposed framework.

Acknowledgement

This research was fully funded by the Deanship of ScientificResearch at Jouf University, Al-Jouf, Saudi Arabia on 2019/2020 with grant number (40/222) and the APC was funded by Jouf University(JU)

REFERENCES

[1] Bhatt, C., Dey, N., and Ashour, A.S.: 'Internet of things and big data technologies for next generation healthcare', 2017

[2] Laplante, P.A., and Laplante, N.: 'The internet of things in healthcare: Potential applications and challenges', It Professional, 2016, 18, (3), pp. 2-4

[3] Yuehong, Y., Zeng, Y., Chen, X., and Fan, Y.: 'The internet of things in healthcare: An overview', Journal of Industrial Information Integration, 2016, 1, pp. 3-13

[4] Almusaylim, Z.A., and Zaman, N.: 'A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)', Wireless Networks, 2019, 25, (6), pp. 3193-3204

[5] Alaba, F.A., Othman, M., Hashem, I.A.T., and Alotaibi, F.: 'Internet of Things security: A survey', Journal of Network and Computer Applications, 2017, 88, pp. 10-28

[6] Kaur, H., Atif, M., and Chauhan, R.: 'An Internet of Healthcare Things (IoHT)-Based Healthcare Monitoring System': 'Advances in Intelligent Computing and Communication' (Springer, 2020), pp. 475-482

[7] Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., Virtanen, S., Tenhunen, H., and Isoaho, J.: 'End-to-end security scheme for mobility enabled healthcare Internet of Things', Future Generation Computer Systems, 2016, 64, pp. 108-124

[8] Li, S., Tryfonas, T., and Li, H.: 'The Internet of Things: a security point of view', Internet Research, 2016, 26, (2), pp. 337-359

[9] Pramanik, P.K.D., Nayyar, A., and Pareek, G.: 'Chapter 7 - WBAN: Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring: Architecture and Protocols', in D. Jude, H., and Balas, V.E. (Eds.): 'Telemedicine Technologies' (Academic Press, 2019), pp. 89-119

[10] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., and Shamshirband, S.: 'Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications', Egyptian Informatics Journal, 2017, 18, (2), pp. 113-122

[11] Darwish, A., and Hassanien, A.E.: 'Wearable and implantable wireless sensor network solutions for healthcare monitoring', Sensors, 2011, 11, (6), pp. 5561-5595

[12] Bayo-Monton, J.-L., Martinez-Millana, A., Han, W., Fernandez-Llatas, C., Sun, Y., and Traver, V.: 'Wearable sensors integrated with Internet of Things for advancing eHealth care', Sensors, 2018, 18, (6), pp. 1851

[13] Khan, S.F.: 'Health care monitoring system in Internet of Things (IoT) by using RFID', in Editor (Ed.)^(Eds.): 'Book Health care monitoring system in Internet of Things (IoT) by using RFID' (IEEE, 2017, edn.), pp. 198-204

[14] Pérez, J.B., Encinas, A.H., Martín-Vaquero, J., Queiruga-Dios, A., Nova, A.M., and González, J.T.: 'Proposal of Wearable Sensor-Based System for Foot Temperature Monitoring', in Editor (Ed.)^(Eds.): 'Book Proposal of Wearable Sensor-Based System for Foot Temperature Monitoring' (Springer, 2017, edn.), pp. 165-172

[15] Bhatia, M., and Sood, S.K.: 'A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective', Computers in Industry, 2017, 92-93, pp. 50-66

[16] Saheb, T., and Izadi, L.: 'Paradigm of IoT big data analytics in the healthcare industry: A review of scientific literature and mapping of research trends', Telematics and Informatics, 2019, 41, pp. 70-85

[17] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., and Kwak, K.-S.: 'The internet of things for health care: a comprehensive survey', IEEE Access, 2015, 3, pp. 678-708

[18] Khan, A., Jhanjhi, N., Humayun, M., and Ahmad, M.: 'The Role of IoT in Digital Governance': 'Employing Recent Technologies for Improved Digital Governance' (IGI Global, 2020), pp. 128-150

[19] Adhikary, T., Jana, A.D., Chakrabarty, A., and Jana, S.K.: 'The Internet of Things (IoT) Augmentation in Healthcare: An Application Analytics', in Editor (Ed.)^(Eds.): 'Book The Internet of Things (IoT) Augmentation in Healthcare: An Application Analytics' (Springer, 2019, edn.), pp. 576-583

[20] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., and Farouk, A.: 'Secure medical data transmission model for IoT-based healthcare systems', IEEE Access, 2018, 6, pp. 20596-20608

[21] Luo, E., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J., and Atiquzzaman, M.: 'Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems', IEEE Communications Magazine, 2018, 56, (2), pp. 163-168

[22] Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., and Priyan, M.: 'Centralized fog computing security platform for IoT and cloud in healthcare system': 'Fog Computing: Breakthroughs in Research and Practice' (IGI global, 2018), pp. 365-378

[23] Almulhim, M., and Zaman, N.: 'Proposing secure and lightweight authentication scheme for IoT based E-health applications', in Editor (Ed.)^(Eds.): 'Book Proposing secure and lightweight authentication scheme for IoT based E-health applications' (IEEE, 2018, edn.), pp. 481-487

[24] Almulhim, M., Islam, N., and Zaman, N.: 'A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications', INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 2019, 19, (1), pp. 107-120

[25] Elhayatmy, G., Dey, N., and Ashour, A.S.: 'Internet of Things based wireless body area network in healthcare': 'Internet of things and big data analytics toward next-generation intelligence' (Springer, 2018), pp. 3-20

[26] Iraqi, Y., and Mekouar, L.: 'Dynamic Adaptation for WPANs Collision Prevention in eHealth Environments', IEEE Access, 2019, 7, pp. 86730-86738

[27] Iraqi, Y., Rachidi, T., and Gawanmeh, A.: 'Collision-Prevention Conditions for Wireless Personal Area Networks', IEEE Networking Letters, 2018, 1, (1), pp. 22-25

[28] She, H., Lu, Z., Jantsch, A., Zheng, L.-R., and Zhou, D.: 'A network-based system architecture for remote medical applications', in Editor (Ed.)^(Eds.): 'Book A network-based system architecture for remote medical applications' (2007, edn.), pp.

[29] Lou, Z., Wang, L., Jiang, K., Wei, Z., and Shen, G.: 'Reviews of wearable healthcare systems: Materials, devices and system integration', Materials Science and Engineering: R: Reports, 2020, 140, pp. 100523

[30] Kim, T.-Y., Youm, S., Jung, J.-J., and Kim, E.-J.: 'Multi-hop WBAN construction for healthcare IoT systems', in Editor (Ed.)^(Eds.): 'Book Multi-hop WBAN construction for healthcare IoT systems' (IEEE, 2015, edn.), pp. 27-28

[31] Pervez Khan, M., Hussain, A., and Kwak, K.S.: 'Medical applications of wireless body area networks', International Journal of Digital Content Technology and its Applications, 2009, 3, (3), pp. 185-193

[32] Poongodi, T., Rathee, A., Indrakumari, R., and Suresh, P.: 'IoT Sensing Capabilities: Sensor Deployment and Node Discovery, Wearable Sensors, Wireless Body Area Network (WBAN), Data Acquisition': 'Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm' (Springer, 2020), pp. 127-151

[33] Wu, T., Wu, F., Redouté, J.-M., and Yuce, M.R.: 'An autonomous wireless body area network implementation towards IoT connected healthcare applications', Ieee Access, 2017, 5, pp. 11413-11422

[34] Negra, R., Jemili, I., and Belghith, A.: 'Wireless body area networks: Applications and technologies', Procedia Computer Science, 2016, 83, pp. 1274-1281

[35] Shaikh, Y., Parvati, V., and Biradar, S.: 'Survey of Smart Healthcare Systems using Internet of Things (IoT)', in Editor (Ed.)^(Eds.): 'Book Survey of Smart Healthcare Systems using Internet of Things (IoT)' (IEEE, 2018, edn.), pp. 508-513

[36] Pramanik, P.K.D., Upadhyaya, B.K., Pal, S., and Pal, T.: 'Chapter 1 - Internet of things, smart sensors, and pervasive systems: Enabling connected and pervasive healthcare', in Dey, N., Ashour, A.S., Bhatt, C., and James Fong, S. (Eds.): 'Healthcare Data Analytics and Management' (Academic Press, 2019), pp. 1-58

[37] Kamgueu, P.O., Nataf, E., and Ndie, T.D.: 'Survey on RPL enhancements: A focus on topology, security and mobility', Computer Communications, 2018, 120, pp. 10-21

[38] Umamaheswari, S., and Negi, A.: 'Internet of Things and RPL routing protocol: A study and evaluation', in Editor (Ed.)^(Eds.): 'Book Internet of Things and RPL routing protocol: A study and evaluation' (2017, edn.), pp. 1-7

[39] Gao, L., Wu, C., Yoshinaga, T., and Ji, Y.: 'Performance Evaluation of RPL-Based Sensor Data Collection in Challenging IoT Environment', in Editor (Ed.)^(Eds.): 'Book Performance Evaluation of RPL-Based Sensor Data Collection in Challenging IoT Environment' (Springer, 2018, edn.), pp. 275-285

[40] Kharrufa, H., Al-Kashoash, H., Al-Nidawi, Y., Mosquera, M.Q., and Kemp, A.H.: 'Dynamic RPL for multi-hop routing in IoT applications', in Editor (Ed.)^(Eds.): 'Book Dynamic RPL for multi-hop routing in IoT applications' (IEEE, 2017, edn.), pp. 100-103

[41] Kharrufa, H., Al-Kashoash, H.A., and Kemp, A.H.: 'RPL-based routing protocols in IoT applications: A Review', IEEE Sensors Journal, 2019, 19, (15), pp. 5952-5967

[42] Kharrufa, H., Salman, N., Lei, M., and Kemp, A.: 'A Performance Evaluation of RPL in Mobile IoT Applications: A Practical Approach', IFAC-PapersOnLine, 2019, 52, (24), pp. 312-317

[43] Mishra, S., Singh, P., Arora, D., and Agrawal, K.K.: 'Analyzing and evaluating the performance of 6L0WPAN and RPL using CONTIKI', in Editor (Ed.)^(Eds.): 'Book Analyzing and evaluating the performance of 6L0WPAN and RPL using CONTIKI' (IEEE, 2017, edn.), pp. 1100-1105

[44] Sankar, S., and Srinivasan, P.: 'Mobility and Energy Aware Routing Protocol for Healthcare IoT Application', Research Journal of Pharmacy and Technology, 2018, 11, (7), pp. 3139-3144

[45] Kamble, A., Malemath, V.S., and Patil, D.: 'Security attacks and secure routing protocols in RPL-based Internet of Things: Survey', in Editor (Ed.)^(Eds.): 'Book Security attacks and secure routing protocols in RPL-based Internet of Things: Survey' (IEEE, 2017, edn.), pp. 33-39

[46] Lamaazi, H., and Benamar, N.: 'A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function', Ad Hoc Networks, 2020, 96, pp. 102001

[47] Iqbal, M.A., and Bayoumi, M.: 'Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT', in Editor (Ed.)^(Eds.): 'Book Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT' (IEEE, 2016, edn.), pp. 523-530

[48] Hu, J., Wu, K., and Liang, W.: 'An IPv6-based framework for fog-assisted healthcare monitoring', Advances in Mechanical Engineering, 2019, 11, (1), pp. 1687814018819515

[49] Nasri, F., and Mtibaa, A.: 'IoT Platform for Healthcare System: Protocols Interoperability', International Journal of Applied Engineering Research, 2017, 12, (22), pp. 12510-12518

[50] Jia, S., Luckie, M., Huffaker, B., Elmokashfi, A., Aben, E., Claffy, K., and Dhamdhere, A.: 'Tracking the deployment of IPv6: Topology, routing and performance', Computer Networks, 2019, 165, pp. 106947

[51] Reddy, R.M., and Neerugatti, V.: 'Anomaly Based Technique for Detection and Prevention of Black Hole Attacks in RPL Based Networks', in Editor (Ed.)^(Eds.): 'Book Anomaly Based Technique for Detection and Prevention of Black Hole Attacks in RPL Based Networks' (2018, edn.), pp.

[52] Gafurov, K., and Chung, T.-M.: 'Comprehensive Survey on Internet of Things, Architecture, Security Aspects, Applications, Related

Technologies, Economic Perspective, and Future Directions', Journal of Information Processing Systems, 2019, 15, (4)

[53] Airehrour, D., Gutierrez, J., and Ray, S.K.: 'Securing RPL routing protocol from blackhole attacks using a trust-based mechanism', in Editor (Ed.)^(Eds.): 'Book Securing RPL routing protocol from blackhole attacks using a trust-based mechanism' (IEEE, 2016, edn.), pp. 115-120

[54] Adat, V., and Gupta, B.: 'Security in Internet of Things: issues, challenges, taxonomy, and architecture', Telecommunication Systems, 2018, 67, (3), pp. 423-441

[55] Hussain, K., Hussain, S.J., Jhanjhi, N., and Humayun, M.: 'SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET', in Editor (Ed.)^(Eds.): 'Book SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET' (IEEE, 2019, edn.), pp. 1-4

[56] Glissa, G., Rachedi, A., and Meddeb, A.: 'A secure routing protocol based on RPL for Internet of Things', in Editor (Ed.)^(Eds.): 'Book A secure routing protocol based on RPL for Internet of Things' (IEEE, 2016, edn.), pp. 1-7

[57] Sharma, D., Mishra, I., and Jain, S.: 'A detailed classification of routing attacks against RPL in Internet of Things', International Journal of Advance Research, Ideas and Innovations in Technology, 2017, 3, (1), pp. 692-703

[58] Mangelkar, S., Dhage, S.N., and Nimkar, A.V.: 'A comparative study on rpl attacks and security solutions', in Editor (Ed.)^(Eds.): 'Book A comparative study on rpl attacks and security solutions' (IEEE, 2017, edn.), pp. 1-6

[59] Perrey, H., Landsmann, M., Ugus, O., Schmidt, T.C., and Wählisch, M.: 'TRAIL: Topology authentication in RPL', arXiv preprint arXiv:1312.0984, 2013

[60] 60 Mayzaud, A., Badonnel, R., and Chrisment, I.: 'A Taxonomy of Attacks in RPL-based Internet of Things', 2016

[61] Sahay, R., Geethakumari, G., and Modugu, K.: 'Attack graph—Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT', in Editor (Ed.)^(Eds.): 'Book Attack graph—Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT' (IEEE, 2018, edn.), pp. 308-313

[62] Hussain, S.J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N., and Humayun, M.: 'IMIAD: Intelligent Malware Identification for Android Platform', in Editor (Ed.)^(Eds.): 'Book IMIAD: Intelligent Malware Identification for Android Platform' (IEEE, 2019, edn.), pp. 1-6

[63] Narayan, S.: 'A Review on Elliptic Curve Cryptography', International Journal of Emerging Technology and Innovative Engineering, 2018, 4, (12)

[64] Kavitha, S., Alphonse, P., and 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', Journal of medical systems, 2019, 43, (8), pp. 260

[65] Elhoseny, M., Shankar, K., Lakshmanaprabu, S., Maseleno, A., and Arunkumar, N.: 'Hybrid optimization with cryptography encryption for medical image security in Internet of Things', Neural computing and applications, 2018, pp. 1-15

[66] Mahto, D., Khan, D.A., and Yadav, D.K.: 'Security analysis of elliptic curve cryptography and RSA', in Editor (Ed.)^(Eds.): 'Book Security analysis of elliptic curve cryptography and RSA' (2016, edn.), pp. 419-422

[67] Rahimi Moosavi, S., Nguyen Gia, T., Rahmani, A.-M., Nigussie, E., Virtanen, S., Isoaho, J., and Tenhunen, H.: 'SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways', in Editor (Ed.)^(Eds.): 'Book SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways' (Elsevier, 2015, edn.), pp. 452-459

[68] Alromaihi, S., Elmedany, W., and Balakrishna, C.: 'Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications', in Editor (Ed.)^(Eds.): 'Book Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications' (IEEE, 2018, edn.), pp. 140-145

[69] Khemissa, H., and Tandjaoui, D.: 'A lightweight authentication scheme for e-health applications in the context of internet of things', in Editor (Ed.)^(Eds.): 'Book A lightweight authentication scheme for e-health applications in the context of internet of things' (IEEE, 2015, edn.), pp. 90-95

[70] Zeadally, S., Isaac, J.T., and Baig, Z.: 'Security Attacks and Solutions in Electronic Health (E-health) Systems', Journal of Medical Systems, 2016, 40, (12), pp. 263

[71] Gope, P., and Hwang, T.: 'BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network', IEEE Sensors Journal, 2016, 16, (5), pp. 1368-1376

[72] Moosavi, S.R., Nigussie, E., Levorato, M., Virtanen, S., and Isoaho, J.: 'Performance analysis of end-to-end security schemes in healthcare IoT', Procedia computer science, 2018, 130, pp. 432-439

[73] Zakaria, H., Bakar, N.A.A., Hassan, N.H., and Yaacob, S.: 'IoT Security Risk Management Model for Secured Practice in Healthcare Environment', Procedia Computer Science, 2019, 161, pp. 1241-1248

[74] Tao, H., Bhuiyan, M.Z.A., Abdalla, A.N., Hassan, M.M., Zain, J.M., and Hayajneh, T.: 'Secured data collection with hardware-based ciphers for IoT-based healthcare', IEEE Internet of Things Journal, 2018, 6, (1), pp. 410-420

[75] Baker, S.B., Xiang, W., and Atkinson, I.: 'Internet of things for smart healthcare: Technologies, challenges, and opportunities', IEEE Access, 2017, 5, pp. 26521-26544

[76] Alraja, M.N., Farooque, M.M.J., and Khashab, B.: 'The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception', IEEE Access, 2019, 7, pp. 111341-111354

[77] Solangi, Z.A., Solangi, Y.A., and Aziz, M.S.A.: 'An empirical study of Internet of Things (IoT)—Based healthcare acceptance in Pakistan: PILOT study', in Editor (Ed.)^(Eds.): 'Book An empirical study of Internet of Things (IoT)—Based healthcare acceptance in Pakistan: PILOT study' (IEEE, 2017, edn.), pp. 1-7

[78] Fatima, S., and Sayeed, A.: 'IOT based health care monitoring and tracking system using GPS and GSM Technologies', Int J Prof Eng Stud, 2017, 8, (5), pp. 2017

Dr. Mamoona Humayun has completed her PhD. in Computer Architecture from Harbin Institute of Technology, China. She has 12 years of teaching and administrative experience internationally. She is an active reviewer for a series of journals. She has supervised various Masters and Ph.D. thesis. Her research interests include Global software development, requirement engineering, knowledge management, Cyber Security, and wireless sensor networks.

Dr. Noor Zaman has completed his PhD. in IT from University Technology Petronas (UTP) Malaysia. He has 19 years of teaching and administrative experience internationally. He has an intensive background of academic quality accreditation in higher education related to ABET. Dr. Zaman is Associate Editor and Editorial Assistant Board for several reputable journals including IEEE Access Journal, TPC for several IEEE conferences around the globe, Active reviewer for a series of Q1 journals. He has authored several research papers in ISI indexed and impact factor research journals\IEEE international conferences, edited 09 books international reputed Computer Science area books, supervised a great number of postgraduate students, and external thesis examiner to his credit. He has successfully completed more than 19 international funded research grants. He also served as Keynote speaker for several conferences around the globe. He also chaired international conference sessions and presented session talks internationally. He has strong analytical, problem solving, interpersonal and communication skills. His areas of interest include

Cyber Security, Wireless Sensor Network (WSN), Internet of Things IoT, Mobile Application Development, Ad hoc Networks, Cloud Computing, Big Data, Data Sciences, and Software Engineering.

Malak Alamri received her master's degree from King's College London, UK in 2014. She did her bachelor's degree in computer science from Taibah University in 2007. She has 8 years of teaching and administrative experience. She is an active teacher and researcher, her research interests include software engineering, Computer Vision and Mobile Applications.