Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.024802
Article

Tech Science Press

Energy-efficient and Secure Wireless Communication for Telemedicine in IoT

Shital Joshi[1], S. Manimurugan[2,3], Ahamed Aljuhani[2,*], Umar Albalawi[2] and Amer Aljaedi[2]

[1]Department of Computer Science, Oklahoma State University, Oklahoma, USA
[2]College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
[3]Industrial Innovation and Robotics Center, University of Tabuk, Tabuk, Saudi Arabia
*Corresponding Author: Ahamed Aljuhani. Email: A_aljuhani@ut.edu.sa

Received: 31 October 2021; Accepted: 10 December 2021

Abstract: The Internet of Things (IoT) represents a radical shifting paradigm for technological innovations as it can play critical roles in cyberspace applications in various sectors, such as security, monitoring, medical, and environmental sectors, and also in control and industrial applications. The IoT in E-medicine unleashed the design space for new technologies to give instant treatment to patients while also monitoring and tracking health conditions. This research presents a system-level architecture approach for IoT energy efficiency and security. The proposed architecture includes functional components that provide privacy management and system security. Components in the security function group provide secure communications through Multi-Authority Ciphertext-Policy Attributes-Based Encryption (MA-CPABE). Because MA-CPABE is assigned to unlimited devices, presuming that the devices are reliable, the user encodes data with Advanced Encryption Standard (AES) and protects the ABE approach using the solutions of symmetric key. The Johnson's algorithm with a new computation measure is used to increase network lifetime since an individual sensor node with limited energy represents the inevitable constraints for the broad usage of wireless sensor networks. The optimal route from a source to destination turns out as the cornerstone for longevity of network and its sustainability. To reduce the energy consumption of networks, the evaluation measures consider the node's residual energy, the number of neighbors, their distance, and the link dependability. The experiment results demonstrate that the proposed model increases network life by about 12.25% (27.73%) compared to Floyd–Warshall's, Bellman–Ford's, and Dijkstra's algorithms, lowering consumption of energy by eliminating the necessity for re-routing the message as a result of connection failure.

Keywords: Energy-efficiency; energy consumption; Internet of Things; telemedicine; wireless sensor networks

1 Introduction

The internet services have become indispensable for business, health, and governmental activities and operations. Its significance and relevance in daily life have grown substantially, whether for economic growth, technological developments, or social services. The Internet of Things (IoT) is one such application model that has attracted attentions to link anything and everyone while also delivering various services [1–3]. Connecting sensors, computers, and networks for communications, monitoring, and control is not a new paradigm, but the IoT expands this concept a step further by connecting everyday objects, not just computers, which could be then utilized for data generation, collections, and transmission with minimal human involvement. The connectivity among IoT devices for collectively transmitting collected data or deploying new services has also opens the door to delegate intelligent tasks to these devices [4].

The progress and practical application of these IoT devices transform everything into smart objects. Nowadays, IoT devices are widely linked with energy management and home automations devices to form what is called "smart home". As a result, family members may remotely manage household appliances willingly or based on data acquired for increasing the efficiency or security. Also, the IoT devices such as fitness wearable devices that are connected with network-based health monitoring systems for human health tracking and monitoring, which consequently pave the land for smart health monitoring systems.

In relation to smart cities, the IoT devices can be embedded in vehicles connected to broadband networks, traffic control systems, and also as sensor nodes along the road that communicates with each other to detect and reduce congestions. IoT may also be utilized in agriculture, security, and energy industry. However, IoT paradigm itself faces challenges that should be taken in considerations when it's adopted to be utilized effectively. Some of these IoT challenges, which should be properly considered and examined [5,6]:

- Inter-Operability and Inter-Connectivity: A wide range of IoT systems must be linked or consolidated into a single platform. Combining these devices, made by many manufacturers, into a single common platform is quite difficult.
- Heterogeneity: Because IoT architecture can includes a wide range of devices, each has a unique hardware structure, transamination media, and network configurations. All of these devices must be compatible with a global information and communication infrastructure. In practice, it is not easy to find a generic technique that works well for all off-the-shelf devices.
- Security: Government regulations may prohibit sensitive data from being transmitted via IoT communication networks. Note, because one of the primary purposes behind IoT paradigm is to gather as much data as possible, it is critical to guarantee that the data flow in such system is protected throughout the whole networks.
- Quality of Service (QoS): The communication channels should be good enough to handle a large volume of network traffic among the network's nodes (i.e., potentially sensors and remote servers) and also towards the data collector platform.
- Dynamic changes: IoT devices should be able to alter their status dynamically according to the various conditions, such as wake up, sleep mode, termination connections, as well as essential updates regarding their operating systems and working circumstances.
- Large scale: Often IoT systems have a massive number of IoT devices involved, which would require a robust and scalable control system to manage such number of devices.

The smart health systems, which is one of the beneficiaries of the IoT systems, present additional challenges as the health monitoring systems are application-specific and not mutually interoperable due to the heterogeneous underlying architecture (i.e., for each different application). This makes it harder to reduce costs and more difficult for users to switch between applications or move to a better service provider. The IoT could be used in healthcare to track hospitalized patients who require special medical treatment, in which sensors capture extensive data regarding the user health conditions, and store such data and process it in the cloud. The resultant data is then wirelessly transmitted to the service provider for further analysis.

As with the medical treatments, various sensors gather patient's health data, perform a few complicated analyses, and then share the results with a medical expert for further analysis. This has the potential to provide effective and timely medical guidance and treatments. Likewise, it may be utilized to monitor the health of any individual remotely. The success of IoT applications in health care dependents on many stages of effective deployment [7]:

- Using various sensor equipment to closely and precisely track the health status.
- The efficiency of IoT devices depends on many factors, such as power consumptions, operational cost, reliability, accuracy, interoperability, and durability.
- Different data collection and integration procedures.
- Network access to the cloud and the service infrastructure.
- Efficient data analysis methods.
- Appropriate user-friendly interfaces.

This paper presents a secure architecture for IoT-based systems in telemedicine. The proposed architecture takes into consideration different functional components to provide system security while also preserve the users' privacy. As the nature of telemedicine technologies allow patients to receive treatments and medical advice remotely, the proposed architecture provides secure communications for patients through Multi-Authority Ciphertext-Policy Attributes-Based Encryption (MA-CPABE) scheme. Adopting such scheme in IoT-based systems is not free from challenges due to resource constraints when assigning MA-CPABE to unlimited IoT devices and sensor nodes suffer from limited energy, which is one of the most constrains for the ubiquitous use of Wireless Sensor Networks (WSN) and indeed raises the demand to improve energy efficiency of IoT sensors. Therefore, the Johnson's algorithm with a new computation measure is utilized in our proposed approach to minimize energy consumption while increasing network lifetime. We analyzed, evaluated, and compared our proposed architecture with other widely used approaches including Floyd–Warshall's, Bellman–Ford's, and Dijkstra's algorithms.

2 Background and Related Work

This section presents the common requirements of the Telemedicine systems and their utility. Also, the role of IoT in the medical field is highlighted. Then, we discuss the related research work that aimed to tackle security and privacy issues for IoT-based systems in healthcare.

2.1 Telemedicine in IoT: A Broad Perspective

Telemedicine is a rapidly evolving technology that allows patients to receive treatment through a remote system [8–11]. Fig. 1 depicts a higher-level representation of Telemedicine with the IoT technologies. For an effective telemedicine system in the context of IoT, there are some main requirements that should be fulfilled. This research can be helpful in the following situations:

- A physician can examine a patient with chronic health problems from a distance without leaving the hospital.
- If workers become sick or injured faraway from hospital, they must be transported to closest capable medical care center or hospital via telemedicine; a doctor should be able to make that decision remotely.
- When a child becomes ill, it may disrupt the working schedule of parents, and especially when urgent childcare is needed for critical situations. To address this issue, parents can use the Telemedicine system to obtain primary care for their children or at least to mitigate the situation acuteness. Hence, it increases the accessibility of healthcare services and outcomes since patients are seen

sooner rather than later [8]. For example, suppose a patient was not feeling well for several days. In that case, he can seek an immediate healthcare service or primary care from a licensed doctor via telemedicine applications rather than visiting in person.

- It saves patients time since they do not have to wait for a physician at an emergency department or hospital. There was no coinsurance and deductible, saving people and industries lost revenue because employees being absent from work.
- It enhances healthcare system in general, particularly for people living in rural locations or conflict zones with no health services or facilities [12].
- Generally, as the IoT-based systems often receive and collect data from various diffused devices, it should sufficiently resistant against any possible DDoS attacks [13,14] since the availability of the system is crucial for legitimate users.

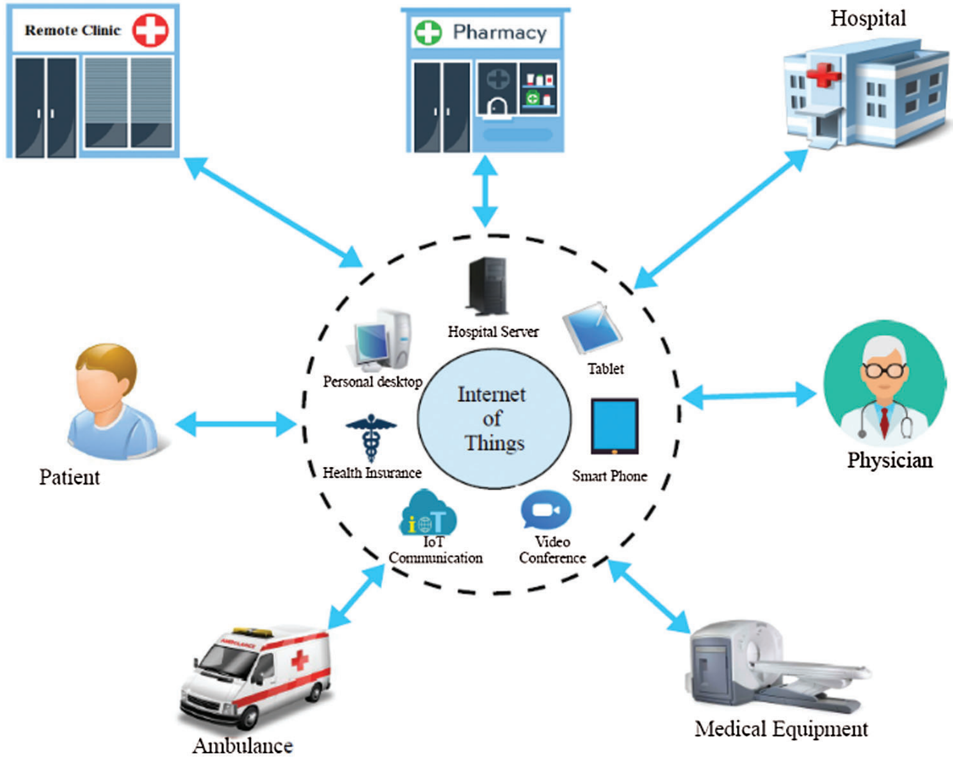

Figure 1: Higher-level overview of telemedicine in the IoT

2.2 The Role of IoT in Telemedicine

The patient has the ability to interact with the medical equipment at any time and from any location. These devices are equipped with sensors that can detect and record patient medical data such as heart rate, blood pressure, and body temperature. The recorded data is then gathered through sensor gateway devices such as mobile phones, tablets, and PCs. The actual sensors cannot be used to communicate with TCP/IP protocols; instead, often low-power protocols are used (i.e., Bluetooth). Furthermore, they cannot connect to the Internet using those protocols. That is why gateway devices are necessary. As a result, gateway devices play an essential role in this communication architecture. Also, in some IoT applications, these IoT devices may rely on IoT hub system for data for various data collection.

The IoT hub system is essentially a Demilitarized Zone (DMZ) service [15] that delivers and receives data from gateway devices. Sensor gateways in hospitals would be network-connected devices that seek data collection. The IoT hub is a software component that listens on different ports for various protocols to communicate with different systems. The primary goal of this technology was to enable bi-directional communication among doctors and patients.

Moreover, the IoT system enables the communication among digital active artifacts and users in a physiological environment. This system involves people as critical system components, which might cause harm if the system fails or exposes private information, which justifies the need for security and privacy within IoT design and references model, as illustrated in Fig. 2. Safety of a system is related to the application domain that is inextricably linked to an IoT framework and its utility. The security measures in the IoT environment depend on the communications security to protect the integrity and secrecy of communicating entities and other related functional elements such as management of identity, authentication, trust and reputations, and authorization [16].

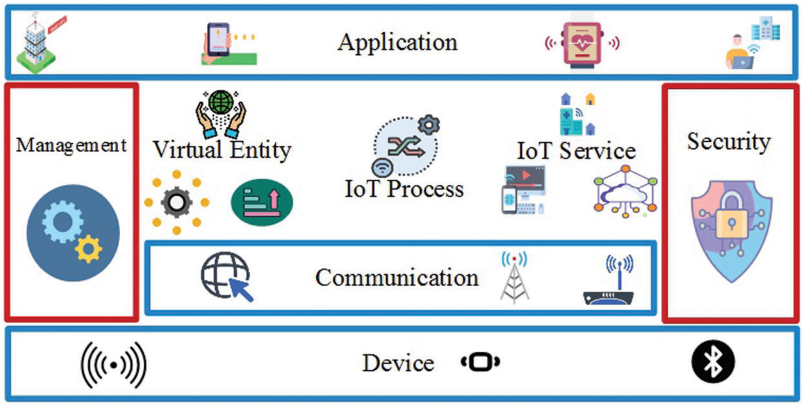

Figure 2: IoT functional model in the system-level architecture

Many research studies have been conducted in the past towards the utility of IoT-based medical services. Zhang et al. [17] proposed a secure, open, and adaptable architectures for IoT and cloud-based health applications. Their proposed model contained different short-distance communication protocols to address medical security issues in such IoT environment. For example, the interoperability when connecting multiple telemedicine devices from different factories and the authentication process to securely authorize users to access the system. To demonstrate the effectiveness of their proposed model, authors provided a reference implementation of the proposed architecture. Ziegler et al. [18] proposed a comprehensive approach to mitigating cyber-physical system (CPS) vulnerabilities using cloud and IoT architectures. Their proposed architecture, known as ANASTACIA, aimed to provide several security and privacy features for monitoring, evaluating, and analysing a wide range of cybersecurity threats. Also, authors in [19] proposed a trust-based decision-making protocol for an IoT-based healthcare model. The system design included a trust protocol running on an IoT devices to properly measure both data and source reliability in order to make an accurate decision for the user. In addition, the proposed trust protocol considered patient's loss of health scores along with reliability of service providers to achieve more accurate decision-making. Their experimental results showed that the proposed model achieved higher decision ratio results when compared to other baseline protocols. Jebri et al. [20] proposed STAC protocol to ensure secure communication and trust management for IoT applications. The STAC protocol aimed to improve the Efficient Anonymous Communication (EAC) protocol by resolving issues such as the setup phase's weaknesses. To ensure privacy, data are transmitted through an anonymous trusted node, where these nodes are identified and established anonymously. Their evaluation results demonstrated that the proposed protocol enhanced security and privacy communications compared with existing protocols.

3 Architecture of Proposed Trusted and Secure Telemedicine in IoT

Fig. 3 depicts an architecture outline of trusted and secure telemedicine model in IoT. The functional components in this research are restrict in the group of security function, which guarantees the privacy management and the system's secure functioning. The group of security function includes factors that provide the following:

- Secure communications (assuring the integrity and confidentiality of messages) between system entities like devices, services, and applications and the privacy acknowledgement of sensitive data related to users.
- User's authentication and permissions management to provide services access for users.
- Privacy methods include anonymizations of resource and service access (services could not identify which user used the data), anonymizations of gathered information, and unlinkability (An outside intruder could not detect the user by monitoring multiple requests executed by the same user).

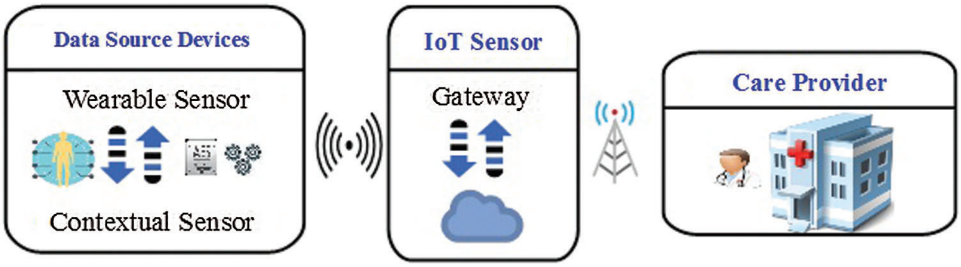

Figure 3: Architecture of trusted and secure telemedicine in IoT

3.1 IoT Sensors

Like computational systems, IoT adapters (gateways) provide networking interface for communicating with sensors (Bluetooth and ZigBee interface) and with the Internet via wireless or wired interfaces. The new gateway's additional function may do preliminary data processing (pattern analysis, compression, and data filtering) before data is encrypted and transmitted to the Internet through an Ethernet network interface. It can have a 1 GHz ARM CPU and 512 MB of RAM and a full operating system including PKI (Public Key Infrastructure) tools like OpenSSL.

3.2 Authentication and Authorization

PKI is a feasible technique for data gathering because it provides an improved authentication level to transmit data in an increasingly insecure medium. In the environment of health care and IoT, a system that delivers patient-based data (body sensor measures) is the sole public key that could be utilized to decode data, and health monitoring applications could utilize the private key to decode data. The appropriate device authentication is accomplished by using PKI digital certificates that protect data transfer, as adopted [21]. Therefore, developing PKI in the context of IoT presents significant problems. Public key encryption necessitates a computational procedure that uses memory resources, which are not accessible in current wireless sensor technologies, specifically for constant data transmission like the cardiac signal. Because it requires less processing than PKI, symmetric encryption may secure communication among the system and IoT sensors.

3.3 Secure Communication: Algorithm and Architecture

The constant incorporation of prominent technologies like wireless communications and the cloud enables new ways of communication in the framework of the IoT. Although for IoT-based systems to realize their full potential, appropriate solutions to their security questions are required. The specific security issues concern secure communication among entities (user and environmental things). An IoT-based system node provides authentication and privacy solutions. It enables the gathering of patient signals and data. As a result, it employs data encryption, safe transmission methods, and control of user access to provide the critical privacy and security that health monitoring system demand. The proposed model incorporates protocols and security methods to satisfy the stated features (four stages).

In this work, a Multi-Authority Ciphertext-Policy Attributes-Based Encryption [22] was proposed to securely transport data while using fine-grained access control in IoT settings. The first phase is a digital solution integrating AES symmetrical encryption standard with MA-CPABE to solve MA-CPABE constraints such as resource needs and speed. Because MA-CPABE is assigned to unlimited devices, presuming that the devices are reliable, the user encodes data with AES and protects the ABE approach using solutions of symmetric key. Just entities with private key combined with the group of attributes matching data could access data matching and encode the symmetrical keys to acquire data in such a scenario. The proposed approach was split into four stages, as shown in Fig. 4. The mathematical symbols and annotations are summarized in Tab. 1. The following pseudocode depicts the proposed algorithm.

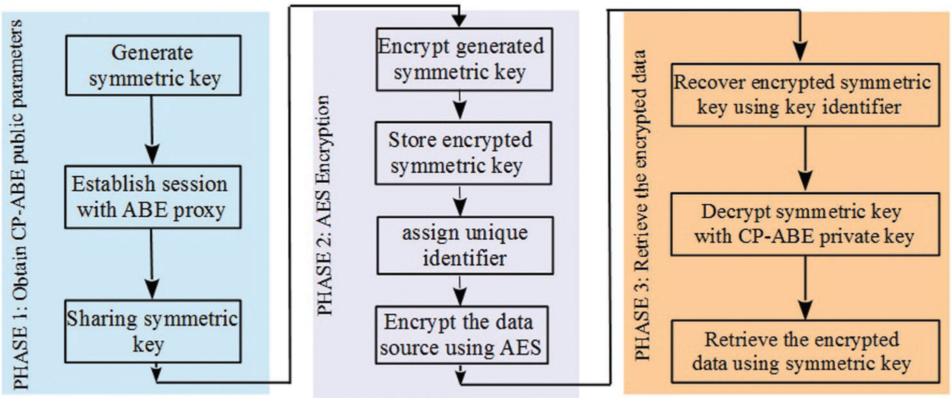
PHASE 1: Obtain CP-ABE public parameters
Generate symmetric key
Establish session with ABE proxy
Sharing symmetric key
PHASE 2: AES Encryption
Encrypt generated symmetric key
Store encrypted symmetric key
assign unique identifier
Encrypt the data source using AES
PHASE 3: Retrieve the encrypted data
Recover encrypted symmetric key using key identifier
Decrypt symmetric key with CP-ABE private key
Retrieve the encrypted data using symmetric key

Figure 4: Proposed model of secure communication

3.4 MA-CPABE and AES Algorithm

The proposed model is based on the sequential MA-CPABE model which performs certain work needed for parallelization process. The key generated using the proposed MA-CPABE and AES algorithm performs parallel processing, and these attributes are handled in an independent manner and the generated key is perfect for parallel processing and the sequential algorithm is completely partitioned and allocated with the data blocks. While processing those attributes and the outcomes require private key. Moreover, the model adopts some neutral approach, and the private key provides local attributes for processing. The major benefits of this approach are the spatial locality and reduced computational overhead. The communication and computation are attained to diminish the execution time.

Algorithm 1

```
Get $\boldsymbol{MACPABE_{para}} \leftarrow \{z_1, z_2, \ldots, zn\}$
Generate $\boldsymbol{key_{symt}} \leftarrow \{\boldsymbol{DIH}||\boldsymbol{ELC}\}$ for process elements //AES_block size
Establish $\boldsymbol{session}$ //process element
Generate $\boldsymbol{key_{symt}} \leftarrow \{\boldsymbol{DIH}||\boldsymbol{ELC}\}$
if $\boldsymbol{ABE_{proxy}} \leftarrow \{\boldsymbol{payload}\}$ then
    Share $\boldsymbol{key_{symt}}$ //block_size
else
    Send $\boldsymbol{payload}$ //process element
End
Send $\boldsymbol{ABE_{proxy}} \leftarrow \{\boldsymbol{MACPABE_{acp}}\}$ //number of attributes;
Encrypt $\boldsymbol{MACPABE_{acp}} \leftarrow \{\boldsymbol{AES}\}$ //process elements and attributes;
Save $\boldsymbol{enkey_{symt}}||\boldsymbol{UID_{symk}}$
Encrypt $\boldsymbol{DS} \leftarrow \{\boldsymbol{AES}\}$ //encrypt data blocks
Complement $\boldsymbol{ENDS} \leftarrow \{\boldsymbol{UID_{symk}}\}$
Decrypt $\boldsymbol{enkey_{symt}} \leftarrow \{\boldsymbol{MACPABE_{priv}}\}$ //decrypt data blocks
Retrieve $\boldsymbol{ENDS} \leftarrow \{\boldsymbol{key_{symt}}\}$ //retrieve the original key size;
End
```

Table 1: List of symbols and annotations

Symbols	Description
$MACPABE_{para}$	Magnetic flux
key_{symt}	Magnetic flux induction and density
$enkey_{symt}$	Encrypted symmetric key
$MACPABE_{ACP}$	MACPABE access policy
UID_{symk}	Unique identifier of symmetric key
$MACPABE_{priv}$	MACPABE private key
DIH	Diffie-Hellman algorithm in ABE proxy
$MACPABE_{lib}$	MACPABE library
$\|\|$	Concatenation operator
DS	Source of data
$ENDS$	Encrypted source of data
ELC	Elliptic curve

4 The Proposed Energy Efficient Routing in WSN

One of the developing technologies is the WSN. It may be utilized for military purposes, environmental monitoring (i.e., climate change and natural catastrophes such as fires and floods), agriculture, transportation, and security. WSN sensor nodes are tiny electronic devices that are dispersed across the area of interest. Electronic devices have a processor to collect data and minimize memory consumption and RF circuits for communications. Above half of the entire energy in the sensor was used in WSN during communications [23]. Since then, the majority of research has concentrated on this essential element of the WSN. WSN communications focused on the transfer of gathered data among the sensor node and the destinations. All sensor nodes have a coverage limitation. This transmission is divided into two types: direct data transmission from source to destination and indirect transmissions (i.e., forwarding gathered data from a sensor node to a close sensor and finally delivering to the SN).

There are potentially many issues in wireless multi-hop network system design such as energy consumption and time consuming. Multi-hop transmission refers to moving data from a sensor to other till it reach the sink node (SN) [24]. Any sensor node can have many neighbors, and the sensor nodes were randomly placed within the coverage region. As a result of randomly distribution sensors, finding an appropriate sensor node for hopping becomes essential in terms of energy usage. A routing problem is how to choose an appropriate path for data transfer from the source to the sink node.

The sensor node plays a significant role in measuring pressure, temperature, movement, chemical, or other physical variables necessary for various applications in an aperiodic or periodic means. When the sensing element in the sensor node gathers this data, it saves it in its memory to process and short-term storage before delivering it to the SN. The SN is a type of node with a lot of computing power, radio frequency components, and storage [25]. The SN's objective is to gather and process all data from adjacent sensor nodes. The numerous sensor nodes attempt to connect with this SN in the multi hop environment.

Sequential Assignment Routing (SAR) [26] was a routing protocol based on network structure. It was a QoS-based protocol designed to reduce energy usage while increasing fault tolerance. REEP [27] was a routing protocol based on data-centric that falls into the similar energy efficiency and stability category as REEP. Sensor network protocol with some standard hierarchical routing protocols that belong to the same category includes the Threshold sensitive energy-efficient sensor networks protocol (TEEN) [28], Low Energy Adaptive Clustering Hierarchy (LEACH) [29,30] algorithms were depended on the creation of a cluster and the selection of the cluster-head that was then liable for transferring data to the SN. Sensor Protocol for Information through Negotiations (SPIN) [31], Distributed Energy Adaptive Routing Algorithms (DEAR) [32] were examples of generic adaptive routing algorithms. In SPIN, sensors' excess energy is taken into account for adaptive routing, but in DEAR, data traffic in sensor node is balanced decentralized to result in energy efficiency. Lately, the bio inspired routing approaches such as Ant Colony Optimizations (ACO) [33], Swarm Intelligences Optimizations Based Routing Algorithms [34], were investigated to reduce global energy consumption. Aside from this [35,36] propose cooperation-based routing systems.

4.1 System Description

An optimization issue to optimize network lifespan with numerous constraints was discussed in this part. WSN included many routing protocols, including shortest path algorithm to accurately route data from a sensor node to the appropriate destination. The shortest path algorithms like Dijkstra's, Bellman–Ford's, and Floyd–Warshall's algorithms were familiar. Bellman–Ford method was utilized to calculate the shortest path in a WSN; however, Floyd-technique Warshall's requires specific changes in a WSN [37,38]. Johnson's algorithm is the shortest path algorithm that solves the shortest path issue for all pairings. The all-pairs shortest path problem accepts a graph with vertices and edges and returns the shortest path between any two vertices in that graph [39]. The Floyd–Warshall algorithm is extremely similar to Johnson's algorithm. Nature-inspired routing methods, such as Ant Colony optimization, can also be employed. However, they frequently take suboptimal pathways and so do not ensure optimality.

Dijkstra's method offers the advantages of being quicker, ensuring optimality, and having less computing complexity. Furthermore, they need a longer execution time. Dijkstra's method was the algorithm of shortest path, with a modified computation metric applied among the nodes. It is utilized in this work with a modification based on the weight factor.

4.2 System Model

In WSN, the static sensors are randomly placed over the sensing field of 200 m × 200 m in the proposed design. The number of sensor nodes varies depending on the circumstance, ranging from 200 to 600. In the lower right corner of the provided space, a single SN is placed. It should be noticed that the sensor node's energy usage. It is determined by the amount of data transferred and transmission distance. If the distance of propagation (d) exceeds the distance of threshold (d_0), the radio communication exponent (usually written as 'n') is four; otherwise, it is two. For the practical WSN, it was presumed that not every link is similar (i.e., the transmission route among sensor nodes changes at random). This means that even if the two nodes were near enough to communicate, they might not have a perfect channel state. This might be caused by a hardware error in one node, channel noise conditions among nodes, or various factors. As a result, each connection is assigned a probability of uniform random reliability ($\boldsymbol{R_{i,j}}$), accounting for all instability connected with nodes 'i' and 'j'. The channel state improves as the value increases ($\boldsymbol{R_{i,j}}$).

The sensor nodes operate in two modes, and its battery level determines the sensor's mode of operation. The initial mode is transmission mode, and in this, the sensor nodes may only send its perceived data to the following adjacent node. If the level of the battery goes under 60% but exceeds 35% of its starting state, it will only work in transmission modes. The next mode is retransmission and reception mode, and in this, the sensor nodes can function as the relay by receiving the signals from a close sensor node and forwarding it to another node. It can function in retransmission and reception modes if the battery exceeds 60% of its starting battery. The sensor node is rendered inoperable if the battery goes under 20% of its starting level. Based on the received signal intensity, each node may calculate the distance to its neighbors [40,41].

4.3 Optimization Problem Formulation

WSN optimization problems are often multi-objective. WSN features such as reliability, energy consumption, energy efficiency, latency, QoS, etc., are optimized. This work primarily focuses on minimizing energy usage to enhance network lifetime. The optimization issue is affected by connection capacity, network throughput, residual energy, and the chance of connection failure. The proposed model intends to provide solution for multi-objective constraints. The optimization is to provide a global solution to establish secure communication among the network model. Hence, the objective function was provided as in Eq. (1).

$$minimize \sum_{i,j\in N} X_{i,j} * g_{i,j} \tag{1}$$

where $\boldsymbol{g_{i,j}}$ denotes the flow terms among nodes 'i' and 'j,' N was the total sensor nodes, and $\boldsymbol{X_{i,j}}$ denotes the edge/link weight among nodes 'i' and 'j.' Flow conservation must be maintained at each node. As a result, the net flow of incoming data was similar to the outgoing data, which was presented as in Eq. (2).

$$minimize \sum_{i,j\in N} g_{j,i} - \sum_{i,j\in N} g_{i,j} \tag{2}$$

Likewise, every connection got some capacities, and every node would meet this criterion as in Eq. (3).

$$0 < g_{ij} < L_{ij} \tag{3}$$

where $\boldsymbol{L_{ij}}$ was the capacity of link among nodes 'j' and 'i'. The flow's non-negativity requirement was specified as in Eq. (4).

$$g_{ij} \in W^{+} = \{0 \; or \; integer \; multiple \; of \; packet \; rate\} \tag{4}$$

The SN must not send data to any nodes, which is expressed as in following Eq. (5).

$$\sum_{i \in B, j \in N} g_{ij} = 0 \tag{5}$$

where set B includes every node considered the SN. In the provided region, there is just one SN for this work.

Every node could consume power that is minimum or equal to its remaining battery capacity. The battery power of $\boldsymbol{V_{init}}$, the energy consumed, $\boldsymbol{Vi}(\leq \boldsymbol{V_{init}})$, for node '*i*' was provided in Eq. (6).

$$V_i = \sum_{i \in N} V_{Tx} * g_{ij} + \sum_{i \in N} V_{Rx} * g_{ji} \tag{6}$$

where $\boldsymbol{V_{Tx}}$ and $\boldsymbol{V_{Rx}}$ were the receiving and transmitting energy for every node. For the optimization problem $\boldsymbol{g_{ij}}$ and $\boldsymbol{V_i}$ are assumed to be the decision variables.

4.4 Shortest Path Algorithm

Johnson's algorithm is a method for finding the shortest routes between any two vertices in a network, where the edges might have positive or negative weights. However, no negative-weight cycles are known to exist. It combines the Bellman–Ford and Dijkstra algorithms to discover the shortest routes rapidly. The procedure either provides a (n*n) matrix of shortest-path weights for all $\boldsymbol{W} = \boldsymbol{w_{ij}}$ pairs of vertices or indicates that the input graph has a negative-weight cycle. Johnson's method works as follows: first, as algorithm 4, generate t F', which has new vertex t with zero weight edges from it to all other nodes. The Bellman–Ford method is then executed on F' with source vertex t as line 2 at algorithm 4. To detect negative weight cycles, the Bellman–Ford method was employed. If this step identifies a negative cycle, the algorithm notifies the issue and exits as line 3 at algorithms 4. Lines 4–12 of method 4 are based on the assumption that F' includes no negative-weight cycles. Lines 4–5 The Bellman algorithm calculates the smallest weight $\boldsymbol{p}(\boldsymbol{u}) = \boldsymbol{h}(\boldsymbol{t}, \boldsymbol{u})$ for each vertex u in a route from t to u. Lines 6–7 use the following algorithm to get the new weights as in Eq. (7).

$$X'(v,u) = X(v,u) + p(v) - p(u) \tag{7}$$

The for loop in lines 9–12 computes the shortest routes weight $\boldsymbol{h}'(\boldsymbol{v}, \boldsymbol{u})$ using Dijkstra's method from the vertex in u. 12th line as demonstrated in Eq. (8), the proper shortest path is stored in a matrix. The final line returns the finished W matrix.

$$w_{vu} = H'(v,u) + p(v) - p(u) \tag{8}$$

4.5 Tailored Johnson's Algorithm

Consider, the graph is G and new vertex is added to the graph where the edges form the vertex to other vertices of G. Later, modify the graph as G' and execute the Bellman–Ford algorithm on G' with source s. The distances are evaluated using Bellman–Ford. If the negative weight cycle is predicted and then return the value. The negative weighted cycle is not created by some vertex as there is no edge to successive vertex and the edges are acquired from the edge. The edges are re-weighted over the original graph and the edges are allocated with newer weight as original weight. Then, eliminate the added vertex and execute Dijkstra's algorithm for each vertex. Some sources and edges from all the vertices of the original graph are added and the shortest distance from the vertices are evaluated using Bellman–Ford algorithm. Once the distance is acquired and eliminates the source vertex and re-weights the edges with specific formula. All the weights are positive, the dijstra's shortest path algorithm for every vertex from the source.

Algorithm 2

```
Execute Johnson $(\boldsymbol{F}, \boldsymbol{x})$
Compute F', where $\boldsymbol{F}'.\boldsymbol{U} = \boldsymbol{F}.\boldsymbol{U} \cup \{\boldsymbol{t}\}$, $\boldsymbol{F}'.\boldsymbol{C} = \boldsymbol{F}.\boldsymbol{C} \cup \{(\boldsymbol{t}, \boldsymbol{u}) : \boldsymbol{u} \in \boldsymbol{F}.\boldsymbol{U}\}$, and $\boldsymbol{x}(\boldsymbol{t}, \boldsymbol{u}) = \boldsymbol{0}$ for all $\boldsymbol{u} \in \boldsymbol{F}.\boldsymbol{U}$
if Bellman–Ford $(\boldsymbol{F}', \boldsymbol{x}, \boldsymbol{t}) == \boldsymbol{FALSE}$ //return minimal vertex
Then the input graph contains a negative weight cycle; //remove negative weights
else for each vertex $\boldsymbol{u} \in \boldsymbol{F}'.\boldsymbol{U}$
set $\boldsymbol{p}(\boldsymbol{u})$ to the value of $\delta(\boldsymbol{t}, \boldsymbol{u})$
computed by the Bellman–Ford algorithm //perform edge distance measure
for each edge $(\boldsymbol{v}, \boldsymbol{u}) \in \boldsymbol{F}'.\boldsymbol{C}$
$\hat{\boldsymbol{x}}(\boldsymbol{v}, \boldsymbol{u}) = \boldsymbol{x}(\boldsymbol{v}, \boldsymbol{u}) + \boldsymbol{p}(\boldsymbol{v}) - \boldsymbol{p}(\boldsymbol{u})$
Let $\boldsymbol{W} = (\boldsymbol{w}_{\boldsymbol{vu}})$ be a new $\boldsymbol{n} \times \boldsymbol{n}$ matrix //modify weights with negative weights
for each vertex $\boldsymbol{v} \in \boldsymbol{F}.\boldsymbol{U}$
run Dijkstra $(\boldsymbol{F}, \hat{\boldsymbol{x}}, \boldsymbol{v})$ to compute $\hat{\delta}(\boldsymbol{v}, \boldsymbol{u})$ for all $\boldsymbol{u} \in \boldsymbol{F}.\boldsymbol{U}$ //run Dijkstra for each vertex from the source
for each vertex $\boldsymbol{u} \in \boldsymbol{F}.\boldsymbol{U}$
$\boldsymbol{w}_{\boldsymbol{vu}} = \hat{\delta}(\boldsymbol{v}, \boldsymbol{u}) + \boldsymbol{p}(\boldsymbol{u}) - \boldsymbol{p}(\boldsymbol{v})$
return W
```

5 Experiment Results

Every simulation was executed on a Dell Power Edge C6321 server with two 2.5 GHz Intel Xeon E52680 v4 14-core processor running on Linux using MATLAB R2017a. The algorithms are performed five times, and the results were plotted using the average of the data instances acquired from the successive five iterations. Here, the k-value is set for successive iterations and it may be of any integer. Generally, investigators set as $k = 1, \ldots 25$ and here the iteration is set for 20. By changing the count of sensor nodes, the modified Dijkstra's performance was compared to Dijkstra's, Bellman–Ford's, and Floyd–Warshall's algorithms. The loss of energy for sender and reception circuits was assumed to be a constant/bit of transmission. The consumed energy by every sensor for detecting is the same. It is ignored because it was less in comparison to the energy required for communications. Likewise, the energy used when nodes were in stand-by, sleep, or idle modes were avoided, and retransmissions in the event of a delivery error was not taken into account. Tab. 2 lists all of the network parameters that were utilized in the simulation.

5.1 Impact of Packet Size

This simulation section considers packets of different sizes to assess their effect on the WSN's overall energy consumption and the total received packets by the SN at the end of experiment. For this, the number of sensors was 300, and all other characteristics are given in Tab. 2.

The total energy consumption related to packet size is tabulated in Tab. 3. As seen in Fig. 5, as the packets size grows from 300 to 1000, so does the network's overall energy usage. Because the route was not changed till one packet transfer was completed, the nodes spend more energy.

Table 2: Network simulation parameters

Parameters	Values
Target area	200 × 200 m^2
Count of sensor nodes	200–600
Count of SN	1
Radio transmissions exponent (n)	$2\ if\ d \leq do$ $4\ if\ d > do$
Sensor node's initial energy (E_{init})	0.5 J
Energy for transmissions (E_{Tx})	300 nJ/bits
Energy for receptions (E_{Rx})	150 nJ/bits
Probability of link reliability (L_{ij})	0.70–0.95
d_0	20 m
Size of packet	200–1000 bits
Battery threshold for retransmission and reception modes (BT2)	60%
Battery threshold for transmission mode only (BT1)	35%
Battery threshold for usable condition (BT)	20%

Table 3: Total consumption of energy *vs.* packet size

Packet size (In bits)	Total energy consumption (In Joules)			
	Johnson's Algorithm	Bellman–Ford's Algorithm	Floyd–Warshall's Algorithm	Dijkstra Algorithm
200	55	60	76	80
300	51	56	72	77
400	58	65	78	82
500	60	72	83	84
600	68	77	87	90
700	76	83	92	93
800	82	88	98	101
900	88	94	108	115
1000	102	108	112	123

Similarly, Tab. 4 represents the number of received packets related to packet size. Fig. 6 demonstrates that when the packet size grows from 200 to 1000, the number of packets received after the simulation falls considerably.

As a result, it is critical to correctly restrict packet size to improve network lifespan, which is directly connected to energy usage. It also allows the SN to accept additional packets with less energy, enhancing the network's energy efficiency.

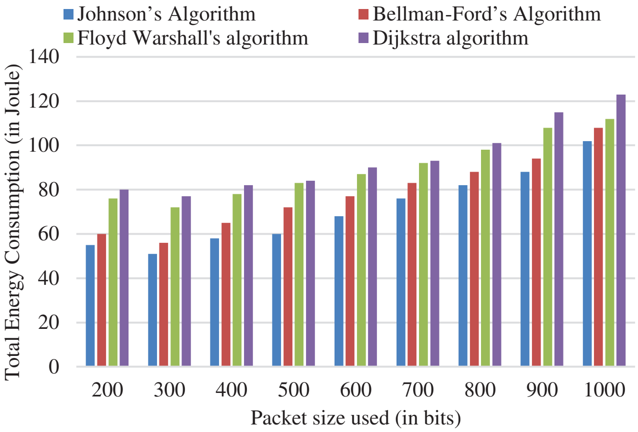

Figure 5: Graphical representation of total consumption of energy *vs.* packet size

Table 4: Total packets received *vs.* packet size

Packet size (In bits)	Number of packet's received (×10000)			
	Johnson's Algorithm	Bellman–Ford's Algorithm	Floyd–Warshall's Algorithm	Dijkstra Algorithm
200	250	208	142	201
300	232	176	121	170
400	201	158	100	148
500	180	130	81	125
600	150	111	58	102
700	133	90	37	81
800	99	72	11	60
900	82	63	7	52
1000	70	42	3	31

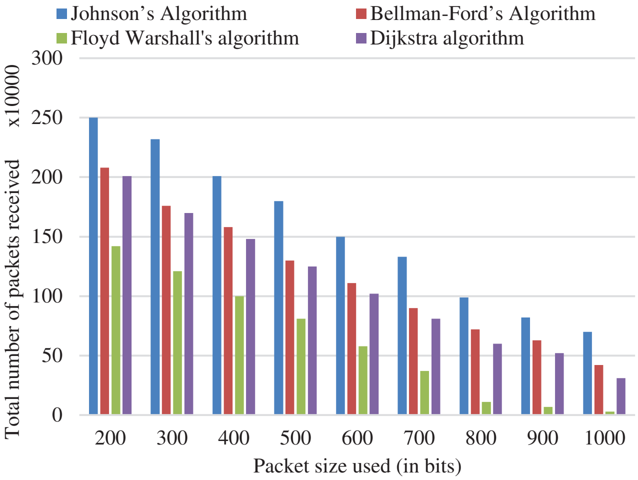

Figure 6: Graphical representation of total packets received vs packet size

5.2 Number of Sensor Node's Impact

This results section considers packets of different sizes to assess their influence on the WSN's overall energy consumption and the received count of packets by the SN at the end of experiment.

Tab. 5 represents the tabulation of total energy consumption related to the number of sensor nodes. Fig. 7 illustrates that when the count of nodes for a particular area of WSN rises from 200 to 600, the overall consumption of energy of the WSN extends constantly.

Table 5: Total consumption of energy *vs.* number of sensor nodes

Number of sensor nodes	Number of packet's received			
	Johnson's Algorithm	Bellman–Ford's Algorithm	Floyd–Warshall's Algorithm	Dijkstra Algorithm
200	17	20	21	23
250	30	35	35	39
300	50	71	72	80
350	78	85	88	90
400	98	106	107	111
450	138	140	132	137
500	150	162	167	170
550	187	198	198	201
600	201	215	220	226

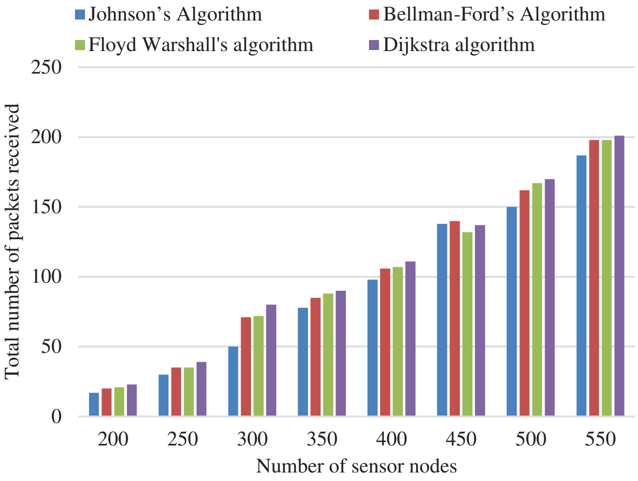

Figure 7: Graphical representation of total consumption of energy vs number of sensor nodes

As the total nodes in a particular region rises, the nodes are closer together, significantly reducing the energy needed for communication. To explain the rise in energy usage, the received number of packets by the SN must be examined. The number of packets received after the experiment rises exponentially as the number of sensor nodes increases as shown in Tab. 6. Fig. 8 demonstrates that the more nodes present, the greater the total packets that may be transmitted. It additionally implies that energy efficiency improves, despite the network's overall energy consumption has grown.

Table 6: Total packets received *vs.* number of sensor nodes

Number of sensor nodes	Number of packet's received (×10000)			
	Johnson's Algorithm	Bellman–Ford's Algorithm	Floyd–Warshall's Algorithm	Dijkstra Algorithm
200	88	76	52	74
250	130	115	70	112
300	222	168	101	160
350	300	269	185	251
400	480	406	223	380
450	742	598	402	575
500	1015	876	505	800
550	1570	1390	783	1357
600	2368	1805	1000	1725

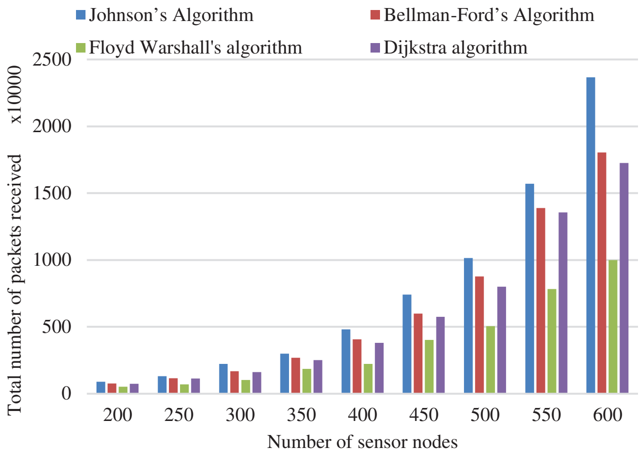

Figure 8: Graphical representation of total packets received vs number of sensor nodes

5.3 Impact of SN Location

To assess the effect of SN location, just the total packets received was examined as a function of the nodes' Euclidean distance from the SN. The total sensor nodes were 300, and size of packet was 300 bits. The sensor field is divided into five zones: 0–20 m, 20–40 m, 40–80 m, 80–160 m, and 160–290 m.

According to Tab. 7, above half of the received packets totally at the SNs come from nodes within a Euclidean distance of 40 m of the SN. Fig. 9 represents the graphical representation of total received packets related to the Euclidean distance from the SN. Nodes located further from the SN contribute less, because these nodes are so far apart, they need a multi-hop method to communicate with the SN. When the relay nodes' energy level falls below BT2, they no longer receive any packets from the distant nodes. In such a scenario, they will have to expend additional energy to connect with the SN.

Table 7: Total packets received vs Euclidean distance from the SN

Euclidean distance from the sink (in meter)	Number of packets received (×10000)			
	Johnson's Algorithm	Bellman–Ford's Algorithm	Floyd–Warshall's Algorithm	Dijkstra Algorithm
20	73	57	39	52
40	58	49	28	44
80	48	33	27	29
160	38	36	17	35
290	23	20	12	17

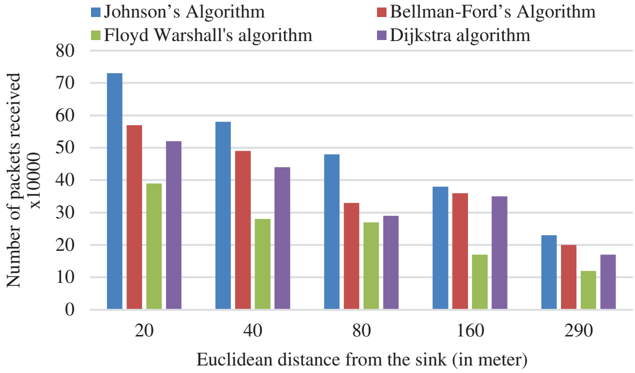

Figure 9: Graphical representation of total received packets vs Euclidean distances from the SN

6 Conclusion and Future Work

This research proposes a new safe and trusted architecture for IoT-assisted telemedicine. Unlike any other previously presented IoT security paradigm, the approach implemented in this work provided security at both the communication connection and the endpoint through privacy management and user authentication. The simulation results demonstrated that the proposed approach overcomes Dijkstra's, Bellman–Ford's, and Floyd–Warshall's approaches in relation to overall consumption of energy and received packets at the SN finally. The following observations are made based on the simulation results:

- Based on energy consumption, the total nodes increased from 200 to 600, and for a 300 bits packet size, the proposed model overcomes Dijkstra's, Bellman–Ford's, and Floyd–Warshall's approaches by 12.25 percent (27.73 percent) to 9.24 percent (11.19 percent), individually.
- Based on the packets received at the SN, the proposed model overcomes Dijkstra's, Bellman–Ford's, and Floyd–Warshall's approaches by 59.24 percent (16.23 percent) to 133.30 percent (36.26 percent) as the number of nodes rose from 200 to 600.

Overall, in terms of energy consumption and packets received related to the packet size and sensor nodes, the proposed model outperforms the compared models in every parameter as seen in results. In future, a privacy method can be examined by running several tests on real-world resource-constrained devices such as sensors. The data from various devices can be compared and studied in depth. Likewise, a more realistic energy consumption scenario will be examined, including energy consumptions by idle/stand-by/sleep modes, node sensing energy, and consumption of energy for retransmission if packets get lost/damaged.

Acknowledgement: The high-level security architecture and preliminary results of this paper have been presented in the following conference articles: [42,43].

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Huang, X. Wu, W. Huang, X. Wu and S. Wang, "Internet of things in health management systems: A review," *International Journal of Communication*, vol. 34, no. 4, pp. 1–19, 2020.

[2] T. Haaker, P. Ly, N. Nguyen-Thanh and H. Nguyen, "Business model innovation through the application of the Internet-of-Things: A comparative analysis," *Journal of Business Research*, vol. 126, no. 3, pp. 126–136, 2021.

[3] A. Guqhaiman, O. Akanbi, A. Aljaedi and C. Edward Chow, "A survey on MAC protocol approaches for underwater wireless sensor networks," *IEEE Sensors*, vol. 21, no. 3, pp. 3916–3932, 2020.

[4] A. Nauman, M. Jamshed, R. Ali, K. Cengiz, K. Zulqarnain *et al.,* "Reinforcement learning-enabled intelligent device-to-device (I-D2D) communication in Narrowband Internet of Things (NB-IoT)," *Computer Communications*, vol. 176, no. 3, pp. 13–23, 2021.

[5] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[6] K. Sha, R. Errabelly, W. Wei, T. A. Yang and Z. Wang, "EdgeSec: Design of an edge layer security service to enhance IoT security," in *2017 IEEE 1st Int. Conf. on Fog and Edge Computing (ICFEC)*, Madrid, Spain, pp. 81–88, 2017.

[7] A. Pawar and S. Ghumbre, "A survey on IoT application, security challenge and counter measure," in *2016 Int. Conf. on Computing, Analytics and Security Trends (CAST)*, Pune, India, pp. 294–299, 2017.

[8] J. Awotunde, A. Adeniyi, R. Ogundokun, G. Ajamu and P. Adebayo, "MIoT-based big data analytic architectures, opportunities and challenge for enhanced telemedicine system," in *Enhanced Telemedicine and e-Health: Advanced IoT Enabled Soft Computing Frameworks*, Springer, Cham, vol. 410, pp. 199–220, 2021.

[9] M. Yamin and B. Alyoubi, "Adoption of telemedicine application among Saudi citizens during COVID-19 pandemic: An alternative health delivery system," *Journal of Infections and Public Health*, vol. 13, no. 12, pp. 1845–1855, 2020.

[10] M. Abdellatif and W. Mohamed, "Telemedicine: An IoT based remote health care systems," *Int. Journal of Online & Biomedical Engineering*, vol. 16, no. 6, pp. 72–81, 2020.

[11] S. Rehan, F. Khan and F. Saleem, "Internet of Things in telemedicine: A discussion regarding to several implementations," *Journal of Information Communications Technologies and Robotic Application*, vol. 10, pp. 17–26, 2018.

[12] M. Hasanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas *et al.,* "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenge," in *IEEE Int. Conf. on Service Computing*, New York, USA, pp. 286–293, 2015.

[13] A. Ramtin, P. Nain, D. Menasche, D. Towsley and E. Silva, "Fundamental scaling laws of covert DDoS attacks," *Performance Evaluation*, vol. 151, no. 2, pp. 1–24, 2021.

[14] A. Ramtin, D. Towsley, P. Nain, E. Silva and D. Menasche, "Are covert DDoS attacks facing multi-feature detectors feasible?," *ACM SIGMETRICS Performance Evaluation Review*, 2021.

[15] A. Westling, "The Korean demilitarized zones (DMZ) as bridge between two Koreas," in *Participant Paper 2010: A World Without Walls*, Berlin, Germany, 2010.

[16] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand and D. Boyle, *From machines-to-machines to the Internet of Thing: Introduction to new age of intelligences*. Amsterdam, Netherlands, Elsevier, 2014.

[17] X. Zhang and N. Zhang, "An open, secured and flexible platforms based on IoT and cloud computing for ambient aiding living and telemedicine," in *2011 Int. Conf. on Computer and Management (CAMAN)*, Wuhan, China, pp. 1–4, 2011.

[18] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim and S. Bianchi, "ANASTACIA: Advanced networked agent for security and trust assessments in CPS IoT architecture," in *2017 Global Internet of Things Summit*, Geneva, Switzerland, pp. 1–6, 2017.

[19] H. Al-Hamadi and I. R. Chen, "Trust-based decisions making for health IoT system," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1408–1419, 2017.

[20] S. Jebri, M. Abid and A. Bouallegue, "STAC-protocol: Secured and trust anonymous communications protocol for IoT," in *2017 13th Int. Wireless Communication and Mobile Computing Conf.*, Valencia, Spain, pp. 366–371, 2017.

[21] C. Douklas, I. Maglogianis, V. Kouffi, F. Malammateniou and G. Vassilacopoulos, "Enabling data protections though pki encryptions in IoT m-health device," in *2012 IEEE Int. Conf. on Bioinformatics & Bioengineering*, Larnaca, Cyprus, pp. 25–29, 2012.

[22] J. Bethencourt, A. Sahai and B. Waters, "Ciphertexts-policy attribute-based encryptions," in *2007 IEEE Symp. on Security and Privacy*, Berkeley, CA, USA, pp. 321–334, 2007.

[23] M. Halgamuge, M. Zukerman, K. Ramamohanarao and H. Vu, "An estimation of sensors energy consumptions," *Progresses in Electromagnetic Research B*, vol. 13, pp. 258–294, 2009.

[24] J. Dai, K. Ishibashi and Y. Yamao, "Highly efficient multi-hop packet transmission using intra-flow interference cancellation and maximal-ratio combining," *IEEE Transactions on Wireless Communication*, vol. 14, no. 11, pp. 5998– 6011, 2015.

[25] N. Iliev and I. Paprotny, "Review and comparison of spatial localization methods for low-power wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5971–5987, 2015.

[26] K. Sohrabhi, J. Ghao, V. Ailawadi and G. J. Potie, "Protocol for self-organizations of wireless sensor networks," *IEEE Personal Communication*, vol. 6, no. 4, pp. 17–28, 2000.

[27] N. Sharma, I. Kaushik, N. Singh and R. Kumar, "Performance measurement using different shortest path techniques in wireless sensor network," in *2019 2nd Int. Conf. on Signal Processing and Communication (ICSPC)*, Tamil Nadu, India, pp. 295–299, 2019.

[28] A. Manjeswar and D. P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in *Int. Workshop on Parallels and Distributed Processing Symp.*, San Francisco, California, USA, pp. 2009–2015, 2001.

[29] W. Heinzelmann, A. Chandhrakasan and H. Balakrishna, "Energy efficient communications protocols for wireless microsensors network," in *Proc. of Annual Hawaii's Int. Conf. on Systems Science*, Hawaii, USA, pp. 10–15, 2000.

[30] W. Heinzelmann, A. P. Chandhrakasan and H. Balakrishna, "An application-specific protocols architectures for wireless microsensors network," *IEEE Transactions on Wireless Communications*, vol. 11, no. 4, pp. 661–671, 2002.

[31] W. Heinzelmann, J. Kulik and H. Balakrishna, "Adaptive protocols for information disseminations in wireless sensor network," in *Proc. of the 5th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking*, Seattle Washington, USA, pp. 174–185, 1999.

[32] C. Ok, P. Mithra, S. Lei and S. Kumar, "Distributed energy adaptive routings for wireless sensors network," in *IEEE Int. Conf. on Automations Sciences and Engineering*, Arizona, USA, pp. 906–911, 2007.

[33] J. Zhang, J. Yu, Z. Si-Wang and Y. Lin, "A survey on positions-based routings algorithm in wireless sensors network," *Algorithms*, vol. 3, no. 11, pp. 159–183, 2009.

[34] C. Whang and Q. Lee, "Swarm intelligences optimizations based routing algorithms for wireless sensors network," in *Int. Conf. on Neural Network and Signals Processing*, Nanjing, China, pp. 137–142, 2008.

[35] J. Habib, A. Grayeb and A. G. Aghadam, "Energy efficient cooperatives routings in wireless sensors network: A mixed integers optimizations frameworks and explicit solutions," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3425–3438, 2013.

[36] H. Garavi and B. Hou, "Cooperatives diversity routings and transmissions for wireless sensors network," *IET Wireless Sensor Systems*, vol. 13, no. 3, pp. 278–289, 2013.

[37] P. Khaan, G. Khonar and N. Chakraborrty, "Modifications of Floyd Warshall algorithms for shortest paths routings in wireless sensors network," in *Annual IEEE Indian Conf.*, Pune, India, pp. 1–7, 2014.

[38] M. Umalae and S. D. Markhande, “Energy-efficient routings algorithms on the targets tracking in wireless sensors networks,” in *Int. Conf. on Information Process*, Pune, India, pp. 176–181, 2015.

[39] M. Okwu and I. Emovon, “Application of Johnson’s algorithm in processing jobs through two-machine system,” *Journal of Mechanical and Energy Engineering*, vol. 4, no. 1, pp. 33–38, 2020.

[40] A. Seyedi and B. Sikdar, “Energy efficient transmission strategies for body sensor networks with energy harvesting,” *IEEE Transactions on Communications*, vol. 58, no. 7, pp. 2116–2126, 2010.

[41] R. Wu, M. Chen, Y. Su and H. J. Siddiqui, “A novel location-based routing algorithm for energy balance in wireless sensor networks,” in *2009 WRI Int. Conf. on Communications and Mobile Computing*, Yunnan, China, pp. 568–572, 2009.

[42] U. Albalawi and S. Joshi, “Secure and trusted telemedicine in Internet of Things,” in *Proc. of IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, pp. 30–34, 2018.

[43] J. Joshi and U. Albalawi, “Energy efficient routing considering link robustness in wireless sensor networks,” in *Proc. of the IEEE Int. Conf. on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, India, pp. 3116–3120, 2017.