IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier 10.1109/ACCESS.2021.Doi Number*

# FoG-oriented Secure and Lightweight Data Aggregation in IoMT

**Muhammad Azeem[1], Ata Ullah[1], Humaira Ashraf[2], NZ Jhanjhi[3], Mamoona Humayun[4], Sultan Aljahdali[5], Thamer A. Tabbakh[6]**

[1] Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan; {aullah@numl.edu.pk , muhammadazeem0493@gmail.com }
[2] Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad 44000Pakistan. {humaira.ashraf@iiu.edu.pk }
[3] School of Computer Science and Engineering, SCE, Taylor's University, Malaysia. {noorzaman.jhanjhi@taylors.edu.my}
[4] Department of Information Systems, College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia.
mahumayun@ju.edu.sa
[5] Sultan Aljahdali, Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif
21944, Saudi Arabia, Email: aljahdali@tu.edu.sa
[6] Material Research Science Institute, King Abdulaziz City for Science and Technology (KACST), Riyad, 6086, Kingdom of Saudi Arabia.
ttabbakh@kacst.edu.sa

Corresponding author: NZ Jhanjhi and Ata Ullah {noorzaman.jhanjhi@taylors.edu.my, and aullah@numl.edu.pk }

**ABSTRACT** Internet of Medical Things (IoMT) is becoming an essential part of remote health monitoring due to the evolution of medical wireless sensors and intelligent communication technologies. IoT-based healthcare applications are employed in the medical centers to provide continuous health monitoring of a patient. However, recent smart medical devices have limited resources to handle the huge amount of healthcare data. IoMT faces several challenging issues, like security, privacy, anonymity, and interoperability. In data aggregation and communication, the privacy and security of medical information is a demanding task. Therefore, we proposed a suitable scheme to overcome the limitations of existing research studies. This paper presents an Efficient and Secure Data Transmission and Aggregation (ESDTA) scheme to enhance aggregation efficiency and data security. Our proposed work provides secure data aggregation and data forwarding of healthcare parameter values by employing the Secure Message Aggregation (SMA) algorithm and Secure Message Decryption (SMD) algorithm at the Mobile Node (MN) and Fog Node FN, respectively. From a security perspective, the proposed scheme preserves the data integrity and also protect against several security threats like data fabrication and replay attack. The proposed scenario is simulated through simulation tool NS 2.35. The simulation results prove that aggregation at the MN effectively reduces transmission and communication costs. Furthermore, the effective computation at the fog node minimizes the storage and computational cost at the cloud server. Thus, the analysis of the proposed scheme shows the supremacy of our proposed work. We compare our scheme with other related secure data aggregation-based schemes in terms of communication cost, energy consumption, resilience, storage and computational cost.

**INDEX TERMS** IoT, healthcare, fog computing, security, key establishment, authentication, anonymity, data aggregation.

## I. INTRODUCTION

The Internet of Things (IoT) [1] is playing a significant part in wireless sensor networks such as remote monitoring and management. IoT has raised the participation of smart devices in the healthcare domain by providing effective solutions. Along with also raising various challenging research issues [2]. Smart healthcare applications have opened the channel for the commencement of several remote healthcare services. These healthcare services utilize IoT as a medium for remote sensing and monitoring of patient health [3]. Several massive scale domains where the IoT applications are usually applied, the healthcare domain is one of them. In the real-world scenario, the implementation of IoT in healthcare is presented by a particular category that is usually known as the Internet of Medical Things (IoMT). Therefore, IoT applications lead to the concept of the IoMT [4]. It has attained lots of attention because healthcare devices are interconnected by the internet to provide broad applicability for remote patient monitoring. In this context, medical professionals provide continuous monitoring of patient health parameters to provide more accurate and less cost remote services. The medical sensor devices are attached to the body of a patient to calculate physiological parameters including blood pressure, temperature, blood sugar, blood oxygen and heart rate [5]. Although, smart wearable medical sensors are cheap and support mobility with limited resources of energy, storage, and memory. Therefore, the collected data of a patient is sent to the collector node for data aggregation like smart mobiles, tabs, and Personal Digital Assistant (PDA) [6]. The patient's aggregated data is forwarded to a cloud server through a FN.

Fog devices performs various computing tasks on collected data and transmits data towards various servers for storage. The term "Fog computing" was introduced by cisco in 2012 to process the aggregated data locally at the edge of the network with FNs [7]. The basic aim of FN is to enhance the computation abilities at the network edge. Its edge computing features not only provide low latency, interoperability, and local processing but also provide a better quality of services in IoT enabled applications [8]. The patient's healthcare data is periodically aggregated and transmitted towards cloud servers for data analysis. Thus, server response time increases because of the large amount of data and transmission delay [9]. Therefore, the FN reduces the communication and computation overhead at the cloud servers and also balancing the load at the neighboring fog devices to efficiently handling the real-time data in emergency scenarios. it also processes the data and predicts intelligent decisions to effectively control the critical condition of the patient. In this context, continuous connectivity of smart devices with internet enhances the chance of various security attacks [10].

In IoMT, the security of data and privacy of a patient is quite important owing to the deployment of smart devices in open networks. Security preserved the integrity, confidentiality, and anonymity of data along with authentication and authorization for system accessibility [11]. Whereas, privacy preserved [12] the integrity of data and also guaranteed the confidentiality of patient information. Hence, the main hurdle while constructing a security and privacy strategy for healthcare is to maintain a balance among security and efficiency of the system [13]. In the case of IoT, security and privacy are extremely valuable requirements to protect sensitive data during transmission [14]. Besides security, data compression performs a vital role in the aggregation and transmission of healthcare data. The compression capacity is based on the compression ratio. Compression reduces the utilization of resources while sending the aggregated data from sensor nodes to base station [15].

In lightweight and secure schemes, data aggregation methods play an essential part through effective communication cost and energy consumption. [16]. The Sensor nodes send the generated healthcare values to the aggregator node. In remote monitoring of patient health, data aggregation is a primary research topic for efficient data transmission. In this scenario, security is becoming a primary concern for continuous observation of patient health conditions in IoMT [17]. Mostly, sensor nodes are placed in a hostile environment along with unsafe communication mediums lead to several security attacks. Moreover, the security of the patient health information both at the edge nodes and the communication medium is essentially important. Efficient data aggregation and security of patient data are a main challenging concern in IoT-enabled healthcare. Therefore, effective data aggregation and transmission schemes are required that protect against several security threads.

In this paper, we present an Efficient and Secure Data Transmission and Aggregation (ESDTA) scheme for a remote health monitoring system. In our system model, the smart collector nodes aggregate the received data and symmetric key is utilized for data encryption and decryption. The fog node decrypts the message and performs computations on received data. The main contributions of this work are as follows:

1) We present a fragmentation based session key sharing among sensing devices and the collectors.
2) Next, we utilize lightweight symmetric key-based encryption. Sensor nodes are utilized a data compression method to reduce the data size.
3) The proposed data aggregation method explores the delimiter based data aggregation from different collectors. The repeating values are replaced with Boolean values to indicate redundancy and saving storage space and transmission cost.
4) Finally, the delimiter based message extraction mechanism is presented for fog nodes. It also involves the decryption process.

The rest of the paper is organized as follows; Section II presents the review of existing literature. Section III illustrates the system model and Section IV explores the proposed work. The results and analysis is explored in section V. Finally, Section VI concludes our work.

## II. RELATED WORK

This section focuses the several different essential concerns of security in terms of data gathering, data aggregation, and transmission. We also target the importance of fog computing in terms of security, privacy and data compression in healthcare.

### *A. SECURE DATA AGGREGATION*

The data aggregation helps to reduce redundant communications and provides efficient bandwidth utilization and energy consumption. Security and privacy are the main concerns for data aggregation in remote healthcare monitoring applications because of sensor nodes deployment in hostile environments. Therefore, a Secure Authentication and Prescription Safety (SAPS) scheme anonymously provides remote patient monitoring and also provides secure communication among patient and medical experts [18]. HMAC protocol provides secure data aggregation with end-to-end data authentication with better resource utilization [19]. Xiong et al. [20], presented a two-hop scheme for wireless body area network (WBAN). Both data aggregation and authentication is conducted at the edge node. For security, it generates session keys to achieve data anonymity. Song et al. [21], presented a multifunctional data aggregation while protecting against several security attacks. Khalid et al. [22], discuss an end-to-end communication scheme that provides efficient energy consumption. One-Time Pad (OTP) encryption scheme is employed to provide security against malicious nodes. Fatemeh et al. [23] introduced data aggregation-based scheme provide encrypted data analysis to protect data.

### B. FOG COMPUTING

Fog computing is mostly implemented for real-time data computation and storage. In fog computing, security is the main concern for data aggregation and transmission [24]. Rahul et al. [25], present a fog-based framework for healthcare. Pseudo identity is utilized to identify each patient's information separately. The Efficient Health Data Aggregation (EHDA) scheme presents secure communication among the smart nodes.  Aggregator node employs message receiving algorithm to aggregate the encrypted and compressed data that received from the sensor nodes. The message receiving algorithm is also employed at the fog node to decrypt the data that received messages of aggregator nodes and extract the node-level data for analysis. Moreover, symmetric key-based encryption is utilized but inter-communication among the aggregator nodes enhances the communication cost [26]. An anonymous and secure aggregation scheme (ASAS) protects the identity of the nodes by employing pseudonyms. Homomorphic encryption is employed to protect data integrity. Although, this scheme saves bandwidth by utilizing the data aggregation technique. However, the redundant data transmission enhances the communication, computational, and storage cost both at the fog and cloud servers. [27]. An Anonymous Privacy-Preserving scheme with Authentication (APPA) protects the identity of smart devices. Asymmetric keys are employed for data encryption and pseudonym certificate for data calculation. Although, this scheme provides efficient multilevel authentication and security. However, the performance of the scheme is reduced with the increase in the number of devices. Moreover, this scheme is the right choice but in the case of limited devices [28]. Rongxing et al. [29], present a fog-based aggregation protocol that employs the one-way hash method to evade bad data injection. At the FN, a secret key is used to perform hashing and data aggregation. Abdullatif et al. [30], introduce a fog-assisted secure framework for privacy preservation of data. Clustering-based techniques are applied for local processing and also provide analysis and storage for encrypted data. Hong et al. [31], introduced a cooperative scheme for authentication and access control by applying cyphertext-based encryption. It preserves integrity of data with similarity determination. Qinlong et al. [32], explored fog-assisted security and secure data access by computation outsourcing and ciphertext update.

### C. PRIVACY AND SECURITY

Privacy and security are the main concern for protecting the data integrity and identity of individuals. Several challenges need to overcome by designing appropriate security and privacy based solutions for IoMT [33]. Secure Privacy Preserved Data Aggregation (SPPDA) scheme that is based on bilinear pairing. This scheme provides efficient data aggregation by employing the aggregate signature method. A homomorphic-based bilinear ElGamal cryptosystem to preserve data privacy, authenticity, and confidentiality. The communication cost and transmission cost are greatly reduced by employing data aggregation and batch verification. An Efficient and Privacy-Preserving Aggregation (EPPA) scheme efficiently aggregates data and applies a Paillier cryptosystem for privacy preservation. Superincreasing sequence is applied to construct a cyphertext of multidimensional data [34]. The Priority based Health Data Aggregation (PHDA) scheme provides privacy preservation by applying Paillier and a homomorphic cryptosystem. Same as, EPPA is applied a superincreasing sequence [35]. Lin et al. [36], provide multidimensional data aggregation that applies superincreasing sequence and additionally perturbation method. Chen et al. [37], presented a scheme that provides privacy-assured data aggregation and not guaranteed data integrity and authenticity while aggregating data.  Zhu et al. [38], introduce a secure and privacy preserved aggregation protocol for wireless body area network. A bilinear pairing based cryptosystem applied for secure data aggregation. Ashutosh et al. [39], introduced remote healthcare monitoring along with anonymity and security of data. A dynamic distributed architecture for preserving privacy (DDAP) scheme presents a secure aggregation method for remote healthcare monitoring [40]. Xiaodong et al. [41], provide privacy against malicious terminal nodes. At the fog node, the redundant values are removed from the received data. Further, the data aggregation method is employed at the fog node to preserve the bandwidth.

### D. DATA COMPRESSION

Data compression performs an essential role in IoMT to save limited resources. Therefore, several compression-based schemes minimizing the storage cost and data transmission cost. Robinson et al. present a hybrid algorithm TTTD-H by combining TTTD and Huffman protocols. It provides better performance and compression ratio but enhanced compression time [42]. A Secure and Scalable Deduplication (SSD) scheme employs a record linking algorithm for the deduplication of healthcare data. A semi-honest model is utilized to preserve the integrity of healthcare information and protect the identity of patients [43]. Ren et al. [44], present a data aggregation scheme based on sensitive data where compression schemes are applied to reduce communication costs and energy consumption. Othman et al. [45], introduce a aggregation and compression-based scheme for WBAN. Similarly, a Priority based Compressed Data Aggregation (PCDA) scheme provides priority-based data compression. Moreover, this scheme protect the integrity of the received information by employing cryptographic hash algorithm [46].

## III. SYSTEM MODEL AND PROBLEM STATEMENT

In this section, we present the system model for IoT-enabled healthcare applications. Our proposed model supports the patient health monitoring at a distant location.

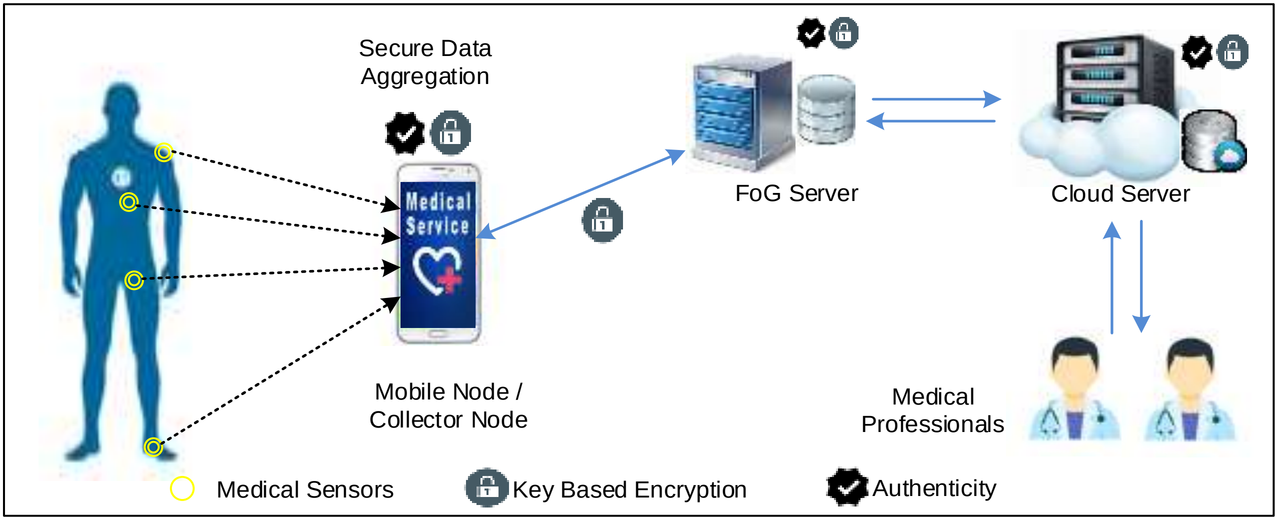


FIGURE 1. Data collection and secure data aggregation scenario

In Figure 1, we illustrate the system workflow for secure data forwarding from the end node to the cloud server. Intelligent wearable Sensor Nodes (SNs) collect the patient healthcare values such as body temperature, blood pressure, oxygen level, and heartbeat. Set of SN is represented as { $SN_1, SN_{i+1}, \ldots SN_n$ } and n denotes the number of nodes. The SNs forward collected data to the Mobile Node (MN) for aggregation of healthcare parameters for transmitting towards Fog Node (FN). Finally, FN collects the messages from the MNs. It provides data computation and storage at the edge of the network. Moreover, it concatenates the received information as per the required format then transmits the formatted data to the cloud. In our proposed scheme, we have assumed that in the collection phase SNs are placed on the body of the patient and collect the healthcare parameter values. SNs also compress these values before forwarding these values to the AN. Besides this secure data aggregation algorithm at the edge nodes provides secure and efficient data aggregation and transmission. We assume that SNs and AN are communicate by using a secret key and the same case for AN and FN communication. Moreover, we assume that FN forwards the data to the public cloud server after computing the data and formatted the data in the required format of the cloud server.

The system model provides a secure data aggregation and data transmission model for monitoring the patient's health at a distant location. The method of secure data transmission from sensor nodes to the cloud server is as follows. At first, the SNs gather the healthcare values of the patient. Data is encrypted using symmetric key-based encryption. Every SN forwards the encrypted message toward the mobile or collector node. The data compression method is applied to reduce the size of the health parameter values. The data aggregation methods are applied to aggregate the encrypted and compressed messages. MN is an intermediate node between the FN and SNs. MN provides secure data processing at the edge of the network. After that, it transmits the aggregated data to the FN. The data decryption and decompression methods are employed at the FN. The received message is decrypted through symmetric-key-based data encryption. The data decompression method is applied to extract health parameters of the patients. FN also applied some computational operation on the received data before transmitting the formatted data to the cloud repositories for storage. Medical experts access the required data from the cloud repositories. Thus, only authenticated users can only access the sensitive health information of patients for data analysis and prescription.

In our proposed communication design, WiFi technology is utilized between mobile and fog nodes. MN is available within the range of SNs, so there is direct communication among these nodes. The MNs use the internet as a medium to communicate with FN because the distance between these nodes is long. Our communication design has the following features: i) The symmetric key-based data encryption is employed for secure communication. ii) Each SN can only interact with the individual MN. iii) MN provides secure data aggregation and transmission of medical data toward the Fog node. iv) FNs provide local data processing and storage. v) A single cloud server is employed for secure data access and storage. The main problem is that the transmission of collected information among the cell phones / mobile nodes is not secure. In the context of non-cooperative mobile nodes, there is the probability of a malicious node in neighboring mobile nodes [26]. Malicious nodes are not directly decrypted data because data is encrypted through a secret key. It causes the denial of service attack by dropping the aggregated messages instead of forwarding them to the fog node. Mostly, the ordinary compression rate and redundant data transmission increase the storage and communication cost.

## IV. EFFICIENT AND SECURE DATA TRANSMISSION AND AGGREGATION (ESDTA) SCHEME

In this section, we present ESDTA scheme to overcome the main challenging issues of IOMT such as secure data collection, aggregation, and transmission. In IoMT, security is a prime concern for data sharing-based application. Hence, the ESDTA scheme provide secure data sharing and this scheme is divided into 3 phases: i) Data collection, compression and encryption at SNs, ii) Data aggregation and encryption at MN, iii) Data decryption and removal of redundant data at FN. Moreover, the list of notations is shown in Table 1.

**TABLE 1. List of Notations**

| Symbol | Quantity |
|---|---|
| $CD_i$ | Compressed information at SNs |
| $SK_{Fi}$ | Key between SNs and FN |
| $C_i$ | Cipher text at SNs |
| $SN_{id}$ | Sensor nodes ID |
| $TS$ | Time stamp |
| $N_i$ | Nonce value for $SN_i$ |
| $H$ | Hash function |
| $AV_{SN}$ | Aggregated values at SN |
| $RV_{MN}$ | Received data at Mobile node |
| $C_m$ | Aggregated message at MN |
| $HPV_{Ri}$ | Currently received healthcare values |
| $HPV_{Ri}$ | Last received healthcare values |
| $E_{K_{SN-MN}}$ | Secret key between SN and MN |
| $SK_{F1}, SK_{Fm}$ | Session key fragments |
| $E_{SK_{MN-FN}}$ | Secret key between MN and FN |
| HPV | Healthcare parameter values |
| Ꭓ | XOR operation |

### A. DATA COLLECTION AND COMPUTATION AT SN

In this section, intelligent SNs collect the healthcare values and transmit the encrypted information to the MN. Data compression and symmetric key-based encryption are utilized for effective data communication. Initially, SNs take the healthcare parameter values $(HPV)$ for different sensors like temperature, heartbeat, ECG, glucose level etc. These aggregated values are represented as $AV_{SN} = \{HPV_i : HPV_{i+1} \ldots : HPV_n\}$ where colon ":" is used as delimiter and $i$ is varied from 1 to $n$. The compressed healthcare values are represented as $CD_i = \{\mathrm{Compr}(AV_{SN})\}$. After that, SN obtains session key as $E_{SK_{SN-MN}} = H(SN_{id})$ Ꭓ $H(N_i)$ Ꭓ $H(CD_i)$ where Ꭓ represents the XOR operation. SN uses session key to encrypt the $CD_i$. Equation (1) explores the encrypted message sent from SN to MN where ID of sensing device is represented as $SN_{id}$, SN's time stamp as $TS_{SD_i}$ which is mandatory to ensure the message freshness and guard against replay attack. The nonce value $N_i$ ensures correct challenge response. The message $M_1$ is given in (2) whose hash $H(M_1)$ is taken to ensure message integrity on the receiving side.

$$\mathrm{E}_{\mathrm{K}_{\mathrm{SN-MN}}}\{\mathrm{SN}_{\mathrm{id}},\ \mathrm{TS}_{\mathrm{SN}_{\mathrm{i}}}, \mathrm{N}_{\mathrm{i}}, \mathrm{SK}_{\mathrm{F1}}, \mathrm{E}_{\mathrm{SK}_{\mathrm{SN-MN}}}\{\mathrm{CD}_{\mathrm{i}}\}, \mathrm{H}(\mathrm{M}_1)\} \quad (1)$$

$$\mathrm{M}_1 = (\mathrm{SN}_{\mathrm{id}} || \ \mathrm{TS}_{\mathrm{SN}_{\mathrm{i}}} \ || \ \mathrm{N}_{\mathrm{i}} \ || \ \mathrm{SK}_{\mathrm{F1}} \ || \ \mathrm{E}_{\mathrm{SK}_{\mathrm{SN-MN}}} \ \{\mathrm{CD}_{\mathrm{i}}\}) \qquad (2)$$

To share the session key with MN, the session key is divided into $m$ fragments as $SK_{F1}$ and $SK_{Fm}$ which are shared in $m$ consecutive messages shared between SN and MN. Next, the SN transmits the $m$ messages towards MN which are encrypted using the secret key $E_{K_{SN-MN}}$ between SN and MN. The value of $m$ can be more than or equal to 2 as per the acceptable delay threshold for sharing the messages as given in equation (3) for $m$=2 where message $M_2$ is given in equation (4). The MN can aggregate all the messages form an SN and identify the duplicate HPVs to replace them with a one-bit flag with a value 0 to show that the value is same as previous. In many cases, the HPVs remain the same for a person for a certain period of time.

$$\mathrm{E}_{\mathrm{K}_{\mathrm{SN-MN}}}\{\mathrm{SN}_{\mathrm{id}},\ \mathrm{TS}_{\mathrm{SN}_{\mathrm{i+1}}}, \mathrm{N}_{\mathrm{i+1}}, \mathrm{SK}_{\mathrm{Fm}}, \mathrm{E}_{\mathrm{SK}_{\mathrm{SN-MN}}} \ \{\mathrm{CD}_{\mathrm{i+1}}\}, \mathrm{H}(\mathrm{M}_2)\} \qquad (3)$$

$$\mathrm{M}_2 = \mathrm{SN}_{\mathrm{id}} || \ \mathrm{TS}_{\mathrm{SN}_{\mathrm{i+1}}} || \ \mathrm{N}_{\mathrm{i+1}} || \ \mathrm{SK}_{\mathrm{Fm}} || \ \mathrm{E}_{\mathrm{SK}_{\mathrm{SN-MN}}} \ \{\mathrm{CD}_{\mathrm{i+1}}\} \quad (4)$$

### B. MESSAGE RECEIVING AND AGGREGATION AT MN

In this section, a Secure Message Aggregation (SMA) algorithm is employed at the MNs to aggregate the received messages from SNs. In this context, each SN can forward the collected and encrypted information to the MN but each node can only interact with an individual MN at a time. Moreover, the secure data aggregation method of SMA algorithm is explored as follows. The encrypted and compressed message $RV_{MN}$ is received from the SN at MN. Every $RV_{MN}$ contains $SN_{id}$, $TS_{SD_i}$, $N$, $SK_{Fi}$, $CD_i$ and hash of message. The MN checks the difference of timestamp ($TS_{MN}$ - $TS_{SN_i}$) < Δt to verify message freshness. Otherwise, drop the outdated message. Next, MN computes the hash $H(M_1)$ and matches it with the hash $\mathrm{H}'(M_1)$ of the received message $RV_{MN}$ and vice versa. The messages at the MN are concatenated by employing comma as a delimiter to construct an aggregated message $(C_m)$. In this context, if the calculated hash is not matched with the received one then the message is discarded due to integrity violation. Then, MN construct an encrypted message $(M_3)$ and this message further encrypted by employing secret key $\mathrm{E}_{\mathrm{K}_{\mathrm{MN-FN}}}$. After that, MN forwards the encrypted message to the FN as given in equation (5) and (6).

$$\mathrm{E}_{\mathrm{K}_{\mathrm{MN-FN}}}\left\{\mathrm{MN}_{\mathrm{id}}, \mathrm{TS}_{\mathrm{MN}_{\mathrm{i}}}, \mathrm{N}_{\mathrm{i}}, \mathrm{SK}_{\mathrm{Fn}}, \mathrm{E}_{\mathrm{SK}_{\mathrm{MN-FN}}}\{\mathrm{C}_{\mathrm{m}}\}, \mathrm{H}(\mathrm{M}_3)\right\} (5)$$

$$M_3 = (MN_{id} || TS_{MN_i} || N_i || SK_{Fn} || E_{SK_{MN-FN}} \{C_m\}) \quad (6)$$

*Algorithm 1: Secure Data Aggregation at Mobile Node*

```
Initialize $C_m$ = null
MN: Receive message $RV_{MN}$ = { $SN_{id}, TS_{SN_i}$ , $N_i$ , $SK_{Fi}$ , $E_{SK_{S-R}}$ {$CD_i$}, $H(M_1)$} from SN
If ($TS_{MN}$ - $TS_{SN_i}$) < Δt then
    If $H(M_1)$ equals $H'(M_1)$ then
        $C_m$ = $RV_{MN_i}$ || "," || $RV_{MN_{i+1}}$|| "," || $RV_{MN_n}$
    Else
        Message dropped for integrity violation
    End if
Else
    Drop outdated message
End if
```

### C. MESSAGE EXTRACTION AT FOG NODE

Secure Message Decryption (SMD) algorithm at the FN receives compress and encrypted messages $Dm_{FN} = \{MN_{id}, TS_{MN}, N, C_m, H(M_3)\}$ from all MNs. Initially, the SMD algorithm examines the message freshness and integrity violation at the FN.

*Algorithm 2:Message Extraction & decryption at FoG node*

```
Decrypt the message using symmetric key to get
$Dm_{FN} = \{MN_{id}, TS_{MN}, N, SK_{Fn}, C_m, H(M_3)\}$ from $MN$
If ($TS_{FS}$ - $TS_{MN}$) < Δt then
    If ($H(M_3)$ equals $H'(M_3)$ then
        For count 1 to n
            $List_{EM_{SN}}$ = Split ($C_m$ , ":") // ":" as delimiter
            Extract $CD_i$ form $C_i$ by utilizing decompression
                if ($H(C_{i_{SD}})$ equals $H'(C_{i_{SD}})$) then
                    Extract $HPV$ from $List_{EM_{SN}}$
                    If ($HPV_{Ri}$ equals $HPV_{Oi}$) then
                        Insert Boolean for same values
                    Else
                        Store values without change
                    End if
                Else
                    Message dropped for integrity violation
                End if
    Else
        Message dropped for integrity violation
    End if
Else
    Drop outdated message
End if
```

In this context, the symmetric key-based encryption is utilized to decrypt the received message. Next, check the timestamp of the received message ($\boldsymbol{TS_{FS}}$ - $\boldsymbol{TS_{MN}}$) < Δt. In case the condition is true, then calculate the hash function $\boldsymbol{H(M_3)}$ of received message and compare with the pre-computed hash $\boldsymbol{H'(M_3)}$ in the message. After calculating the hash, extract the received message. To extract the original healthcare values loop is utilized from 1 to n where n is the number of SNs that forwards health parameters. FN decompresses the healthcare data and splits $\boldsymbol{C_m}$ using colon. Before extracting the HPV from the cipher text $\boldsymbol{C_{i_{SD}}}$, the hash $\boldsymbol{H(C_{i_{SD}})}$ of received ciphertext is compared to check the integrity of received message. After that, the list of encrypted messages $\boldsymbol{List_{EM_{SN}}}$ is extracted by decrypting HPVs. It extracts the healthcare parameter values of each SN.

The SMD algorithm helps to remove the redundant values at the fog node. When the encryption procedure is completed, healthcare values are compared with the last received patient healthcare values of the same SN. In case the recent $HPV_{Ri}$ and last received $HPV_{Oi}$ values are the same, then store 0 instead of storing large bits of received values. It is a level 2 data duplication at the FN. In the end, the is processed as per the format of the cloud and the processed information is forwarded to the cloud server for storage.

For the security proof of the protocol, we employed symmetric key-based data encryption and key fragments are transmitted over the network for secure data transmission. Moreover, the hashing function is utilized to check the message integrity by comparing the hash values and also protect the original message from different security threats. The random nonce value is employed to enhance the security of our encrypted message. Thus, in the simulation paradigm, the proposed scheme resists several security threats like data fabrication, denial of service attack, and reply attack. From a security and storage point of view, the proposed scheme better security and storage in contrast to EHDA, SPPDA, APPA, ASAS.

## V. RESULTS AND ANALYSIS

In this section, our proposed scheme is validated by comparing with conventional methods. Therefore, an extensive simulation is conducting by using simulation tool NS 2.35.

### A. EXPERIMENTAL SETUP

The simulation setup is conducted on the machine with Windows 10 Pro 64-bit, Core i5 processor, 8GB RAM, and 500 GB solid-state drive. A list of simulation parameters is mentioned in Table 2.

TABLE 2. **List of Simulation Parameters**

| Parameters | Values |
|---|---|
| Network Field | 1600 × 1600 m |
| Node numbers | 20~200 |
| Cluster radius | 500 m |
| Sensing radius | 160 m |
| Initial energy | 1200 J |
| Transmission Power at Node | 0.928 µJ |
| Receiving Power | 0.052 µJ |
| Channel Type | Wireless |
| Propagation Model | Two Ray |
| Transmission Power at AN | 0.6143 µJ |
| Receiving Power | 0.052 µJ |
| Physical Type | Wireless Physical |

| | |
|---|---|
| Mac Protocol Type | Mac/802–11 |
| Queue type | DropTail/PriQue |
| Antenna Type | Omni Antenna |
| Max Packet in Queue | 60 |
| Router Trace | ON |
| Mac Trace | OFF |
| Agent Trace | ON |
| Nodes per Group | 8–40 nodes |
| Original Unit Data Size | 60–500 bytes |
| Number of Messages | 64–128 messages |
| Given Time Slot | 0.1–1.0 s |
| Responding Node Count | 50–200 nodes |

In simulation setup, the area of 1600 × 1600 meters is considered for the deployment of SNs. The maximum number of SNs are 200 and each SN can collect and forward data at the range of 160m. In the simulation scenario, we prefer Omni antennas to equally receive signals from all directions. At the start of the simulation the initial energy of the SNs is 1200 joules. A two ray propagation model is employed to predict the route failures among the receiving and transmitting antennas. The drop trail queue is employed to set the 60 packets as the maximum length of the queue. Moreover, router trace and agent trace is ON and mac trace is OFF. TCL files are employed for node deployment, node's parameter initialization and message initiation. We have managed separate classes for the collector node, sensing devices and the fog node with appropriate parameter configurations. The separate functions are created by using C language to attain the functionality of data sending and receiving. The AWK scripts are utilized to obtain results from trace files. Our presented scheme is analyzed with the relevant aggregation schemes such as EHDA, SPPDA, APPA, and ASAS. The results show the supremacy of the proposed work.

### B. EXPERIMENTAL EVALUATION

In an experimental evaluation, we analyze ESDTA against several secure and aggregation based schemes to evaluate the performance of proposed scheme in terms of communication cost, energy consumption, resilience, storage, and computational cost.

#### 1) COMMUNICATION COST

The communication cost for the secure transmission of aggregated data packets in the network is illustrated in this section. Mostly, a huge amount of data consumes more energy and enhances the communication cost. Figure 2(a) elucidates that 16000 bytes of data is forwarded from the SNs where ASAS, APPA, SPPDA, and EHDA transmit 15200 bytes, 14000 bytes, 11550 bytes, and 9300 bytes respectively. ASAS provides more cost while transmitting information in the network. Moreover, ESDAT forwards only 8860 bytes. Results prove that ESDTA provides 40%, 32%, 16%, and 3% less communication cost in contrast to ASAS, APPA, SPPDA, and EHDA, sequentially.

The communication costs based on energy and it can be estimated as $C_c = (E_s * N) + (M * E_r) + (D * E_s)$. Therefore, $E_s$ indicates the amount of energy is utilized for a transmission of a single message. $E_r$ indicates the amount of energy is utilized for receiving an individual message. N means the number of messages are transmitted, M indicates the number of the received message, and D denotes the number of data packets that are dropped. Figure 2(b) explains that 96 messages are transmitted in the network. Based on the configuration of sensor nodes, the transmission power = 0.6143 μ-Joules and receiving power = 0.052 μ-Joules also considered. In this context, the communication cost in terms of energy is estimated with related schemes and the values are 21.7352 μ-Joules, 22.2431 μ- Joules, 22.6453 μ-Joules, 22.8436 μ-Joules, and 28.3795 μ-Joules for ESDTA, EHDA, SPPDA, APPA, and ASAS, sequentially. Results illustrate that the proposed scheme archives 3%, 5%, 6%, and 23% less communication cost in terms of energy as compared to EHDA, SPPDA, APPA, and ASAS, respectively.

#### 2) ENERGY UTILIZATION

The energy consumption is examined during the aggregation of data at the MNs. The initial energy of each MN is set to 12,000 joules. Moreover, the residual energy of the nodes is printing in the trace files. The AWK scripts are used to obtain energy consumption by finding out the difference between the recent and last values at different levels of data aggregation. Figure 2(c), explains the impact of energy utilization of MN in particular instants during data aggregation at SNs. The results demonstrate that MN utilizes 0.00183 μ-Joules at 0.3 seconds. MN consumes 0.00541 μ-Joules energy at 0.9 seconds for aggregating data and forwarding to the fog node.

The sensing devices consumes a large amount of energy to aggregate the data and share with collector nodes. Figure 2(d) illustrates energy utilization at the SN nodes. The initial energy of a sensor node is set to 1200 joules. Moreover, at the particular time of 6 seconds, 0.00331 μ-Joules, 0.00396 μ-Joules, 0.00484 μ-Joules, 0.00553 μ-Joules, 0.00597and μ-Joules for ESDTA, EHDA, SPPDA, APPA, ASAS, respectively. ESDTA achieves 6%, 13%, 19%, and 22% better energy consumption at the SNs in contrast to EHDA, SPPDA, APPA, and ASAS, respectively.

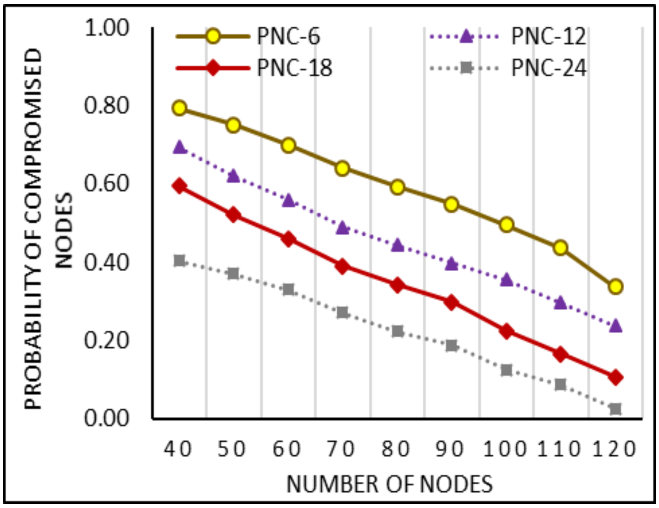
#### 3) RESILIENCE

In the case of secure data aggregation and transmission, malicious nodes also respond with the other responding nodes in data exchange. Hence, the resilience for compromised nodes is calculated by measuring the probability of malicious nodes as $\boldsymbol{Pr_C = 1 - (\frac{N-3}{C})/(\frac{N-2}{C}) = \frac{C}{N-2}}$ where N denotes the responding node and C expresses the compromised nodes. N-2 represents the elimination of sender and receiving from the calculation of malicious nodes. N-3 is a neighboring node that is eliminated to measure the probability of not compromised.

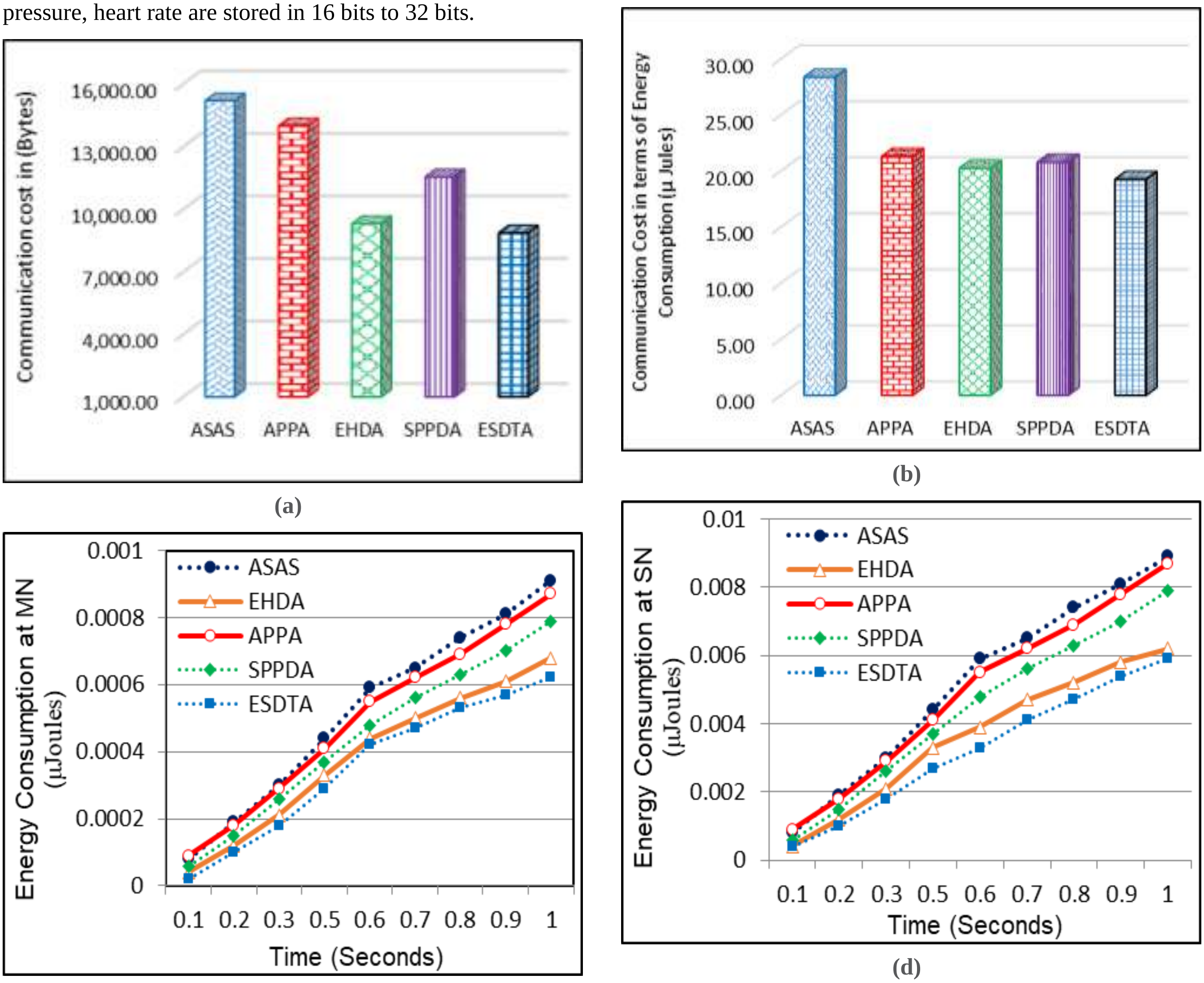
Figure 2(e) illustrates the probability of compromising responding nodes. Results are discussed in the case of 90 responding nodes and the probability of malicious nodes is 0.5481, 0.3981, 0.2981, and 0.1881 for PCN =6,12,18,24 respectively. The results demonstrate that the probability of compromised nodes decreased and increased with the number of responding nodes. The probability of compromised nodes is higher when the probability of compromised responding nodes is 6 and 26. The probability of compromised nodes decreased when the probability of compromised nodes is 6 and 110 responding nodes. Figure 2(f) demonstrates the amount of compromised bytes during data exchange. In this context, responding nodes are varied from of 40 nodes to 120 nodes. Results show that for 110 responding nodes, the number of compromised bytes are 25.125 bytes, 78.375 bytes, 155.250 bytes, and 167.617 bytes when the compromised nodes are varied as 6, 12, 18 and 24, respectively.

### 4) STORAGE COST

The storage space is measured in both normal and critical situations. Figure 3(a), illustrates the transmission of sensitive healthcare parameters values of patients in normal health conditions. In this context, the integral values related to patient’s healthcare parameters like temperature, blood pressure, heart rate are stored in 16 bits to 32 bits.



(e)

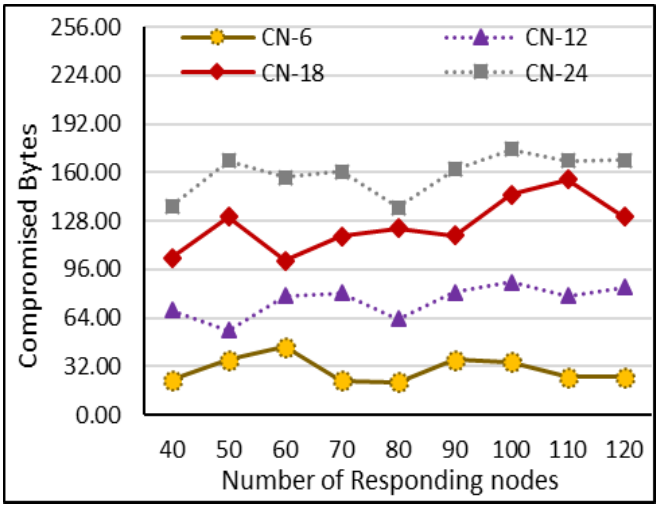


(b)

(a)

(c)

(d)



(f)

**Figure 2.** **Communication Cost in Terms of (a) Bytes Exchanged and (b) Energy Consumption, Energy Consumption at (a) MN and (b) SN, Probability of Compromised Nodes is presented in (e) and Probability of Compromised Bytes in (f)**

In this context, healthcare parameter values under the normal range are replaced with 1-bit boolean value to show that the value is almost same as previous as per threshold difference in range of values. The data values of the size 100-400 bytes are transmitted to inspect the impact on storage. For example, temperature value is under the normal range so instead of storing the whole value a bit Boolean value is stored. Therefore, ESDTA reduces the size of data for storage up to 80%. Thus, results show that ESDTA provide 40% better storage occupation than EHDA. In the case of SPPDA, APPA, and ASAS, the transmitted data bytes are stored without data compression. Moreover, ESDTA achieves 80% better storage as compared to SPPDA, APPA and ASAS.

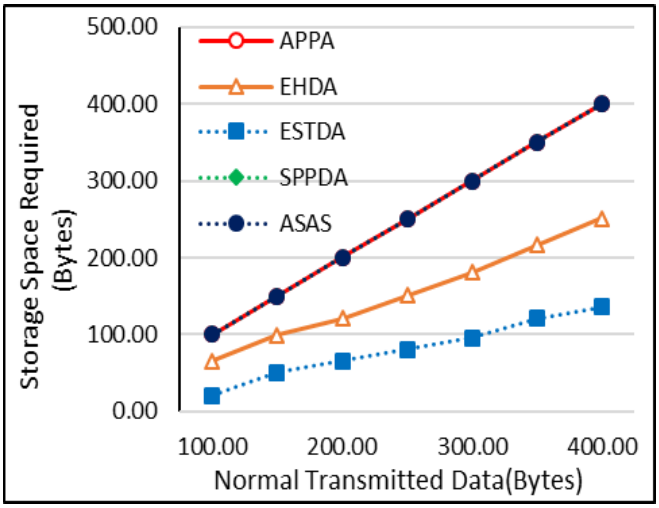
Figure 3(b), illustrate the emergency condition of patient health. In this context, when critical health parameters values of patient are transmitted on priority basis. The health parameters values are generating after every 3 min. Mostly; health parameters are not changing after very short interval. For example, temperature of patient in critical situations also not changing in every 2-3 minutes. Hence, the last received values are same as the current value than 1bit Boolean value is stored for current value or upcoming current values until a change occur. Therefore, ESDTA decreases the data storage space up to 40%. The analysis demonstrates that ESDTA provide 20% better storage utilization in contrast to EHDA. Moreover, ESDTA attains 40% better storage as compared to SPPDA, APPA and ASAS.

### 5) COMPUTATION COST

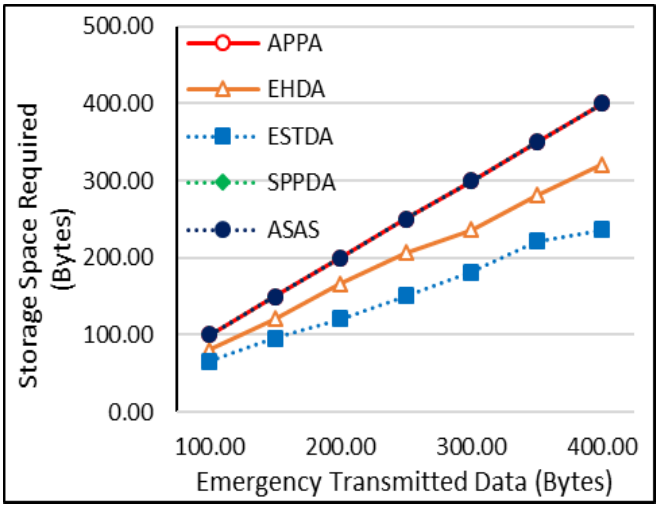
In the aggregation phase, the mobile node aggregates the healthcare parameters of the patients by using the colon as a delimiter. Fog node extracts the healthcare parameter values for removal or redundant values. The hash functions are employed to check the integrity of the received message. In Figure 4, we illustrate the computation cost in terms of the number of smart devices. In Fog-enabled healthcare systems little improvement in the efficiency of SNs deliver large benefits. Thus, the ESDTA scheme is quite helpful in resource-limited SNs. Therefore, the proposed scheme is analyzed with other related schemes. We observe that when the number of nodes is 60, the computational cost ESDTA, SPPDA, APPA, EHDA, and ASAS is 16.75 ms, 23.87 ms, 25.13 ms, 17.45 ms and 27.47 ms, respectively. ESDTA provide 24%, 26%, 3%, and 32% better computational cost in contrast to EHDA, SPPDA, APPA, and ASAS The analysis shows that ESDTA provides low computational cost while comparing other data aggregation schemes.

## C. COMPARISON AND EVALUATION MATRIX

In this section, we present the evaluation matrix of the proposed scheme ESDTA with other counterparts such as EHDA, SPPDA, APPA, and ASAS in terms of communication cost, energy consumption, storage, computational cost. In communication cost analysis, ESDTA provides 23% better communication cost in terms of transmitted bytes and 20% better communication cost in terms of energy consumption as compared to counterparts.



(a)



(b)

**Figure 3.** **Storage Cost for Data Size**

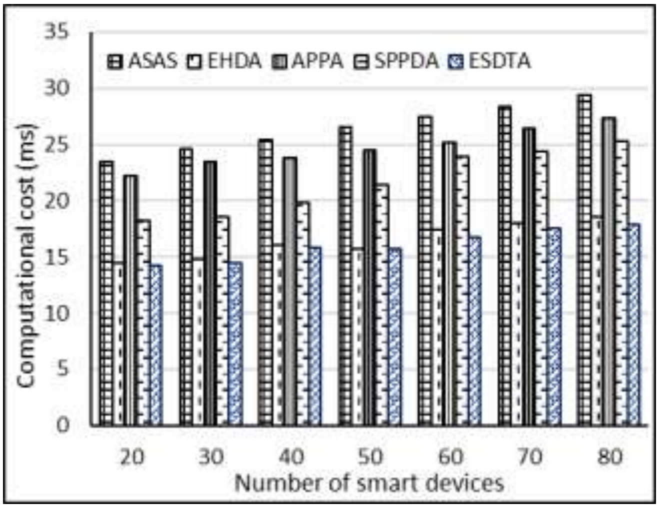


**Figure 4. Computation Cost**

In case of energy consumption, ESDTA provides 43% better energy consumption at the SN. Moreover, ESDTA provides 50% better storage and 61% better communication cost in contrast to others existing data aggregation-based schemes. Our proposed scheme and other counterparts are evaluating against several parameters in Table 3. In this table, we consider 5 different levels such as Very High (VH), High (H), Medium (M), Low (L), Very Low (VL), Not Supported (NS). The analysis show that ESDTA provide better results against other related healthcare based schemes.

**TABLE 3. Evaluation of schemes against several parameters**

| Parameters | ESDTA | EHDA | ASAS | APPA | SPPDA |
|---|---|---|---|---|---|
| Data Aggregation | VH | H | M | H | H |
| Energy Efficiency | H | H | L | M | H |
| Resilience for Compromised Nodes | M | M | VL | M | L |
| Data Compression | H | M | NS | NS | NS |
| Scalability | M | M | L | VL | L |
| Redundant Data | VL | L | H | H | M |
| Storage Utilization | L | M | VH | M | M |
| Security | H | H | H | H | H |

## VI. CONCLUSION

In IoMT, medical applications provide real-time monitoring of patient health parameter values. Smart medical devices efficiently and securely forward the healthcare information at the remote servers. Although different schemes provide several solutions for secure and efficient data aggregation and transmission of data. However, the recent research studies also facing several issues in terms of secure and effective data transmission and aggregation. Therefore, this paper presents an Efficient and Secure Data Transmission and Aggregation (ESDTA) scheme. It provides a secure and efficient exchange of patient data. The proposed scheme validates the system and security model for remote patient monitoring and also protects from the number of security attacks. For secure and lightweight data transmission, a data aggregation algorithm is employed at the MN, and a message extraction algorithm is employed at the fog node. Moreover, NS 2.35 tool is utilized to perform an extensive simulation. The results prove the validity of our proposed scheme. we compare our scheme with other related secure data aggregation-based schemes in terms of communication cost, computational cost, energy consumption, resilience, and storage. In the future, a more effective data aggregation method is implemented to further improve the efficiency and security of our proposed scheme.

## REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] N. Scarpato, A. Pieroni, L. Di Nunzio, and F. Fallucchi, “E-health-IoT Universe: A Review,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 6, p. 2328, 2017.

[3] M. M. Dhanvijay and S. C. Patil, “Internet of Things: A survey of enabling technologies in healthcare and its applications,” *Comput. Networks*, vol. 153, pp. 113–131, 2019.

[4] G. Gardasevic, K. Katzis, D. Bajic, and L. Berbakov, “Emerging Wireless Sensor Networks and Internet of Things Technologies — Foundations of Smart Healthcare,” *Sensors*, vol. 20, no. 13, pp. 1–30, 2020.

[5] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IoT security based on a layered architecture of sensing and data analysis,” *Sensors*, vol. 20, no. 13, pp. 1–19, 2020.

[6] R. A. Khan, “The state-of-the-art wireless body area sensor networks : A survey,” vol. 14, no. 04, pp. 1–23, 2018.

[7] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, pp. 1–22, 2017.

[8] V. Chang, F. Firouzi, N. Constant, K. Mankodiya, M. Badaroglu, and B. Farahani, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2017.

[9] X. Jia and D. He, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wirel. Networks*, vol. 25, pp. 4737–4750, 2018.

[10] H. Abdulaziz *et al.*, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.

[11] J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives," *Comput. Networks*, vol. 148, pp. 295–306, 2019.

[12] J. C. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, "Privacy Preserving Multi-Objective Sanitization Model in 6G IoT Environments," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5340–5349, 2021.

[13] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," *IEEE Trans. Ind. Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[14] and C. P. Nada Alhirabi, Omer Rana, "Security and privacy requirements for the Internet of Things : A survey," *ACM Trans. Internet Things*, vol. 2, no. 1, pp. 1–37, 2021.

[15] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[16] T. Han, L. Zhang, S. Pirbhulal, W. Wu, V. Hugo, and C. De Albuquerque, "A novel cluster head selection technique for edge-computing based IoMT systems," vol. 158, pp. 114–122, 2019.

[17] M. Papaioannou *et al.*, "A Survey on Security Threats and Countermeasures in Internet of Medical Things ( IoMT )," pp. 1–15, 2020.

[18] Z. Mahmood, H. Ning, A. Ullah, and X. Yao, "Secure Authentication and Prescription Safety Protocol for Telecare Health Services Using Ubiquitous IoT," *Appl. Sci.*, vol. 7, no. 10, pp. 1–22, 2017.

[19] H. Khemissa and D. Tandjaoui, "A Lightweight Authentication Scheme for E-health applications in the context of Internet of Things," in *9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 90–95.

[20] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Networks*, vol. 129, pp. 429–443, 2017.

[21] S. Han, S. Zhao, Q. Li, C. Ju, and W. Zhou, "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation With Fault Tolerance," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 1940–1955, 2016.

[22] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, "LSDAR : A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks," *Sustain. Cities Soc.*, vol. 54, pp. 1–9, 2020.

[23] F. Rezaeibagha, Y. Mu, S. Member, K. Huang, and L. Chen, "Secure and Efficient Data Aggregation for IoT Monitoring Systems," *IEEE Internet Things J.*, vol. 14, no. 8, pp. 1–8, 2020.

[24] Z. Liao *et al.*, "Distributed Probabilistic Offloading in Edge Computing for 6G-enabled Massive Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5298–5308, 2021.

[25] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S. J. Lim, "Privacy ensured e-Healthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019.

[26] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Netw. Appl.*, vol. 13, pp. 163–174, 2019.

[27] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 712–719, 2018.

[28] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, 2019.

[29] R. Lu, S. Member, and K. Heung, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[30] A. Alabdulatif, I. Khalil, X. Yi, and M. Guizani, "Secure Edge of Things for Smart Healthcare Surveillance Framework," *IEEE Access*, vol. 7, pp. 31010–31021, 2019.

[31] H. Liu, X. Yao, T. Yang, and H. Ning, "Cooperative privacy preservation for wearable devices in hybrid computing-based smart health," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1352–1362, 2018.

[32] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941–12950, 2017.

[33] M. Humayun and N. Z. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT — A Survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[34] R. Lu, X. Liang, S. Member, and X. Li, "EPPA : An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1632, 2012.

[35] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "PHDA : A Priority Based Health Data Aggregation with Privacy Preservation for Cloud Assisted WBANs," *Inf. Sci. (Ny).*, pp. 130–141, 2014.

[36] X. Lin, R. Lu, and X. S. Shen, "MDPA : multidimensional privacy-preserving aggregation scheme for wireless sensor networks," *Wirel. Commun. Mob. Comput.*, vol. 10, no. 6, pp. 843–856, 2010.

[37] L. Chen, R. Lu, Z. Cao, K. Alharbi, and X. Lin, "MuDA : Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Netw. Appl.*, vol. 8, pp. 777–792, 2015.

[38] H. Zhu, L. Gao, and H. Li, "Secure and Privacy-Preserving Body Sensor Data Collection and Query Scheme," *Sensors*, vol. 16, no. 2, pp. 1–16, 2016.

[39] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, pp. 1–17, 2019.

[40] S. Darwish, I. Nouretdinov, and S. Wolthusen, "A dynamic distributed architecture for preserving privacy of medical IoT monitoring measurements," in *International Conference on Smart Homes and Health Telematics (ICOST)*, 2018, pp. 146–157.

[41] X. Shen, L. Zhu, C. Xu, K. Sharif, and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Inf. Sci. (Ny).*, vol. 514, pp. 118–130, 2020.

[42] R. Raju, M. Moh, and T. S. Moh, "Compression of Wearable Body Sensor Network Data Using Improved Two-Threshold-Two-Divisor Data Chunking Algorithms," in *International Conference on High Performance Computing and Simulation, HPCS*, 2018, pp. 949–956.

[43] K. Y. Yigzaw, A. Michalas, and J. G. Bellika, "Secure and scalable deduplication of horizontally partitioned health data for privacy-preserving distributed statistical computation," *BMC Med. Inform. Decis. Mak.*, vol. 17, no. 1, pp. 1–19, 2017.

[44] J. Ren, G. Wu, and L. Yao, "A sensitive data aggregation scheme for body sensor networks based on data hiding," *Pers. Ubiquitous Comput.*, vol. 17, no. 7, pp. 1317–1329, 2013.

[45] S. Ben Othman, U. R. Prince, and H. Sousse, "Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks," in *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 188–195.

[46] A. B. B. Soufiene and A. T. and H. Youssef, "Lightweight and confidential data aggregation in healthcare wireless sensor networks," *Emerg. Telecommun. Technol.*, vol. 27, no. 4, pp. 576–588, 2017.