Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.025514
Article

Tech Science Press

Paillier Cryptography Based Message Authentication Code for IoMT Security

S. Siamala Devi[1], Chandrakala Kuruba[2], Yunyoung Nam[3,*] and Mohamed Abouhawwash[4,5]

[1]Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, 641042, India
[2]Department of Computer Science and Engineering, Vignan Nirula Institute of Technology and Science, Guntur, 522009, India
[3]Department of Computer Science and Engineering, Soonchunhyang University, Asan, 31538, Korea
[4]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[5]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI, 48824, USA
*Corresponding Author: Yunyoung Nam. Email: ynam@sch.ac.kr
Received: 26 November 2021; Accepted: 11 January 2022

Abstract: Health care visualization through Internet of Things (IoT) over wireless sensor network (WSN) becomes a current research attention due to medical sensor evolution of devices. The digital technology-based communication system is widely used in all application. Internet of medical thing (IoMT) assisted health-care application ensures the continuous health monitoring of a patient and provides the early awareness of the one who is suffered without human participation. These smart medical devices may consume with limited resources and also the data generated by these devices are large in size. These IoMT based applications suffer from the issues such as security, anonymity, privacy, and interoperability. To overcome these issues, data aggregation methods are the solution that can concatenate the data generated by the sensors and forward it into the base station through fog node with efficient encryption and decryption. This article proposed a well-organized data aggregation and secured transmission approach. The data generated by the sensor are collected and compressed. Aggregator nodes (AN) received the compressed data and concatenate it. The concatenated and encrypted data is forward to fog node using the enhanced Paillier cryptography-based encryption with Message Authentication code (MAC). Fog node extracts the forwarded data from AN using Fog message extractor method (FME) with decryption. The proposed system ensures data integrity, security and also protects from security threats. This proposed model is simulated in Network Simulator 2.35 and the evaluated simulation results proves that the aggregation with MAC code will ensures the security, privacy and also reduces the communication cost. Fog node usages in between Aggregator and base station, will reduce the cloud server/base station computational overhead and storage cost. The proposed ideology is compared with existing data aggregation schemes in terms of computational cost, storage cost, communication cost and energy cost. Cost of communication takes 18.7 ms which is much lesser than existing schemes.

Keywords: Fog; IoMT; wireless sensor network; cloud; aggregation; encryption; decryption; energy

1 Introduction

Internet of things [1] consists of exchanging the data where there is a interconnection between objects and humans. High quantity of data is generated from these sources and travelled through the wireless networks in a bidirectional way for remote monitoring. Evolution of these IoT devices and digital technologies, many healthcare domains are providing effective and efficient solutions and diagnosis. Which is also raised many challenging issues related to security and big data processing [2]. Smart devices with intelligent sensors focus on IoT development and play a major role in the fields such as data mining, healthcare, cities, agriculture, buildings, transportation, and industry [3]. IoT used as a medium for remote healthcare monitoring of patients [4] that connect patients and objects that make the life simpler [5]. These smart devices collect various kind of information and transform to cloud repositories for processing [6,7].

Wearable sensor devices of the patients send the data related to patient health to nearby network server. This network ensures the patient data authentication and provides the diagnosis result in case of emergency scenario [8] termed as Internet of Medical Things (IoMT) [9]. In healthcare application, many IoT devices are involved over the network. Hence, security of these data transmission should be considered because medical professionals are monitored these data continuously and provide more relevant and accurate services to the patients. The wearable devices are fitted to the patient's hand/any parts to calculate the parameter values such as blood pressure, heartbeat, temperature, and blood oxygen, etc., [10]. The collected data are forwarded to collector node such as tabs, smart phones, and personnel digital assistant (PDA) for aggregation [11]. This aggregated data is then forwarded to cloud server for processing.

The limit of processing the data with available bandwidth will leads to emergence of fog computing which provide the distributed storage and services with cloud. The term Fog Server is invented by Cisco [12], for processing local data at the edge of network with fog nodes [13]. The medical data from IoT device are aggregated and stored to cloud for further processing. Due to the huge data and delay, the response times will increase [14]. Hence, Fog node reduces the computation overhead of cloud server and provides the load balance at neighbor fog devices that can handle the data efficiently to provide effective solutions in a timely manner.

The constant connection between the devices over the network leads various security attacks [15]. Fog integrated IoT provides the services as more efficient, secure, and reliable for the users [16]. In IoMT, fog node and collector nodes at the edge will provide best solutions because of system low power, energy, and bandwidth [17]. To rectify issues in IoMT, fog computing and cloud computing are the best combination [18,19]. To protect the sensitive patient data during transmission, IoMT requires efficient secure and privacy mechanisms [20]. In aggregation, compression also performs vital role to reduce the storage. The capacity of the compression is based on compression ratio. This will reduce the resource utilization of sensor nodes while sending aggregated data to cloud server [21]. In this context, security, effective communication cost with less storage is a primary concern about patient health monitoring in IoMT [22]. While transmitting the data from mobile phones, it may not be secure. Neighboring mobile nodes may act as a malicious node to hack the patient sensitive data. It will cause denial of service (DoS) attack that can drop the aggregated message instead of forwarding it.

The ordinary data compression and aggregation methods are increase the storage and communication cost. In this article, we introduce an effective data compression and data aggregation plan for real time healthcare monitoring. Collector node in the model will aggregate the data from sensing devices and utilize Paillier cryptosystem with message authentication code (PC-MAC) based data encryption and data decryption. The fog nodes perform message decryption and perform local computation to reduce the cloud server overhead. The contribution of this work is as follows:

- Patient health data received from sensor node (SN) is compressed to reduce its size and encrypted using PC-MAC. The encrypted message is forwarded to Aggregator Node (AN) for aggregation.
- The proposed data aggregation scheme aggregates the data from SN using the delimiter and the redundancy of the data is avoided with the Boolean value and MAC code.
- Fog node received the data from AN and performs decryption and message extraction using proposed fog message extractor with the delimiter for local storage processing.
- Efficiency of the proposed system is simulated and evaluated by comparing with the existing data aggregation methods. Proposed scheme ensures security with the implementation of PC-MAC, integrity with the use of MAC code, reduced the size with the implementation of compression and fog node reduces the computational overhead of cloud server.

The remaining section of this article is shown Section 2 explains about the literature data aggregation schemes. Section 3 illustrates the proposed data aggregation methodology. Simulation results are explored, and result discussion is done in Sections 4 and 5 concludes the proposed work with merits and future direction.

2 Literature Work

This part discusses about the research work related to data aggregation methods for IoT and IoMT related to healthcare. Data aggregation method provides the redundant reduced communication with efficient energy and bandwidth utilization. Li et al. [23] proposed a hop method for wireless body area network (WBAN). Data authentication and aggregation are performed at the network and the security is ensure with session key generation. Haseeb et al. [24] proposed communication method for energy efficient consumption. To provide security, one time pad encryption technique is used to detect the attacks. An Anonymous and Secure Aggregation technique in [25] is proposed pseudonyms to protect the node's identity. To protect the data integrity, homomorphic encryption is used. This method reduces the bandwidth utilization but due to redundant data transmission, computational cost and communication cost are increased. An Anonymous Privacy Preserving scheme with Authentication (APPA) [26] ensures the smart devices identity with asymmetric key encryption and for data calculation, pseudonym certificate employed. This method ensures multilevel security and authentication. But this method is better for limited number of devices. Abdullatif et al. [27] proposed a fog framework for data privacy using clustering techniques.

Liu et al. [28], proposed cipher text-based encryption with cooperative scheme for access control that ensures the integrity of the sensor data. Saha et al. [29] proposed fog assisted healthcare system with pseudo identify to identify the patient's data individually. EHDA (Efficient health data aggregation) methods [30] provide smart nodes with secure communication. AN use message receiving method for aggregation on compressed data from smart nodes of sensor. FN employs receiving based message algorithm and decrypts the aggregated data for analysis. EPPA (Efficient and privacy preserving aggregation) [31–33] method aggregates the data efficiently using Paillier cryptosystem. To construct multidimensional data cypher text, super increasing sequence method used.

Health data aggregation with priority [34] proposed and offers a data privacy using Paillier and homo-cryptosystem. Zhu et al. [35] proposed privacy preserved aggregation method for Wireless body area network (WBAN) using bilinear pairing cryptosystem for aggregation. Shen et al. [36] proposed an aggregation method for data to protect from malicious nodes. Redundant values are removed at Fog Node (FN) and to preserve bandwidth, data aggregation method employed. Farahani et al. [37] discussed about the big issues related to aggregation via fog node and cloud.

In terms of scalability, privacy, and security, it discusses the case study to point out the essential for healthcare monitoring. discussed about the emerging technologies used for IoT enabled healthcare applications. They also discussed about the security challenges and open issues for future research directions. Azeem et al. [38] proposed efficient fog-oriented data aggregation scheme for IoMT. This model used secure aggregation and secure decryption of message to ensure the security and integrity. Ullah et al. [39] presents a survey about the secure data transmission and data collection for fog-based healthcare architecture. They discussed about fog based efficient and reliable data collection schemes for smart city, smart grid, and smart vehicle. With all these discussions, security and integrity on IoMT is still a challenging issue with low computation and energy consumption.

3 Proposed Paillier Cryptosystem with MAC Methodology

This section proposed an IoT enabled healthcare model which supports the monitoring of patient health at distant location. Overview of this proposed technique is given in Fig. 1. This system illustrate the data forwarding form medical sensor IoT devices to base station/ cloud server. Wearable IoT sensor devices act as a Sensor Nodes (SN) collects the patient data related to healthcare parameters such as oxygen level, body temperature, heartbeat, blood pressure, etc., the SN set is represented as SN1, {SN2,…,SNn-1} where n∈[1,N], N-number of sensor nodes. SN collects the data and compress the values then forward into Aggregation Node (AN). AN transmit the encrypted and aggregated data into Fog node (FN) which is the edge node that provide secure transmission and helps to decrease the Computational problems and energy consumed by cloud server. SN and AN communicate the data through Paillier cryptosystem with MAC code-based encryption technique. AN and FN also communicate the data in secure with the PC-MAC approach. FN compute and format the data in the cloud server required format and forward it into cloud server for analysis.

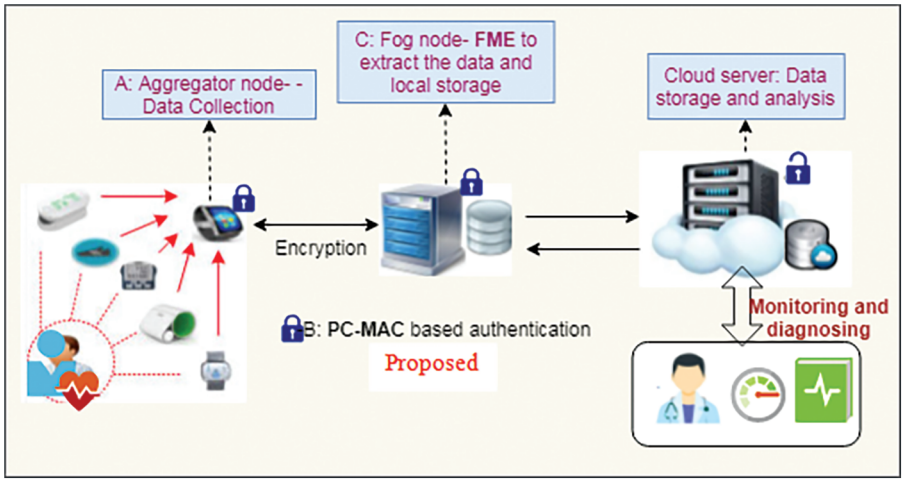

Figure 1: Proposed fog assisted IoMT enabled data aggregation system model

Proposed secured aggregation and transmission system model is as follows: First, SN collects the patient healthcare parameter values. The gathered data are encrypted using PC-MAC scheme-based encryption. Each SN of the network forward the encrypted data into AN. SN also responsible for compress the data to decrease the value size of the parameter. This will reduce the storage cost. Data aggregation technique is used to aggregate the data and compress it. AN is the mediator of SN and FN which provides the data processing at the network edges. The aggregated data are then forwarded into FN. FN performs the

decryption process of PC-MAC and decompression of the health parameters. FN perform local storage and computation as per the need of cloud then forward the data into cloud server repositories. Authenticated medical experts can access the patient health data from cloud server for diagnosis.

In IoMT security is the major challenge that needs to be considered. The proposed secure aggregation and transmission model can overcome this challenge with three phases of processing. (A) Sensor data collection, compression and encryption using PC-MAC (B) Data aggregation and data encryption at AN, (C) Data/message decryption and message retrieval using Fog Message Extractor method and remove the data redundant. A notation listed in this proposed model is listed in Tab. 1 and three phases are discussed as follows:

Table 1: Notations used

Notation	Description
Cd_i	Compressed data of Sensor Node
T	Sensing device time stamp
SN_{id}	Sensor Node id
MAC	Sensing device Mac code concatenated with PC key
m	Original message
n	Number of sensor nodes
c	Encrypted cipher text by sensor device
K_{SN-MN}	Key from SN to MN
A_m	Aggregated and encrypted message by AN
R_{AN}	Received message by AN
AN_{id}	Aggregator node id
HP	Health parameter value
HP_{recent_i}	Health parameter value of recently received
$HP_{last\ recieve_i}$	Health parameter value of last received

3.1 Sensor Data Collection and Compression

Smart sensor nodes (SN) gather the health parameters and forward the data into AN. Data compression and PC-MAC- encryption are used for effective data transmission. Initially SN collects the health based parameters (HP) for various sensors and these aggregated data are denoted as SNAgg= {HPi, HPi+1,…, HPn } where i$\in [1, n]$. The method of data compression is used to compress the collected HP values and it is represented as in Eq. (1)

$$CompData(Cd)_i = \{compr(SNAgg)\} \tag{1}$$

Sensing devices encrypt the compressed data and transfer to it's AN using homomorphic encryption method called Paillier cryptosystem [40]. It is the asymmetric algorithm that provides secure and faster encrypting and decryption. MAC is a cryptographic construction that is used to identify the falsification

of the messages. It is represented using one way hash function, secret key generated by PC and the message of length m. This MAC will increase the integrity and the receiver needs to recalculate the MAC code with its decryption to ensues the authenticity. Based on PC, key generation, encryption and decryption, MAC code creation is declared in step by step.

PC-MAC encryption at sensor node:

Step 1: Key generation: Randomly choose two prime numbers called p and q which is independent to each other as $\gcd(pq,(p-1)(q-1)=1)$

Calculate $t=pq$ and $\lambda=1$ cm, choose random integer number $g\epsilon Z_{t^2}^{*}$

Ensure t divides g by checking the modular multiplicative inverse defined as in Eq. (2)

$$\mu=(G(g^{\lambda} mod\ t^2))^{-1} mod\ t \tag{2}$$

where $L(x)=x-1/t$

Public key is (t,g) and private key is (λ,μ)

Step 2: Encryption: given message m where $0\leq m\leq t$ and random number r where $r\leq m\leq t$, ciphertext is calculated as in Eq. (3)

$$C=g^{m}.r^{t} mod\ t^2 \tag{3}$$

Step 3: MAC code is represented as in Eq. (4)

$$MAC=Hash_k(m) \tag{4}$$

Step 4: Decryption: given cipher text c, original message is calculated as in Eq. (5)

$$m=G(c^{\lambda} mod\ t^2).\mu mod\ t \tag{5}$$

The message m1 is given as in Eq. (6) from SN to AN. For message m2, the code is generated as in Eq. (7). Likewise, the messages are compressed and encrypted using this phase and send from SN to AN.

$$m1=\{SN_{id}||T_{SN_i}||K_{SN-MN}||MAC_{SN_i}(cd_i)\} \tag{6}$$

$$m2=\{SN_{id}||T_{SN_{i+1}}||K_{SN-MN}||MAC_{SN_{i+1}}(cd_{i+1})\} \tag{7}$$

where,

SN_{id}- Sensor node id, t- time stamp for corresponding sensor node, K- key generated and Cd-compressed data.

3.2 Data Aggregation Using Aggregation Node Message Aggregation Method (AN-MA)

The messages generated from phase I are aggregated using AN-SMA method. Each SN forwards the data encrypted to AN. Each individual SN can communicate with AN at a time. At AN, each message received is represented as RAN which contains SN_{id}, $T_{SN_{i+1}}$, K_{SN-MN}, Cd_i and MAC code. Message retrieval and aggregation using this phase is stated in Algorithm 1:

Algorithm 1: Data aggregation using AN-MA

Step 1: Initialize A_m=null

Step 2: AN: Receive message as $R_{AN} = \{SN_{id}||T_{SN_i}||K_{SN-MN}||MAC_{SN_i}(cd_i)\}$ from SN

Step 3: if $T_{AN} - T_{SN} < \Delta t$ then

Step 4: if $MAC_{SN_{m1}} == MAC_{AN_{m1}}$ *then*

Step 5: $$A_m = R_{AN_i} \parallel R_{AN_{i+1}} \parallel \ldots \parallel R_{AN_n} \quad (8)$$

Step 6: else

Step 7: Drop the message due to integrity violation

Step 8: End if

Step 9: Else

Step 10: discard the outdated message

Initially, the aggregate message variable is set as null. AN check the timestamp of the messages received as in step 3 to check the message freshness. If it is true, then AN can compare the MAC code generated by AN for that message with MAC code by SN. If so, AN concatenate the messages as in step 5. If not, AN drop the message due to integrity violation. If the MAC code doesn't match, then the messages are discarded due to loss of freshness. Now, AN forward this aggregated message to FN.

3.3 Message Extraction Using Fog Message Extraction (FME) Method

Server of Fog receives the aggregated messages from all AN using FME. FN received the message from AN as in the form $\{AN_{id}, T_{AN}, A_m, MAC_{A_m}\}$ from all AN. FN can decrypt the message with PC-MAC decryption approach in phase A. FN checks the timestamp of the received message from AN. If the message is fresh, then calculate the MAC for received message and compare it with received MAC which is stated in Algorithm 2.

Algorithm 2 Fog message extraction with MAC

Step 1: decrypt the message using step 4 of Algorithm 1 and get

$De_{FN_m} = \{AN_{id}, T_{AN}, A_m, K_{FN}, MAC_{A_m}\}$

from AN

Step 2: if $T_{FN} - T_{AN} < \Delta t$ then

Step 3: if $MAC_{AN\,A_m} == MAC_{FN\,A_m}$ then

Step 4: for i=1 to n

Step 5: $list_{SN} = split(A_m, '', '')$ ',' delimeter

Step 6: extract Cd_i from $A_m$using decompression

Step 7: extract HP from $list_{SN}$

Step 8: if $(HP_{recent_i} == HP_{lastrecieve_i})$ then // redundancy check

Step 9: store the Boolean value

Step 10: else

(Continued)

Algorithm 2: (continued)

Step 11: store the original value
Step 12: end if
Step 13: end for
Step 14: Else
Step 15: message dropped due to integrity violation
Step 16: End if
Step 17: Else
Step 18: drop outdated message
Step 19: End if

Server in fog received the aggregated cipher text of all the AN and check for newness. If it is true then MAC for FN is calculated and compared with MAC for AN. If both are same then FN decompress the data and split the aggregated data to receive the health parameter values for i is 1 to number of nodes with the delimiter comma (,). HP values are extracted with the decryption method. Redundancy of the system is further improved with the step 8 to check the HP values of recently received with HP values last received. If there is match, then it returns the Boolean value 0. Or else original value is returned.

After checking the integrity violation and freshness, the extracted messages are forwarded to cloud server for storage and analysis. Hence, security of the proposed model is ensured with PC-MAC data encryption. MAC code of the message can be used to check the integrity by comparing the values which also protect the original message from threats. Compression based aggregation will reduce the storage cost. Proposed model security is further enhanced with the second level of security using the comparison between the health parameter received recent and last received. Fog node between AN and cloud will reduce the computational overhead of the cloud storage. Thus, the proposed model is secure and safe transmission over IoMT enabled WSN which resists security threats such as denial of service attack, data fabrication and replay attack.

4 Simulation Results and Discussions

The proposed efficient and secure aggregation model is simulated using NS 2.35 with the simulation parameters listed in Tab. 2. Separate classes are managed for FN, SN and collector node with corresponding configuration of parameters. To achieve the data sending functionality and receiving functionality, separate functions are created using C language.

Table 2: Simulation parameter

Parameter	Value
Field of network	1700 * 1700 m
Number of nodes	30–300
Sensing radius	150 m
Cluster radius	500 m
Energy initialized	1100 J

(Continued)

Table 2 (continued)

Parameter	Value
Transmission power at node	0.911 μJ
Power of Receiving	0.051 μJ
Channels used	Wireless
Transmission power at AN	0.612 μJ
MAC protocol type	802.11
Type of Antenna	Omni antenna
Maximum packets at queue	50
Nodes per group	10–40
Total messages	60–120 messages
Initial slot of time	0.1–1 s
Responding count of node	60–300 nodes
Propagation model	Two rays

The proposed scheme results are evaluated with the existing data aggregation methods like ASAS [25], APPA [26], EHDA [30] and SPPDA [41], in terms cost of communication in terms exchanged bytes, energy cost for AN and SN, storage cost in terms of data transmission and computation cost [42–50].

4.1 Communication Expenditure

Cost of communication for aggregated data packets of the proposed model is illustrated. Generally, more energy consumed by large data which will increases the cost of communication. Since it is based on energy, the computation is estimated based on Eq. (9).

$$CC = (E_s * N) + (M * E_r) + (D * E_s) \tag{9}$$

where,

E_s- Energy utilized for single message transmission, E_r- Energy used for receiving single message, N- Total messages transmitted, M- received messages count, D- Number of dropped data packets. Fig. 2 illustrate that 16000 bytes of data are transmitted over the network from SN. EHDA, SPPDA, ASAS and APPA transmit 9200 bytes, 11000 bytes, 15300 bytes and 14000 bytes respectively. Whereas our proposed aggregation scheme transmits only 7300 bytes of data. This evaluated results proves that the proposed scheme communication cost is 11.8%, 23%, 50% and 41% less than EHDA, SPPDA, ASAS and APPA respectively.

Communication cost in terms of energy is illustrated in Fig. 3. Based on the sensors, data transmission power in micro joules is 0.612 μJ and receiving power is 0.051 μJ is considered. The estimated values to transmit 100 messages for the schemes EHDA, SPPDA, ASAS, APPA and proposed model are 22.5142 μJ, 22.6571 μJ, 28.0161 μJ, 23.8123 μJ and 20.1273 μJ sequentially. Proposed scheme obtains 2.03%, 2.15%, 6.73% and 3.14% less communication cost in terms of energy than other existing approaches such as EHDA, SPPDA, ASAS and APPA respectively.

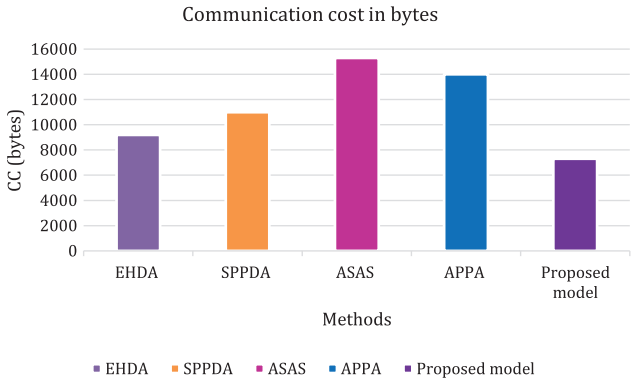

Figure 2: Communication cost in bytes

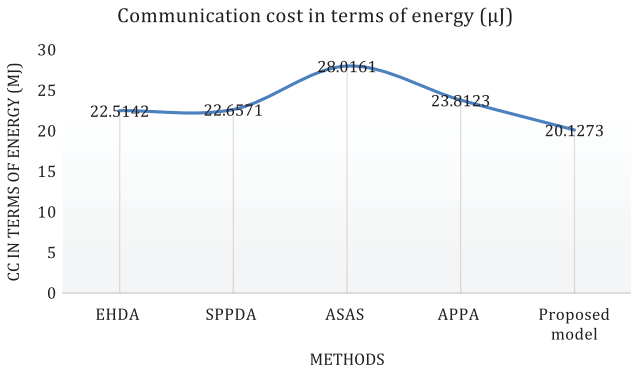

Figure 3: CC in terms of energy

4.2 Energy Cost

Energy consumption of the proposed method is examined in terms of utilization at AN and energy utilization at SN. The initial energy value is set as 1100 J. Fig. 4 illustrates the energy utilization of AN while data aggregation. At a particular time of 0.5 s 0.000168 μJ, 0.000167 μJ, 0.000181 μJ, 0.000165 μJ and 0.00153 μJ for EHDA, SPPDA, ASAS, APPA and proposed model which proves that proposed model secures less energy than other existing approaches.

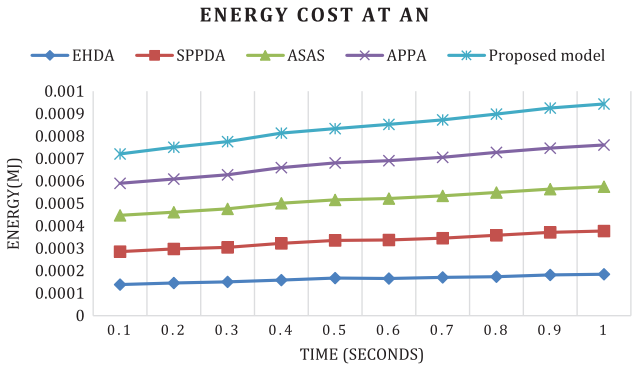

Figure 4: Energy utilization at AN

Energy utilization at SN is shown in Fig. 5 with the initial energy of 1100 J. The results shows that SN utilizes 0.00148 μJ at 0.3 s and 0.00178 μJ at 0.9 s. Various other existing approaches EHDA, SPPDA, ASAS and APPA energy utilization at time 0.3 s are 0.00151 μJ, 0.00153 μJ, 0.00172 μJ and 0.00152 μJ respectively. This result proves that proposed scheme utilized less energy than other existing methods.

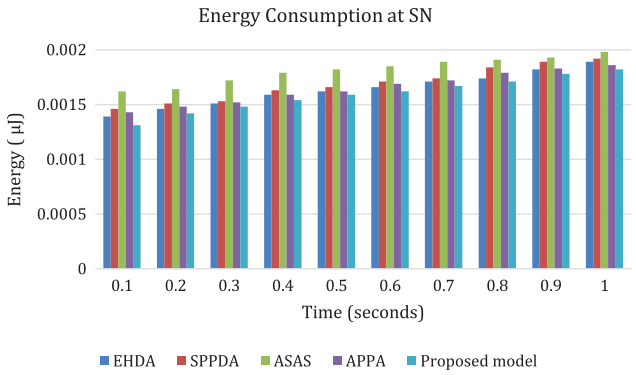

Figure 5: Energy utilization at SN

4.3 Storage Cost

The storage space measurement for patient normal health condition is evaluated in this section. Fig. 6 illustrates the storage space required to transmit the normal patient sensitive health parameter values such as temperature, blood pressure, heartbeat. These parameters are represented as integral values and stored in 16 bits to 32 bits. With the compression technique proposed system need less storage to store these messages. Data values are transmitted in100–500 bytes for evaluation. Proposed model reduces the data storage up to 85%. The evaluated results shows that proposed scheme secure 50% of reduced storage than existing approaches such as EHDA, SPPDA, ASAS and APPA. In the situation of SPPDA, ASAS and APPA, data are transmitted without data compression techniques therefore it consumes larger storage. Compared to these approaches, proposed model obtained 80% of reduced storage.

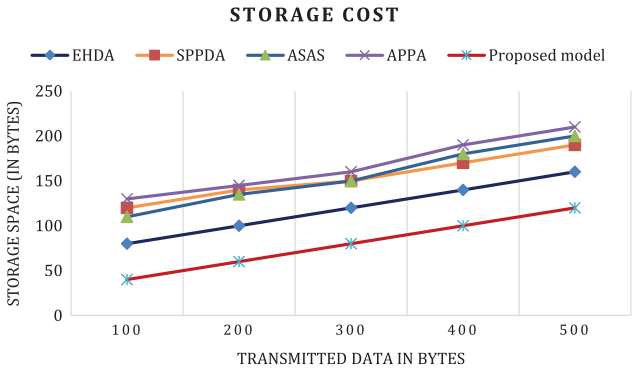

Figure 6: Storage cost comparison

4.4 Computation Cost

In phase C, the aggregator node aggregates the HP of the patients using comma delimiter and forwards to FN. These messages are extracted by FN and it checks the integrity using the MAC code. Fig. 7 shows that computation cost comparison of stated methods in terms of number of devices. For evaluation considered the number of nodes is 80. Computational cost of proposed model, EHDA, SPPDA, ASAS and APPA is

18.29 ms, 19.04 ms, 20.391 ms, 21.29 ms and 22.18 ms respectively. Proposed model provides 7%, 2%, 3% and 3.8% of better computational cost than, EHDA, SPPDA, ASAS and APPA. Hence, compare to other existing approaches, proposed model secures less computational cost.

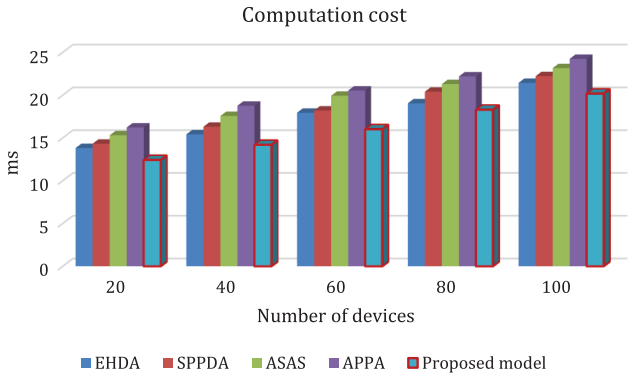

Figure 7: Computation cost comparison

Hence in all the kind of evaluations, proposed model secure best performance than other existing approaches. Compared to traditional aggregation approaches, proposed method is high in security aggregation, energy saving and compression. This method is also scalable and less storage utilization than other approaches which will prove that the proposed method is ensures the secure data transmission of health care data over the network.

5 Conclusion

IoMT ensures the better standard of human life with communication of smart devices, digital technologies, and applications. It is quite challenging task to transmit the sensitive health data of patients through WSN using data aggregation method. Therefore, this article proposed an effective and secure compression and data aggregation scheme using PC-MAC encryption algorithm with AN and fog server message extraction method. This model securely monitored the online patient data exchange by avoiding several security attacks and ensures the efficient exchange of patient data. To ensures the security, proposed model use PC-MAC code for encryption and decryption between SN to AN and AN to FN. From the simulation results using NS2.35 proposed model obtained low communication cost of 7300 bytes while transmitting data in bytes and 20.12 μJ in terms of energy than other existing approaches such as EHDA, SPPDA, ASAS and APPA. In energy consumption at SN and AN, proposed model secures minimum energy with various time slots. In terms of storage cost at various numbers of data transmitted, proposed model secures less storage space in bytes than existing approaches. In terms of computation cost at various number of devices, proposed model obtained less computational overhead than other algorithms. In future, more efficient data aggregation scheme is implemented with the extension of our proposed model for real time monitoring of healthcare data.

Acknowledgement: This research was supported by Korea Institute for Advancement of Technology(KIAT) grant funded by the Korea Government(MOTIE) (P0012724, The Competency Development Program for Industry Specialist) and the Soonchunhyang University Research Fund.

Funding Statement: This research was supported by a grant of the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI21C1831) and the Soonchunhyang University Research Fund.

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

References

[1] L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," *Computer 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," *Management*, vol. 21, no. 44, pp. 46, 2017.

[3] M. Aazam, S. Zeadally and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 46–52, 2018.

[4] M. M. Dhanvijay and S. C. Patil, "Internet of things: A survey of enabling technologies in healthcare and its applications," *Computer Networks*, vol. 153, no. 2, pp. 113–131, 2019.

[5] R. Mahmud, F. L. Koch and R. Buyya, "Cloud-fog interoperability in IoT-enabled healthcare solutions," in *Proc. ICDCN*, Varanasi, India, pp. 1–10, 2018.

[6] J. N. S. Rubí and P. R. L. Gondim, "Iomt platform for pervasive healthcare data aggregation, processing, and sharing based on onem2m and openehr," *Sensors*, vol. 19, no. 19, pp. 4283, 2019.

[7] A. Gatouillat, Y. Badr, B. Massot and E. Sejdić, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810–3822, 2018.

[8] M. Usak, M. Kubiatko, M. S. Shabbir, O. Viktorovna Dudnik, K. Jermsittiparsert *et al.,* "Health care service delivery based on the Internet of things: A systematic and comprehensive study," *International Journal of Communication Systems*, vol. 33, no. 2, pp. e4179, 2020.

[9] G. Gardašević, K. Katzis, D. Bajić and L. Berbakov, "Emerging wireless sensor networks and internet of things technologies—foundations of smart healthcare," *Sensors*, vol. 20, no. 13, pp. 3619, 2020.

[10] 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. 3625, 2020.

[11] R. A. Khan and A. S. K. Pathan, "The state-of-the-art wireless body area sensor networks: A survey," *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, pp. 1550147718768994, 2018.

[12] F. Y. Okay and S. Ozdemir, "A secure data aggregation protocol for fog computing based smart grids," in *Proc. CPE-POWERENG*, Doha, Qatar, IEEE, pp. 1–6, 2018.

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

[14] X. Jia, D. He, N. Kumar and K. K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[15] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "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.

[16] Y. Yuehong, Y. Zeng, X. Chen and Y. Fan, "The internet of things in healthcare: An overview," *Journal of Industrial Information Integration*, vol. 1, no. 2, pp. 3–13, 2016.

[17] P. Hu, S. Dhelim, H. Ning and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, no. 3, pp. 27–42, 2017.

[18] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito and O. Rana, "Fog computing for the internet of things: A survey," *ACM Transactions on Internet Technology (TOIT)*, vol. 19, no. 2, pp. 1–41, 2019.

[19] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," *Telecommunications Policy*, vol. 37, no. 4–5, pp. 372–386, 2013.

[20] N. Alhirabi, O. Rana and C. Perera, "Security and Privacy Requirements for the Internet of Things: A Survey," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–37, 2021.

[21] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow *et al.,* "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Communications Surveys &Tutorials*, vol. 20, no. 1, pp. 416–464, 2017.

[22] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop *et al.,* "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, vol. 17, no. 1, pp. e4049, 2020.

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

[24] 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," *Sustainable Cities and Society*, vol. 54, no. 2, pp. 101995, 2020.

[25] H. Wang, Z. Wang and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Generation Computer Systems*, vol. 78, no. 11, pp. 712–719, 2018.

[26] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li *et al.,* "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *Journal of Network and Computer Applications*, vol. 125, no. 2, pp. 82–92, 2019.

[27] 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.

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

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

[30] A. Ullah, G. Said, M. Sher and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 163–174, 2020.

[31] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[32] M. Shanmugam and A. Ramasamy, "Sensor-based turmeric finger growth characteristics monitoring using embedded system under soil," *International Journal of Distributed Sensor Networks*, vol. 10, no. 6, pp. 476176, 2014.

[33] S. Maheswaran, P. Kuppusamy, S. Ramesh, T. Sundararajan and P. Yupapin, "Refractive index sensor using dual core photonic crystal fiber-glucose detection applications," *Results in Physics*, vol. 11, pp. 577–578, 2018.

[34] 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," *Information Sciences*, vol. 284, no. 22, pp. 130–141, 2014.

[35] H. Zhu, L. Gao and H. Li, "Secure and privacy-preserving body sensor data collection and query scheme," *Sensors*, vol. 16, no. 2, pp. 179, 2016.

[36] X. Shen, L. Zhu, C. Xu, K. Sharif and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Information Sciences*, vol. 514, no. 3, pp. 118–130, 2020.

[37] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant *et al.,* "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, no. 7, pp. 659–676, 2018.

[38] M. Azeem, A. Ullah, H. Ashraf, N. Jhanjhi, M. Humayun *et al.,* "FoG-oriented secure and lightweight data aggregation in IoMT," *IEEE Access*, vol. 9, pp. 111072–111082, 2021.

[39] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun *et al.,* "Secure healthcare data aggregation and transmission in IoT—A survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[40] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT '99*, Prague, Czech Republic, Springer, pp. 223–238, 1999.

[41] C. Zhang, C. Li and J. Zhang, "A secure privacy-preserving data aggregation model in wearable wireless sensor networks," *Journal of Electrical and Computer Engineering*, vol. 2015, no. 5, pp. 1–9, 2015.

[42] M. Abdel Basset, D. El-Shahat, K. Deb and M. Abouhawwash, "Energy-aware whale optimization algorithm for real-time task scheduling in multiprocessor systems," *Applied Soft Computing*, vol. 93, pp. 106349, 2020.

[43] M. Abdel-Basset, R. Mohamed, M. Abouhawwash, K. Ripon Chakrabortty and J. Michael, "EA-MSCA: An effective energy-aware multi-objective modified sine-cosine algorithm for real-time task scheduling in multiprocessor systems: Methods and analysis," *Expert Systems with Applications*, vol. 173, pp. 114699, 2021.

[44] M. Abdel-Basset, R. Mohamed and M. Abouhawwash, "Balanced multi-objective optimization algorithm using improvement based reference points approach," *Swarm and Evolutionary Computation*, vol. 60, pp. 100791, 2021.

[45] H. Seada, M. Abouhawwash and K. Deb, "Multiphase balance of diversity and convergence in multiobjective optimization," *IEEE Transactions on Evolutionary Computation*, vol. 23, no. 3, pp. 503–513, 2019.

[46] M. Abouhawwash and A. M. Alessio, "Multi objective evolutionary algorithm for PET image reconstruction: Concept," *IEEE Transactions on Medical Imaging*, vol. 40, no. 8, pp. 2142–2151, 2021.

[47] M. Abdel-Basset, N. Moustafa, R. Mohamed, O. Elkomy and M. Abouhawwash, "Multi-objective task scheduling approach for fog computing," *IEEE Access*, vol. 9, no. 3, pp. 126988–127009, 2021.

[48] M. Abouhawwash, "Hybrid evolutionary multi-objective optimization algorithm for helping multi-criterion decision makers," *International Journal of Management Science and Engineering Management*, vol. 16, no. 2, pp. 94–106, 2021.

[49] S. T. Suganthi, A. Vinayagam, V. Veerasamy, A. Deepa, M. Abouhawwash *et al.,* "Detection and classification of multiple power quality disturbances in microgrid network using probabilistic based intelligent classifier," *Sustainable Energy Technologies and Assessments*, vol. 47, no. 4, pp. 101470, 2021.

[50] N. Mittal, H. Singh, V. Mittal, S. Mahajan, A. K. Pandit *et al.,* "Optimization of cognitive radio system using self-learning salp swarm algorithm," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3821–3835, 2022.