




# Secure Healthcare Data Aggregation Scheme for Internet of Things

Muhammad Azeem and Ata Ullah 

Department of Computer Science, National University of Modern Languages,  
Islamabad 44000, Pakistan  
muhammadazeem0493@gmail.com, aullah@numl.edu.pk

**Abstract.** Internet of things (IoT) involves massive number of smart devices that can communicate across different networks to exchange data. IoT enabled smart healthcare data is aggregated for transmitting to FoG server. Healthcare data is sensitive in nature, so there is a need to provide protection against various security attacks. This paper presents a secure healthcare based data aggregation (SHDA) scheme to transmit sensitive data from sensor nodes to collector nodes that further transmit to the FoG node. It includes a proposed model for data collection from sensing devices and aggregate at collector nodes. Next, we present the message receiving algorithm at collector node and message extraction algorithm at FoG node. SHDA is simulated using NS2.35 in Fedora Core 16 where TCL is used for node deployment and C language is used for message handling among devices. AWK script are used to get the results of simulations from trace files. Results prove the dominance of our scheme as compared to counterparts in terms of communication cost, computation cost and energy consumption.

**Keywords:** Privacy · Security · Healthcare · Data aggregation · FoG computing · IoT

## 1 Introduction

The evolution of healthcare Internet of things (IoT) introduce an interconnection between patient, medical professionals, medical sensors and trusted servers [1]. A healthcare IoT improve the quality and efficiency of patient medical treatment [2, 3]. Smart sensing devices and medical instruments and wearable medical devices are helpful for remotely monitoring healthcare data in smart healthcare IoT network [4]. Medical cyber physical system composed of a network of medical sensing devices and provides high quality of healthcare services [5]. In IoT enable smart healthcare based WSNs are helpful in monitoring patient health. Sensing devices are used for measuring patient health like temperature, blood pressure, glucose and heartbeat [6]. Patient sensitive data aggregated through smart wearable sensing devices and this aggregated after processing received to doctor or medical consultant to observe the present health condition of patient. Sensing devices are broadly appropriate in physical world scenarios [7, 8].

In IoT based healthcare system, FoG node basically a device with capability of temporarily data storage, data computation and network connectivity. FoG layer provide low latency and high response time in this way increasing the capability of healthcare systems [9]. In FoG based healthcare architecture sensing nodes aggregate patient data and transmit this collected data on FoG server and after some processing on locally store data. FoG server upload this locally store and processed data on cloud server [10]. FoG computing provides local data analysis on aggregated data from smart sensing devices. In smart healthcare architectures implementation of FoG node reduce computation overhead at cloud server [11]. Middleware between cloud and IoT devices known as FoG is a right choice when services require fast response, data filtration, pre-processing, security and privacy [12].

In smart healthcare technology provides mechanism to remotely monitor healthcare data from wearable sensors. In this way security and privacy are backbone of the smart healthcare so security threads and privacy requirements are the primary challenges in smart healthcare [13]. Technologies like smart phones and wearable devices turned healthcare into smart personal healthcare [14, 15]. In IoT based WSNs mobile phones gain a lot of attention worldwide. Mobile phones used sensor node and collector node but mobile phone as a sensor node is a challenging due to mobility of sensor nodes. On the other-hand mobile phone is a right choice to use as a collector node that helps to easily communicate with medical consultants and doctors [16]. IoT smart healthcare applications provide benefit for personal human healthcare. On the other-side security and privacy are still challenging issue in smart personal healthcare [17]. In healthcare scenario secure data aggregation and data transition to the trusted server are still challenging issue. In wireless body area network sensing devices are attached to the body of the patient and these devices aggregate secure data and transfer over the server and medical professional access this data in this scenario remotely secure data transmission and privacy of the patient and medical professional are the main challenges in remote healthcare [18].

The main problem is secure data aggregation from smart devices (SDs) to FoG node. In aggregation scenario, collection and transmission of data are challenging issues and security of data in healthcare also a challenging task because while aggregating and sharing data high risk of security threads. This paper introduces a FoG based secure healthcare based data aggregation scheme. In our work, peer to peer communication involves wearable SDs that exchange data to collector nodes (CNs). Next, the CNs share data to FoG server efficiently to reduce communication cost. Moreover, FoG node sends query request through CNs and the SDs that have responded to fulfill query scenario.

This paper presents a proposed scheme on privacy preserved and secure healthcare data aggregation FoG based scheme. Our proposed work is simulated using NS2.35 in Fedora Core 16. TCL and C languages are used for node deployment and message sharing. We formulated AWK script to get the results of simulations from trace files. Our main contributions in this work are as follow.

- (1) We have explored an extensive amount of literature to discuss different schemes for data aggregation. Schemes are categorized into secure aggregation schemes and secure healthcare based schemes.

- (2) Next, we present the secure healthcare based data aggregation scheme (SHDA). It formulates a system model where sensing devices and FoG nodes are shown.
- (3) Next, we propose Message Receiving Algorithm (MRA) for collector node and Message Extraction Algorithm (MEA) for FoG node.
- (4) Finally, simulation scenario is explored to extract results.

Rest of the paper is organized as follows; Sect. 2 explores the literature review for various secure healthcare data aggregation schemes. In Sect. 3, we present our proposed model for SHDA along with message receiving and extraction algorithms. Section 4 explores results and analysis whereas Sect. 5 concludes our work.

## 2 Literature Review

In this section, we discuss various privacy preserved secure aggregation schemes and also healthcare based secure aggregation scheme. In this way, we further divided this section into two sections first section contain secure aggregation schemes and second section contain healthcare base secure data aggregation schemes.

### 2.1 Secure Data Aggregation Schemes

In this section, we discussed data aggregation schemes. In discussion, we briefly describe the main key features of these schemes and their contributions in physical world. This portion includes only secure data aggregation schemes. We also discussed methods and techniques of secure data aggregation schemes.

Huang et al. [19] formulate a control and secure data access scheme. It depends upon ciphertext attribute based encryption and attribute based signature in IoT enabled FoG computing. In attribute based data encryption scenario, sensing nodes share ciphertext to FoG server. FoG server perform encryption and decryption data and further upload data to cloud server and in data receiving perspective a user can access data whose attribute satisfy the required policies. The system provides secure data access control and secure update ciphertext. Wang et al. [20] introduce a secure aggregation scheme (ASAS). This proposed architecture using pseudonyms and homomorphic encryption to preserved the privacy of aggregated data and protect the identity of sensing nodes. This scheme provides low computational overhead at cloud server and saves bandwidth between FoG and cloud servers. In contrast energy consumption and communication cost increased. End nodes anonymously share data to the FoG server and while preserving the integrity of received data from end nodes and share data to the cloud server.

Guan et al. [21] discussed a device oriented privacy preserved data aggregation scheme. This work provides pseudonym certificate autonomous update and privacy for aggregated data. In limited devices scenario, it provides high performance. In this formulated work, End nodes aggregate data from smart devices and share this data to the FoG node and it performs local processing on data and share this locally processed data to the cloud server. On Cloud server further processing and analysis are performed. Independent certificate services like trusted certification and local certification

authority both of them provide secure and privacy preserved data collection. Lu et al. [22] proposed a lightweight and privacy preserved data aggregation scheme. In this system to aggregate data at one device combine homomorphic encryption and Chinese Remainder Theorem. At network edges one-way hash chain technique is used to filter aggregated data from false data injection attacks. In this way network filter data locally at the edge devices and send it to the control center. Sensing devices are subdivided according to their functionality. proposed scheme efficient because of low computational and communication cost.

## 2.2 Healthcare Based Secure Data Aggregation Schemes

In this section, we discussed data aggregation schemes. In discussion, we briefly describe the main key features of these schemes and their contributions in physical world. This portion includes only secure healthcare based data aggregation schemes. We also discussed methods and techniques of schemes as follows.

Ullah et al. [23] introduces an efficient healthcare data aggregation scheme. It uses secure heterogeneous IoT based compression mechanism. Secure data transfer from sensing node to collector node and message receiving algorithm used to receive data at collector node. Compression performed on received data at collector node in this way reduce data size and low energy consumption for communication. This work use peer to peer communication between sensing nodes and node to node between collector nodes. Data received from sensing nodes is transmit to the FoG node and at FoG node message extraction algorithm use to collect data from collector nodes and after collecting data at FoG node in specific time stamp perform some local processing on aggregated data and then share this processed data over the cloud server. Hamza et al. [24] presents a lightweight authentication scheme for smart healthcare system. Proposed work focus on the security of healthcare system and using HMAC to authenticate the collected data during data transmission. In system model wearable sensor nodes attached with the patient body and this aggregated data send on edge node and edge node further share this data with the base station or FoG server. In this way for secure data aggregation proposed scheme provide authentication for sensitive healthcare data both at sensing devices and FoG server. This scheme only applicable for devices security of healthcare system. Mahmood et al. [25] introduces secure authentication and prescription safety scheme. It ensures security and privacy of both patient and medical consultants while remotely conversation. It also provides anonymity and untraceability of patient and doctor during session key generation and secure data transmission to the reliable server. Proposed work uses symmetric key to authenticate the participants and provide secure data transmission between patient and the medical consultant. Moosavi et al. [26] presents an efficient and secure authorization and authentication architecture for healthcare. Privacy and security plays a vital role while transmission of patient sensitive medical healthcare data. The aim of their work is the secure authentication and authorization of the remote patients and healthcare professionals. Proposed work used distributed smart healthcare gateway to authenticate and authorized the remote users in this way reduce the overhead of medical sensors so they are not performing these security protocols. Proposed architecture is more secure than the centralized delegated architecture because between smart healthcare gateway and

medical sensor nodes it uses secure key management scheme and it depend upon the DTLS handshake protocol. Proposed solution provide scalable and reliable security for end-to-end healthcare systems.

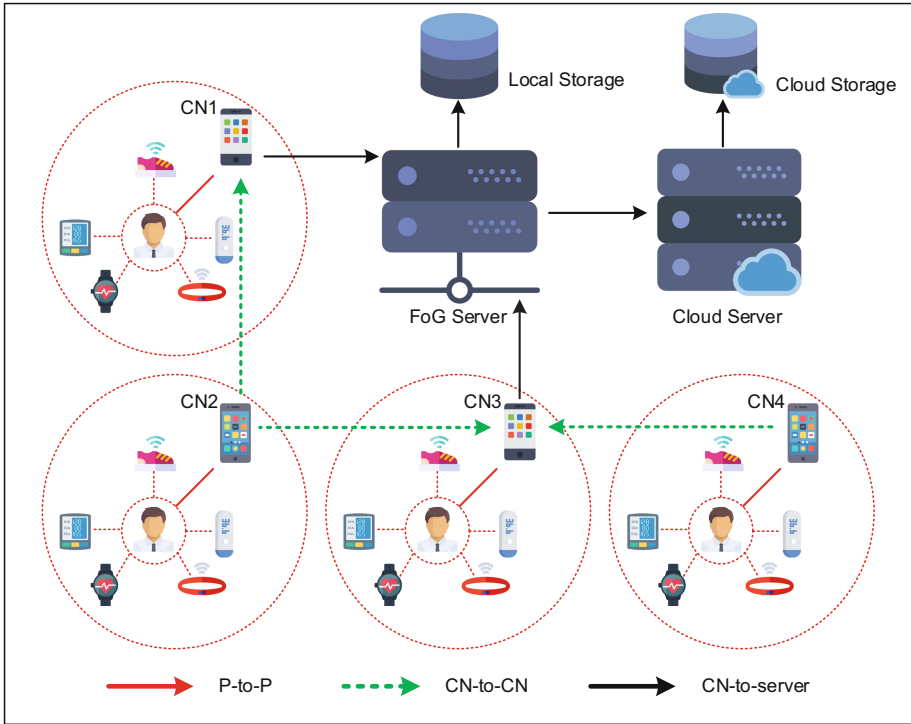
Haiping et al. [27] introduces healthcare system (HES) framework that collect data from the medical sensors of wireless body area network. This collected data transmit through the wireless sensor network and this medical data through gateway uploaded in the wireless personal area network. The main features of proposed work are easily deployed wireless sensor networks, direct communication between edge devices and medical devices and privacy preserving approach. HES framework involves the GSRM scheme for secure data transmission and key distribution and HEBM scheme expert system analyze medical data and formulate the results automatically and also provide privacy for medical data. Yang et al. [28] formulate a lightweight break glass access control (LiBAC) system this system provides to paths one for normal condition and other for emergency situation for accessing encrypted healthcare data. In normal condition attribute based access policy user use secret key access and decrypt the medical data. On the other-hand in emergency condition break glass access is a password based access and password set by a patient shared with the emergency contact persons (ECP) in this way these person decrypt secret key using password and timely decrypt the patient medical data. Proposed framework is lightweight so consume less space and low transmission overheads.

### 3 Proposed Solution

We present the system model and proposed secure data aggregation algorithm. We also present a smart healthcare based secure data aggregation scheme. In our case proposed work reduce storage cost and computation cost at cloud server comparing proposed schemes with those schemes discussed in literature review section.

#### 3.1 System Model

In our proposed system model, we present a communication architecture for smart sensing devices in smart healthcare scenarios and elaborate it in Fig. 2. Proposed healthcare model consist of different types of wearable smart sensing devices (SD). Like peer to peer communication SD aggregate medical data and transmit sensitive data to an assigned collector nodes (CN). Suppose in our work all SD may not transmitting data in cyclic way and may be transmit data on request of FoG server or selected threshold delay. It helps to avoid sensing hindrance in case of large no of sensing devices exchange sensitive healthcare data. In this model, medical SD sending sensitive data to CN and collector nodes sending received data to the FoG server. In Fig. 1, we only show four CNs to elaborate basic concept of CN to SD data aggregation and CN to CN data aggregation. In physical world scenario large number of CN are present and some CN nodes directly send collected data to the FoG server. CN1 and CN3 are directly send data to the FoG server. On the other-hand, if CN cannot send data directly to the FoG server so aggregated data is send to the FoG server through neighboring CN. For example, we assume CN2 can exchange data with CN4 and CN4 used as an



**Fig. 1.** System model for FoG-oriented smart data aggregation in IoT

intermediate node and transfer this data to the FoG server in this way CN4 also directly get data from the SD and also exchange data with the neighboring CNs. In peer to peer communication scenario, if intermediate CNs are far away from the FoG server and size of data carrying by intermediate nodes increased after sending from any individual node in this way communication cost highly increased. On the other-side data mostly not compressed it increases the over-head at FoG and Cloud server. We assume if devices transmit the data in cyclic way and large amount of devices transmitting healthcare sensitive data it will cause hindrance in sensing procedure. It's a challenging issue to formulate a green sensing mechanism to avoid sensing hindrance.

In our proposed model, Collector nodes received the aggregated data and moves towards sensor nodes. FoG part in data aggregation. In this scenario, records are easily maintaining on the basis of device ID in FoG server.

### 3.2 Secure Healthcare Based Data Aggregation (SHDA) Scheme

In our proposed section, we formulate solution for identified problem by presenting secure healthcare data aggregation scheme. Our proposed work further divided into three phases SD sensing data and transfer to CNs, message receiving at CN and extraction at base station. We elaborated our proposed scenario with two algorithms

first message receiving algorithm at CN and message extraction algorithm at FoG node. In this section Table 1, shows the list of notations.

**Table 1.** List of notations

Notations	Description
$ID_{SD_i}$	ID of sensing devices
$HP_V$	Healthcare parameter values
$TS_{SD_i}$	Sensing devices time stamp
$n$	Total number of SDs transmit data to CN
$C_i$	Ciphertext at SDs
$M_i$	Decrypted message sending from sensing devices to CN
$H(C_v)$	Hash of concatenated values
$A_m$	Aggregated message at CN
$M_{FS}$	Decrypted message from CN to FoG node
$List_{M_{SD_i}}$	List of messages from sensing devices
$E_{k_{SD_i-CN}}$	Symmetric key between CN and sensing devices
$E_{k_{CNi-FS}}$	Symmetric key between FoG node and CN

FoG server formulate data according to the required format and upload to the cloud server after aggregating data from multiple regions in certain threshold time. In Phase-1 sensing devices share sensing data to the CN. In this way, SDs encrypting data using preloaded keys and share these keys with FoG node and start sharing data to CNs while doing this only those SDs share data which satisfied the required conditions. ANs directly share data with FoG server only when it is one-hop away from FoG server. otherwise CNs share data with intermediary CN to transmit data over FoG server. An intermediate CN collect data and use delimiter to differentiate with its own data and aggregated data from other CN.

In our proposed SHDA scheme, sensor nodes collect healthcare parameter values ( $HP_V$ ). Cipher text  $C_i = E_{k_{SD_i-CN}}\{ID_{SD_i}, HP_V, TS_{SD_i}, H(ID_{SD_i}||HP_V||TS_{SD_i})\}$  is obtained by using symmetric key. It concatenates  $ID_{SD_i}||HP_V||TS_{SD_i}$  values and sensor nodes send data at CN. In phase-2, we introduce MRA at CN which shown in Algorithm 1. It received message from sensing nodes and also received from the other aggregated nodes. In Algorithm 1, CN receives the message from all sensor nodes. In message receiving algorithm decrypt the ciphertext ( $C_i$ ) to get  $ID_{SD_i}, HP_V, TS_{SD_i}$  as  $M_i$ . It also concatenate values. After that calculate the time stamp of data ( $TS_{CN} - TS_{SD_i}$ )  $< \Delta t$ . If condition true so message is fresh otherwise discard it. In case, condition is true calculate the hash of the received parameters  $H'(C_v)$  equals  $H(C_v)$ . In this way, if condition false so message discarded because of data integrity violation. On the other-hand, if condition true aggregated message concatenate with  $M_i$  to get aggregated message at collector node ( $A_m$ ).

---

 Algorithm No. 1 : Message Receiving Algorithm (MRA) at CN
 

---

```

Initialize  $A_m = \text{null}$ 
1. Decrypt  $C_i$  to get  $M_i =$ 
 $\{ ID_{SD_i}, HP_V, TS_{SD_i}, H(C_v) \}$  from SD
2. If  $(TS_{CN} - TS_{SD_i}) < \Delta t$  then
3.   If  $H'(C_v)$  equals  $H(C_v)$  then
4.      $A_m = A_m \parallel \text{":"} \parallel M_i$ 
5.   Else
6.     Message discarded because of integrity violation
7.   End if
8. Else
9.   Discard outdated message
10. End if

```

---

In phase-3, introduces proposed message extraction algorithm at FoG node shown in Algorithm 2. In this proposed algorithm,  $C_{CNq} = E_{k_{CNi-FS}} \{ ID_{CNq}, A_m, TS_{CNq}, H(ID_{CNq} \parallel A_m \parallel TS_{CNq}) \}$  Aggregated message received from the collector node at the FoG node. At FoG node while using (MEA) get  $M_{FS}$  by separating  $ID_{SD_i}, HP_V, TS_{SD_i}$  and also and also  $ID_{SD_i} \parallel HP_V \parallel TS_{SD_i}$  concatenate values. In next step of algorithm, we calculate the time stamp of data  $(TS_{FS} - TS_{CNq}) < \Delta t$ . If condition true so message is fresh otherwise discard it. In case, condition is true calculate the hash of the received parameters  $H'(C_b)$  equals  $H(C_b)$ . In this way, if condition false so message discarded because of data integrity violation. In next step, if condition true then loop count from 1 to n and q = 1 to n and  $List_{M_{SDi}}$  is a list of messages received from sensing nodes and split received data and using colon as a delimiter. In the end extract the health parameter values ( $HP_V$ ) from list of messages received from sensing devices ( $List_{M_{SDi}}$ ).

---

 Algorithm No. 2 : Message Extraction Algorithm (MEA) at FoG Node
 

---

```

Initialize  $A_m = \text{null}$ 
1. Decrypt  $C_i$  to get  $M_i =$ 
 $\{ ID_{SD_i}, HP_V, TS_{SD_i}, H(C_v) \}$  from SD
2. If  $(TS_{CN} - TS_{SD_i}) < \Delta t$  then
3.   If  $H'(C_v)$  equals  $H(C_v)$  then
4.      $A_m = A_m \parallel \text{":"} \parallel M_i$ 
5.   Else
6.     Message discarded because of integrity violation
7.   End if
8. Else
9.   Discard outdated message
10. End if

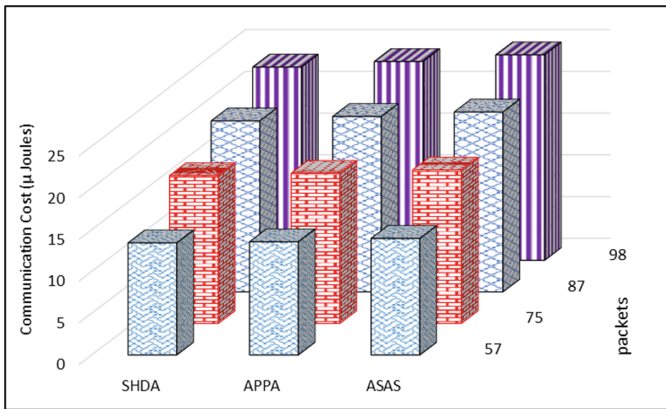
```

---



## 4 Results and Analysis

Our work validated through simulation by installing multiple sensors in a specific area and separately formulate each type of node by placing suitable class with functions for receiving, sending, encrypt and decrypt algorithms. We simulated our proposed scheme using NS2,35 on Fedora core and TCL files have configuration of nodes, deployment of nodes. Separate classes are created using C language for applying the sending and receiving functionality of SDs and CDs and also provide functions for applying encryption and decryption. Our proposed scheme used AWK script files to attain values of results from trace files. We compared our scheme with other schemes and this comparison shows the supremacy of our scheme.



**Fig. 2.** Communication cost

In Fig. 2, we calculate the communication overhead at low power devices like SDs. shown the supremacy of SHDA scheme while comparing with ASAS and APPA schemes. Results prove that our proposed scheme has low communication overhead as compared with other two schemes at low power devices. Using simulated values presents the communication cost with no of packets. In Fig. 3, we calculate the computation cost in terms of data aggregation at CNs. Our proposed SHDA scheme shown supremacy in terms of computational cost while comparing with APPA and ASAS. Results of simulation show that our proposed scheme has less computation cost as compared with other two schemes. Presents the computation cost with number of smart devices. In Fig. 4, we compare energy consumption with time at CNs. Proposed scheme SHDA compare with APPA and ASAS schemes. Simulation results show the supremacy of our proposed scheme and provide less energy consumption.

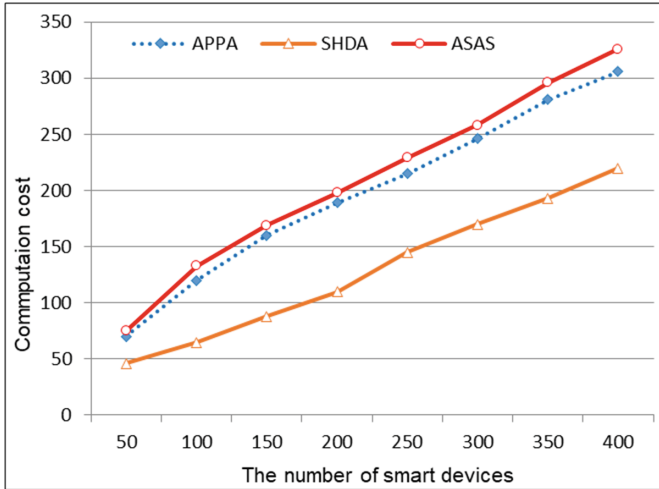


Fig. 3. Computation cost

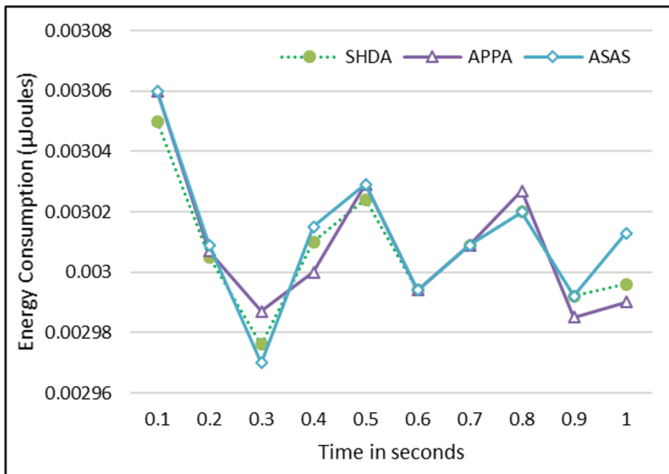


Fig. 4. Energy consumption

## 5 Conclusion

Our proposed SHDA scheme ensures the security of data while transmitting from SDs to CN that further transmits to FoG server. MRA and MEA algorithms receive and extract the data at collector and FoG nodes, respectively. In this case, the collector node can directly transmit to FoG node when one-hop away, otherwise, intermediate nodes are involved. During extraction, delimiter is used to differentiate between data sending devices like SDs and CN, respectively. Our proposed work validates through

simulation using NS 2.35 in Fedora Core 16. We use TCL for node deployment and for message handling we use C language. Results are extracted using AWK script from multiple trace files as per deployment scenarios. trace files using. Results prove the supremacy of proposed SHDA scheme in terms of less communication cost, less computation cost and less energy consumption.

## References

1. Rodrigues, J.J.P.C., et al.: Enabling technologies for the internet of health things. *IEEE Access* **6**, 13129–13141 (2018)
2. Scarpato, N., Pieroni, A., Di Nunzio, L., Fallucchi, F.: E-health-IoT universe: a review. *Int. J. Adv. Sci. Eng. Inf. Technol.* **7**(6), 2328 (2017)
3. Yin, Y., Zeng, Y., Chen, X., Fan, Y.: The Internet of Things in healthcare: an overview. *J. Ind. Inf. Integr.* **1**, 3–13 (2016)
4. Qi, J., Yang, P., Min, G., Amft, O., Dong, F., Xu, L.: Advanced Internet of Things for personalised healthcare systems: a survey. *Pervasive Mob. Comput.* **41**(600929), 132–149 (2017)
5. Dey, N., Ashour, A.S., Shi, F., Fong, S.J., Tavares, J.M.R.S.: Medical cyber-physical systems: a survey. *J. Med. Syst.* **42**(4), 1–10 (2018)
6. Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S.C., Zhang, Y.T.: Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Trans. Biomed. Eng.* **65**(12), 2751–2759 (2018)
7. Kulkarni, A., Sathe, S.: Healthcare applications of the Internet of Things: a review. *Int. J. Comput. Sci. Inf. Technol.* **5**(5), 6229–6232 (2014)
8. Zhu, T., Dhelim, S., Zhou, Z., Yang, S., Ning, H.: An architecture for aggregating information from distributed data nodes for industrial internet of things. *Comput. Electr. Eng.* **58**(August), 337–349 (2017)
9. Chang, V., Firouzi, F., Constant, N., Mankodiya, K., Badaroglu, M., Farahani, B.: Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. *Futur. Gener. Comput. Syst.* **78**, 659–676 (2017)
10. Hu, P., Dhelim, S., Ning, H., Qiu, T.: Survey on fog computing: architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **98**, 27–42 (2017)
11. Mahmud, R., Koch, F.L., Buyya, R.: Cloud-fog interoperability in IoT-enabled healthcare solutions, pp. 1–10, December 2017 (2018)
12. Aazam, M., Zeadally, S., Harras, K.A.: Fog computing architecture, evaluation, and future research directions. *IEEE Commun. Mag.* **56**(5), 46–52 (2018)
13. Wu, W., Pirbhulal, S., Li, G.: Adaptive computing-based biometric security for intelligent medical applications. *Neural Comput. Appl.* 1–16 (2018). <https://doi.org/10.1007/s00521-018-3855-9>
14. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., Shamshirband, S.: Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Informatics J.* **18**(2), 113–122 (2017)
15. Liu, H., Yao, X., Yang, T., Ning, H.: Cooperative privacy preservation for wearable devices in hybrid computing based smart health. *IEEE IoT J.* **4662**(1), 1–11 (2018)
16. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The Internet of Things for health care: a comprehensive survey. *IEEE Access* **3**, 678–708 (2015)
17. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. *IEEE IoT J.* **4**(5), 1250–1258 (2017)

18. Lin, H., Yan, Z., Chen, Y., Zhang, L.: A survey on network security-related data collection technologies. *IEEE Access* **6**, 18345–18365 (2018)
19. Huang, Q., Yang, Y., Wang, L.: Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. *IEE Access* **5**, 1–9 (2017)
20. Wang, H., Wang, Z., Domingo-Ferrer, J.: Anonymous and secure aggregation scheme in fog-based public cloud computing. *Futur. Gener. Comput. Syst.* **78**, 712–719 (2018)
21. Guan, Z., et al.: “APPA: an anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *J. Netw. Comput. Appl.* **125**(June 2018), 82–92 (2019)
22. Lu, R., Heung, K., Lashkari, A.H., Ghorban, A.A.: A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **5**, 3302–3312 (2017)
23. Ullah, A., Said, G., Sher, M., Ning, H.: Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN (2019)
24. Khemissa, H., Tandjaoui, D.: A lightweight authentication scheme for e-health applications in the context of Internet of Things. In: *Proceedings of NGMAST 2015 9th International Conference on Next Generation Mobile Applications Services and Technology*, pp. 90–95 (2016)
25. Mahmood, Z., Ning, H., Ullah, A., Yao, X.: Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT. *Appl. Sci.* **7**(10), 1069 (2017)
26. Moosavi, S.R., et al.: SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **52**(1), 452–459 (2015)
27. Huang, H., Gong, T., Ye, N., Wang, R., Dou, Y.: Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Trans. Ind. Inf.* **13** (3), 1227–1237 (2017)
28. Yang, Y., Liu, X., Deng, R.H.: Lightweight break-glass access control system for healthcare internet-of-things. *IEEE Trans. Ind. Inf.* **14**(8), 3610–3617 (2018)