A Novel Fog and Cloud based Holistic Secure Framework for Smart Healthcare

Suparna Biswas
Maulana Abul Kalam Azad University of Technology, WB.
Department of Computer Science & Engg.

ABSTRACT

Smart healthcare is indispensable in human life to provide comfortable living to people providing easy, affordable, efficient healthcare monitoring and support. Smart healthcare is realizable due to advancement and success of several green and smart enabling technologies such as Internet-of-things, RFID sensors, cloud and fog computing, big data etc. Health data is sensible information that needs privacy. Moreover, such sensible information in smart healthcare system travels through open wireless link which is vulnerable to security attacks and threats. Data is security attack prone even when stored in sensors, fog or cloud nodes. Success of smart healthcare depends on correctness of health data to be available at care giver's end in real-time for advice generation, monitoring and provide appropriate support required. To ensure data security and privacy in healthcare several works have been proposed but most of the works ensures security in a specific layer i.e. sensing layer, communication layer and processing layer. But data secure in one layer may get affected by security breach in other layer. Proposed framework ensures a holistic security of health data by applying trust at resource constrained sensors layer and combination of private and public key cryptography at fog layer and cloud layer to ensure data confidentiality, authentication and non-repudiation.

General Terms

Security, Trust, Fog and Cloud Coputing et. al.

Keywords

Internet-of-things, framework, cryptography, privacy, attack model, smart healthcare etc.

1. INTRODUCTION

Due to advancement in communication and semiconductor technology, internet-of-things, cloud and fog computing, big data etc. are successful and hence smart applications are not a concept, but reality. Population in most of the cities are increasing globally [1] but resources e.g. infrastructure, healthcare facility, energy or power source etc. are not increasing proportionately. Hence smart management of available resources needs to be done to ensure availability of resources as per requirement. Technologies make smart management feasible. Smart applications generally have a three layer architecture [2] where data acquisition is done at sensing layer using sensors, then data are transmitted to upper layer through heterogeneous communication links both wired or wireless in communication layer, upper layer is the processing layer usually realized using cloud server that can disseminate resources required to store, process and retrieve information from big sensor data. Different smart applications are smart transportation, smart healthcare, smart energy management etc. In all applications original data should reach to processing layer in real time to generate control or feedback information for manipulation required in the system to achieve desired performance in proper time. But in some applications with this timeliness and correctness of data, another important factor is data sensitivity such as patient health data. Patient health data needs to be kept private to prevent data access by illegitimate user or thing. So, data privacy and security along with timeliness are the key factors for successfully implementing smart applications such as healthcare. Now, in healthcare health data sensed by the sensors get transmitted to the processing layer either at fog device or cloud via heterogeneous communication links. Hence data is vulnerable to security attacks and threats such as information leakage, data modification or alteration, routing attack to mislead about intended destination etc. Any such successful attack will lead to either increased latency dissatisfying the low latency requirement of healthcare, wrong advice generation based on modified data causing failure to smart healthcare support, loss of confidentiality falsifying need of privacy in case of eavesdropping or information leakage etc. Several works have been proposed to ensure data security but almost of them are aimed to provide data security at a specific layer [3]. A holistic secure smart healthcare framework is essential to ensure end-to-end data security. To reduce communication delay of data from sensor to cloud, some elementary processing are offloaded to fog devices intermediate between sensors and cloud. Fog device are distributed hence failure can be avoided as in case of failure of one fog node, another can be exploited, hence reliability also increases. But as number of participating objects are getting increase in handling sensitive data requiring privacy and security, off-the-shelf encryption and decryption techniques to be selected and applied intelligently to satisfy resource constraints of components at each layer and links in between of layers.

Rest of the work is organized as follows: Section 2 describes literature survey, section 3 depicts existing cloud based architecture proposed fog and cloud based architecture is presented in section 4 section 5 illustrates attack model followed by algorithm and flowchart in section 6 and respectively Section 8 illustrates analytical comparison between end-to-end delay in fog and cloud finally whole work concludes at section 9.

2. LITERATURE SURVEY

In [3], authors propose a security technique to ensure security of data between sensors to fog nodes. Sensors encrypt data before sending to fog nodes using light weight cryptography techniques such as Elliptic Curve Cryptography technique. At fog nodes, decryption will take place. The security requirement considered here is data confidentiality. The proposed security scheme is suitable for what type of applications is not specified. But it is very much necessary as every application has a unique performance requirement such as end-to-end delay or latency, throughput etc. Moreover, here, how fog to cloud communication would take place securely is not considered. But as we know, sensors generate big data, it is not feasible to store, process and retrieve information of big data at resource constrained fog nodes in place of cloud. So proposed security scheme does not ensure holistic security of data required for smart applications. In [4], authors presents Fog computing paradigm as a computing platform alternative to cloud to ensure data processing closer to the origin of data to improve various QoS parameters such as latency, network traffic, scalability etc. Smart city application targeted here is smart traffic management. Several applications such as healthcare, augmented reality, smart traffic management etc. have very low latency requirement and inclusion of fog computing in smart application architecture can ensure that. Experimental result shows that latency using fog nodes is less than that using cloud. No exclusive security technique has not described in this work. In [5], This paper highlights in detail security breaches, counter measures and security requirements in fog computing as this area is not widely explored till date. This work is a guidance to the designers, developers and maintenance people of fog based systems. Several potential security issues in fog have been identified and reported such as wireless security issue, data security issue, virtualization issue, malware protection issue, communication security issue etc. Proper threat or attack model for fog computing is still a topic of exploration. In [6] authors present a security model to demonstrate how securely health data can be stored in cloud using fog support. Pair-wise-cryptography has been used between fog nodes and cloud. This implementation ensures authentication and data confidentiality of sensitive patient health data..

2.1 Our Contribution

Proposed work tries to contribute in following salient points:

1. A holistic secure fog supported and cloud based framework for healthcare application.
2. Trust and cryptography are combined.
3. Consideration of screening layer to offload computation partially from processing layer.
4. Both normal and abnormal health data are handled for timely response.

3. CLOUD BASED 3 - LAYER ARCHITECTURE FOR HEALTHCARE

Smart healthcare application with cloud support has three-layer architecture as shown in figure 1. Three layers are: sensing layer, communication layer and processing layer. Sensing layer comprises of sensors that sense data and send to PDA through short range communication such as wifi, Bluetooth, zigbee, wimax etc. Communication layer is comprised of heterogenous communication wireless links and internet through which data is transmitted to processing layer. Data reaches to processing layer i.e. cloud from PDA through access point and internet connection. Data gets processed at cloud for information extraction, saved for future offline usage or online access by legitimate users. In cloud based architecture sensor data is directly sent to cloud, central processing point without being processed at any intermediate point. Here the capacity and resource pool of cloud environment is exploited to meet the customized resource requirement to save, process and access big health data. But communication cost increases as data gets processed at further point from its point of origin, one of contributor to this communication cost may be network congestion. Moreover, reliability may be poor due to failure probability of central processing facility.

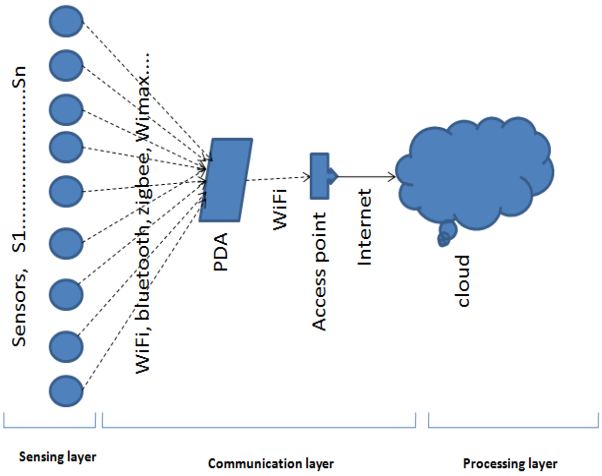


Fig 1. Cloud based three-layer smart healthcare architecture

4. PROPOSED FOG ASSISTED CLOUD BASED 4-LAYER ARCHITECTURE OF SART HEALTHCARE

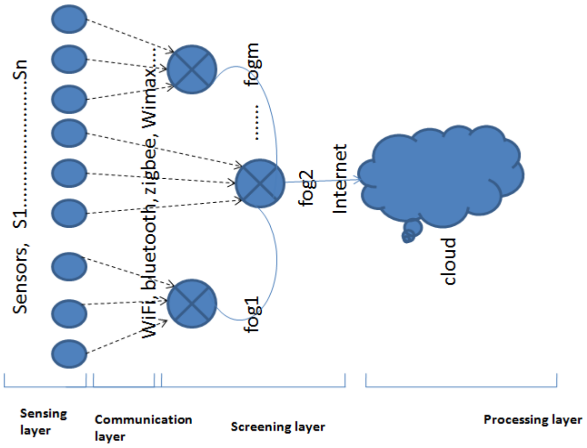


Fig 2. Fog supported cloud based four-layer smart healthcare architecture

Proposed fog supported cloud based smart healthcare architecture is shown in figure 2. Here sensor data at sensing layer are forwarded through communication layer to a number of distributed fog nodes. Here fog nodes are entrusted with performing some pre-processing on sensor data before sending to cloud. This pre-processing of data may be completely application dependant. In healthcare, maximum permissible end-to-end delay or latency of health data is 250 ms [8]. Sensors related to healthcare may be body sensors, environmental sensors or ambient sensors. These sensors generate big data and are geographically distributed. Now as per guidelines of Cisco [9], fog computing can be considered if sensors are large in number, placed geographically distributed way and generating big data, application requires response in less than a second. Smart healthcare scenario described below fits in and hence needs fog support.

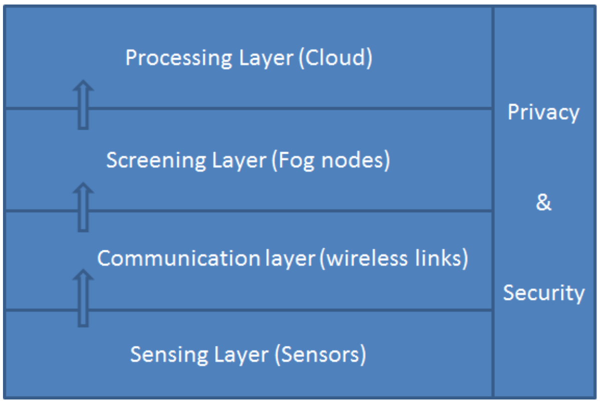

Processing Layer (Cloud)
Screening Layer (Fog nodes)
Communication layer (wireless links)
Sensing Layer (Sensors)
Privacy
&
Security

Fig. 3: Proposed secure architecture for end-to-end secure health data transmission

Above figure 3 considers end-to-end security and privacy need in proposed architecture for healthcare system. First layer is sensing layer comprising of heterogenous sensors placed n distributed manner in human body or in ambience or environment. Data sensing rate, data size, data value or range are different and the sensors as well. All sensed data are transmitted to layer 3 .e. screening layer through layer 2 .e. communication layer. Now, communication layer is comprised of heterogenous links having varying bandwidth, capacity, link quality etc. e.g. WiFi, Bluetooth, Zigbee, Wimax, HiperLAN etc. Senstive health Data are vulnerable to security attacks and threats while getting transmitted through these links which are insecure. Now one of the security measure that can be taken are off-the-shelf encryption techniques to encrypt the data at sensor nodes before transmission. Now encryption of data increases computation overhead for key generation, encryption operation at sensor end. Sensors are resource constraint devices having limited storage and processing capacity. Hence low overhead alternative security measure has to be taken. In [10], a trust evaluation technique of sensor nodes based on data freshness have been proposed. Applying this technique, data at layer 3 can be ensured only from trusted sensors. This trust based method will add negligible overhead in terms of a number of message passing and this is feasible at sensors level. Once data from trusted sensors only reached to layer 3 i.e. fog layer which is termed as screening layer here because this layer is entrusted for screening health data based on some predefined threshold value as per standard medical database [11] to find the data to be normal or abnormal. In case of normal data, data will be transmitted to layer 4 or processing layer i.e. cloud layer in encrypted format as from layer 3 to layer 4 data will be exposed to the vast security attacks and threats of wireless internet. If data is in abnormal range, then data will reach directly to doctor's local server or PDA for immediate access. In this case also, data will be transmitted in encrypted format through internet connection. Now Fog devices have storage, computing and communication capability more than sensors but less than cloud. Hence responsibility of storage, processing and information retrieval of big health data are not imposed on fog nodes. Rather only screening responsibility i.e. threshold based checking is done at fog nodes and hence this layer is termed as screening layer. Off-the-shelf private key encryption technique DES is applied to encrypt health data at fog nodes before sending to cloud. Now in cloud encrypted data has to be decrypted using the same secret key. But secure sharing of secret key has to be ensured. Using public key cryptography such as RSA this can be implemented. Secret key will be encrypted using private key of fog node and in cloud encrypted key will be decrypted using corresponding public key. Similarly in case of abnormal data, encrypted secret key will be decrypted at doctor's PDA or server using public key of fog node. Once secret key is available, encrypted health data can be successfully decrypted at cloud or doctor's server. Thus end-to-end secure health data transmission can be implemented combining trust, private and public key encryption and decryption techniques.

5. ATTACK MODEL

Sensors, fog and cloud based 4-layered smart healthcare architecture is comprised of heterogenous nodes and links having varying characteristics, limitations, challenges, resources and proneness to security attacks and threats. The attack model for such system should specify attacks at each layer. Sensors may come under the control of advisory both physical and logical way. Sensors are prone to physical damage or replacement by other illegitimate nodes, impersonation attack etc. Some malicious nodes may increase power while transmitting some fake messages intended for unnecessary overhearing hence energy drainage of legitimate nodes. Thus sensing of vital health signals may unknowingly stopped due to lack of sufficient energy in the node and this may cause havoc to patient's life. Rogue fog node is a threat in fog computing [12]. A rogue fog node is a node that pretends to be a legitimate fog node and communicate with legitimate fog nodes to connect to it. An insider attack may take place in which the administrator who is responsible to manage fog nodes, but intentionally creates an instance of rogue fog node rather than a legitimate one. Moreover, man-in-middle attack is possible in fog computing where the gateway may come under control of a fake node by getting compromised or replaced by a fake node. Once successful, the adversary may access illegally incoming and outgoing data stream from edge devices and cloud, can modify or delete or re-route user data falsifying destination node etc. Hence, presence of illegitimate fog node is a big threat to user data privacy and security. Internet connection between fog and cloud is exposed to Denial of service attack, man-in-the-middle attack. Cloud computing devices and system may suffer from authentication and denial-of-service attacks.

6. FLOWCHART

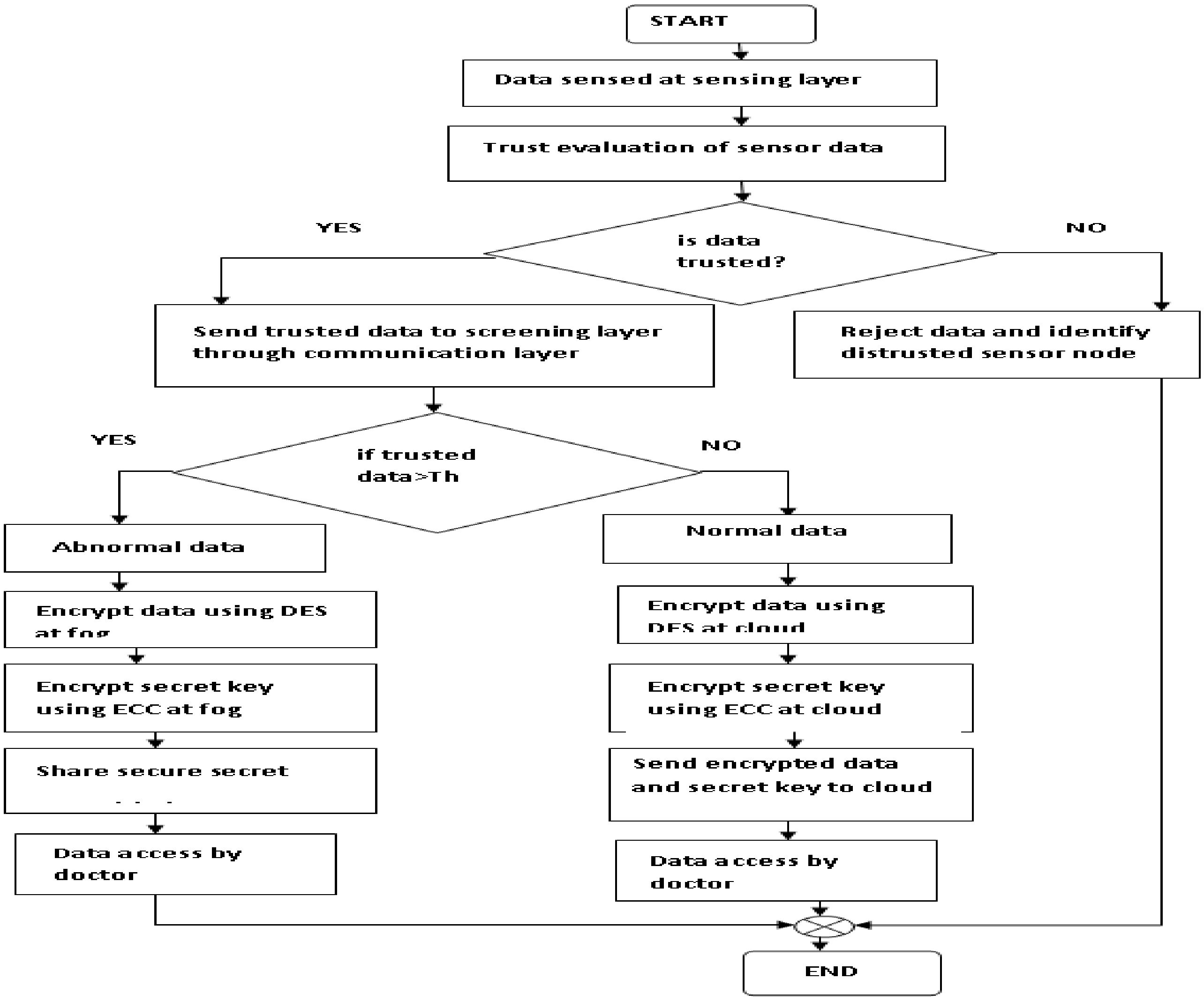
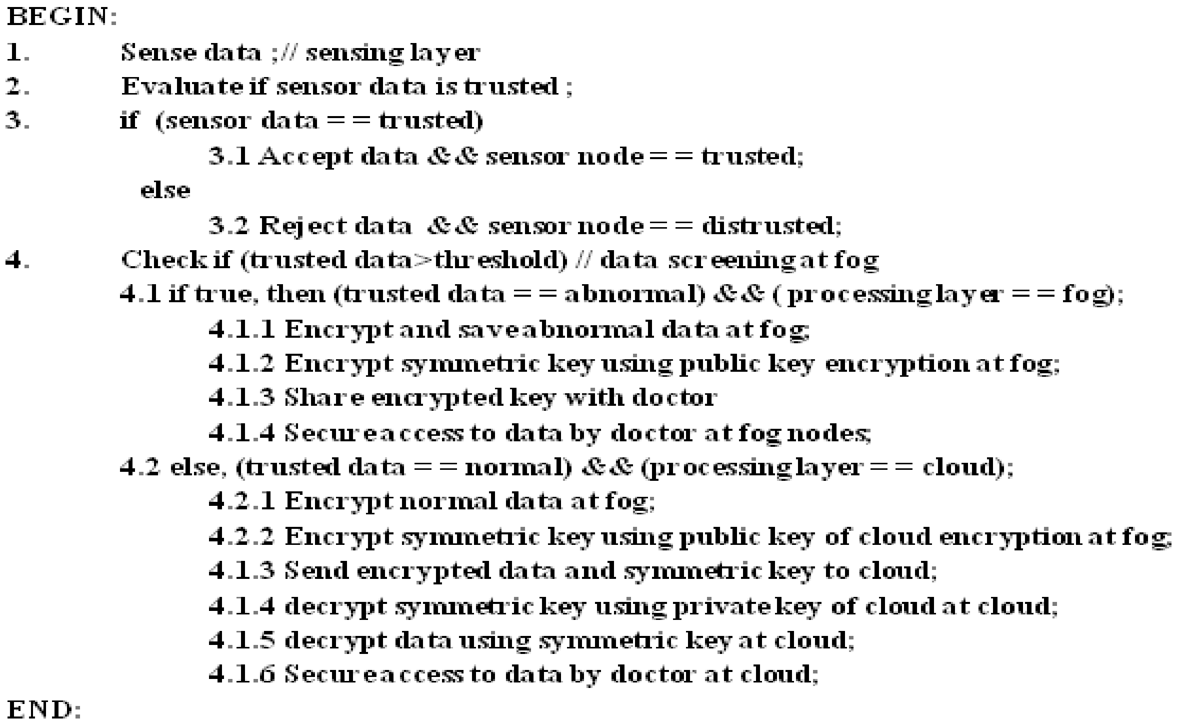

START
Data sensed at sensing layer
Trust evaluation of sensor data
YES
is data trusted?
NO
Send trusted data to screening layer through communication layer
Reject data and identify distrusted sensor node
YES
if trusted data>Th
NO
Abnormal data
Normal data
Encrypt data using DES at fog
Encrypt data using DES at cloud
Encrypt secret key using ECC at fog
Encrypt secret key using ECC at cloud
Share secure secret
Send encrypted data and secret key to cloud
Data access by doctor
Data access by doctor
END

Fig.4 Flowchart depicting end-to-end secure data flow in healthcare

7. ALGORITHM



```
BEGIN:
1.      Sense data ;// sensing layer
2.      Evaluate if sensor data is trusted ;
3.      if (sensor data = = trusted)
            3.1 Accept data && sensor node = = trusted;
    else
            3.2 Reject data && sensor node = = distrusted;
4.      Check if (trusted data>threshold) // data screening at fog
        4.1 if true, then (trusted data = = abnormal) && ( processing layer = = fog);
            4.1.1 Encrypt and save abnormal data at fog;
            4.1.2 Encrypt symmetric key using public key encryption at fog;
            4.1.3 Share encrypted key with doctor
            4.1.4 Secure access to data by doctor at fog nodes;
        4.2 else, (trusted data = = normal) && (processing layer = = cloud);
            4.2.1 Encrypt normal data at fog;
            4.2.2 Encrypt symmetric key using public key of cloud encryption at fog;
            4.1.3 Send encrypted data and symmetric key to cloud;
            4.1.4 decrypt symmetric key using private key of cloud at cloud;
            4.1.5 decrypt data using symmetric key at cloud;
            4.1.6 Secure access to data by doctor at cloud;
END:
```

8. ANALYTICAL COMPARISON BETWEEN END-TO-END DELAY IN FOG AND CLOUD

$D_{Si} = Sensor_i(D)$ // i=1……..n

$TR_{D_{Si}} = DF_{trust}(D_{Si})$ // at sensing layer

$E_{Shared\_key_j}\left(T_{D_{Si}}\right)$ // j=1……..m, at screening layer, m<<n

$E_{pub\_cloud}\left(Shared\_key_j\right)$ // at screening layer

$Shared\_key_j = D_{pri\_cloud}\left(E_{pub\_cloud}\left(Share\_key_j\right)\right)$
// at processing layer

$TR_{D_{Si}} = D_{Shared\_key_j}\left(E_{Shared\_key_j}\left(T_{D_{Si}}\right)\right)$

$T_1 = Time_{\_to\_sense}$

$T_2 = Time_{\_to\_compute\_trust}$

$T_3 = Time_{\_to\_communicate\_to\_fog}$

$T_4 = Time_{\_to\_screen\_at\_fog}$

$T_5 = Time_{\_to\_encrypt\_trusted\_data\_at\_fog}$

$T_6 = Time_{\_to\_encrypt\_secret\_key\_at\_fog}$

$T_7 = Time_{\_to\_transmit\_encrypted\_trusted\_normal\_data\_to\_cloud}$

$T_8 = Time_{\_to\_transmt\_encrypted\_secret\_key\_to\_cloud}$

$T_9 = Time_{\_to\_transmit\_encrypted\_trusted\_data\_to\_cloud}$

$T_{10} = Time_{\_to\_access\_data\_at\_cloud}$

$T_{11} = Time_{\_to\_access\_data\_at\_fog}$

i) When processing layer is cloud:
Time to send normal data securely from sensors to cloud is given in eqn. 1….

$$T_{S\_to\_C} = T_1 + T_2 + T_3 + T_4 + T_5 + T_6 + T_7 + T_8 + T_9 + T_{10} \quad \ldots\ldots(1)$$

ii) When processing layer is fog:
Time to send normal data securely from sensors to fog is given in eqn. 2….

$$T_{S\_to\_f} = T_1 + T_2 + T_3 + T_4 + T_5 + T_6 + T_{11} \quad \ldots\ldots(2)$$

Hence, $T_{S\_to\_f} < T_{S\_to\_C}$

Though this analytical time component comparison between end-to-end delay using fog and cloud considers security components also, in [5] authors experimentally show the end-to-end delay comparison between fog and cloud without security as given in fig.5. Here the time to process the tuple at fog node is much less than that in cloud. And obviously the increased delay in cloud is due to communication delay and network congestion from fog to cloud through internet.

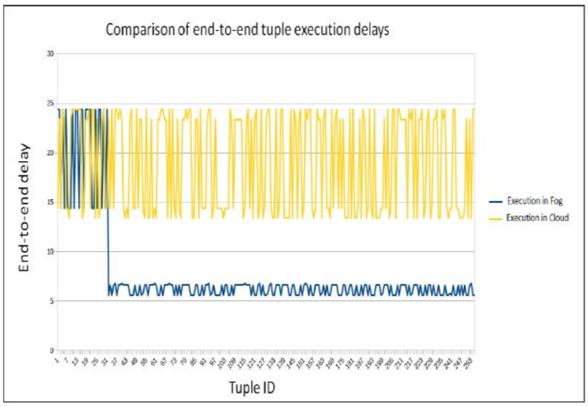


Fig.5 End-to-end tuple execution delay in fog and cloud [5]

9. CONCLUSION

Smart applications based on smart technologies are in demand. One of such application is healthcare which is needed to give people a quality of life. Sensors, fog and cloud supported four layer architecture has been proposed to handle both normal and abnormal health data satisfying low latency requirement for timely response. Health condition when health data are abnormal is considered to be emergency and for quicker response, health data are processed at fog layer to ensure processing closer to the sensors, point of origin of data. Normal health data are processed in cloud. Health data generated at sensors, screened at fog, exposed to internet to send to cloud. At each point data is vulnerable to various security attacks and threats from which needs to be protected to maintain privacy and security of sensitive health data. Attack model has been described to specify attacks considered at each point. In proposed secure architecture, to cope up with resource limitation at sensor layer, light weight trust technique is applied to find trusted data and trusted sensor node. To ensure confidentiality symmetric key cryptography such as DES may be applied. To ensure security of symmetric key upon which success of cryptography depends and also to prevent access to symmetric key by illegitimate node, key is encrypted using light weight cryptography such as ECC so that only intended user can decrypt key even if there may be eavesdropping or information leakage. Analytical comparison between end-to-end delay of fog and cloud based healthcare solutions is given for better understanding and insight.

10. REFERENCES

[1] Digital economy and smart metropolises : a joint future...https://www.slideserve.com/.../digital-economy-and-smart-metropolises-a-joint-future..

[2] J-Soo Jeong, O. Han, Y. You, “ A Design Characteristics of Smart Healthcare System as the IoT Application”, Indian Journal of Science and Technology, Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102547, October 2016, ISSN (Print) : 0974-6846.

[3] AA Diro et.al., “Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication”, IEEE Access, vol.6, pages 26820 – 26830, 2018.

[4] S.Yi, Z.hao, Z.Kin, Q.li, “Fog Computing: Platform and applications”, Third IEEEWorkshop on Hot Topics inWeb Systemsand Technologies, pages 73-78, 2015.

[5] A.V. Dastjerdi, H. Gupta, R.N. Calheiros, S.K. Ghosh, and R. Buyya. 2016. Chapter 4 - Fog Computing: principles, architectures, and applications. In Internet of Things: Principles and Paradigms, Rajkumar Buyya and Amir Vahid Dastjerdi (Eds.). Morgan Kaufmann, 61 – 75.

[6] S. Khan, S. Parkinson, Y. Qin,Fog, “Computing Security: a Review of Current Applications and Security Solutions”, Journal of Cloud Computing, Advances, Systems and Applications.

[7] 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," in IEEE Access, vol. 5, pp. 22313-22328, 2017

[8] Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., Jamalipour, A.: Wireless Body Area Networks: A Survey. IEEE Commun. Survey. Tutor. pp. 1–29 (2013).

[9] Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, white paper, cisco, 2015.

[10] S.Roy, S.Biswas, “A Novel Trust Evaluation Model based on Data Freshness in WBAN”, in proceedings of eHacon 2018 (springer).

[11] A.M. Rahmani et.al., “Exploiting Smart e-Health Gateways at the edge of Healthcare Internet-of-Things: A Fog Computing Approach”, PII: S0167-739X(17)30212-1, DOI: http://dx.doi.org/10.1016/j.future.2017.02.014, Future Generation Computer Systems.

[12] S. Yi, Z. Qin, and Q. Li, “Security and Privacy Issues of Fog Computing: A Survey”, International Conference on Wireless Algorithms, Systems and Applications, pages 685-695, WASA 2015, Springer.