Integrated Secure Health Domain System using IoT

Nagarjuna Valeti, V.Ceronmani Sharmila

Abstract: Fog computing plays major role in health care system. Fog performs well compare with cloud computing. Health care system needs more enhancements because there sensitivity. It is very important to secure the data in the health care system. Though there are many systems for health care security still there are issues to secure the data transfer from client to the fog by cloud computing. In the previous papers, we have discussed QOS parameters and various preventions to transmission of data from sensors to fog. IOT is most widely used in health systems to increase the performance which adopted with fog computing. In this paper, the integrated secure health domain system (ISHDS) used to overcome the system failures and providing the security for the health care data in various situations.

Keywords: Fog computing, cloud, IOT. Edge Computing (EC),

I. INTRODUCTION

In rural areas, multiple health care centres are placed with basic amenities in for providing first-aid to the patients. No automated systems are present in the rural clinics, everything is based on manual work such as using paper for saving patient details and sample reports. It is very difficult to use many systems in many multiple places for the analysis of patient health records. It is very costly to develop and transfer the data with automated systems by using machines. Many possibilities are available to increase the effectiveness and efficiency based on the delivery process of traditional health care and some of the existing technologies such as mobile & wireless with low cost and quality of service (QoS). One more issue identified in this system is using mobile in rural areas becomes the lack of service availability because of the slow response.

Enhancement and utilization of Wireless Body Area Networks (WBANs) are viewed as key research regions for improving medicinal services quality [1]. Unavoidable medicinal services observing gives rich relevant data to deal with the odd states of incessantly sick patients. Steady checking and an early therapeutic reaction not just build the existence nature of older and incessantly sick individuals yet additionally help families and guardians by giving fantastic social insurance to their young infants and incapacitated kids [1-2]. The significance of the WBANs can't be promising; the same number of utilization and models are now in advancement. For instance, some WBANs are devoted to the nonstop perception of intellectual illnesses, for example, Alzheimer's, epilepsy, and Parkinson's ailment. Another huge headway in WBANs is the arrangement of modest sensors embedded in the human body or incorporated into the texture.

Fog computing is used to reduce the size of the data which is sent to the cloud and subsequently improve effectiveness. The quick advancement of various smart devices is relevant to create smart items which are connected with the network devices for sensing the data which is integrated with IoT.

In this paper, ISHDS and sensors are utilized to transfer the data to the cloud by using FC. The figure: 1 shows the process of the ISHDS.

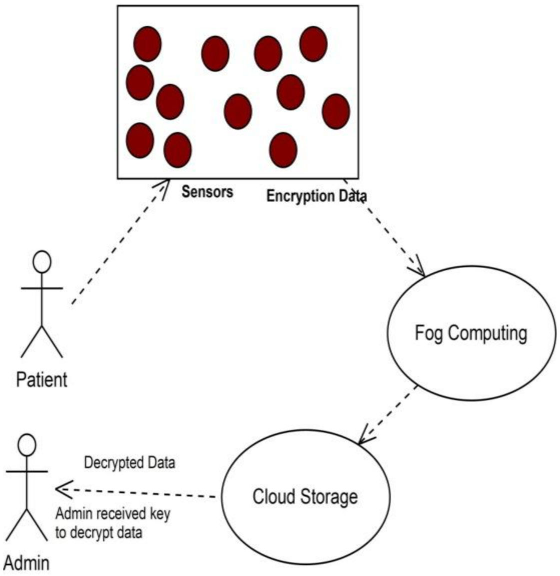

Figure: 1, System Architecture

II. LITERATURE SURVEY

In FC, is a unique variant computing method that needs to improve the CC requirements and services to use the cloud network and also this will reduce the issues such as network delay which can be occurred by service implements. Edge registering uses figuring assets close IoT gadgets for neighbourhood stockpiling and fundamental information preparing. As per Cisco [3], by 2020, 50 billion gadgets will be associated with the Internet. Thus, edge figuring will likewise require more noteworthy adaptability so as to deal with this colossal convergence of gadgets [4].

Manuscript published on November 30, 2019.
* Correspondence Author

Nagarjuna Valeti*, Faculty, Sri Harshini Degree & PG College, AP, India, nagarjuna.valeti@gmail.com

V.Ceronmani Sharmila, Associate Professor, Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, India, csharmila@hindustanuniv.ac.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Edge gadgets can't deal with numerous IoT applications viewing for their restricted assets, which results in asset dispute and expands handling inertness.

Fog computing offers tremendous points of interest for postponing touchy mist based application [9] [10]. Various issues such as data buffering and power management to solve the issues in transferring the data without loss [11]

III. SECURITY ISSUES IN EXISTING IOT HEALTH CARE SYSTEM

There are four stages to directional a weakness and characterizing analysis scope, using software to acknowledge vulnerabilities, reports are analyzed, and endeavor to misuse the system utilizing the proverbial vulnerabilities. The IoT can comprehend associate extreme turning of social protection advantages subordinate upon the association of various useful devices, that by then address a good space of the billions concerning internet associated devices that require facilitate these days accessible [12].

The security vulnerabilities IOT remedial contraptions impact various explicit types for in-clinic equipment together with symptomatic provides e. G, tomography machines conjointly CT scanners, remedial equipment life facilitate gear, Internet-associated contraptions for screening patients that may keep track for resolution plans. IOT innovations empower the handling information and administrations from all of those gadgets thus on encourage upbeat specialists to urge to precise and convenient data concerning the patients' standing, nevertheless additionally to style ill health the board forms for anticipation, conclusion, and treatment. There’s an oversized cluster of varied security vulnerabilities IOT medical gadgets incorporate;

A. Secret key hacking: Medical gadgets are to be ensured by feeble passwords which will be hacked. Programmers notice passwords to access appliance setup knowledge.

B. Poor Security Patching: Some healthful gadgets are inefficaciously fastened, on the grounds that some fix has not nevertheless been sent on the appliance. Inefficaciously fastened gadgets are defenceless against malware and completely different assaults that makes them a noticeable objective for programmers.

C. **Denial of service attacks:** Medical gadgets are light-weight, plus compelled, creating them nerveless to the disclaimer of administration assaults. The transmission of co-occurring solicitations to the appliance will create it stop, disengage from the system or maybe clothed to be out of request.

D. Decoded info transmission: Attackers screen prepare thus on listen in and take passwords. The transmission of decoded info accesses the appliance thus on separate knowledge for transmission malevolent directions [13].

Encryption

Security is most widely discussed in this paper. The DES (Data Encryption Standard) algorithm is a secure encryption algorithm in present software and cloud storage. The people will call this "secret code making".

The process of DES works at bits, or double numbers- the 1s traditional to advanced PCs [14]. every gathering of 4 bits makes up a positional representation system, or base 16, number. Paired "0001" is reminiscent of the positional representation system range "1", parallel "1000" is reminiscent of the positional representation system range "8", "1001" is reminiscent of the positional representation system range "9", "1010" is reminiscent of the positional representation system range "An", and "1111" is reminiscent of the positional representation system range "F".

This algorithm used to collect the 64 message bits, which is similar to 16 positional representation system numbers. To encode the encrypted data DES uses the "keys" that belongs to the 16 positional representation system numbers. Thus DES is the most powerful encrypted algorithm.

The Steps for encryption:

Initialize two large prime numbers (X, Y) and X must be interlinked to Y.

By using this equation the A is calculated

A=X*Y-------- (1)

Euler function (T) is calculated by using this equation:

$T = (X - 1) * (X + 1) * (Y - 1) * (Y + 1)$ ------- (2)

The variable E is called a random number

which is selected and E is smaller than T but larger than 1

- E is related to T internally or not to be checked.
- If E is internally related to T, then E is the hybrid public key
- calculate R with (N):
- $R (N) = \text{Hybrid} \{(X- 1) * (X+ 1) * (Y- 1) * (Y+ 1)\}$ (3)
- The D value is calculated iteratively until D reaches this equation:
- $D * \text{EMod } R (N) = 1$ (4) After D value is generated, then D is the LUC private key.

Integrated Security System

The integrated security system works with the data encryption and key generation for the patient data for secure in cloud database. The following steps explain the ISS.

Accuracy

We can compute the measure of accuracy from the measures of availability and working as specified below.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + TN} * 100$$

- Start Sensors at patient level.
- Start cloud Server.
- Initialize fog devices.
- Start transmission of data to cloud storage.
- Sensors at the patient level have the encryption implementation and all the data of the patient encrypted and generate the key.
- The key sends to the doctor to access the patient records.
- The DES algorithm is used to encrypt and decrypt the data.

IV. EXPERIMENTAL RESULTS:

The experimental setup is done with java and MYSQL as backend. Using Netbeans 8.0.2 in java it is very easy to implement the proposed Integrated Security System (ISS). Results show the performance of proposed system. Table-1 shows the performance of the proposed system.

Table: 1 Show the Performance of the ISS based on accuracy and time (Sec)

	Existing System	ISS
Accuracy	86%	97%
Time (Sec)	20.87	16.21

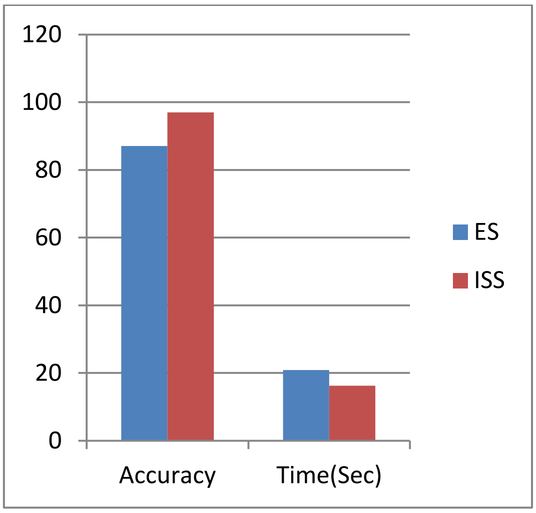

Figure: 2, Performance Comparison of two parameters Accuracy and Time (Sec)

V. CONCLUSION

In this paper, the integrated security system (ISS) is implemented in fog computing and WSN environment. Security is merged with the health care system to save the data without loss. DES is the encryption algorithm used to secure the patient data and provide an integrated health care system with fog computing. After the various metrics are observed the accuracy of the data security is mostly improved with the ISS.

REFERENCES

1. H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey," Computer Networks, vol. 54, no. 15, pp. 2688–2710, 2010.
2. A. Grady, S. Yoong, R. Sutherland, H. Lee, N. Nathan, and L.Wolfenden, "Improving the public health impact of eHealth and mHealth interventions," Australian and New Zealand Journal of Public Health, vol. 42, no. 2, 2018.
3. Cisco, "White paper: fog computing and the internet of things: extend the cloud to where the things are," Tech. Rep., Cisco, 2015.
4. L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: towards a comprehensive definition of fog computing," ACM SIGCOMM Computer Communication Review, vol. 44, no. 5, pp. 27–32, 2014.
5. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16, Helsinki, Finland, August 2012.
6. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ''Fog computing and its role in the Internet of Things,'' in Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC), New York, NY, USA, 2012, pp. 13–16.
7. ''Predix architecture and services,'' General Electric, Boston, MA, USA, Whitepaper, Sep. 2015, accessed on Nov. 11, 2016. [Online]. Available: https://cloudfront.net
8. Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, ''Mobile edge computing—A key technology towards 5G,'' Eur. Telecommun. Standards Inst., Sophia Antipolis, France, White Paper 11, 1st ed., Sep. 2016. [Online]. Available: http://etsi.org.
9. Y. Chen, W. Shen, H. Huo, and Y. Xu, "A smart gateway for health care system using wireless sensor network," in 2010 Fourth International Conference on Sensor Technologies and Applications, pp. 545–550, Venice, Italy, July 2010.
10. K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: a programming model for largescale applications on the internet of things," in Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing, pp. 15–20, Hong Kong, China, August 2013.
11. Nagarjuna Valeti and V Ceronmani Sharmila, Optimizing cloud health Care Data Transmissions using Fog, 2019 J. Phys.: Conf. Ser. 1228 012008
12. C. Hufford. (2017). Security Vulnerabilities IoT Medical Devices on Wi-Fi Networks. Available: https://www.nextgenges.com/author/craig/.
13. E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H.Chen, "Assessing medical device vulnerabilities on the IOT", in Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on, 2017, pp. 176-178: IEEE.
14. B.Naveen Kumar, P. Nageswara Rao, Enhanced Access Control of third party Data in Cloud Computing, IJDCST, June-2016, Issue- V-4, I-4, SW-11.

AUTHORS FROFILE

Valeti Nagarjuna, Working As A Computer Faculty In The Department Of Computer Science In Sri Harshini Degree & Pg College, Ongole. He Received His Mca From Vision Institute Of Science & Technology, Bapatla, Anu, Andhra Pradesh, India In 2012. He Received His M.Tech From Kkr & Ksr Institute Of Technology And Science, Guntur, Jntu Kakinada, Andhra Pradesh, India In 2014. He Has Five Years Of Teaching Experience In Degree &Pg College. His Areas Of Interest Fog Computing And His Interesting Domains Are Data Mining, Cloud Computing Etc.

V.Ceronmani Sharmila, Joined Hindustan Group Of Institutions In 2003 And Currently Working As Head-Centre For Networking And Cyber Defense, & Hod (I/C) In Department Of Information Technology, School Of Computing Sciences. She Received Her Ph.D Degree From Hindustan Institute Of Technology And Science, Chennai, India In 2016. She Has Three Years Of Industrial Experience And Fifteen Years Of Teaching Experience In Engineering Colleges Both Undergraduate And Postgraduate Level. She Has More Than 30 International Journal/Conference Publications. Her Area Of Interest Is Cyber Security, Computer Networks (Mobile Ad Hoc And Sensor Networks), Applications Of Graph Theory, Image Processing, Cloud Computing, Internet Of Things (Iot) And Very Large Scale Integration (Vlsi).