Utilizing Fog Computing to Secure Smart Health Care Monitoring (SHM) in Smart Cities

Elena Ljubimova, Alexey Yumashev, Afanasiy Sergin, B. Prasad, and E. Laxmi Lydia

Abstract Currently, a large number of cloud-based facilities are being prolonged to the network's edge, with the goal of reducing response time and bandwidth costs in activities such as healthcare in smart cities. Smart health concepts use Internet-related wearable devices for e-monitoring and diagnostics in order to provide low-cost healthcare. The healthcare sector is being confronted with new issues as the amount of complexity of patient data grows day by day. Smart Healthcare Monitoring (SHM) is required to make the healthcare structure smarter in order to preserve data and ensure confidentiality. An SHM is made up of various IoT devices, sensors, and actuators that gather and store statistics from the patient's physique. Cloud computing-based storage is the most frequent method for storing data in the SHM but it is very costly. To overcome this problem, fog computing is used to process the information close to the body device system, which minimizes latency and enhances throughput. In this chapter, we proposed a secure service-oriented fog computing architecture that has been validated using a publicly available dataset. Fog computing uses privacy-preserving techniques to secure data and solve privacy concerns. The findings and discussions confirm the suggested architecture's suitability for SHM applications. The prototype was created utilizing a use case and a sequence diagram. The test cases are taken from online repositories. In comparison to a similar technique, the

E. Ljubimova
Department of Mathematics and Applied Computer Science, Kazan Federal University, Elabuga Institute of KFU, Elabuga, Russia

A. Yumashev
Doctor of Medicine, Department of Prosthetic Dentistry, Sechenov First Moscow State Medical University, Moscow, Russia
e-mail: umalex99@yandex.ru

A. Sergin
Pedagogical Sciences, Department of Theories and Principles of Physical Education and Life Safety, North-Eastern Federal University named after M.K. Ammosov, Yakutsk, Russia

B. Prasad · E. L. Lydia (✉)
Department of Information Technology, VR Siddhartha Engineering College (A), Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, Andhra Pradesh, India
e-mail: elaxmi2002@yahoo.com

V. Bhateja et al. (eds.), *Information System Design: Communication Networks and IoT*,
Lecture Notes in Networks and Systems 1057,
https://doi.org/10.1007/978-981-97-4895-2_26

proposed method's implementation, and security analysis display high security, low energy, and low power.

Keywords Health care monitoring (HCM) · Fog computing · IoT devices · Smart cities

1 Introduction

One of the most important aspects of smart cities is intelligent healthcare. The field of smart healthcare arose from a desire to progress the SHM management, better utilize its resources, and lower costs while preserving or even improving quality securely. Gadgets are used as wearables to identify the patient's conditions and the critical data are reserved privately and securely. The drawbacks of outdated network topologies, where information is delivered and conventional to/from the networks fundamental, become obvious when the quantity of network-associated devices endures growing at a rapid rise. These gadgets, which are enabled by earlier access grids, not only mandate reduced latency and quicker speeds while getting information from the system but also produce a growing volume of information to deliver. Furthermore, due to the hardware limitations of some edge strategies, particularly portable policies, there is a strong mandate for divesting jobs, resulting in further blocks in a previously crowded system. The growth of the Internet of Things (IoT) strategies, as well as the anticipated bandwidth demand from new 5G system [1] strategies and requests, necessitates other results and manners to meet these novel requirements. Protected infrastructure is needed for the distribution, storage, and dispensation of public health data. It might be evaluated to identify areas where diseases are causing serious problems, allowing for the provision of appropriate healthcare. Sickness and infection transmission are frequently linked to the eco-friendly site. The overview of fog computing is demonstrated in Fig. 1.

Fog computing is used to improve real-life data examination of sicknesses and other difficulties, as well as their sites. Because health statistics are varied, mixing them with present healthcare amenities, interoperability, and other issues can be challenging. Fog Computing [2] is a novel solution that offers a less power node for enhancing throughput and lowering potential on the edge of several schemes at the customer layer. These novel requirements necessitate new resolutions and designs. For long-standing analytical statistics, fog computing needs less cloud storage and transmission control. Fog computing has been effectively used in Healthcare Monitoring (HM) [3] and smart city industries. The given model for a fog-based SHM has the primary benefit of lowering latency and conserving bandwidth. Because device mass is cumulative every single day, a great volume of data is being formed, and transmitting all of the information gathered from IoT [4] strategies to fog for storing and dispensation consumes a portion of bandwidth, traffic flow will rise. Since processing ends at the entry itself, the suggested model solves these issues. The simulation findings indicate how the model can optimize resources to decrease

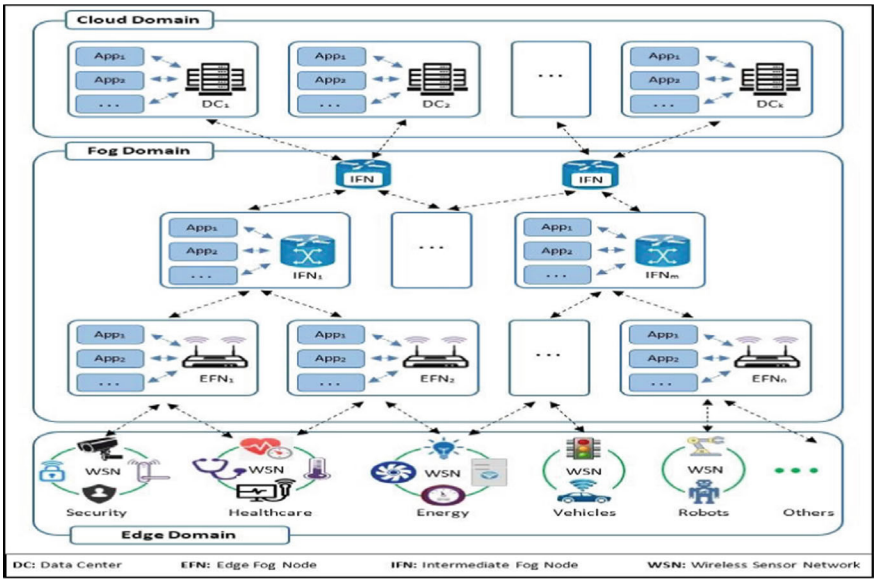

Fig. 1 Overview of fog computing

potential needs for patients with various health complications, allowing healthcare practitioners to make quick and real-time diagnoses [5]. Some of the privacy and security challenges [6] in the previous research are listed in Fig. 2.

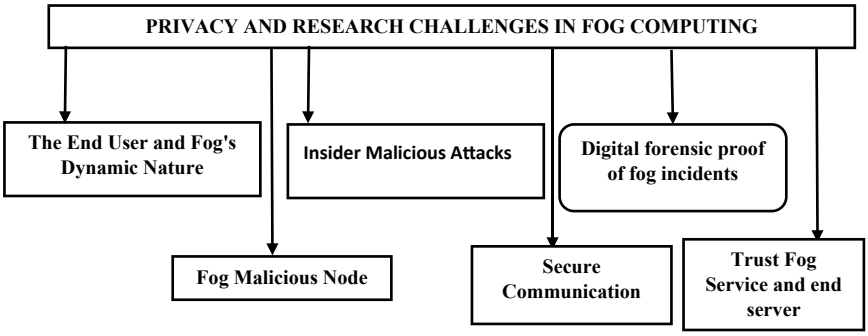

Fig. 2 Some of the privacy and security challenges [6]

2 Key Principles

The main objectives of this chapter to secure the transfer of health data are stated as follows:

1. Proposed a Safe Service-Oriented Fog Computing Architecture and privacy-preserving approaches to improve security characteristics of Smart Healthcare Monitoring (SHM) in smart cities for effective, efficient, and secure data sharing.
2. Using the win–win spiral model, the prototype development is sketched for the association among the various security features demonstrated with use case and sequence diagrams in the Unified Modelling Language (UML).
3. The comparative study of the traditional method and a novel security analysis architecture enhances higher security and privacy and low latency, power, and energy.

3 Relevant Works

The paper [7] presented a protected IoT-based well-being monitoring system in which a microcontroller performs vital dispensation and directs dynamic indications through Wi-Fi. The paper of [8] presented an Electrocardiogram (ECG) service-based approach for the production, dispensation, storage, and investigation of ECG information streams employing specific wearables. Edge computing has given basis dispensation since its inception and current improvements. In reality, edge computing has developed a pervasive element of the healthcare business, allowing doctors and physicians to refer their patients widely using the technology. Several investigations relating to cloud-based IoT facilities have been supported in a similar framework, but they still face challenges such as excessive interruptions, high bandwidth necessities, and optimized computing. These concerns are especially important in emergency [9] situations because quick judgments and activities are required to safeguard the patient's life [10]. Data analysis has been made easier because of cloud computing, which has supplied unlimited storage and computational capacity. It made the move from desktop to fog servers more easily. Cloud computing and other web technologies have combined to provide an open ecosystem with common resources [11]. In businesses that interconnect tools, skills, and knowledge to rear the assembly, management, and application of topographical data, cloud architecture has offered a stable foundation. Geospatial web services [12] are used by many cloud platforms to expose application functionality. Clients can question and apprise several sorts of cloud services using this method. It also includes a standard mechanism for integrating various cloud apps with initiative SOA architecture in the software cloud.

With the introduction of cloud computing technologies, a slew of safety and confidentiality concerns arose. Cloud data services are connected with a variety of safety fears, including not only outdated safety threats like network snooping, prohibited attacks, and Denial of Service (DoS) attacks, but also precise cloud computing fears

like cross-station attacks, virtualization vulnerabilities, and cloud service misuse. The dangers are limited by the security criteria listed below [13, 14]. Because fog is considered a significant allowance of cloud computing, some safety and confidentiality problems that arise in cloud computing are expected to have an unavoidable influence on fog computing. If safety and confidentiality concerns are not addressed, fog computing adoption will be delayed, based on the fact that 74 percent of Information Technology (IT) directors and Chief Information Officers (CIO) discard cloud computing due to safety and confidentiality concerns [15]. Because fog computing is silent in its infancy, little research has been done on safety and confidentiality issues [16]. Because fog computing is presented in the context of the Internet of Things (IoT) [17] and evolved from cloud computing, fog computing [18] inherits cloud safety and confidentiality vulnerabilities [19].

4 Design of a Prototype

The spiral model of the Object-Oriented Software Engineering (OOSE) approach is the key focus for prototype development of SHM-Fog, i.e. Fog-based agenda. The software development follows a succession of steps in the OOSE WIN–WIN spiral model, which includes requirements prerequisite planning, investigation, growth strategy, action, and challenging, and complete component and framework opinion. The method is essential and incremental with each execution, refining the analysis and development stages through the valuation and testing of a completed module. Furthermore, the suggested agenda's incremental growth approach permits the difficulty of building this framework to be broken down into smaller, more manageable chunks of growing complications [20]. So, in SHM-Fog, there are three phases to be distinct. Phase 1 is the proposed framework of the SHM-fog framework, Phase 2 demonstrates UML diagrams [21], and Phase 3 is the secure SHM for a smart city healthcare system using test cases from online repositories.

4.1 Proposed Framework

Monitoring patients' health results influences the health doctor's investigation and results, the systems must be trustworthy. A mistake or a delay in the results might have major repercussions, such as erroneous treatment or a delayed reaction to an emergency, all of which can have a detrimental impact on the patient. In many instances outdated SHM finished up of sensor devices, gateways, and cloud servers are unable to meet the high potential necessities. Advanced SHM systems using fog computing are described to overcome the drawbacks of traditional health-monitoring systems. Figure 3 depicts the system's architecture with fog computing. It consists of several key components, including a sensor layer, smart gateways with a fog layer, and cloud servers with end-user access.

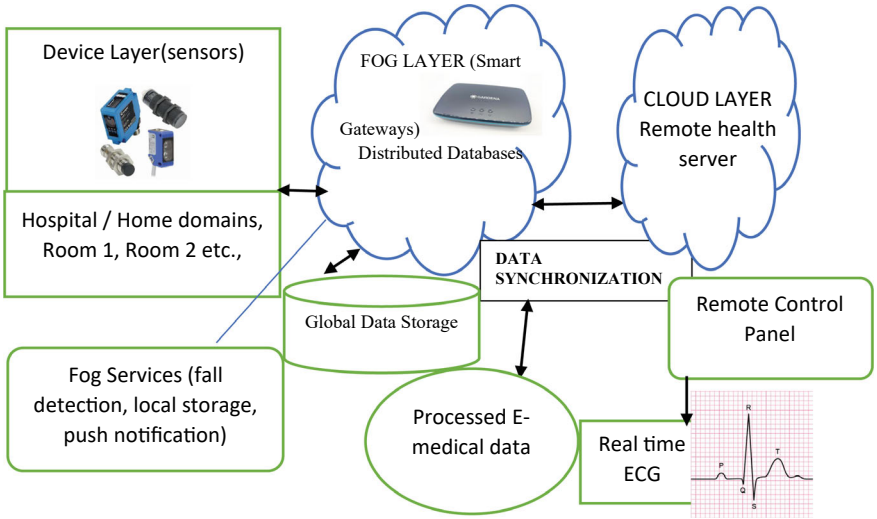

Fig. 3 Proposed three-tier SHM-fog computing architecture

The following is a description of the functionality of the various layers of the architecture. A sensor node is made up of three major components: sensors, a microcontroller, and a radio receiver message mark. A Secure Digital (SD) [22] card can be inserted into a radar node for impermanent data storage in some apps. Sensors (such as Electrocardiogram (ECG) [6], moistness, and temperature sensors) are cast off to capture appropriate information from the atmosphere as well as e-health information from the human body. Fog computing is a convergent system of fog services-enabled smart openings. Depending on the proposition's needs, a smart entry might be moveable or safe in a specific spot. Each type of entrance has its particular set of advantages and disadvantages. A permanent gateway, on the other hand, is typically built with a powerful device that is powered by a wall socket. A permanent gateway, on the other hand, can easily handle huge computational operations and distribute more composite facilities with superior data. For supporting E-healthcare, fog computing facilities located in a fog layer of smart entries are diverse. These services are unique in that they must meet stringent latency and data quality criteria. It includes security supervision, fault tolerance, classification, localhost with an operator crossing point, and network supervision, in accumulation to the typically cast-off fog services like push notification, local data storing, and data dispensation.

4.2 UML Diagrams

The details of the use case model and sequence diagram are specified using the SHM-Fog described in the above framework. The use case and sequence diagram of the SHM-Fog framework are presented in Figs. 4 and 5.

The suggested SHM-Fog architecture is more protected than cloud-based backgrounds for the delivery of health data. As a consequence, the following portion of the outcome and conversation section discusses edge investigation and comparison analysis of existing cloud frameworks with SHM-Fog frameworks using appropriate parameters.

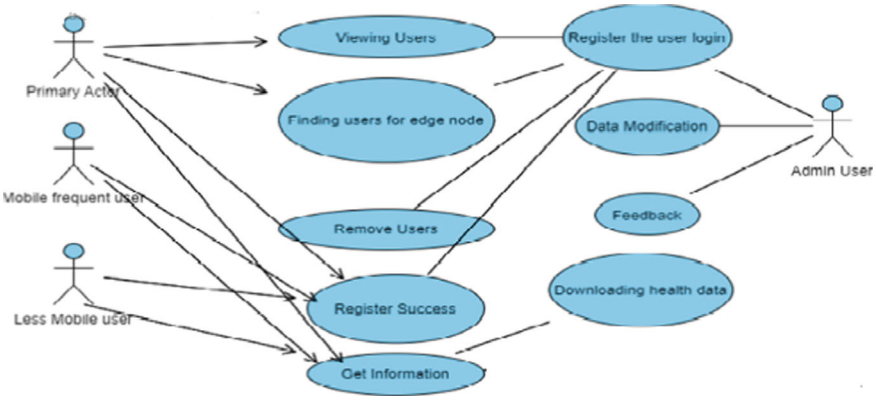

Fig. 4 Use case diagram

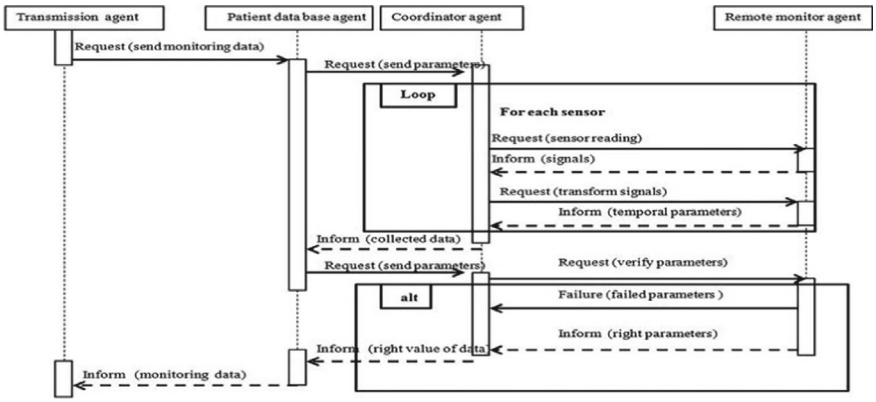

Fig. 5 Sequence diagram of patient data

4.3 Secured SHM-Fog Model

A smart city is collects data from many kinds of IoT devices and uses that information to accomplish actions and give insights. IoT devices may gather health information, convert it to data, and then use it to improve the quality of healthcare. SHM-fog applications include the following: For the mature, fall discovery is meant to be more operative. Patients are monitored remotely using wearable sensors. Figure 1 shows the five elements that make up the system: reliable experts, patients, fog nodes, cloud storage, and service providers. The system is initialized by a reliable expert, who also offers registering services and creates structure public keys, structure master keys, and secret keys for additional organizations. Patients communicate health information that is acquired by health care devices or physically entered by them. Patients communicate the ciphertext to a fog node after encrypting their common information. In close immediacy to patients, a fog node could be a health entry or a router. Healthcare contextual and sophisticated computer skills are mastered by fog nodes. It pre-processes the common ciphertext and re-encrypts it before sending the new ciphertext to cloud storage.

Figure 6 demonstrates the searchable encoding in the SHM-FOG Model. When there are numerous data owners and receivers, this approach might be used. The patient's body is fitted with a collection of body sensors, and the data collected is compiled in the sensing device. Later, a file named Patient Health Record (PHR) is created. This PHR is created in the patient's medicinal telephone and sent to the fog in an encoded format. Before being stored in the fog, information will be sent to a Reliable Third Party (Edge server) for the resulting activities. All of the information is assumed to be in text presentation. The model's operation is described below: There is an Attribute Centre (AC) in this prototypical that calculates the randomness of features and sets the rate of those features. Characteristics are prioritized based on their standards, and each one is given a predetermined value. SHM AC is the name of the algorithm that will be executed on AC. A Key Generator (KG) is included in this model, and it calculates the key for the information depending on the values of specified constraints. PHR stores these standards, and a top-secret key will be produced based on two of them. SHM ENC specifies the algorithm that will be used on KG. A Query Processor (QP) is used in this model to handle query dispensation. The algorithm for Privacy-Preserving Searchable Encryption (PPSE) is shown in Algorithm 1.

Algorithm 1: SHM_ENC Privacy Preserving Searchable Encryption (PPSE)

1: method Input: (Index Table t1).

2: OUTPUT: Table t 2 and t 3.

3: START.

4: Calculate K ind and K text = H [keyword || attribute index (I)].

5: Generates EI = SHM Enc Kind [ω 1 _ Idd1], SHM ENC Kind [ω 2 _ I dd2]…Enc Kind [ω m _ I ddn].

6: encoded_index_Table t2. create = [keyword || text ID].

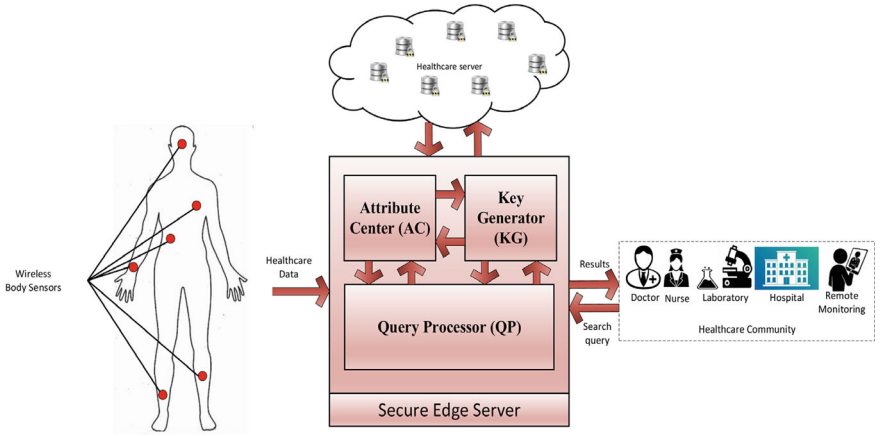

Fig. 6 Searchable encoding in SHM-fog model

7: ED. generate = Enc K doc [d1], E NC K doc [d2], E NC K doc [d3] .... Enc K doc [dn].

8: Table t.

Step 1: A Key Generator (KG) is used to conduct a randomized algorithm. For the text and index encryption, 2 keys will be produced in this phase: K ind and K text. The shredded value of a keyword and feature index (Table 1) is used to generate these keys.

Step 2: Make a phone call to the Enc Kind organization (). This function encrypts the keyword set SHM Kind (ω1, ω2,ω3…ωm) created in the phase. The function will accept the keywords 1 and D1 as input and output Encrypted Index (EI).

Step 3: Generates an encoded index table in which each keyword encoded index is stored in table t2 together with the textID as shown in Table 2.

Step 4: Make a phone call to SHM doc (). This function encrypts each text in Set d and saves the Encoded Document (ED) in Table t3 with the text ID as demonstrated in Table 3. It provides the user with secret key ks. The key is used to create a trapdoor that may be utilized to do exploration and finding processes.

Table 1 Index table (t1)

Document	Document identification	Priority index	Keywords
d1	IDd1	1	ω 1, ω 2, ω 3
d2	IDd2	2	ω 4, ω 5, ω 6
d3	IDd3	3	ω 2, ω 4
d4	IDd4	4	ω 1, ω 3, ω 5

Table 2 Encoded index table (t2)

Keywords	Document identification	Encoded index
ω 1	IDd1, IDd4	*ENC Kind* [ω 1 _ *ID D* 1], *ENC Kind* [ω 1 _ *ID D* 4]
ω 2	IDd2, IDd3	*ENC Kind* [ω 3 _ *ID D 2*], *ENC Kind* [ω 3 _ *ID D* 3]
ω 3	IDd2, IDd3, IDd4	*ENC Kind* [ω 2 _ *ID D* 2], *ENC Kind* [ω 2 _ *ID D* 3], *ENC Kind* [ω 2 _ *ID D* 4]
ω 4	IDd3	*ENC Kind* [ω 4 _ *ID D* 3]
ω 5	IDd4	*ENC Kind* [ω 5 _ *ID D* 4]

Table 3 Table (t3)

Document identification	Priority index	Encoded index
IDd1	1	*ENC K doc*(*D* 1)
IDd2	2	*ENC K doc* (*D 2*)
IDd3	3	*ENC K doc* (*D* 3)
IDd4	4	*ENC K doc* (*D 4*)

5 Performance Evaluation

The comparative study shows that the proposed SHM-fog framework outperforms traditional IoT systems with the below evaluation.

A. High Security

Figure 7 shows that the encoding on the device takes longer than the encoding on the receiver. When it has features indicated in the admittance policy, the data encoding on the device with traditional IoT and SoA takes around 35 s, however, SHM-fog takes only 8 s when $R = 1$ at a similar attribute number, greatly reducing the time lag. Because there are suitably (1 R) periods of complete encoding divested to the fog node from the patient, the encoding time on the fog node rises with the number of features and rises when $R = 1.2$ reduces to $R = 1$. The encoding time on the fog node rises as sickness hazard groupings. When the fog node classifies more illness risk groups.

B. Low Consumption

Efficient and privacy-preserving fog-assisted Health Data Sharing is demonstrated in below Fig. 8.

When encoding is used on a patient with resource-constrained e-healthcare devices, energy consumption is a key concern. We use Power Tutor to screen energy consumption in the SHM-fog framework utilizing in-built battery-operated power devices and information on battery-operated release behaviour to evaluate energy usage. With different patients 1, 2, and 3, we show the relationship between the number of attributes (x-axes) and the energy consumption (y-axis) in terms of j

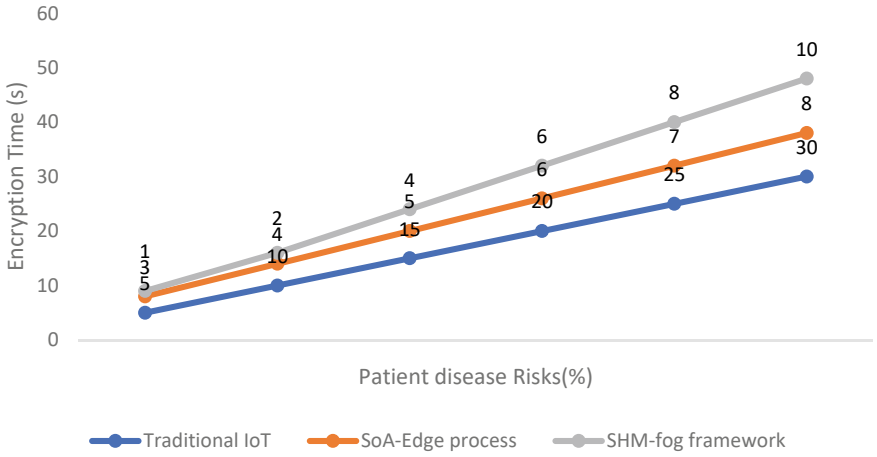

Fig. 7 Comparison of traditional IOT, SoA, and encoded SHM-fog framework

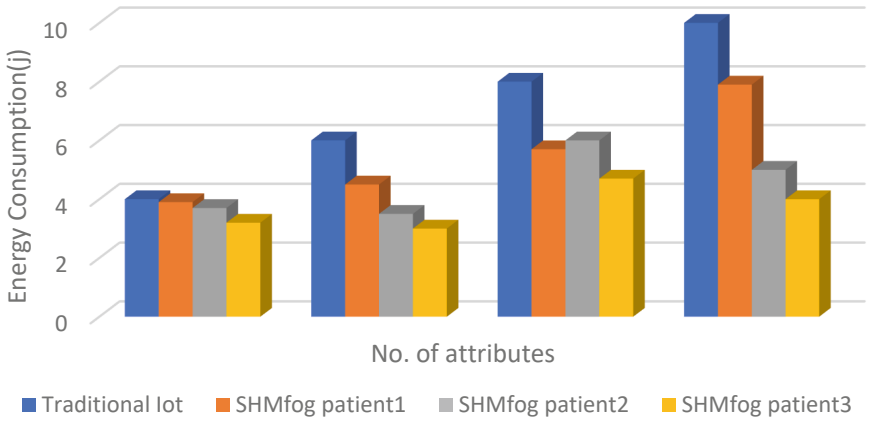

Fig. 8 Energy consumption of SHM-fog and traditional IoT framework

on the phone. At a similar number of characteristics, we can show that SHM-fog consumes less energy than and about equals R times that of traditional IoT, SoA-Edge. Meanwhile, as the attribute proportion R is reduced from 1/2 to 1/4, SHM-fog energy usage reduces as more encoding is divested to the fog node from the patient.

6 Conclusion and Future Enhancement

To some extent, SHM-fog computing architecture can solve the security problems of standard IoT edge architecture in smart cities. By integrating fog as an intermediate layer and carrying it out at the edge, data safety, correctness, and reliability are improved, as well as the latency percentage and total service value. Since many IoT plans are established and the requirement for fast processing grows, the IoT-Fog-cloud building will become more frequently employed in the near imminent. The solution can be improved in the future by creating a dependable real-time information monitoring scheme that uses the manner described above as its foundation. And to show how much fog may improve the typical SHM-fog design by computational proof in terms of high security, low latency, and low energy. The different security challenges can be resolved by improving the SHM-fog framework in the future. In the future, we will consider emergency situations when sharing data and enable quick access to policy updates and revocations.

References

1. Bishoyi PK, Misra S (2021) Enabling green mobile-edge computing for 5G-based healthcare applications. IEEE Trans Green Comm Network 5(3):1623–1631. https://doi.org/10.1109/tgcn.2021.3075903
2. Carvalho G, Cabral B, Pereira V, Bernardino J (2021) Edge computing: current trends, research challenges and future directions. Computing 103(5):993–1023. https://doi.org/10.1007/s00607-020-00896-5
3. Saini J, Dutta M (2020) Applications of IoT in indoor air quality monitoring systems, In: Raj P, Chatterjee J, Kumar A, Balamurugan B (eds) Internet of things use cases for the healthcare industry. Springer, Cham. https://doi.org/10.1007/978-3-030-37526-34
4. Jo J, Jo B, Kim J, Kim S, Han W (2020) Development of an IoT based indoor air quality monitoring platform. J Sens, Article ID 8749764, 14 p. 2020. https://doi.org/10.1155/2020/8749764
5. Kaivonen S, Ngai E (2019) Real-time air pollution monitoring with sensors on citybus. Digital Comm Network. https://doi.org/10.1016/j.dcan.2019.03.003
6. Mukherjee M, Matam R, Shu L, Maglaras L, Ferrag MA, Choudhury N, Kumar V (2017) Security and privacy in Fog computing: challenges. IEEE Access 5:19293–19304. https://doi.org/10.1109/access.2017.2749422
7. Divya A, Keerthana K, Kiruthikanjali N, Nandhini G, Yuvaraj G (2017) Secured smart healthcare monitoring system based on IoT. Asian J Appl Sci Tech 1(2); Navyashree K, Soundarya S, Suhani HS, Gulafshan F, Kumar VR (2017) Secured smart healthcare monitoring system based on internet of things. Int J Eng Res Tech 5(20)
8. Siam AI, Abouelazm AR, El-Bahnasawy NA, El-Banby G, El-Samie FEA (2019) Smart health monitoring system based on IoT and cloud computing. In: Proceedings of International Conference on Electronic Engineering, pp 37–42
9. Yang Z, Zhou Q, Lei L, Zheng K, Xiang W (2016) An IoT cloud based wearable ECG monitoring system for smart healthcare. J Med Syst 40(286)
10. Pace P, Aloi G, Gravina R, Caliciuri G, Fortino G, Liotta A (2019) An Edge-based architecture to support efficient applications for healthcare industry 4.0. IEEE Trans Indust Inform 15(1):481–489

11. Yang C, Huang Q, Li Z, Liu K, Hu F (2017) Big data and cloud computing: innovation opportunities and challenges. Int J Digital Earth 10(1):13–53
12. AL Kharouf RA, Alzoubaidi AR, Jweihan M (2017) An integrated architectural framework for geoprocessing in cloud environment. Spatial Inform Res, 1–9
13. Wang T, Zhang G, Liu A, Bhuiyan MZA, Jin Q (2019) A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing. IEEE Internet Things J 6(3):4831–4843
14. Chen M, Li W, Hao Y, Qian Y, Humar I (2018) Edge cognitive computing based smart healthcare system. Future Generat Comp Syst 86:403–411
15. Perera G, Qin Y, Estrella JC, Reiff-Marganiec S, Vasilakos AV (2017) Fog computing for sustainable smart cities: a survey. arXiv preprint arXiv:1703.07079
16. Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P (2018) Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Future Generat Comp Syst 78(2):641–658
17. Gia TN, Sarker VK, Tcarenko I, Rahmani AM, Westerlund T, Liljeberg P, Tenhunen H (2018) Energy efficient wearable sensor node for IoT-based fall detection systems. Elsevier, Microprocessors and Microsystems
18. Rauf A, Shaikh RA, Shah A (2018) Security and privacy for IoT and fog computing paradigm. In: Paper presented at: 2018 15th Learning and Technology Conference (L&T), 2018; Jeddah, Saudi Arabia
19. Muhammed T, Mehmood R, Albeshri A, Katib I (2018) UbeHealth: a personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities. IEEE Access 6:32258–32285. https://doi.org/10.1109/ACCESS.2018.2846609
20. Roy A, Roy C, Misra S, Rahulamathavan Y, Rajarajan M (2018) Care: criticality-aware data transmission in CPS-based healthcare systems. In: Paper presented at: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO
21. Mahmud R, Koch FL, Buyya R (2018) Cloud-fog interoperability in IoT-enabled healthcare solutions. In: Proceedings of the 19th International Conference on Distributed Computing and Networking (ICDCN), Varanasi, India
22. Schuiki F, Schaffner M, Gürkaynak FK, Benini L (2019) A scalable near-memory architecture for training deep neural networks on large in-memory datasets. IEEE Trans Comput 68(4):484–497. https://doi.org/10.1109/TC.2018.2876312