International Journal of Medical Engineering and Informatics

ISSN online: 1755-0661 - ISSN print: 1755-0653
https://www.inderscience.com/ijmei

A secure health monitoring system based on fog to cloud computing

Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari

DOI: 10.1504/IJMEI.2022.10050253

Article History:
Received: 11 January 2022
Accepted: 09 July 2022
Published online: 12 December 2024

A secure health monitoring system based on fog to cloud computing

Hafida Saidi*

STIC Lab,
University of Abou Bekr Belkaid,
Chetouane Tlemcen 13000, Algeria
Email: hafida.saidi@univ-tlemcen.dz
*Corresponding author

Nabila Labraoui

LRI Lab,
University of Abou Bekr Belkaid,
Tlemcen 13000, Algeria
Email: Nabila.labraoui@univ-tlemcen.dz

Ado Adamou Abba Ari

DAVID Lab,
Université Paris-Saclay,
University of Versailles Saint-Quentin-en-Yvelines,
45 Avenue des États-Unis, 78035 Versailles Cedex, France
and
Department of Computer Science,
University of Maroua,
P.O. Box 814, Maroua, Cameroon
Email: ado-adamou.abba-ari@uvsq.fr

Abstract: Nowadays, the elderly can receive care in their home and enable physicians to follow their diseases in real-time. However, these technologies suffer from several issues like security and privacy-preserving data challenges. In this paper, we proposed a HIPAA-compliant framework that enables security and privacy-preserving medical data based on fog-to-cloud (F2C) computing. Our aims are to define a system that solves the privacy and security issues with remote elderly monitoring. The F2C infrastructure is used to provide better security of medical data and allow a real-time diagnosis of the elderly. Furthermore, F2C combines the benefits of cloud and fog computing such as providing permanent storage, reducing computation load and data transmission delay, and enhancing the security challenges. Simulation results suggest that F2C technology delivers better performance in terms of latency, cost, and energy consumption.

Keywords: elderly healthcare; wearable sensors; fog to cloud computing; AES-ECC encryption; internet of medical things; IoMT.

Reference to this paper should be made as follows: Saidi, H., Labraoui, N. and Ari, A.A.A. (2025) 'A secure health monitoring system based on fog to cloud computing', *Int. J. Medical Engineering and Informatics*, Vol. 17, No. 1, pp.30–43.

Biographical notes: Hafida Saidi is a PhD student at the STIC Lab of the University of Tlemcen, Algeria. She received her Master's in Computer Engineering, 'Networks and Distributed Systems', from the University of Tlemcen, Algeria in 2017 and she is preparing her PhD thesis in the same domain. Currently, her research is focused on security and data privacy in the healthcare area, blockchain and cloud computing.

Nabila Labraoui is a Full Professor in Computer Engineering at the University of Tlemcen, Algeria. She received her PhD in Computer Engineering and the HDR from the University of Tlemcen, Algeria. Her current research interests include VANETs, wireless ad hoc sensor networks, security and trust management for distributed and mobile systems, cognitive radio, cloud computing and big data security.

Ado Adamou Abba Ari is an associate researcher at the DAVID Lab of the Université Paris-Saclay, France and Associate Professor at LaRI Lab of University of Maroua, Cameroon. He received his PhD in Computer Science in 2016 from the Université Paris-Saclay in France with the higher honours. He also received his Master of Business Administration (MBA) in 2013, Master of Science (MSc) in Computer Engineering in 2012 and Bachelor of Science (BSc) in Mathematics and Computer Science in 2010 from the University of Ngaoundéré, Cameroon. His current research is focused on wireless networks, IoT and IA.

This paper is a revised and expanded version of a paper entitled 'Remote health monitoring system of elderly based on fog to cloud (F2C) computing' presented at 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 9–11 June 2020.

1 Introduction

Nowadays, elderly people need to visit doctors regularly for their checkups and diagnosis. With the advance in technology, the emergence of the internet of medical things (IoMT) will facilitate the development of elderly remote monitoring systems (Ahmid et al., 2022; Silas and Rajsingh, 2019). Moreover, several technological challenges need a ubiquitous deployment of computing models throughout the hospital to share health data with different users (Saidi et al., 2020). These technologies allow the elderly to be assisted by health professionals when they are in their home, enable physicians to follow their diseases, and provide suggestions in real-time (Fiore et al., 2018; Almeida et al., 2017).

To collect real-time medical information, wearable sensors can be used. The sensors will generate huge amounts of data that must be processed rapidly and stored sustainably by using innovative storage infrastructures. Since sensors have limited resources (Saidi et al., 2019), integration with F2C computing plays a major role (Atlam et al., 2017). F2C computing is a new paradigm that enhances the synergy between cloud and fog

computing (Farahani et al., 2018). The main benefits of this infrastructure are high computing, storage capabilities, reduced network traffic, and low communication latencies (Saidi et al., 2020). However, using F2C computing raises many security concerns (leakage, waste, or theft). To overcome these challenges, it is necessary to reinforce security measures. Indeed, privacy and security must meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was enacted by the US Government to implement the security and privacy of healthcare data for American citizens (US Department of Health and Human Services, 2021). HIPAA's main security requirements are as follows:

1 Patient's understanding: Patients have the right to know how their personal and sensitive health data is stored and used by a healthcare provider.

2 Confidentiality: Medical records must be kept away from users who should not access them.

3 Data integrity: This ensures that manipulation of medical data is strongly prohibited.

Hence, the shared health data should be a true representation of original information without any form of alteration.

In this paper, we propose a HIPAA-compliant framework that enables security and privacy-preserving medical data based on F2C computing for elderly remote monitoring. For this purpose, cryptography techniques are adopted to ensure the security of medical data.

The contributions of this paper are as follows:

1 Proposing a remote health monitoring [remote elderly monitoring (REM)] framework based on the F2C computing.

2 All medical records including personal and electronic health records must be encrypted before sharing and storing them.

3 Applying a hybrid encryption scheme for secure data storage and data sharing.

4 Evaluating the proposed system by comparing the performances of fog and cloud computing.

The rest of this paper is structured as follows: in Section 2 related works are reviewed. In Section 3, we describe our proposed approach with the design goals. Section 4 defines the security model. In Section 5, we present the results of the performance evaluation. Finally, we draw a conclusion and future work.

2 Related work

The security of the healthcare systems is always at risk and can be breached by intruders. In this section, we will briefly introduce some related works on the security and privacy of cloud-based healthcare data.

Thilakanathan et al. (2014) proposed a cloud-based network for the secure sharing of health data. However, requests of the users must first pass through a trusted party before accessing the cloud where data are stored. Indeed, this scheme has limited scalability. In (Wang et al., 2017), the authors developed a new identity based proxy re-encryption

(IBPRE) scheme for ensuring the security and privacy of the E-health cloud system. However, the authors were unable to verify the performance of other encryption techniques. In Kahani et al. (2016), the authors used the zero-knowledge protocol to verify and preserve the anonymity of the identity of users. However, by storing the patients' medical data in the cloud, patients have lost control over their health data. Another scheme was designed by Guan et al. (2015) that suggested the security and privacy of the data stored in the cloud by introducing the mask-certificate attribute-based encryption (MC-ABE) scheme. However, the use of encryption methods requires a high degree of overhead computing. In Wang et al. (2019), the authors proposed a scheme based on a fully homomorphic design for the protection of medical data residing in the cloud. Zuo et al. (2018) developed a model based on attributes encryption to protect data in cloud computing. The main concept of this research work is to allow the decryptor to verify the validity of the ciphertext. Wang (2018) proposed a secure data sharing scheme to ensure the confidentiality of data using symmetric encryption and attribute-based encryption techniques to keep data outsourced to the cloud securely. An attribute-based encryption method was proposed by Shahina et al. (2016) to encrypt the patient's health record in cloud computing to protect the user's personal health data. Yeh et al. (2015) proposed the HealthDep system, an encrypted Electronic Medical Records (EMR) duplication scheme for cloud-assisted eHealth systems. Zhang et al. (2018) described a privacy-preserving disease prediction system (PPDP) in a cloud-based e-healthcare system. The system encrypts the patients' historical medical data and outsources them to the cloud server.

Despite the benefits of cloud computing like flexibility, reliability, unlimited computing capacity, cost efficiency, and elasticity (Masip-Bruin et al., 2016; Verma and Sood, 2018), it has also a few issues and challenges concerning security and privacy. Indeed, using the cloud alone can cause delays during the transfer of data in which reliability, efficiency, and time play an important role (Tao and Shuijing, 2016). Hence, the centralised cloud computing model has to be extended to a distributed one such as fog computing (Yi et al., 2015; Kharel et al., 2017) which refers to dividing tasks and offloading them to more than one node (Paul et al., 2018).

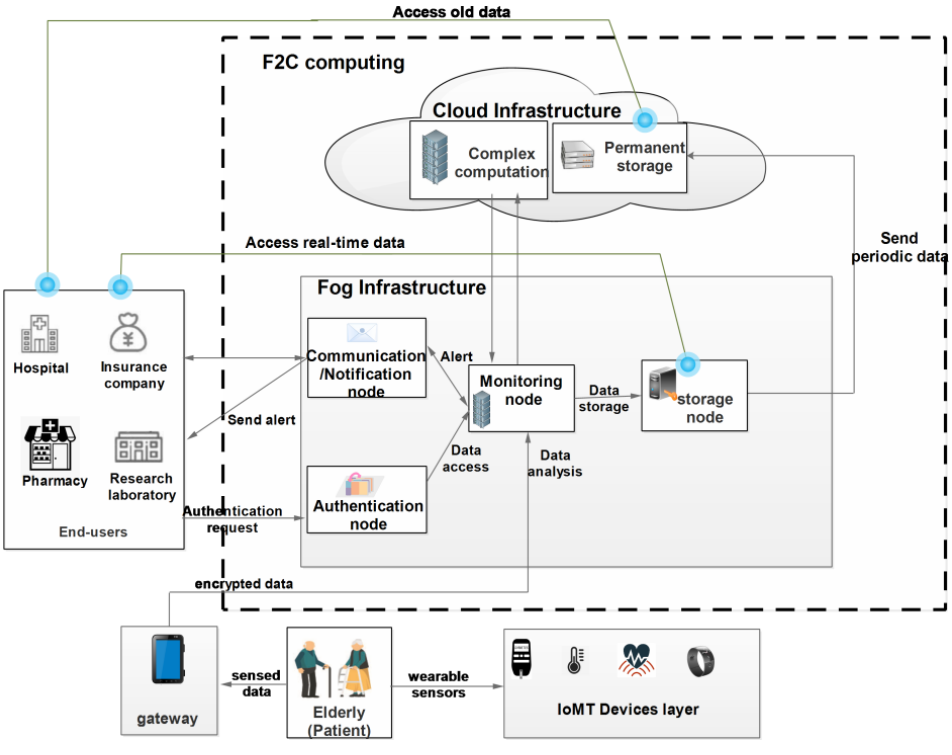
Compared to cloud computing, fog computing is a decentralised computing infrastructure that enhances security because of its proximity to the end devices (Guan et al., 2018; Rahmani et al., 2018). The main challenge of fog computing is to sort out the sensitive data related to the elderly's health by providing real-time processing (Gu et al., 2015; Hassen et al., 2019) with strict latency requirements (Baktyan and Zahary, 2018; Silva et al., 2019) and decreasing the security gaps.

Therefore, to address the security limitations of the cloud-based healthcare solutions, we propose in this paper the F2C computing model that solves the HIPAA privacy and security issues with remote elderly monitoring.

3 System model and design goals

In our framework, the older persons are monitored in real-time permitting different users (doctors, nurses, pharmacists, researchers, etc.) to access health data at any time and from anywhere (Mancy and Vigila, 2022).

Figure 1 System overview (see online version for colours)



3.1 System model

The architecture of our system is composed of the following layers: the IoMT devices layer, the gateway layer, the end-user layer, and the F2C computing layer, as presented in Figure 1.

- *IoMT devices layer* – Includes several types of wearable sensors such as blood pressure sensors, body temperature sensors, etc. Likewise, it can include different sensors embedded in a smartphone. The IoMT devices are allowed to initiate the process by sensing and collecting medical data. Data sensed are compared with the previous data value, only the difference data is transmitted to the gateway to minimise the number of packets circulating in the network and save sensors and mobile energy.
- *End-user layer* – The end-user has different privileges under diverse situations. This layer includes all remote users who assist the elderly such as physicians, nurses, pharmacists, and family members.
- *Gateway layer* – Plays a key role in our model by bridging the gap between the IoMT devices layer and the F2C computing layer. It is based on the mobile phone and used to collect and process the sensed data, then perform the encryptions of health records. The resulting data are transmitted to the F2C computing layer.
- *F2C computing layer* – Consists of two sub-layers:

a Fog computing

It is used to perform filtering, storing, analysing, and processing of encrypted medical data in real-time. Fog computing is composed of the following nodes:

- Authentication node – the authentication phase is crucial in the healthcare domain, it plays a significant role in REM systems to protect patient's privacy and security.
- Temporary storage node – this node provides transient storage of the encrypted data and sends periodic data to the cloud for permanent storage.
- Monitoring and notifications node – the aim of this node is to analyse data, prevent and detect elderly diseases, and provide useful information about the elderly. In addition, it sends notifications to end-users in the case of an emergency.
- Communication node – through this node, all end-users can collaborate securely, and work together to improve the elderly's health.

b Cloud computing

This sub-layer is responsible for the permanent storage and the execution of tasks that the fog sub-layer is unable to manage. Furthermore, it is introduced to manage larger and more complex healthcare data in the IoMT environment.

3.2 Design goals

According to the system model, our design goal concentrates on proposing a secure, efficient, and privacy-preserving medical data scheme.

- *Security:* The proposed schemes should enable strong confidentiality in the data transmission.
- *Efficiency:* The proposed system should support the real-time transmission of medical data from a huge number of IoMT devices.
- *Privacy preservation:* An attacker should not have access to patients' personal data during system communications. Even if several IoMT devices cooperate with each other, they should not infer other patients' private data.

4 Security model

4.1 Lightweight security scheme (L2S)

To ensure the security and privacy required by HIPAA regulations and provide medical data sharing without violating HIPAA compliance, all medical records including personal and electronic health data must be encrypted before sharing and storing them. In this context, we propose a L2S model. The L2S system is a hybrid algorithm that incorporates the advantages of two encryption schemes, the elliptic curve cryptography (ECC) (Goudarzi et al., 2022) and the advanced encryption standard (AES) (Abdullah, 2017), in terms of encryption and decryption time, security, key management, and key length (Hafsa et al., 2017).

This hybrid algorithm was proved to be lightweight because the key generation time was calculated as the lowest in comparison with other encryption algorithms (Habib et al., 2018).

4.1.1 AES-ECC hybrid algorithm

Our hybrid encryption scheme is divided into two parts: plaintext encryption and key encryption. ECC is the most appropriate technique to use along with AES to get the data secured from unauthorised use (Hafsa et al., 2017). ECC will generate two keys, public and private, that will be used by the AES algorithm. The data encryption will be done using the AES symmetric key. Then the AES symmetric key is encrypted using the ECC's public key. For data decryption at the receiver end, it is the reverse of the encryption process. First, the encrypted AES key is decrypted with the ECC algorithm. Then, the encrypted data is decrypted by the AES key.

The main reason for using AES and ECC together is because AES has major issues in key exchange as it has the same shared key for both encryption and decryption (Basnet et al., 2019). In addition, the hybrid encryption technique provides maximum strength by using the lowest possible energy in the IoMT devices, reducing the time needed for encrypting the message and reducing the amount of energy required for the sensor (Basnet et al., 2019).

a Public key generation using ECC
- Select any number n as the prime number.
- Select any number for the generation of the public key as P where $P < n$.
- Compute the point on the curve as G where $G > n$.
- Calculation of public key is: $PK = P*G$.

b Encryption phase
- An AES key K is chosen.
- Encrypt data (D) using AES key K.
- Then, AES key K is encrypted using the ECC algorithm, generates (K_e), and add it to the ciphertext (D_e).
- The encrypted data (D_e) and AES encrypted key (K_e) are transmitted to the fog storage.

c Decryption phase
- The encrypted AES key (K_e) is decrypted with ECC algorithm.
- Then, the encrypted data (D_e) is decrypted by AES algorithm using key K.

4.2 Case study: fall detection algorithm

To illustrate the different features of our system, we describe a case study in which medical data of the elderly are managed through our framework. Fall in the elderly population is one of the most important monitoring cases that we can study. When a fall has happened, the IoMT devices layer collects and sends the acceleration data to the gateway (mobile phone) (Saidi et al., 2019). The gateway will generate an AES symmetric key and encrypt all the personal and medical data. The AES symmetric key

will then be encrypted using the patient's ECC public key. The encrypted data contents and encrypted symmetric key will then be sent to the fog for storage.

To share the data with a geriatrician, the gateway will partition the patient's ECC private key into 2 random parts. The first partition will be sent to the fog storage and the second one will be sent to the geriatrician. By doing this, the untrusted user has no knowledge of the full private key. When the geriatrician receives the notification, he sends an access request to the authentication node. If the request is accepted, the fog partially decrypts the AES symmetric key using the partial key supplied by the gateway and sends the encrypted data contents and partially decrypted symmetric key to the geriatrician. The doctor uses the ECC partial key received from the gateway to fully decrypt the symmetric key and finally decrypt the data contents. Thus, the geriatrician can check the fall parameters such as the elderly location, and then he uses the communication node to call an ambulance.

5 Security analysis

The main aim of the proposal is the safety issue for the confidentiality and the privacy of the medical data stored in the F2C storage. The proposed work is hybrid in nature, which contains two stages.

5.1 Confidentiality

L2S hybrid algorithm enables strong confidentiality in the data transmission for IoMT. We adopt two-level encryption to guarantee the confidentiality of medical data since a good encryption scheme should resist all kinds of known attacks. In our proposed approach, the data is fully encrypted with the help of AES-ECC methods. Therefore, if an attacker gets access to the uploaded file, this file will be useless because the information was already encrypted and the attacker has no knowledge of the AES-ECC keys.

Also, the hybrid algorithm protects sensitive data from unauthorised access and attacks. It provides authentication, enhanced time, and validation of data integrity. So, using this hybrid approach, sharing and accessing the data is secure.

5.2 Privacy

Our scheme can protect patients' privacy against the L2S. During the communication and data transmission process, the attacker cannot learn any personal information about the patient because we also utilise AES-ECC encryption to protect personal data. This will resist any attacks from both outsiders and insiders attempting to obtain sensitive data without permission. The patient's privacy is protected on top of the security for health data.

6 Performance evaluation

In this section, we discuss some simulation results showing the impact of our proposed framework-based F2C solution on facilitating the remote monitoring of elderly people

without violating HIPAA compliance. We have used the FogWorkflowSim (Liu et al., 2019) simulator to demonstrate the benefits of deploying our framework on fog computing instead of cloud computing.

6.1 Simulation setup

FogWorkflowSim simulator runs on a desktop computer with the following characteristics: Intel core i7-6500U, CPU 2.50 GHz, 8 GB RAM, and Microsoft Windows 10 OS. It is developed in Java JDK 1.8.

FogWorkflowSim can:

1 Setup a simulated F2C computing environment.

2 Analyse and compare the performance of different computing models with the following performance metrics: time, energy, and cost.

To store the performance metrics and computation techniques, many libraries are used like all-in-fog, all-in-cloud, and simple. These libraries include many workflow scheduling algorithms such as MinMin, MaxMin, first come first serve (FCFS), RoundRobin, particle swarm optimisation algorithm (PSO), and genetic algorithm (GA) (Liu et al., 2019).

In our experiments, the Montage workflow has been used to evaluate the impact of a diverse number of tasks performed in cloud and fog computing based on the following performance metrics: latency, energy, and cost.

6.2 Results and discussion

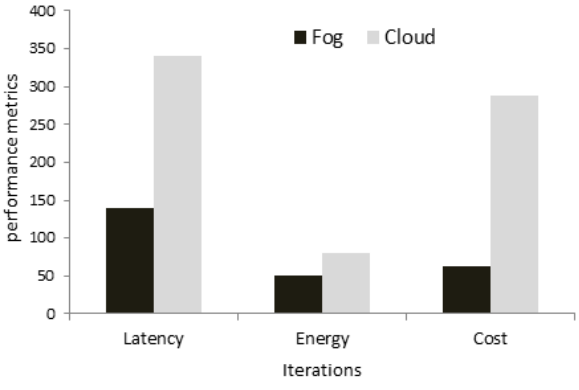
In our F2C environment, we consider the infrastructure based on one fog computing, one cloud computing, and five IoMT devices.

A summary of experimental results on latency, energy consumption, and cost consumption in both fog and cloud computing is shown in Figure 2. We can observe that using the fog layer reduces the latency, energy consumption, and cost when compared to using only cloud computing, as illustrated in Table 1.

Table 1 Comparison of performance parameters for two different environments

	Average latency (s)		*Average energy consumption (Joules)*		*Average cost ($)*
	Our model	*Gill et al. (2019) model*	*Our model*	*Gill et al. (2019) model*	*Our model*
Cloud computing	0.337	24.33	79.11	101.30	288
Fog computing	0.138	8.30	48.58	51.10	63

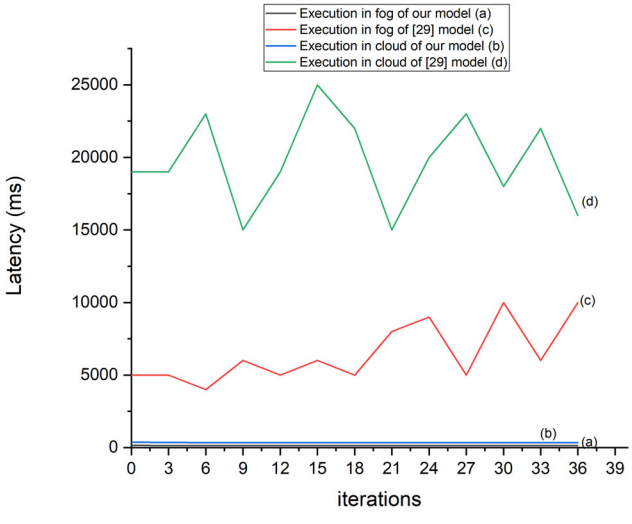
Figure 2 Summary of experimental results



We have also compared the performance evaluation of our scheme with those of the (Gill et al., 2019) scheme. The authors proposed a model that manages the data of heart patients. They have used the iFogSim toolkit to analyse the performance of the proposed model in a fog-enabled cloud environment.

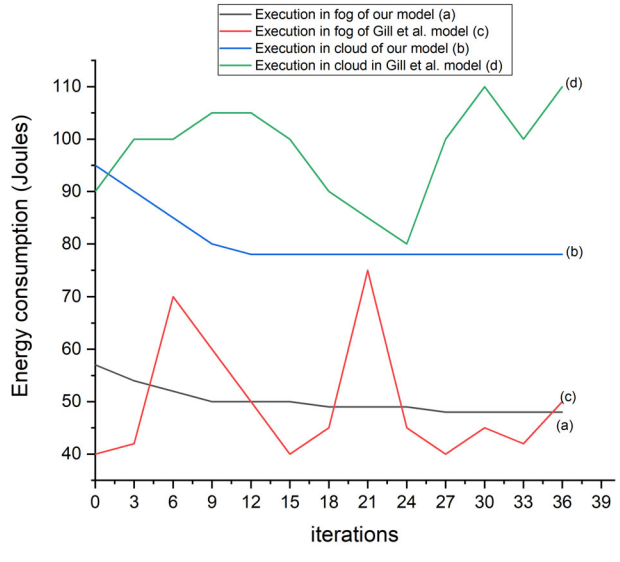
We notice in Figure 3(a) that fog performs better than the cloud in terms of latency; it reduces 41% average latency as compared to the cloud. Also, we observe that the latency computed by the simulator used in our model is less than the latency computed in Gill et al. (2019) model.

Figure 3 (a) Latency comparison of fog and cloud computing (b) Energy consumption comparison of fog and cloud computing (c) Cost comparison of fog and cloud computing (see online version for colours)

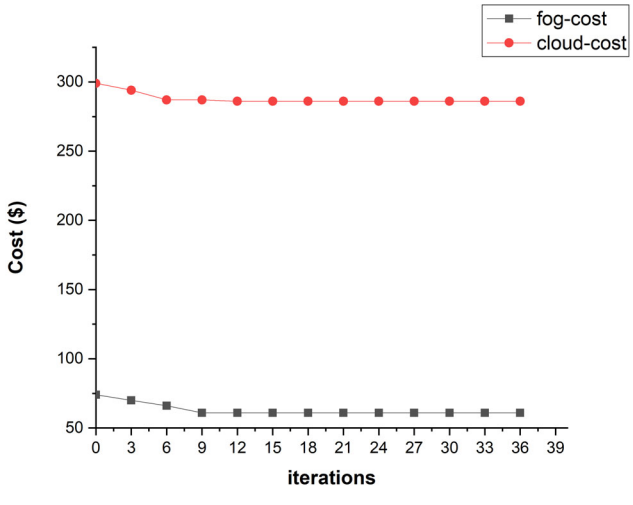


(a)

Figure 3 (a) Latency comparison of fog and cloud computing (b) Energy consumption comparison of fog and cloud computing (c) Cost comparison of fog and cloud computing (continued) (see online version for colours)



(b)



(c)

Figure 3(b) describes the consumption of energy for fog and cloud environments to process different numbers of tasks launched by sensor patients. Fog reduces 44% of average energy consumption as compared to the cloud. From the results, we observe that the energy consumption computed by the simulator used in our model is less than the energy consumption computed in Gill et al. (2019) model.

Figure 3(c) shows the results on tasks execution cost. We can note that the execution cost in fog computing is lower than the cloud. This shows that fog computing is the better one for cost optimisation.

From the simulation results, we notice that the proposed scheme is better than others in terms of latency, energy consumption, and cost. Furthermore, it shows the efficiency of using fog for data processing and cloud computing just for storage. These simulation results indicate the impact of our proposed F2C based solution aiming to better and faster make decisions regarding the illness of elderly people.

7 Conclusions and future work

Our paper proposes a framework for elderly health monitoring systems based on the fog to cloud computing. F2C computing is a new paradigm that ensures high computing and low latencies, as well as enhances the security and privacy of personal and electronic health data as recommended by HIPAA. Therefore, this research study aims to setup approaches to boost the security of medical data and the privacy of personal data in the F2C environment. For this reason, a L2S approach was proposed based on the AES-ECC hybrid protocol. The performance of the model is evaluated using the FogWorkflowSim toolkit, which demonstrates that fog computing increases the efficiency of the entire system. In our future direction, perspectives will focus more on achieving effective solutions to preserve elderly big data privacy. To go further, we will try to solve the problem of privacy approaches using blockchain technology by implementing a decentralised access control scheme to secure access to medical data.

References

Abdullah, A.M. (2017) 'Advanced encryption standard (AES) algorithm to encrypt and decrypt data', *Cryptography and Network Security*, Vol. 16, No. 1, pp.1–11.

Ahmid, M., Kazar, O. and Kahloul, L. (2022) 'A secure and intelligent real-time health monitoring system for remote cardiac patients', *Int. J. Medical Eng. Informatics*, Vol. 14, No. 2, pp.134–150.

Almeida, A., Fiore, A., Mainetti, L., Mulero, R., Patrono, L. and Rametta, P. (2017) 'An IoT-aware architecture for collecting and managing data related to elderly behavior', *Wireless Communications and Mobile Computing*, Vol. 2017, 17pp, Article ID: 5051915.

Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R.J. and Wills, G.B. (2017) 'Integration of cloud computing with internet of things: challenges and open issues', in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, pp.670–675.

Baktyan, A.A. and Zahary, A.T. (2018) 'A review on cloud and fog computing integration for IoT: platforms perspective', *EAI Endorsed Transactions on Internet of Things*, Vol. 4, No. 14, p.156084.

Basnet, A., Alsadoon, A., Prasad, P.W., Alsadoon, O.H., Pham, L., Elchouemi, A. (2019) 'A novel secure patient data transmission through wireless body area network: health tele-monitoring', *International Journal of Communication Networks and Information Security*, Vol. 11, No. 1, pp.93–104.

Farahani, B., Firouzi, F., Chang, V.I., Badaroglu, M., Constant, N. and Mankodiya, K. (2018) 'Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare', *Future Generation Computer Systems*, Part 2, Vol. 78, No. 2, pp.659–676.

Fiore, A., Caione, A., Zappatore, D., De Mitri, G. and Mainetti, L. (2018) 'Deploying mobile middleware for the monitoring of elderly people with the internet of things: a case study', *Cloud Infrastructures, Services, and IoT Systems for Smart Cities. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Vol. 189, pp.29–36, Springer, Cham.

Gill, S.S., Arya, R., Wander, G. and Buyya, R. (2019) 'Fog-based smart healthcare as a big data and cloud service for heart patients using IoT', *Springer Nature Switzerland AG 2019*, pp.1376–1383.

Goudarzi, S., Soleymani, S.A., Anisi, M.H., Azgomi, M.A., Movahedi, Z., Kama, N. and Khan, M.K. (2022) 'A privacy-preserving authentication scheme based on elliptic curve cryptography and using quotient filter in fog-enabled VANET', *Ad Hoc Networks*, 1 April, Vol. 128, p.102782.

Gu, L., Zeng, D., Guo, S., Barnawi, A. and Xiang, Y. (2015) 'Cost efficient resource management in fog computing supported medical cyber-physical system', *IEEE Transactions on Emerging Topics in Computing*, Vol. 5, No. 1, pp.108–119.

Guan, Y., Shao, J., Wei, G. and Xie, M. (2018) 'Data security and privacy in fog computing', in *IEEE Network*, Vol. 32, No. 5, pp.106–111.

Guan, Z., Yang, T. and Du, X. (2015) 'Achieving secure and efficient data access control for cloud-integrated body sensor networks', *International Journal of Distributed Sensor Networks*, Vol. 11, No. 8, p.101287.

Habib, M.A., Ahmad, M., Jabbar, S., Ahmed, S.H. and Rodrigues, J.J. (2018) 'Leaiot: a lightweight encryption algorithm toward low-latency communication for the internet of things', *IEEE Consumer Electronics Magazine*, Vol. 7, No. 6, pp.1–7.

Hafsa, A., Alimi, N., Sghaier, A., Zeghid, M. and Machhout, M. (2017) 'A hardware-software co-designed AES-ECC cryptosystem', *IEEE International Conference on Advanced Systems and Electric Technologies*, pp.50–54.

Hassen, H.B., Dghais, W. and Hamdi, B. (2019) 'An e-health system for monitoring elderly health based on internet of things and fog computing', *Health Information Science and Systems*, Vol. 7, No. 1, pp.1–9.

Kahani, N., Elgazzar, K. and Cordy, J.R. (2016) 'Authentication and access control in e-health systems in the cloud', *IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp.13–23.

Kharel, J., Reda, H. and Shin, S. (2017) 'An architecture for smart health monitoring system based on fog computing', *Journal of Communications*, Vol. 12, No. 4, pp.228–233.

Liu, X., Fan, L., Xu, J., Li, X., Gong, L., Grundy, J. and Yang, Y. (2019) 'FogWorkflowSim: an automated simulation toolkit for workflow performance evaluate on in fog computing', *34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pp.1114–1117.

Mancy, L. and Vigila, SM. (2022) 'Protection of encrypted medical image using consent based access control', *International Journal of Medical Engineering and Informatics*, Vol. 14, No. 1, pp.43–51.

Masip-Bruin, X., Marín-Tordera, E., Tashakor, G., Jukan, A. and Ren, G. (2016) 'Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems', in *IEEE Wireless Communications*, Vol. 23, No. 5, pp.120–128.

Paul, A., Pinjari, H., Hong, W.H., Seo, H.C. and Rho, S. (2018) 'Fog computing-based IoT for health monitoring system', *Journal of Sensors*, 22 October, Vol. 2018, 7pp, Article ID: 1386470.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. and Liljeberg, P. (2018) 'Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach', *Future Generation Computer Systems*, Part 2, Vol. 78, pp.641–658.

Saidi, H., Labraoui, N., Ari, A.A.A. and Bouida, D. (2020) 'Remote health monitoring system of elderly based on fog to cloud (F2C) computing', *IEEE International Conference on Intelligent Systems and Computer Vision (ISCV)*, pp.1–7.

Saidi, H., Labraoui, N., Ari, A.A.A., Semahi, I. and Mamcha, B.R. (2019) 'Real-time aging friendly fall detection system', *IEEE International Conference on Image and Signal Processing and their Applications (ISPA)*, pp.1–6.

Shahina, S., Minni, G. and Yasin, S. (2016) 'Sharing personal health records in cloud with scalable and secure using ABE', *International Journal of Emerging Technology in Computer Science & Electronics*, Vol. 23, No. 8, p.86.

Silas, S. and Rajsingh, EB. (2019) 'A novel patient friendly IT enabled framework for selection of desired healthcare provider', *International Journal of Medical Engineering and Informatics*, Vol. 11, No. 1, pp.14–40.

Silva, A., Gibeon, S., Aquino, J., Sávio, R., Melo, M. and Egídio, D.J.B. (2019) 'A fog computing-based architecture for medical records management', *Wireless Communications and Mobile Computing*, Vol. 2019, p.16, Article ID: 1968960.

Tao, J. and Shuijing, H. (2016) 'The elderly and the big data how older adults deal with digital privacy', *International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, pp.285–288.

Thilakanathan, D., Chen, S., Nepal, S., Calvo, R. and Alem, L. (2014) 'A platform for secure monitoring and sharing of generic health data in the cloud', *Future Generation Computer Systems*, 1 June, Vol. 35, pp.102–113.

US Department of Health and Human Services (2021) *Health Insurance Portability and Accountability Act* [online] https://www.hhs.gov/hipaa/for-professionals/index.html (accessed June 2022).

Verma, P. and Sood, S.K. (2018) 'Cloud-centric IoT based disease diagnosis healthcare framework', *Journal of Parallel and Distributed Computing*, 1 June, Vol. 116, pp.27–38.

Wang, H. (2018) 'Anonymous data sharing scheme in public cloud and its application in e-health record', *IEEE Access*, 22 May, Vol. 6, pp.27818–27826.

Wang, X., Bai, L., Yang, Q., Wang, L. and Jiang, F. (2019) 'A dual privacy-preservation scheme for cloud-based eHealth systems', *Journal of Information Security and Applications*, 1 August, Vol. 47, pp.132–138.

Wang, X., Ma, J., Xhafa, F., Zhang, M. and Luo, X. (2017) 'Cost-effective secure e-health cloud system using identity based cryptographic techniques', *Future Generation Computer Systems*, 1 February, Vol. 67, pp.42–54.

Yeh, L., Chiang, P., Tsai, Y. and Huang, J. (2015) 'Cloud-based fine-grained health information access control framework for lightweight-IoT devices with dynamic auditing and attribute revocation', *IEEE Transactions on Cloud Computing*, 12 November, Vol. 6, pp.532–544.

Yi, S., Hao, Z., Qin, Z. and Li, Q. (2015) 'Fog computing: platform and applications', in *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, pp.73–78, IEEE.

Zhang, C., Zhu, L., Xu, C. and Lu, R. (2018) 'PPDP: an efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system', *Future Generation Computer Systems*, 1 February, Vol. 79, pp.16–25.

Zuo, C., Shao, J., Wei, G., Xie, M. and Ji, M. (2018) 'A-secure ABE with outsourced decryption for fog computing', *Future Generation Computer Systems*, Vol. 78, No. 2, pp.730–738.