A Secure Fog-cloud Architecture using Attribute-based Encryption for the Medical Internet of Things (MIoT)

Suhair Alshehri, Tahani Almehmadi
Department of Information Technology
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah 21589, Saudi Arabia

***Abstract*—The medical internet of things (MIoT) has affected radical transformations in people's lives by offering innovative solutions to health-related issues. It enables healthcare professionals to continually monitor various medical concerns in their patients, without requiring visits to hospitals or healthcare professionals' offices. The various MIoT systems and applications promote healthcare services that are more readily available, accessible, quality-controlled, and cost-effective. An essential requirement is to secure medical data when developing MIoT architectures, as MIoT devices produce considerable amounts of highly sensitive, diverse real-time data. The MIoT architectures discussed in previous works possessed numerous security issues. The integration of fog computing and MIoT is acknowledged as an encouraging and suitable solution for addressing the challenges within data security. In order to ensure data security and to prevent unauthorized access, medical information is kept in fog nodes, and safely transported to the cloud. This paper presents a secure fog-cloud architecture using attribute-based encryption for MIoT to protect medical data. It investigates the feasibility of the proposed architecture, and its ability to intercept security threats. The results demonstrate the feasibility of adopting the fog-based implementation to protect medical data, whilst conserving MIoT resources, and the capability to prevent various security attacks.**

***Keywords*—MIoT; fog computing; cloud computing; ciphertext-policy; attribute-based encryption; security**

I. Introduction

Technology has transformed the lives of both individuals and organizations. Electronic healthcare services are considered to be an essential factor in the digital transformation of healthcare, helping to expand both the field and the kinds of healthcare services available, to improve the quality of healthcare services' delivery, and to reduce the cost associated with it [1].

The medical internet of things (MIoT) now leads technological advancements in healthcare, with the emergence of wearable and implantable medical devices and other technologies that enable the capture of medical data contributing to the considerable growth in this field. The value of the MIoT in the healthcare business is expected to increase to $534.3 billion by 2025, concurrent with an upsurge in the number of individuals with chronic conditions. According to the Grand View Research, this rise supports the need for technologically advanced medical devices [2].

The cost of healthcare services has increased significantly in recent years, although the costs concerned can be minimized via the industry's rapid digital transformation by improving operational efficiency [1]. Organizational and patient-care operations are enhanced when healthcare institutions are given real-time access to data generated by medical devices and MIoT-based devices. However, these advancements cause many challenges, particularly those related to the security and privacy of medical information [3].

Medical information is extremely susceptible to security threats [18], and the challenges imposed by privacy and security concerns hamper the widespread implementation of MIoT-based services. Thus, maintaining the confidentiality and safekeeping of information collected by MIoT devices remains a major research topic and must be prioritized, whether the information concerned is sent over the internet or stored in the cloud. Although the advent of fog computing resolved several issues that were apparent in traditional cloud-based architectures, medical data security remains a concern [4].

The current MIoT architectures that are developed in the literature to protect MIoT data fail to consider the limited capabilities of devices, such as storage and energy capacity, which affects the lifespan of the devices and their effectiveness in capturing and transmitting signals [4], [5], [7], [8], [9]. Thus, in order to ensure the adequate protection of medical information for MIoT services, a secure fog-cloud architecture is needed.

This paper develops a secure fog-cloud based architecture for the MIoT to ensure the security of medical data, while preserving the resources of these devices. It utilizes fog nodes to perform the encryption of the medical data, instead of MIoT devices using ciphertext-policy attribute-based encryption (CP-ABE). This is considered to be an ideal solution for protecting the privacy of medical data, as the data is encrypted by fog nodes before being stored in the cloud. The paper also considers minimizing the energy consumption of the processing overhead, improving the availability, and reducing the latency. The main contributions of this paper are as follows:

Our main contributions of this paper are as follows:

1) The design and development of a secure fog-cloud system using attribute-based encryption (ABE) for MIoT environments;

2) The definition of a set of requirements for achieving secure fog-cloud systems for MIoT environments;
3) The evaluation of the proposed system, in terms of a performance analysis, including network use, energy consumption, and security analysis.

This paper is organized as follows: Section II presents the fundamental details of the attribute-based encryption (ABE) employed in this paper. Section III discusses the current state of the art, focusing on the techniques that integrate ABE with fog computing. Section V-C defines a set of requirements for achieving secure fog-cloud architectures for MIoT environments. Section IV presents the proposed model, and Section V provides the evaluation results of the proposed model. Finally, Section VI concludes the paper.

II. Background

In widely distributed environments, especially the cloud environment, the symmetric encryption technologies with the same key for encrypting and decrypting suffer from key distribution and management issues. However, asymmetric encryption methods that use public and private keys lack computational efficiency [13], because the data owner is required to specify the identity of each recipient and their public key in advance, in order to implement the encryption algorithm, and to send the encrypted data to each recipient separately. This means the encryption process is repeated, according to the number of recipients. Since this type of individual scheme cannot be used to encrypt data once and send it to several users, ABE has emerged as a suitable solution for reducing the significant computational overhead of traditional encryption operations, while preserving data confidentiality and access control.

ABE is a novel and secure method for data sharing. It performs encryption and decryption while it obtains flexible access control [19], and was first introduced by Sahai and Waters [6]. It is an encryption mechanism that allows individuals to encrypt and decrypt data according to their attributes, such as job function, department, and specialty. ABE is an asymmetric cryptographic technique for one-to-many encryption that changed the traditional understanding of public-key encryption [6]. In traditional public-key encryption, the message is encrypted for a specific recipient using the recipient's public-key. In contrast, in ABE, one public-key is used to control access to encrypted data, using access policies and attributes [10].

Meanwhile, CP-ABE is a type of ABE that addresses the open challenge to organize access control and maintain the security of sensitive data, especially for internet of things (IoT) applications [13]. In a CP-ABE scheme, attributes are associated with the individual's secret key, and the encrypted message is associated with an access policy. Thus, authorized individuals can decrypt the message only if their secret keys and the associated attributes satisfy the decrypted message's access policy. This allows the storage of confidential data encrypted using CP-ABE on untrusted servers, without implementing authentication controls for the data access [13].

According to the extant literature, there are additional advantages to CP-ABE, compared to traditional cryptographic techniques [13], [20], [21], [22]. These advantages are as follows:

- It provides a high level of data confidentiality.
- It enables encrypted access control mechanism for access control applications.
- It reduces communication overload, because the generation of a user's secret key occurs only once.
- It achieves collusion resistance, because each attribute is associated with a polynomial or a random number that prevents legitimate users from colluding with each other.
- It supports user scalability; as the number of authorized users increases, the system can work efficiently.

A CP-ABE scheme consists of four fundamental algorithms: setup, encrypt, key generation, and decrypt. A detailed description of these algorithms can be found in [6].

III. Related Work

The model of the MIoT is believed to be tremendously valuable for remote health monitoring systems. The critical nature of the functions that use these systems requires a great degree of precision and accessibility. The lack of accessibility and punctuality, as well as the reliability of cloud-based IoT is a much debated topic, particularly regarding instances when the internet connection becomes undependable, and/or slower than expected. Furthermore, due to the centralized resource management and policies set by service providers that are related to the nature of cloud computing, the systems are susceptible to infiltration. An electronic healthcare system cannot be sustained with this vulnerability, due to the necessity to protect medical data. This necessitates the adoption of fog-based MIoT systems to overcome the limitations of cloud-based MIoT systems.

Fog computing is a distributed platform that generates a new layer between the cloud and MIoT devices that decreases the amount of processing done in the cloud, thereby allowing more efficient and effective service delivery. However, fog computing involves a number of security issues that are inherited from the cloud itself, including the ability to verify identities, to authenticate user inputs, to enforce access control, and to preserve privacy. Several procedures exist that can be applied to resolve the issues faced by fog computing.

In their work, Alrawais et al. [4] proposed a key exchange protocol based on the CP-ABE that can be employed to facilitate authentic transmissions between the set of fog nodes and the cloud, while maintaining confidentiality. To accomplish this goal, the researchers integrated digital signature techniques with a CP-ABE protocol, within which they studied the effectiveness of the protocol, in terms of both performance and security. To demonstrate its practicality, the protocol was implemented and contrasted with the certificate-based scheme. The results indicated that the protocol proposed was more practicable, as well as more effective than the certificate-based schema. However, the study did not examine the security requirements between the fog nodes and the end users.

Meanwhile, Vohra and Dave [5] held a similar view to Alrawais et al. [4], and investigated the privacy problems in fog computing, and the efficiency of the ABE schema suggested in [6]. The outcomes of the investigation demonstrated that ABE successfully guarded sensitive information, but that this method alone was not adequate, due to several security problems, such as backward and forward issues. Thus, a number of methods, such as re-encryption, were suggested by previous researchers, and Vohra and Dave [5] recommended a system that used CP-ABE for encryption and re-encryption to provide access control for the communication between the cloud and the fog. According to the findings of this study, the schema suggested demonstrated improved operation and protection. However, there was a need to reduce the number of messages generated to enhance system efficiency.

In contrast, Zhang et al. [7] presented an access control mechanism using a CP-ABE approach for the secure sharing of data that supported the outsourcing of fog computing for complex encryption and decryption operation. In this approach, a number of operations were implemented locally by the data owner and end user, such as implementing the symmetric algorithm on the data, and additionally encrypting or decrypting the symmetric key, partly via the CP-ABE algorithm. However, the study neglected the limited resources of smartphones, as these operations drain their energy and resources.

Meanwhile, Porwal [8] modified the CP-ABE protocol to enhance the secure exchange of content keys between the IoT, fog devices, and the cloud by exploiting the hierarchy in the attribute set of access policy to obtain a single integrated access policy. In order to reduce the cost of storage, to distribute encrypted content, and to reduce the number of decryption operations, a fog device and cloud received solely entitled content keys using one decryption operation. Despite the limited resources within IoT devices, the study assumed that they were capable of implementing advanced encryption standard (AES) to protect data, and that they shared the content keys used for encryption with fog devices and the cloud that might be unreliable and untruthful.

Finally, Fan et al. [9] considered the problem that when the access policy is sent clearly with the ciphertext it may reveal confidential information, although the CP-ABE scheme provides a secure access policy within the ciphertext (10). Thus, they developed an efficient multi-authority access control mechanism for the fog that supported the IoT. The scheme outsourced partial decryption, and transformed user attributes to anonymous aspects to preserve users' privacy. However, the scheme used fog devices for decrypting only while the complex CP-ABE encryption operations were performed by the data owner on end devices, an approach that is not suitable for IoT devices, because of their limited resources.

A. Data System Requirements in MIoT Environments

The concerns regarding data security, such as data scams, theft, forgery, or destruction, take precedence over the numerous advantages of utilizing fog computing in MIoTs. The primary emphasis of the present research was (1) the safeguarding of information when transporting from sensor network to fog, (2) the safekeeping of data during the transfer from fog to cloud, and (3) the security of data buffering in the fog, and the final storage in the cloud. To achieve these goals, a set of requirements were defined that were based on the previous literature in the field, and then the related work that utilized ABE for the fog-cloud architecture was compared, in terms of these requirements. The comparison is presented in Table I, and the requirements were defined as follows:

- **Confidentiality:** Sensitive data available to authorized users only.
- **Access Control:** Only authorized users can access the functionality and data within the device.
- **Availability:** Medical information can be accessed from anywhere within reach of the cloud services when needed.
- **Integrity:** Unauthorized users cannot change or alter the data.
- **Low-latency:** Protect data near its source; the delay in data protection increases the possibility of attacks on the system, and discloses patients' sensitive medical data.
- **Forward Security:** The prevention of nodes/users who have exited the database from retrieving the information exchanged.
- **Energy-Efficiency:** Preserve energy by transferring the encryption/decryption processes from the end devices to the fog nodes.

TABLE I. DATA SYSTEM REQUIREMENTS IN MIOT ENVIRONMENTS FOR DIFFERENT STUDIES

Design Requirements	References				
	[4]	[5]	[7]	[8]	[9]
Confidentiality	✓	✓	✓	✓	✓
Access Control	✓	✓	✓	✓	✓
Availability			✓		✓
Integrity	✓	✓	✓	✓	✓
Low-latency			✓	✓	✓
Forward Security		✓			✓
Energy-Efficiency					

The limited capabilities of MIoT devices, such as low power and dependence on limited-life batteries, impose restrictions on the kind of operations that can be utilized by these devices. As illustrated by the discussion of the previous studies in this field and Table I, authors of previous work relied on implementing cryptography operations in the IoT devices, which engendered the depletion of their limited resources. This was inconsistent with the energy efficiency requirement that this paper sought to attain, alongside the other security conditions.

IV. THE PROPOSED MODEL

Fog computing can offer a viable solution for handling various security issues in MIoT successfully [11], due to the existence of fog nodes on the network edge that gather confidential health-related data. This thereby provides data processing on the edge, decreasing the transfer of confidential information to the cloud, and supporting the protection of confidentiality by protecting the health-related information in

the fog nodes, and between the fog nodes and the cloud. A variety of procedures can be utilized between the fog nodes and the cloud to preserve data protection [12]. This paper proposes a secure fog-cloud architecture for MIoT to enhance the safety of user data, without affecting the efficient functioning of MIoT. Accordingly, it proposes that fog nodes are an appropriate platform for protecting medical data, due to their closeness to the end-user.

It was necessary to ensure the security requirements for the manipulation of medical data, including transmission and storage, that were identified and discussed in the previous section. Thus a scenario was examined in which the stream of data captured from MIoT devices was transmitted to cloud storage through fog nodes that implemented CP- ABE security. As an advanced type of encryption technology, and the most common type of ABE, CP-ABE addresses the open challenge for maintaining access control, and the security of sensitive data, especially for IoT applications [13]. In a CP-ABE scheme, the attributes are integrated with the user's secret key, and the encrypted text is integrated with an access policy. Therefore, only users with the correct attributes that meet the access policy can decipher the data. Hence, the main advantage of CP-ABE is that it enables the storage of confidential data on an untrusted server, with no need to implement authentication or access control mechanisms [13].

A. System Components

The proposed scheme contains five types of entities: data owner (DO), data user (DU), multiple fog nodes (FN) at the edge, cloud server (CS), and key authority (KA). The model is shown in Figure 1, and the description of the model entities is as follows:

- **Key Authority (KA)** This is responsible for generating cryptographic parameters, and creating the secret keys of all users, according to their attributes. Additionally, the KA has the duty of publishing a list of users (UL) to the FN, and updating the list when adding or revoking a user. This function is necessary to achieve forward security;
- **Data Owner (DO)** This is also referred to as a 'patient' in the proposed scheme. The DO uses MIoT sensors, which are miniature apparatuses with limited capabilities regarding storage, computing processing, and energy. Medical data is collected from the body of the patient and transferred to the fog node linked to the devices. To safeguard the transmissions between the medical devices and the fog, a secure sockets layer (SSL) is used to establish an encrypted channel between the MIoT and the fog node. In the case where the medical device and the FN fail to communicate, the MIoT devices seek the closest alternative FN to contact and transmit the medical data. Each MIoT device has a unique identifying attribute, called an internet protocol (IP) address. The MIoT device can transmit/collect information over the network using its IP address. The framework of the internet affords universal connectivity to medical devices in a heterogeneous network. In MIoT devices, the communication and data transmission is conducted via wireless technology. There are many aspects to consider when using wireless technology. Specifically, for MIoT devices, factors such as energy efficiency, cost-effectiveness, physical dimensions, and user-friendliness must be considered. Hence the suitable wireless specifications for MIoT include Bluetooth, RF4CE, IrDA, Wi-Fi, ZigBee, RFID, NFC, and ANT;
- **Fog Nodes (FN)** These are positioned at the edge of the network, and provide an array of amenities, such as minimal inactivity occasions and real-time functionality. They also control the performance of the encryption processes. Each FN has a unique identity that is connected to the cloud server by an IP network. It is important to note that the structural design of fog computing can facilitate MIoT devices in supplying efficient storage services, processing raw data near its source, and reducing network traffic to prevent congestion, all of which are critical characteristics of MIoT healthcare applications;
- **Cloud Server (CS)** This can store huge amounts of data, and has formidable computing power. It is responsible for storing encrypted data, as well as for processing requests for access to medical data from authorized healthcare providers.
- **Data Users (DU)** These are also referred to as 'healthcare providers', and are the parties who monitor a patient's condition, and request their data from the CS, in order to recommend the appropriate treatment.

B. Security Assumption

In order to simulate the security environment in this study's scheme, the following security assumptions were considered:

- It was assumed that MIoT sensors, FN, and the KA were within the same local network, and that the connection link between them was secure;
- The KA was trusted fully in the scheme, which meant that it would not leak data, or collude with any users;
- Each FN was trusted, but could be vulnerable to attack;
- The CS was a semi-trusted service provider. It was honest and ensured data security, but was curious, and therefore performed analysis to collect private information;
- The DU may collude to gain unauthorized data. It was assumed the revoked DU could not perform data decryption from the FN.

C. CP-ABE Functions

The CP-ABE functions adopted in the scheme were based on [10], where a full description of these algorithms can be found. The main functions included in the proposed solution were as follows:

- **Setup( )$\Longrightarrow$*MK,PK*:** The setup algorithm takes no input, and outputs the master-key (*MK*) and public-key (*PK*);

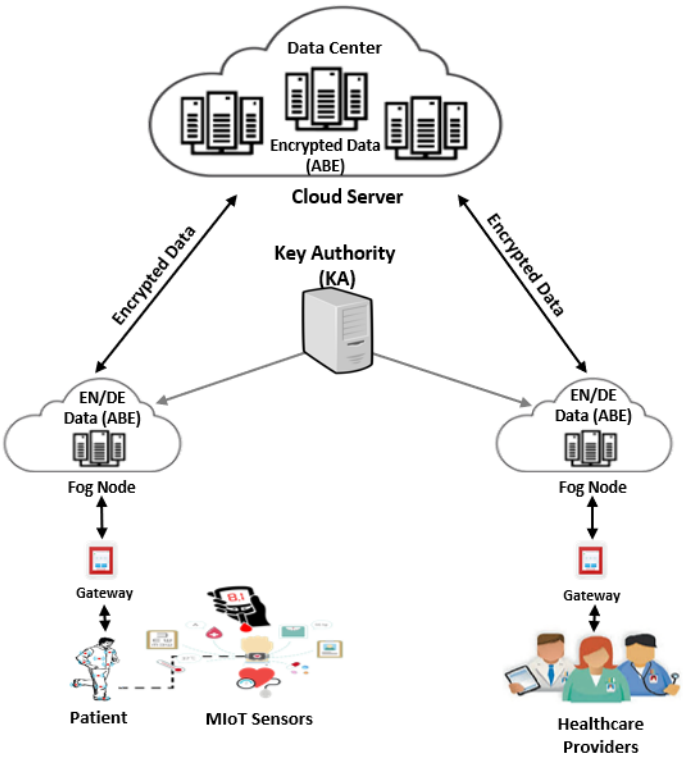

Fig. 1. The Proposed Architectural Design.

- **Encrypt(PK, $Data$, $\mathbb{A}$)$\Longrightarrow CT$:** The encrypt algorithm takes as input the PK, data, and the access-policy ($\mathbb{A}$) of the user. It enciphers the data and outputs a ciphertext (CT) in which only a user who owns a key with a set of attributes that fulfill the $\mathbb{A}$ can decipher the data;
- **KeyGen(MK, S)$\Longrightarrow SK$:** The key-generation algorithm takes as input the MK, and the set of attributes (S) of a user to produce the secret-key (SK) of this user;
- **Decrypt(PK, SK, CT) $\Longrightarrow Data$:** The decrypt algorithm takes as input the PK, SK, and the CT, which contains an $\mathbb{A}$. If the user attributes satisfy the $\mathbb{A}$, then the algorithm deciphers the CT and returns the original data ($Data$).

D. System Workflow

As shown in Fig. 2 the proposed system works in the following steps:

- **Step 1:** The system is initialized, with the KA executing the setup algorithm to generate the MK and the PK. The PK is broadcast to all FN that are connected to the local domain, while maintaining the MK. In addition, the UL is distributed to the FN, which carry the users' identities in the system, SK, S, and $\mathbb{A}$ that are used in the encryption/decryption operations;
- **Step 2:** When receiving the data from the MIoT sensors, the FN performs the encrypt algorithm, after authenticating the identity of the DO via checking the UL to ensure the presence of the user in the system, and to obtain the $\mathbb{A}$ that was used for the encryption. The CT is sent for storage in the CS;
- **Step 3:** If a DU requests data from the CS, the request passes through an FN that first verifies the user's identity from within the UL. This is to prevent users who have left the system from accessing the data, since the data request is sent only to the CS if the user is currently on the UL. Otherwise, the request is rejected;
- **Step 4:** The FN executes the Decrypt algorithm after receiving the CT based on the user's SK that was verified in the UL, then sends the original data to the data user.
- **Step 4:** The FN executes the decrypt algorithm after receiving the CT, based on the user's SK that was verified in the UL, then sends the original data to the DU.

V. Evaluation

In order to represent the proposed model, iFogSim [14], [15], [16] was used to create the physical components and to design the application model as a group of modules, namely the client module, security module, and storage module, that constituted the data processing elements. The client module received the raw ECG signals. It then performed the abstraction process on the signals, and ignored any inconsistent readings.

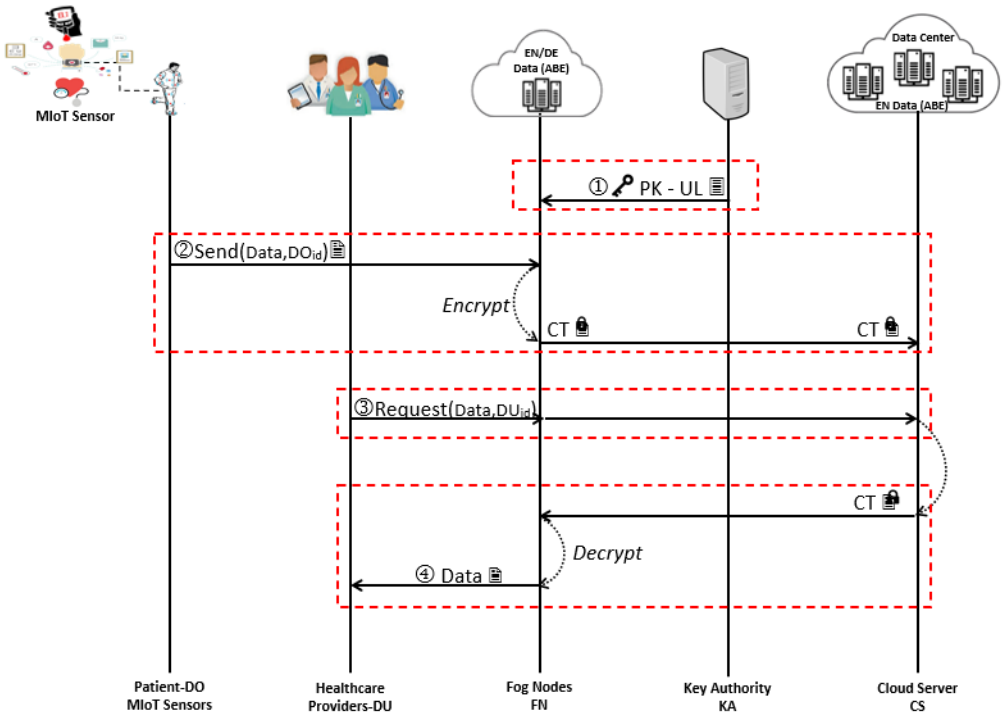

Fig. 2. System Workflow.

If the value of the signal sensed was consistent, it was sent to the security module. In the case of receiving information from the security module, it sent it to the DISPLAY actuator to display. The security module was responsible for protecting the medical data, performing encryption and decryption operations on the data received. The storage module represented the database in the cloud where the encrypted medical data was stored for patients, and recovered when needed.

In addition, this study used CP-ABE, an open-source Java implementation of the ABE scheme found in the paper by Bethencourt et al. [10], and developed by Wang et al. [17], to evaluate the efficacy of the model. Three different placement strategies were tested by implementing the security module, the main module of the present study, in the cloud, fog, or end device, as shown in Fig. 3. The feasibility of the proposed architecture was assessed, in terms of performance, network use, and energy consumption. Furthermore, the capability of the proposed system to deal with the related security vulnerabilities within the MIoT, the FN, and when information was transferred between the FN and the cloud, was examined.

The test was conducted on a local PC with a Windows 10 Home 64bit operating system, a 2.2 GHz Intel Core i7, and an 8GB Memory by Eclipse IDE for Java Developers. In order to test the performance on different sizes of topology, the number of FN was changed, and the number of end devices connected to each FN fixed was retained. Different sizes of network topology were simulated, starting with one FN with four connected end devices, and advancing to 20 FN with 80 connected end devices.

A. Performance Analysis

The various metrics that iFogSim showed were collected, and the results illustrated how different placement strategies for implementing a security module affected the system performance.

1) Time to Security Module:: The time it took to transfer the data from its source to the security module to implement the encryption was the most important factor in this research, as a delay in the transmission of data increased the possibility of the data being attacked. Fig. 4 shows the time taken to transfer the medical data to the security module, illustrating that it decreased significantly when applying the security module to fog devices or end devices. This was more apparent when the number of devices was increased.

The results of the implementation of a security module in the cloud were excluded from the study, which focused on performing a comparison between implementing the security module in the fog and in the end devices, as most of the previous research reviewed focused on implementing the security mechanism in the end devices, because such devices are close to the data source (end users), without considering the limited resources of these devices. In contrast, this study sought to move the security operations to the fog devices to preserve the end devices' resource consumption. As shown in Fig. 5, there was a very small difference in time of not more than six milliseconds between implementing the security module in the fog and in the end devices. This slight delay in data transfer would not affect the data security, especially since the

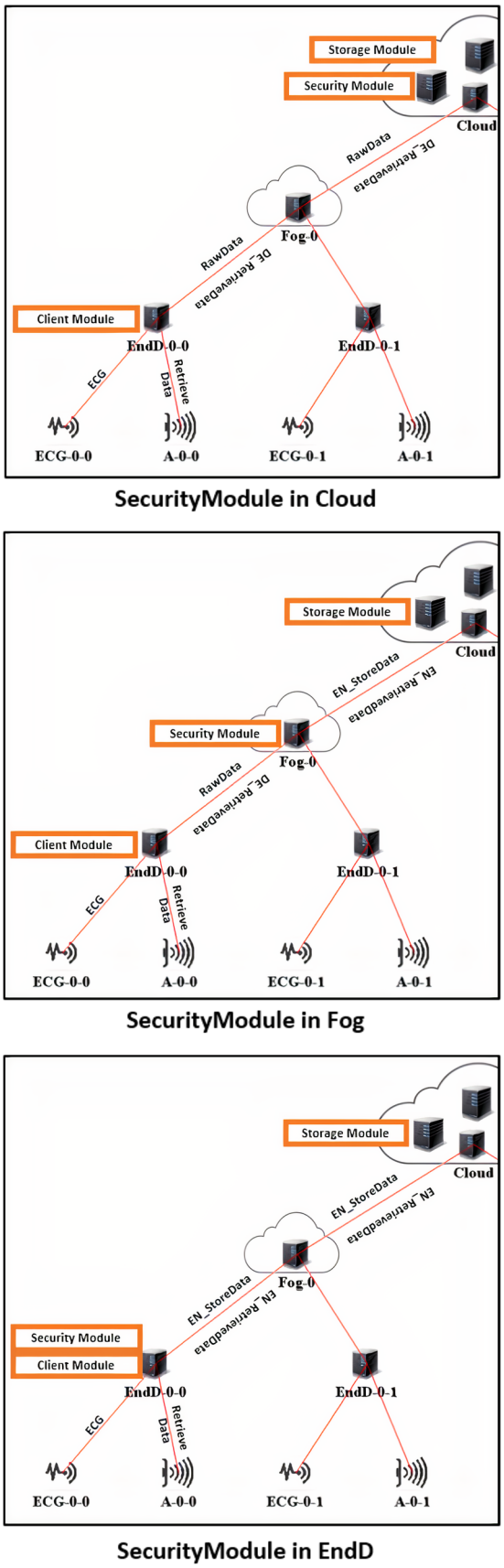

Fig. 3. The Different Placement Strategies.

FN and the end devices were in the same local network, and the connection between them was secure.

2) Network Use:: As shown in Fig. 6, the increase in the number of the connected devices greatly increased the load on the network, especially when implementing the security module in the cloud or end devices. When considering the security module's implementation strategy on the FN, the network use decreased significantly.

This result demonstrated that network congestion can be avoided when adopting a fog-based implementation, as the data is processed near the data source, thereby reducing the amount of information sent to data centers in the cloud significantly. Other placement strategies engender degradation and congestion in the network.

3) Energy Consumption:: MIoTs and end devices, or gateways, have limited processing capability, minimal storage space, and inadequate power, because they are often battery operated, and therefore lack sufficient power to secure medical data. This study sought to preserve the resource consumption, such as the energy resources of the MIoT layer, and consequently recorded various measurements of energy consumption in the end devices, according to different placement strategies for applying the security module.

Fig. 7 shows the average energy resource consumption in the end devices when implementing the security module in the cloud, end device, or FN. A significant reduction in energy consumption was observed in the case of the fog-based implementation that contributed to the preservation of the limited resources in the end devices.

B. Security Analysis

The security of the proposed model was analysed from the perspective of data confidentiality, fine-grained access control, collusion attack resistance, and forward secrecy.

1) Fine-grained Access Control:: This is a mechanism whereby legitimate users are given different access privileges to the data. Fine-grained access control was also attained in the model as it was a feature of the CP-ABE scheme that gave each legitimate user different access to the medical data concerned, according to the user's attributes and role.

2) Data Confidentiality and Privacy:: This is a basic and important requirement when using the cloud for data storage. In this model, it was accomplished using CP-ABE, whereby the medical data was encrypted near its source in the local network, before it was sent for storage in the remote data centers or the cloud. Therefore, no unauthorized user could access the content of the medical information stored there.

3) Collusion Attack Resistance:: In this type of attack, users combine their attributes to obtain unauthorized data illegally. These attacks can be conducted by system users seeking higher access rights, therefore, a system should prevent users from undertaking such attacks. To avoid this kind of attack, and to prevent users from combining their attributes in order to decipher the medical data, the proposed data protection scheme employed CP-ABE; since each attribute was associated with a polynomial or a random number, different users could not collude to obtain higher data access rights.

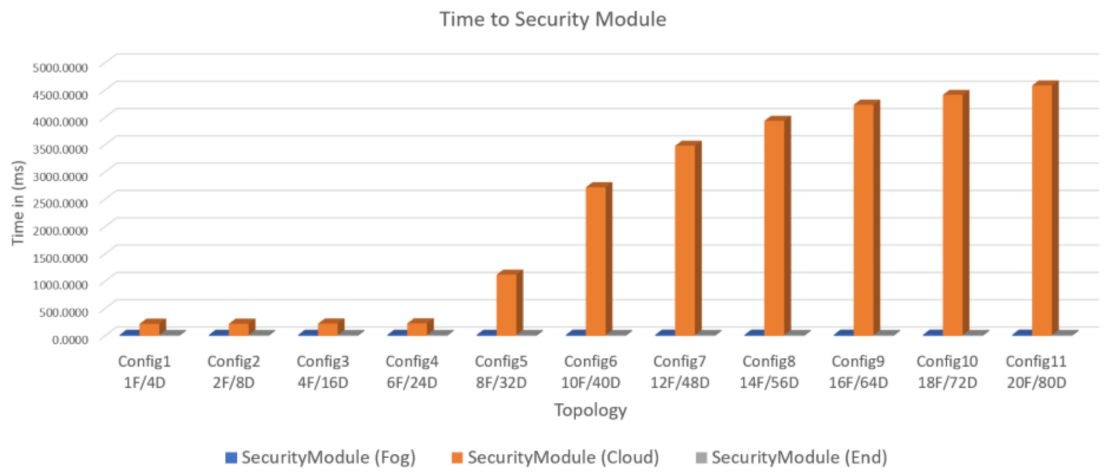

Fig. 4. Time to Security Module.

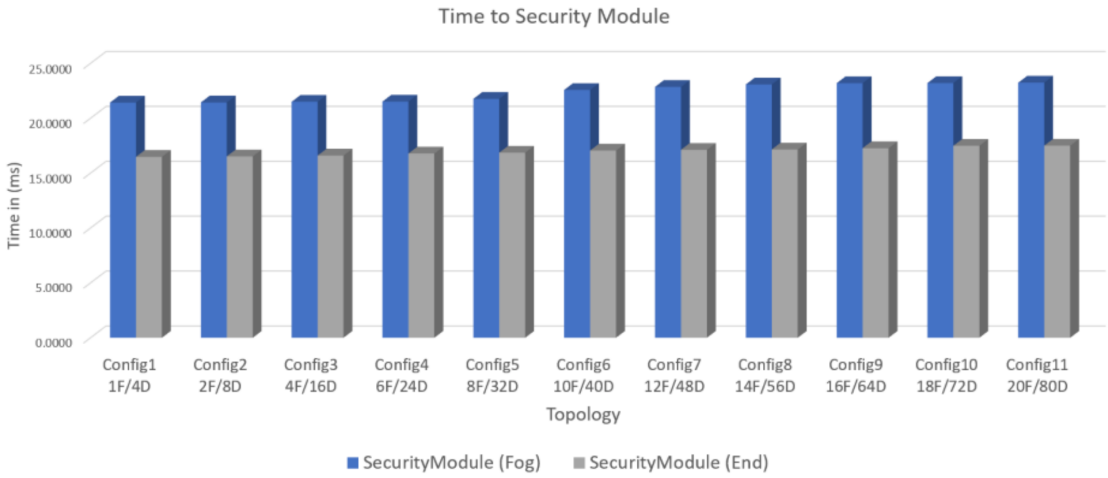

Fig. 5. Time to Security Module - The Comparison between Fog and End Device.

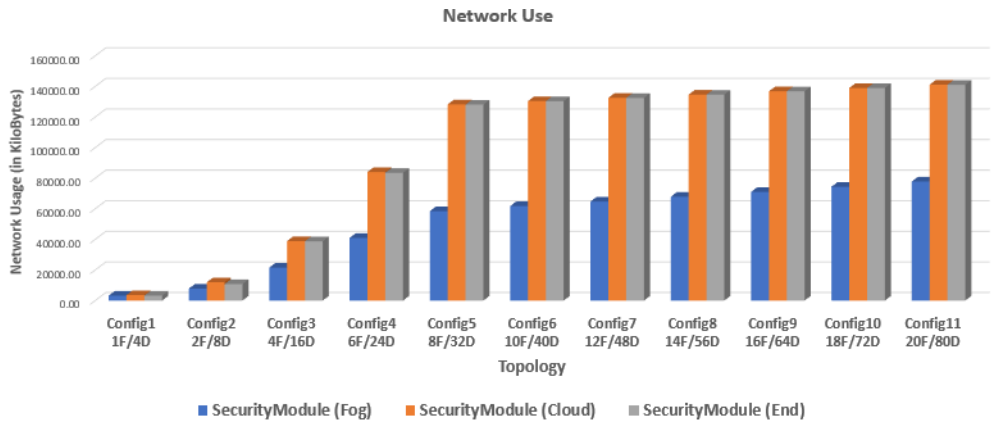

Fig. 6. Network Use.

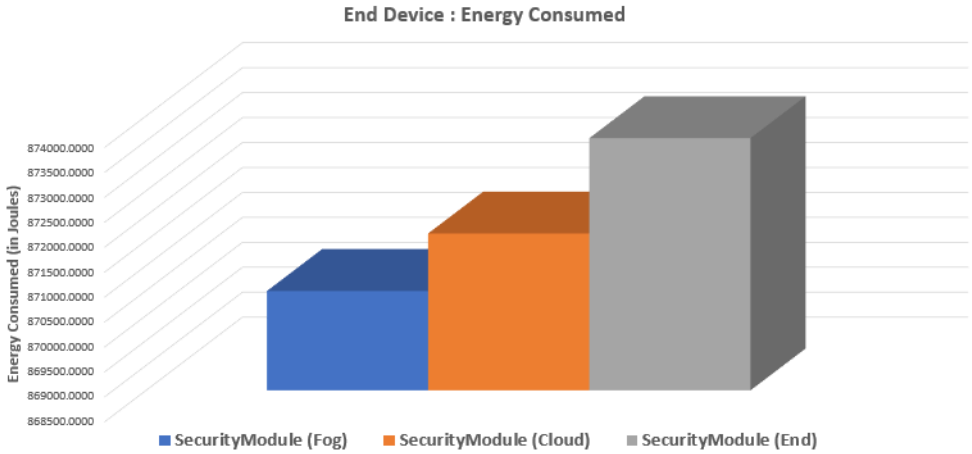

Fig. 7. Energy Consumption.

4) Forward Security:: This involves the prevention of any user who has been revoked from accessing and deciphering the medical data concerned. It was achieved in the proposed model by publishing the UL in the FN that contained the legitimate users with their set of attributes. Once a user left, the list was updated by the KA, thereby preventing the user who had left the system from accessing the medical data.

C. Comparison Analysis

The proposed model was compared with the previous works discussed in Section III in terms of the requirements presented in Section V-C. As previously mentioned in Section V-C, the related works as in [9] relied on MIoT devices to preserve data security and perform complex computations. This engenders the rapid depletion of the end device's energy and occupies it with other non-medical processes that may affect the efficiency of the sensors and the monitoring of vital parameters. In the proposed model, we employed FN to prevent costly computations, and thus, preserve the energy consumption of the MIoT devices. Concisely, the proposed model achieves all the predefined requirements including energy efficiency.

VI. Conclusion

This paper presented a fog-cloud system for the MIoT, in which the resource-limited end devices employed FN to prevent costly computations. It examined the feasibility of the proposed architecture, and the capability of the schema to manage security threats. The results demonstrated the benefits of adopting the fog-based implementation for protecting medical data and conserving MIoT resources, together with the ability to optimize network usage, and to avoid congestion, while reducing the amount of data sent to the data centers in the cloud significantly. It is hoped that the proposed model will encourage the adoption of MIoT devices and services, and thus encourage the healthcare industry to improve patient care services, and provide a better healthcare experience. For future work, we want to consider a technique with a wider range coverage to allow reducing the number of gateways. We also plan to conduct a real-time experiment to validate the proposed model.

References

[1] T. Khubone, B. Tlou, and T. P. Mashamba-Thompson, "Electronic Health Information Systems to Improve Disease Diagnosis and Management at Point-of-Care in Low and Middle Income Countries: A Narrative Review," Diagnostics, vol. 10,5, pp. 327, Multidisciplinary Digital Publishing Institute, 2020.

[2] K. H. Nam, D. H. Kim, B. K. Choi, and I. H. Han, "Internet of Things, Digital Biomarker, and Artificial Intelligence in Spine: Current and Future Perspectives," Neurospine, 16(4), 705–711, 2019.

[3] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare–a review and discussion," IEEE Access, vol. 5, pp. 9206–9222, IEEE, 2017.

[4] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," IEEE access, vol. 5, pp. 9131–9138, IEEE, 2017.

[5] K. Vohra and M. Dave, "Securing fog and cloud communication using attribute based access control and re-encryption," In: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 307–312, IEEE, 2018.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457–473, Springer, Berlin, Heidelberg, 2005.

[7] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," Future Generation Computer Systems, vol. 78, pp. 753–762, Elsevier, 2018.

[8] S. Porwal and S. Mittal, "HE3: A hierarchical attribute based secure and efficient things-to-fog content sharing protocol," Journal of King Saud University-Computer and Information Sciences, Elsevier, 2019.

[9] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy preserving access control scheme for fog-enabled IoT," Future Generation Computer Systems, vol. 99, pp. 134–142, Elsevier, 2019.

[10] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," In: 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 2007, pp. 321-334.

[11] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," In: International conference on wireless algorithms, systems, and applications, WASA 2015. Lecture Notes in Computer Science, vol 9204. Springer, Cham.

[12] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, IEEE, 2017.

[13] R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat, "Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption," Sensors, vol. 19, no. 7, p. 1695, Multidisciplinary Digital Publishing Institute, 2019.

[14] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," Software: Practice and Experience, vol. 47, no. 9, pp. 1275–1296, Wiley Online Library, 2017.

[15] I. Lera, C. Guerrero, and C. Juiz, "YAFS: A Simulator for IoT Scenarios in Fog Computing," IEEE Access, vol. 7, pp. 91745–91758, IEEE, 2019.

[16] R. Buyya; S. N. Srirama, "Modeling and Simulation of Fog and Edge Computing Environments Using iFogSim Toolkit," Fog and Edge Computing: Principles and Paradigms , Wiley, 2019, pp.433-465.

[17] J. Wang, "Java Realization for Ciphertext-Policy Attribute-Based Encryption," Computer Science College of Shandong University, 2012.

[18] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, Kumar R., and R. A. Khan, "Healthcare Data Breaches: Insights and Implications," Healthcare (Basel, Switzerland), 8(2), 133, 2020.

[19] Q. Huang, and L. Wang, and Y. Yang, "Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities," Security and Communication Networks, Hindawi,Volume 2017, Article ID 6426495.

[20] C. Lee, P. Chung, and M. Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments," International Journal of Network Security, Vol.15, pp. 231-240, 2013.

[21] R. N. Lakshmi, R. Laavanya, M. Meenakshi, and C. S. G. Dhas, "Analysis of Attribute Based Encryption Schemes," International Journal of Computer Science and Engineering Communications, Vol.3, Issue 3, pp. 1076-1081, 2015.

[22] S. Moffat, M. Hammoudeh, and R. Hegarty, "A Survey on Ciphertext-Policy Attribute-based Encryption (CP-ABE) Approaches to Data Security on Mobile Devices and its Application to IoT," In Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS '17). Association for Computing Machinery, New York, NY, USA, Article 34.