Pak. J. Engg. Appl. Sci. Vol. 25 July, 2019 (*p.* 89–100)

A Distributed Secure Framework for Sharing Patient's Data among IoMT Devices

M. Asad Bilal*, Muhammad Awais Hassan

Department of Computer Science and Engineering, UET Lahore, Pakistan

* **Corresponding Author:** Email: asadbilal4@gmail.com

Abstract

With encouraging the perspective of the IoT, Internet of Medical Things (IoMT) used different wearable devices and sensors for better quality patient care. It provides a more flexible way to monitor patient's profiles remotely and in real time as compared to the traditional offline healthcare system. However, there are data privacy challenges due to the absence of proper security mechanisms in low power computing devices. The limitation made the data vulnerable to hack and tamper when it transfers from one device to another. In available solutions, the devices send unencrypted data to a central server where it encrypts and forwards, on-demand, to requesting devices. There are two primary challenges in the approach: first, the data link is still vulnerable between the source device and central server; second, the response time of the server gets slower with an increasing number of devices. This paper proposes a secure and faster distributed method, which shares a patient's data from different IoMT devices with healthcare providers without the need for the centralized server. The research harnesses the power of other locally available IoMT devices that have the more computational capability. Our experimental results demonstrate that with the increase in a number of IoMT devices on the network, the percentage of encrypted data transmissions also increase since there are more chances to find a nearby secure device. Results further show that the average response time has been reduced from 0.6ms to 0.4ms using the proposed distributed vs centralized system.

Key Words: Internet of Medical Things, Public Healthcare, Security, Data Privacy, Encryption, Distributed computing

1. Introduction

According to market research (Alsubaei, Abuhussein, & Shiva, 2017), the healthcare IoT market sector is poised to reach $117 billion by 2020, and the exponential rise has given birth to the Internet of Medical things (IoMT). These days healthcare centers are equipping the patients with invasive and non-invasive IoMT devices to collect different physiological parameters like blood pressure, heart rate, and pulse rate. These devices preprocess the received signal and transmit that to the central server through Wi-Fi services (Ma, Wang, Yang, & Miao, 2017). Traditionally, centralized systems store the data which is transferred, on-demand, to the devices of doctors and health care centers. The sharing of a large amount of critical and confidential data through the hybrid cloud (using the private and public cloud) is raising significant security issues and challenges (Alasmari & Anwar, 2016).

Usually, the centralized systems provides data protection from unauthorized users through access control, encryption, and data anonymity (Oh & Kim, 2017). However, these traditional systems face three key challenges: low-key encryption, overloading of system resources, and heterogeneity of various keying techniques. About 70% of the IoMT devices have serious security vulnerabilities that make encryption a fundamental challenge to IoMT devices (Williams & McCauley, 2016). The limited resources such as the low battery, small memory space, and low processing power (M. M. Hossain, Fotouhi, & Hasan, 2015) are the primary reason behind the challenge.The second major issue with the centralized systems is that they have limited capacity to communicate with different devices (Alkeem, Shehada, Yeun, Zemerly, & Hu, 2017). With the increasing number of devices that communicate through the centralized server, the performance of the centralized server begins to downgrade.The third issue is that the IoT devices may have different security encryption techniques, and it is not possible for the server to convert the data in all possible encrypted formats (Singh, Sharma, Moon, & Park, 2017).

These security issues of IoMT devices are causing undesirable results in terms of trust deficit between the patient, hospital, and insurance companies. For example, patients' data can be vulnerable to hackers during cloud transfer or synchronization with interconnected devices in a centralized system because of the higher hop count

distance between the device and the central server. To avoid the threat, the sending device may ask to its nearby devices, with less hop count distance, for the encryption. The purpose of this research is to propose a framework to transfer data more efficiently and securely from one device to another device without the involvement of the central server where the devices can communicate directly with each other. More specifically, the following research questions have been asked.

- How to provide device-level encryption for secure data transmission between the IoMT devices and other digital devices?
- How to improve the efficiency of the IoT healthcare System?

We believe a network of IoMT devices with different capacities and capabilities can collaborate with each other and perform the tasks more efficiently than a centralized system. With reference to this hypothesis, the primary contribution of the paper is a proposal of a distributed architecture for the IoT based E-health systems that allow different devices to handshake, communicate, convert and take the services from each other for securing and fast transfer of the data between these devices.

The next section discusses the proposal of the architecture based on our hypothesis for a given problem statement. After that, we give the experimental design and results to evaluate the system. Next, the discussion section explains the results, and finally, the conclusion section concludes the paper.

2. Literature Review

(M. S. Hossain & Muhammad, 2016) proposed a cloud-based industrial IoT healthcare framework to transfer medical data securely from IoMT devices to medical professionals. This system protected the identities of the data using watermarking and signaled enhancement before sending it to the cloud. Later research revealed that watermarking is an old data securing technique, which fails when an opponent refines his knowledge on a presumably secret key.

(Alsubaei et al., 2017) discussed different IoMT device layer attacks at the network layer. A taxonomy presented for security and privacy of patient data in IoMT. Moreover, the risk assessment method also proposed in the paper to understand and measure the severity level for data sniffing. These attacks, like account hijacking and eavesdropping, happen due to the absence of cryptographic techniques.

(Alkeem et al., 2017) proposed a cloud based new healthcare system which provides different main security requirements like anonymity, authentication, accountability, confidentiality, integrity, and non-repudiation. Authors described that 70% of IoT devices have to face serious security issues due to the unencrypted network services and weak passwords. Moreover, the diversity of IoT devices is also a reason for data insecurity. Therefore, data encryption is essential before sending it to any network. (Tamizharasi, 2017) discussed three types of IoT healthcare providers (centralized, distributed, and cloud based) architectures. Authors revealed that due to the distributed nature of electronic health records, centralized architecture does not provide a better solution. Further, the distributed architecture supports the hospital and clinical management systems.

(Ghanavati, Abawajy, Izadi, & Alelaiwi, 2017) proposed a framework based on IoT infrastructure and provided the facility of remote patient's health status monitoring. Connectivity of WBAN using smartphones was made to cloud services for providing healthcare environment. However, there is energy consumption due to multi-hop transferring between devices and cloud. Security should be considered for remote healthcare monitoring in a distributed environment because data at the central place can be tampered easily.

. (M. M. Hossain et al., 2015) described the security issues of IoT devices regarding their less computing power. Hardware, software, and network level security limitations play an essential role in protecting IoT device data. According to the authors, there are some security computations, which require remarkable computing resources. Therefore, IoT devices cannot afford built-in encryption techniques. With the absence of any cryptographic technique, there is a severe chance of data exploitation by malicious attackers.

(Ahmad et al., 2016) presented a framework using fog computing as an intermediary between the end user and cloud. This framework helped in sharing healthcare information. Data privacy and security was preserved by introducing an integral component termed Cloud Access Security Broker. The purpose of this component was to implement different security policies on the cloud. Fog computing acts as a secure gateway between users and cloud.

(Baccarini et al., 2018) proposed a distributed blockchain based smart contract to

make and write records of all events on the blockchain for real time patient monitoring using smart devices. The limitation in this system rests in perfecting the timing of the transmissions. So, the system cannot be used for emergency response, because the delay increases response time. Therefore, a distributed system for healthcare is required to manage multiple requests efficiently. (Rahulamathavan, Phan, Rajarajan, Misra, & Kondoz, 2017) proposed a blockchain protocol for engaging attribute based encryption and providing end-to-end privacy-preserving IoT ecosystems in decentralized networks. Security achieved by blockchain and attributed based encryption, but it costs computational overheads.

(Yang, Zheng & Tang, 2017) proposed a secure and lightweight distributed IoT healthcare system. Data security was implemented using attribute based encryption with the facility of keyword searches to tackle the challenge of an accumulated effective data retrieval mechanism. However, the major drawback of attribute based encryption is reduced flexibility in revoking attribute.

(Liu et al., 2016) presented an implementation design that used the emerging family of Elliptic Curve library for providing security at distinct levels in IoT. The library has two implementation versions: one provided a high speed while the second one was the memory-efficient version. ECC provides security with low power consumption and less memory space.

(Chung & Park, 2016) proposed a PHR open platform for providing healthcare services to manage chronic disease. The platform collected the healthcare data and managed the records using distributed objects for continuous monitoring of healthcare readings and physical objects connected to WBAN sensors. Data is sent through a wireless channel, and it is secured through the distributed object group framework.

(Vucinic et al., 2014) proposed an architecture based on a secure channel using the soap application protocol. This paper provides new scalable security architecture for IoT that jointly provides end-to-end security (E2E) and access control. It decouples confidentiality and authenticity trust domains that intrinsically supports multicast, asynchronous traffic, and caching. (Chiang & Zhang, 2016) presented a survey for highlighting new security challenges to the IoT. Due to limited resources, the device is unable to perform massive cryptographic operations, and in the case of a centralized system, direct communication to the cloud is not possible. Many constrained devices in the IoT will not be able to support processing intensive remote attestation. Even when they can, forcing a large number of devices to perform remote attestation can result in prohibitively high cost and management complexity. It is stated that existing security solutions will no longer be enough for addressing many new security challenges in the emerging IoT.

(Alam, Chowdhury & Noll, 2011) proposed a functional architecture of the IoT framework to provide secure access. The components of the proposed architecture use semantic ontologies. The authors contributed a functional architecture of the IoT framework to add the intelligence in IoT. Ontologies as a semantic overlay (on top of 'Things') are used with a rule-based service access mechanism. These ontologies and machine-to-machine (M2M) technology offer the Interoperability of security.

(Zachariah et al., 2015) proposed an architecture that leverages the increasingly ubiquitous presence of Bluetooth Low Energy radios to connect IoT peripherals to the Internet. The worldwide network of smartphones provides connectivity and networking architecture for low-power wireless devices that better leverages the opportunities through interoperability between heterogeneous IoT devices. The proposed architecture uses standard on modern smartphones, to provide the primary link between low-power peripherals and capable smartphones. For the application-specific design of device phone interactions, they envisioned an open, two-prong gateway model. The first one leverages any smartphone as a temporary IP router and acts like a normal IP end host. Second, any phone could proxy a Bluetooth profile to the cloud on behalf of a device.

(Saied et al., 2013) proposed a system for trust management between the IoT nodes. The system induces nodes' past behaviors in distinct cooperative services that show how much trust can be put into a node for accomplishing a required task. Eventually, only the best partners proposed a cooperative service to a requesting node. In the presence of erroneous or malicious witnesses, their proposed system effectively fine-tunes nodes' trust levels.

(Alzghoul, 2016) proposed new web-centric middleware architecture to address the interoperability and security challenges in situations where the healthcare providers either rely partially (or completely) on paper-based health records or use local electronic health

records that lack interoperability. The proposed system intends to shift the integration complexity from healthcare providers to the central middleware stack and web services. As the middleware handles the data standards and code, the data can be tempered.

Table 1: Research Matrix Table

Research	Characteristics	IoMT Security	Centralized Security	Distributed Security	Authentication, Authorization
Ahmad et al. 2016	Security	Data protection	Data Protection-Fog computing	-	Access Control
Ghanavati et al. 2017	Remote Patient Monitoring	-	-	-	-
Rahulamathavan et al. 2018	Privacy & Security	Data Security	-	Data Security	Trust, Access Control
Yang, Zheng, and Tang 2017	Lightweight data recovery	Data Security	-	Data Security	Keyword based Access
Baccarini et al. 2018	Security with computational overhead	Data Security	-	Data Security	Trust, Access Control
Ekblaw et al. 2016	Security	Data security	Cloud Storage	-	Access Control
Bradley, El-tawab, and Heydari 2018	Tracking Solution	Localization of Healthcare Center Assets through IoT environment	-	-	Security Holes
Chen et al. 2016	Security	Data Security	Cloud Storage	-	Access Control
M. S. Hossain and Muhammad 2016	Security through watermarking the signals	Watermarked ECG signals	Cloud Data	-	Access Control
Chung and Park 2016	Healthcare services	Data security	-	Secure data transmission	Access Control
A Secure Distributed framework to share Patient's data in IoMT	Security with less response time	IoT Security	Encrypted Data Storage	Cryptographic data transmission	Trust access control

3. Proposed Method

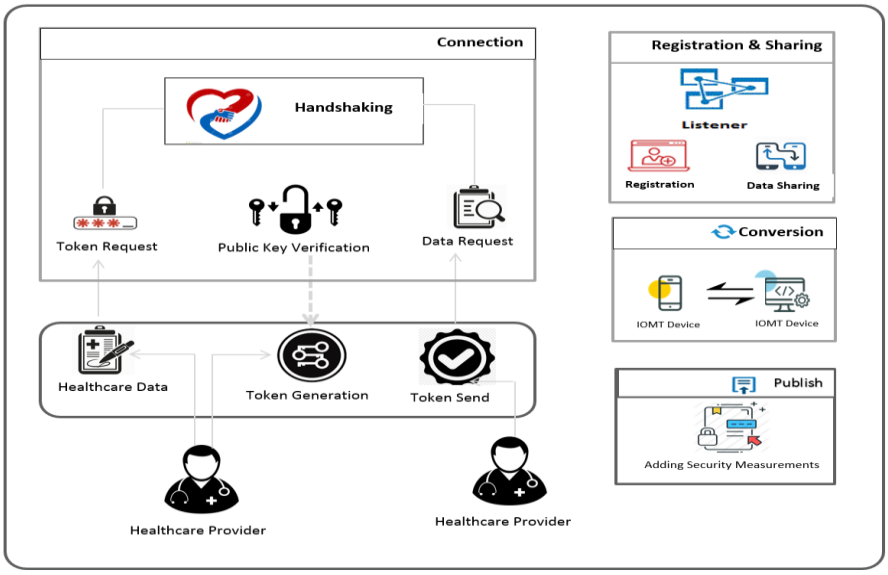

Fig. 1: Architecture diagram of Distributed bases IoMT healthcare system

The proposed system (Fig. 1) is a distributed framework for the security of IoMT device data, which comprises five modules. 1) Handshaking is the entry point that sends a request for data and connection between IoMT devices by sending and receiving tokens. 2) Listener validates the request and sends data if encryption techniques are the same on both the sender and receiver side. Whereas, the control register is also a sub part of the listener, which timely generates registration request and update all the nearby devices.3) An additional security layer, containing different cryptographic techniques, is added to deal with lightweight IoMT devices.

ECC technique suggested in combination with user defined attributes to access data. 4) Conversion applies the required encryption algorithm on data if the device has the capability.5) In the end, the publisher sends data directly to the requesting device and applies the HMAC/digital signature to validate the data coming from an authentic user. The detail of each module is given in the following sections:

A. Handshaking

The module (algorithm 1) deals with two types of requests: the token generation request (Algorithm 1.1) and the data sharing request (Algorithm 1.3). The token generation request requires a patient public key (PK) that he shares with a health care provider through the Universal Resource Identifier (URI). If PK of the patient is validated, a unique token is generated and forwarded to the requesting device that completes the handshaking of source and requesting devices. For the data sharing request (Algorithm 1.3), the response at the patient device is made by validating the token using Algorithm 1.4. Message body in algorithm 1 containing security technique (ST), request type (RT), and token(s) sent to the requesting device as output to establish a secure connection.

B. Listener

Control Registration, sub-module of the listener, initiates a registration request (Algorithm 2.1) after a specific time interval on each IoMT device, which registers the new incoming device on the network. Therefore, all the devices on the network send register requests to its nearby devices by sending its URI and capability (Security technique). The registration is made on the basis of the HOP count. IoMT device gets registers if the HOP count is low for the receiving device. Therefore, all the devices maintain a list of nearby devices and their capability. Secondly, the Listener component validates the incoming request in Algorithm 2.2 and share encrypted data if both IoMT devices are using the same security technique. Input to this component is provided by the handshaking component in the form of a message and token. This component validates the incoming token and checks for the security technique in which data requested. Listener shares data to the requesting IoMT device if and only if both the systems are securing the data using the same encryption technique. However, if there is a difference between both techniques or the device, the module unable to apply any encryption technique. Now, it uses distributed services. In distributed services, conversions are performed to apply the required security technique by using the list of nearby registered devices.

C. Conversion

It verifies whether the nearby device is capable of applying the required encryption technique for the requested IoMT device. The conversion request with data and token is forwarded to apply the required encryption technique. If the receiving device poses the required encryption technique, Algorithm 3 applies conversion. Otherwise, the request is denied if the available security technique does not exist. After applying the security technique, data is sent to the requesting device using the publishing method as an output.

D. Security Layer

The security layer is made up of different encryption techniques e.g., symmetric (DES, 3DES) encryption, Cipher-text policy attributes based encryption, and ECC (Elliptic Curve Cryptography). IoMT are low power computing devices, and some of them are unable to apply even simple encryption techniques; therefore, distributed security services are used in the proposed system. Attribute Based Encryption for high security and Elliptic Curve Cryptographic technique for low power computing devices are being used (Yang et al., 2017). In the proposed system, we are suggesting the combination of both techniques because the single Attribute based encryption uses large private key size, whereas the Elliptic Curve cryptography has poor flexibility in revoking an attribute. Therefore, the proposed system presents a hybrid encryption technique, which is a combination of ECC, and user defined attributes. The user has to provide the key as well as the attributes to decrypt the data. Therefore, the suggested technique is the combination of Ciphertext-Policy Attribute-Based Encryption

(CP-ABE) and Elliptic Curve Cryptography (ECC). These attributes set by the IoMT device that sends its data.

Algorithm 1 : Handshaking
Input: *PublicKey, URI*
Output: *Message, Token*

```
1: Message.RT="Request Type"
2: Message.ST="Security Technique"
3: Handshaking(Message, URI, PK)                    ▷ Main Function
4: if Message.RT= "Generate Token" then
5:     DeviceInfo = RequestDeviceInfo(PK, URI)      ▷ Algorithm 1.1
6: end if
7: if Message.RT= "Request Data" then
8:     Data = RequestDataInfo(DeviceInfo, URI)      ▷ Algorithm 1.3
9: end if
```

Algorithm 1.1: Request Device Information
Input: *PK, URI*
Output: *DeviceInfo*

```
1: RequestDeviceInfo(PK, URI)          ▷ Request for Device Information
2: Message.RT= "Generate Token"                    ▷ Request Type
3: DeviceInfo = Request(URI, PK, Message)          ▷ Algorithm 1.2
4: return DeviceInfo
```

Algorithm 1.2: Resquest
Input: *URI, PK, Message*
Output: *DeviceInfo*

```
1: Resquest(URI, PK, Message)          ▷ Response to Device Info Request
2: if isValid(PK) then
3:     DeviceInfo[]
4:     foreach D in MyIoMTs
5:         DeviceInfo.Token= D.GenerateToken();        ▷ Generate Token
6: end if
7: return DeviceInfo
```

Algorithm 1.3: Request Data Information
Input: *DeviceInfo, URI*
Output: *Data*

```
1: RequestDataInfo(DeviceInfo, URI)                ▷ Request for Data
2: Message.RT= "Data Request"                      ▷ Request Type
3: Message.ST= "ECC"                               ▷ Security Technique
4: Data= DataRequest(DeviceInfo, URI, Message)     ▷ Algorithm 1.4
```

Algorithm 1.4: Data Request
Input: *DeviceInfo, URI, Message*
Output: *Data*

```
1: DataRequest(DeviceInfo, URI, Message)
2: if isValid(DeviceInfo.token) then
3:     Data=SharData(DeviceInfo.Token, Message)     ▷ Send Request for Data
4: end if
5: return Data
```

Algorithm 1: Establish Connection between IoMT devices

Algorithm 2.1: Control Registration
Input: *URI, capability*
Output: *URI, Message*

```
1: System.Thread.Time.Send(20000)
2: RegisterMe(URI, Cap)
3: if (low(HOPcount)) then
4:     Message.Status = "register"
5:     return Message.Status
6: else
7:     Message.Status = "Not Register"
8:     return Message.status
```

Algorithm 2.2: Listener
Input: *Message, Token*
Output: *EncryptedData, Message*

```
1: ShareData(Token, Message)
2: SecurityTechnique= Device.ST          ▷ Get Device Security Technique
3: if (Token != Null  Token = valid) then          ▷ Authenticate Token
4:     if ( (Message.ST = SecurityTechnique)) then  ▷ Check security techniques
5:         return EncryptedData
6:     else
7:         foreach d in IoMTDevices
8:         if (d.Message.staus= "register") then
9:             Conversion(Message, Token, Data)
10:        end if
11:    end if
12:    return invalid token
13: end if
```

Algorithm 2: Listener

Algorithm 3 : Conversion
Input: *Message, Token, Data*
Output: *Data*

```
1: Conversion(Message, Token, Data)
2: RequiredTechnique = Device.Enctechnique        ▷ Device Security technique
3: if (Device.Enctechnique = Message.ST) then
4:     Data = Convert(Data , RequiredTechnique)
5:     Publisih(Data, Token)
6: else
7:     return invalid request
```

Algorithm 3: Conversion

E. Publish

After applying the requested encryption technique the conversion module forwards request to the publish module. The module directly sends the data to the requesting node. To validate that the data is coming from an authentic node, HMAC/digital signature added with the sending data by the publish component, which shows that data is coming from the valid user, and it has not tampered. Therefore, the requested data authenticated and transferred securely to the healthcare provider system.

4. Case Study

A complete case study was designed to understand the whole flow of the proposed system. Fig. 2 illustrates the complete flow to transfer patients' data securely between different IoMT devices. When a patient visits a doctor, the doctor requires his healthcare readings that are stored in the patient's IoMT device. In the first step, the doctor requests device information from the

patient wallet through the Public Key (PK) and Universal Resource Identifier (URI). After validating the PK, the patient wallet generates and sends a response that includes the URIs of the patient devices and corresponding tokens to communicate with these devices.

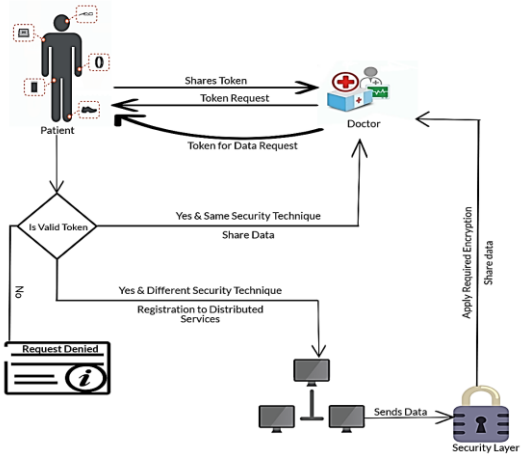

Fig. 2: Flow Diagram

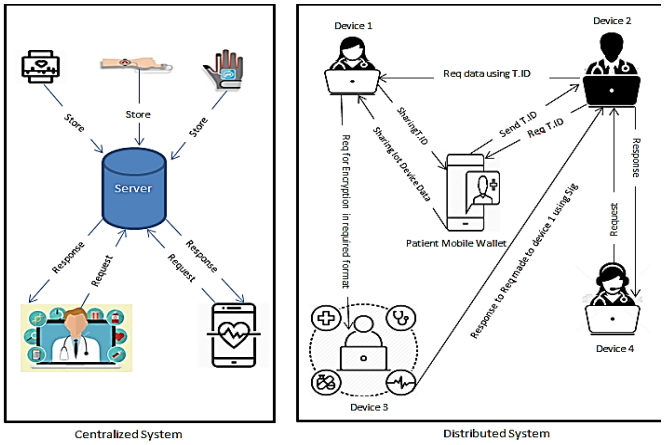

Fig. 3: Centralized and Distributed System

The doctor communicates with the devices to get the patient data using the URI and token information. The patient's device validates the token, and if the token is valid, a secure connection is established between sending and receiving IoMT devices. These devices have additional layers of encryption (device level encryption) that enforces the privacy of content embedded within transaction data. A patient IoMT device checks the security technique of devices that request the data. If both devices have the same encryption techniques, the data is shared. Otherwise, the system locates for a nearby device already registered with the device, to convert the data into the required security format. If there is any device available with the desired capability, the controller forwards a conversion request to the device. Now, control is transferred to the next device that response with encrypted data to the requesting node. To validate whether the data is coming from an authentic node, the sender adds HMAC/digital signature in the data shows the identity of the device. We added a security layer into the framework using the combination of lightweight Elliptic curve cryptography (ECC) with attributes. These attributes are mentioned at the time of the data request. This is how the system can securely send data from the patient's device to the doctor's device.

5. Evaluation

A. Experimental Setup

We developed two simulators to calculate the efficiency of the proposed system. The first simulator consists of a centralized environment where all the devices store their data at a single place. The second simulator is the proposed distributed system in which each device has its local storage. For experimental design, we consider two types of devices: the first type read the heartbeat rate, and the second device measures the blood pressure (systolic, diastolic). We simulated 400 instances of two types of IoMT devices to generate healthcare data (blood pressure, Heartbeat rate). 20% of these devices do not have the ability to provide encryption. Hence, these IoMT devices request to their nearby devices to encrypt their data before sharing it to remote devices. We generated multiple requests for data sharing simultaneously to test the efficiency and security of both centralized and the proposed system.

B. Experiment No. 1

In this experiment, 400 devices scenario was simulated, and during the data transfer, the network traffic was monitored using the Wireshark. In a centralized system, 80% of the requests were transferred in plain text, and those were easily detected through the tool. However, in distributed systems, 20% of requests were vulnerable and readable. As the number of requests increased, the data vulnerability also increases. Fig. 4 and Fig. 5 show the screenshots of a request that has been sniffed by Wireshark during the centralized and distributed experiment.

As compared to the centralized system, the proposed system has shown improved performance. 80% of the requests were transferred

as encrypted data that is unable to read. As the number of devices on network increases, the data vulnerability decreases. The result of a single request showed in Fig. 5.

Fig. 6 explains different 400 IoMT devices' security comparisons in our proposed system. It can be observed in the figure that with the increase in a number of IoMT devices (x-axis) on the network, the chances of secure data transmission also increase (y-axis) as there are more chances to find a nearby secure device. It decreases data vulnerability, and it also minimizes the chances of unencrypted data transmission.

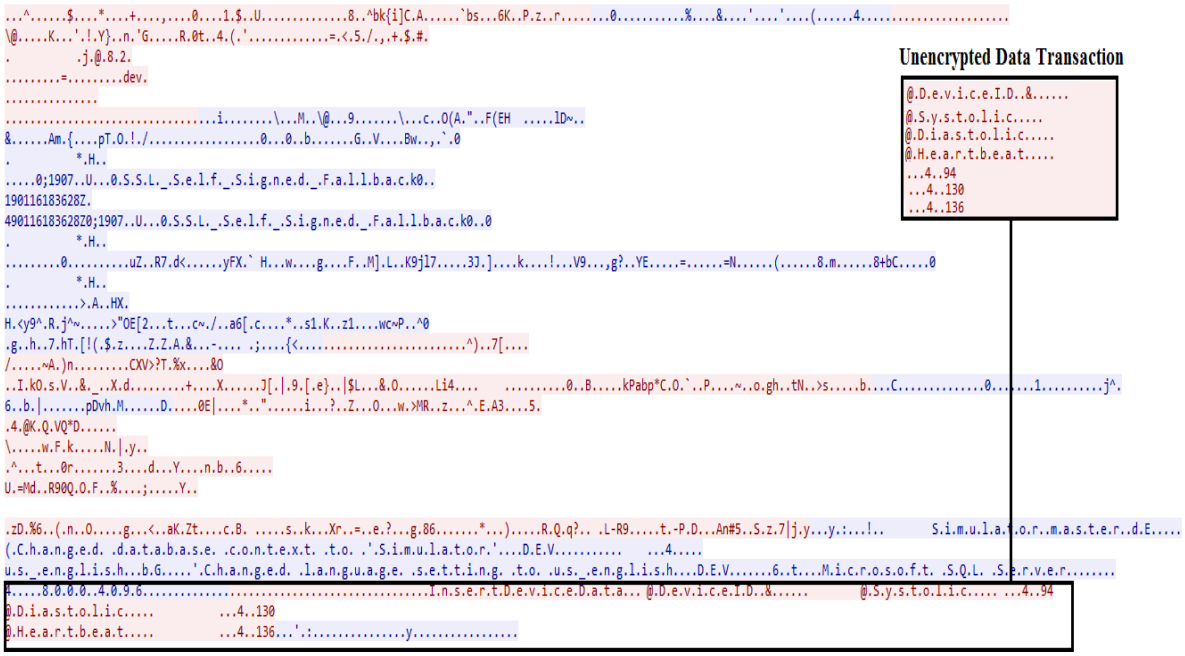

Fig. 4: Unencrypted Data Transaction on Network using Wireshark

Fig. 5: Encrypted Data Transaction on Network using Wireshark

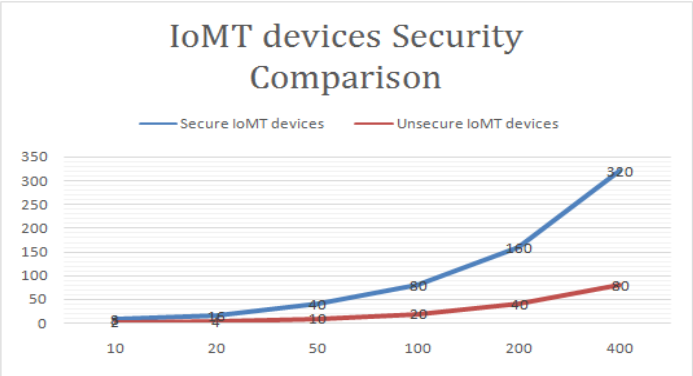

Fig. 6: IoMT devices Security Comparison

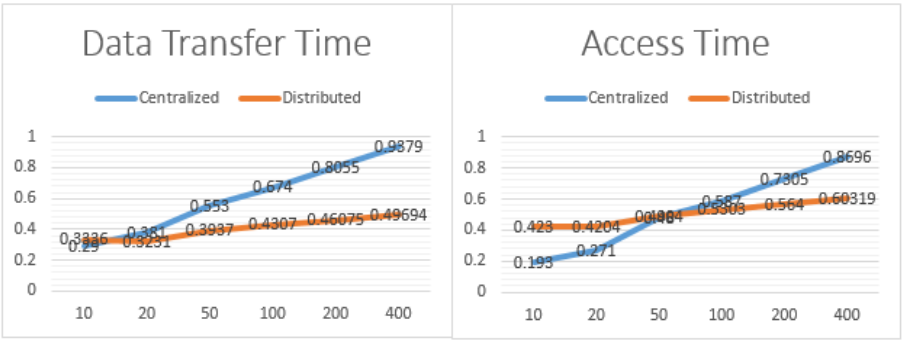

Fig. 7: Data transfer time and Access time

C. Experiment No. 2

In the second experiment, we run the same scenario of 400 devices with 100,000 number of requests for data sharing, but this time, we monitored the time required to complete the request. Average response time of centralized and proposed distributed system is listed in Table 2.

Data transfer (Table 2) is the time taken for the patient's IoMT device to encrypt its data and store locally whereas access time is the time for doctor's IoMT device to get data from patient's device on the network. 20% of the total devices use distributed processing by using encryption services from other devices on the network. Response time for the centralized system is different from the proposed distributed system (Table 2). Results generated using a combination of different devices. If we develop results using ten different IoMT devices and fewer requests, the centralized system gives better results (Fig. 7) than the distributed system. However, in case of an increased number of IoMT devices and data requests, the central server's performance compromises, and it increases the response time. As shown in Table 2, average data transfer time for 400 IoMT devices in a centralized system is 0.60 (ms), whereas it reduced to 0.40 (ms) in a distributed system with the same number of data requests. Access time also reduced from 0.52ms (in a centralized system) to 0.50ms (in a distributed system).

Table 2: Comparison table

		10 Device	20 Device	50 Devices	100 Devices	200 Devices	400 Devices	Average
Centralized	**Data Transfer time (ms)**	0.290	0.381	0.553	0.674	0.8055	0.9379	0.6069
	Access time (ms)	0.193	0.271	0.480	0.587	0.7305	0.8696	0.52185
Distributed	**Data Transfer time (ms)**	0.336	0.3231	0.3937	0.4307	0.46075	0.46075	0.406465
	Access time (ms)	0.423	0.4204	0.4904	0.5303	0.564	0.60319	0.505215

6. Discussion

Healthcare data like blood pressure, heart rate, pulse rate, and other collected through IoMT devices. Patients share their data with doctors and health care centers using these IoMT devices. Proposed distributed architecture for IoT based E-health systems allow different devices to handshake, listen, control, convert, and publish the data to the requesting device. These IoMT devices take services from their neighboring high-level processing device through distributed services to apply required cryptographic techniques for secure and fast transfer of data. An additional security layer proposed for lightweight and low power computing devices. Proposed security layer comprised of a combination of user defined attributes with Elliptic Curve Cryptography (ECC).

In a centralized system, when the data moves between IoMT devices, most of the devices do not have the capability to apply any encryption technique on data before sending it. Therefore the data transfers in plaintext, and it certainly raises the apparent security challenges. The central feature of network results in security issues (data breaching, data revealing) that makes the sensitive patient data available to any participant on the network. Device level encryption implemented in Experiment 1 to facilitate and enforce the privacy of content embedded within transaction data. Encrypted and Unencrypted data in Fig. 4 and Fig. 5 shows the difference between the previous and proposed systems. Data can be quickly revealed and tempered in a centralized system, whereas encrypted data in device level encryption in proposed architecture cannot be revealed and tempered. Only 20% of the total device data reveals in the proposed system as they did not find any suitable nearby device. We can also reduce this percentage by increasing the number of IoMT devices. This shows that the device level encryption in proposed distributed architecture provides a secure data transmission.

Security provided by the symmetric cryptography is low as it makes use of a single public key that is easily accessible. Therefore, for providing reliable security when we make use of simple asymmetric techniques; which provide security, but that is not enough to protect the patient's sensitive data in low power IoMT devices (Yang et al., 2017). When it comes to CP-ABE and ECC cryptographic techniques, the security provided by these techniques is much higher than the techniques discussed above. It is well known that IoT devices are low power devices, and for the computation of private keys, the key size is very large so that the IoT devices cannot work with them to provide security. ECC is well suited for low power IoT devices because it has a small key size and can provide the best security to sensitive patient's records. ECC keys are much smaller than other encryption techniques like RSA keys. ECC key strength is half of the key size, so a 256-bit ECC key has 128 bits of strength. A similarly strong RSA key is 3,076 bits long. However, the single ECC encryption scheme has poor flexibility in revoking attribute (Yang et al., 2017). In order to enable data sharing across healthcare systems, we developed a purpose-built solution based on privacy and security requirements. We suggested an Attribute based Elliptic curve cryptographic (ABECC) encryption technique to secure IoMT device data. Poor flexibility in revoking attribute issue of ECC is handled by adding attributes. Therefore, a combination of ECC with attributes provides an extra security check during data decryption. Comparison in Table 3 shows the security techniques and their proficiencies used in our framework. Table 3 describes the qualitative results from the literature.

Table 3: Comparison of Security Properties

PROPERTIES	SYMMETRIC	ASYMMETRIC	CP-ABE	ECC	ECC+ATTRIBUTES
SECURITY	LOW	MEDIUM	HIGH	HIGH	HIGH
PRIVACY	LOW	MEDIUM	HIGH	HIGH	HIGH
KEY SIZE	LARGE	LARGE	LARGE	SMALL	SMALL
MULTI-LEVEL SECURITY	NO	YES	YES	YES	YES

Multiple data requests are generated at one time to check the efficiency of the system. Average response time calculated for both centralized and distributed systems, and the results in Table 2 show the comparison analysis. It can be observed in Fig. 7 that with fewer IoMT devices and data requests, response time for a distributed system is higher than the centralized system, but as a number of devices and requests increases, the average response time for distributed system decreases and its efficiency improves. Distributed processing is also performed on 20% devices by using encryption services through other devices on network whereas the collective response time of 400 devices remained less than the centralized system. The reason for the difference is due to the device level storage and encryption in a distributed system. It is due to the load on the server in a centralized system that has to handle requests coming from different IoMT devices simultaneously. It shows that distributed architecture provides secure and efficient data transmission.

7. Conclusion and Future Work

This paper proposed suitable architectures and access control techniques for the distributed IoMT healthcare environment clearly with its functionalities. Security layer has been implemented in the proposed system to facilitate device level encryption that enforces the privacy of content embedded within transaction data. To face the challenge of the IoMT device resource constraints, different cryptographic algorithms have been implemented according to the computing power of IoMT devices. Research has proved that Elliptic Curve Cryptography (ECC) is a better technique to work with low power devices as it uses a small key size. We proposed the usage of ECC with attributes as an additional metric to improve the security level. Effectiveness of the proposed system was also examined for multiple data requests through different IoMT devices to verify better average response time of the proposed system. In the future, our security layer may be enhanced in a way to provide encrypted data transmission for the more complex types of data such as images and videos.

8. References

[1] Ahmad, M., Amin, M. B., Hussain, S., Kang, B. H., Cheong, T., & Lee, S. (2016). Health Fog: a novel framework for health and wellness applications. *Journal of Supercomputing*, *72*(10), 3677–3695. https://doi.org/10.1007/s11227-016-1634-x

[2] Alam, S., Chowdhury, M. M. R., & Noll, J. (2011). Interoperability of security-enabled internet of things. *Wireless Personal Communications*, *61*(3), 567–586.

[3] Alasmari, S., & Anwar, M. (2016). Security & privacy challenges in IoT-based health cloud. *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, 198–201.

[4] Alkeem, E. Al, Shehada, D., Yeun, C. Y., Zemerly, M. J., & Hu, J. (2017). New secure healthcare system using cloud of things. *Cluster Computing*, *20*(3), 2211–2229. https://doi.org/10.1007/s10586-017-0872-x

[5] Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and privacy in the internet of medical things: taxonomy and risk assessment. *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, 112–120.

[6] Alzghoul, M. M. (2016). *Towards Nationwide Electronic Health Record System in Jordan*. 650–655.

[7] Baccarini, A. N., Griggs, K. N., Howson, E. A., Ossipova, O., Hayajneh, T., & Kohlios, C. P. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 1–7. https://doi.org/10.1007/s10916-018-0982-x

[8] Bradley, C., El-Tawab, S., & Heydari, M. H. (2018). Security analysis of an IoT system used for indoor localization in healthcare facilities. *2018 Systems and Information Engineering Design Symposium (SIEDS)*, 147–152.

[9] Chen, S., Chiang, D. L., Liu, C., Chen, T., Lai, F., Wang, H., & Wei, W. (2016). Confidentiality Protection of Digital Health Records in Cloud Computing. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-016-0484-7

[10] Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal*, *3*(6), 854–864.

[11] Chung, K., & Park, R. C. (2016). PHR open platform based smart health service using distributed object group framework. *Cluster Computing*, *19*(1), 505–517.

[12] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for

Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. *Proceedings of IEEE Open & Big Data Conference*, *13*, 13.

[13] Ghanavati, S., Abawajy, J. H., Izadi, D., & Alelaiwi, A. A. (2017). Cloud-assisted IoT-based health status monitoring framework. *Cluster Computing*, *20*(2), 1843–1853. https://doi.org/10.1007/s10586-017-0847-y

[14] Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. *2015 IEEE World Congress on Services*, 21–28.

[15] Hossain, M. S., & Muhammad, G. (2016). Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. *Computer Networks*, *101*, 192–202.

[16] Liu, Z., Huang, X., Hu, Z., Khan, M. K., Seo, H., & Zhou, L. (2016). *On Emerging Family of Elliptic Curves to Secure Internet of Things : ECC Comes of Age*. *XX*(XX), 1–12. https://doi.org/10.1109/TDSC.2016.2577022

[17] Ma, Y., Wang, Y., Yang, J. U. N., & Miao, Y. (2017). *Big Health Application System based on Health Internet of Things and Big Data*. 7885–7897.

[18] Oh, S.-R., & Kim, Y.-G. (2017). Security requirements analysis for the IoT. *2017 International Conference on Platform Technology and Service (PlatCon)*, 1–6.

[19] Rahulamathavan, Y., Phan, R. C.-W., Rajarajan, M., Misra, S., & Kondoz, A. (2017). Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 1–6.

[20] Saied, Y. Ben, Olivereau, A., Zeghlache, D., & Laurent, M. (2013). Trust management system design for the Internet of Things: A context-aware and multi-service approach. *Computers & Security*, *39*, 351–365.

[21] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, 1–18.

[22] Tamizharasi, G. S. (2017). *IoT-Based E-Health System Security : A Vision Archictecture Elements and Future Directions*. 655–661.

[23] Vucinic, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2014). OSCAR: Object security architecture for the Internet of Things. *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, *WoWMoM 2014*. https://doi.org/10.1109/WoWMoM.2014.6918975

[24] Williams, P. A. H., & McCauley, V. (2016). Always connected: The security challenges of the healthcare Internet of Things. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 30–35.

[25] Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. *Journal of Network and Computer Applications*, *89*, 26–37.

[26] Zachariah, T., Klugman, N., Campbell, B., Adkins, J., Jackson, N., & Dutta, P. (2015). The internet of things has a gateway problem. *HotMobile 2015 - 16th International Workshop on Mobile Computing Systems and Applications*, 27–32. https://doi.org/10.1145/2699343.2699344