Research Article

iMedPub Journals
http://www.imedpub.com/

American Journal of Computer Science and Information Technology

2019
Vol.7 No.2:38

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

Asad Bilal[1*], Muhammad Awais Hassan[1] and M Shoaib[2]

[1]Department of Computer Science and Engineering, UET Lahore, Pakistan

[2]Institutes of Business and Management, UET Lahore, Pakistan

[*]**Corresponding author:** M Asad Bilal, Department of Computer Science and Engineering, UET Lahore, Pakistan, E-mail: asadbilal4@gmail.com.

Received date: July 8, 2019; **Accepted date:** July 19, 2019; **Published date:** July 29, 2019

Citation: Bilal A, Hassan MA, Shoaib M (2019) A Distributed Secure Framework for Sharing Patient's Data among IoMT Devices. Am J Compt Sci Inform Technol Vol.7 No.2: 38

Abstract

Encouraging prospective of Internet of Medical Things (IoMT) used different wearable devices and sensors for more quality patient care. It provides more flexibility for monitoring patient's record remotely as compare to the traditional healthcare system. However, there are some data security and privacy challenges due to the absence of proper security mechanism in low power computing devices. The currently available security techniques such as watermarking and high-level encryption techniques, to protect patients' record are not sufficient for low-level IoMT devices. It is also observed that 70% of IoT devices have to face security issues due to the unencrypted network services in centralized system. This paper proposed a secure distributed system, which provides device level encryption and share patient's data between different IoMT devices and healthcare providers without the need of the centralized server. The proposed system applies different device level encryption techniques to provide encrypted network services. An Attribute based Elliptic curve cryptographic (ABECC) encryption technique proposed as an additional security layer for lightweight and low power computing devices. The results show that the average response time has been significantly improved using the proposed distributed system as compare to the previous centralized system. In future, the proposed system could enhance in a way to provide encrypted data transmission also for graphical data like ECG and other medical images.

Keywords: Internet of Medical Things; Public Healthcare; Security; Data privacy; Encryption; Distributed computing

Introduction

According to market research [1] 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). In these days, health care centers are equipping the patients with invasive and non-invasive IoMT device to collect different physiological parameters like blood pressure, heart rate, and pulse rate. These devices pre-process the received signal and transmit that to the central server through Wi-Fi services [2].

Traditionally, centralized systems store the data which is transferred, on demand, to the devices of doctors and health care centres. 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 challenges [3]. Usually, data protection from the unauthorized user in a centralized system is done using access control, encryption, and data anonymity [4]. However, these traditional systems face three key challenges: low-encryption, overloading, and heterogeneity. About 70% of the IoMT devices have serious security vulnerabilities [5] that make encryption a fundamental challenge to IoMT devices. The main reason behind the challenge is limited resources such as the short battery, small memory space and low processing power [6].

The second major issue with the centralized systems is that they have limited capacity to communicate with different devices [7]. With the increase in 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 [8].

These security issues of IoMT devices are causing undesirable results. Therefore, patients' data can be vulnerable to hackers during cloud transfer or synchronization with interconnected devices in a centralized system. Now, the time has come to use the distributed technologies [9] that increase the security of the data sharing. 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. The following research questions have been asked more specifically.

1. How to provide device-level encryption for secure data transmission?
2. How the latest security techniques can be used to secure the IOMT health records?
3. How to improve the efficiency of 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.

Literature Review

Hossain and Mohammad [10] proposed a cloud-based industrial IoT healthcare framework to transfer medical data securely from IoMT devices to medical professionals. This system protected identities of the data using watermarking and signal enhancement before sending to the cloud. Later research revealed that watermarking is an old data securing technique, which fails when an opponent refines his knowledge on presumably secret key.

Alsubaei et al. [1] discussed different IoMT device layer attacks at network layer. Taxonomy presented for security and privacy of patient data in IoMT. Moreover, 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 absence of cryptographic technique in low computing power devices. These attacks must be overcome by applying device level encryption in heterogeneous environment.

Alkeem et al. [7] 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 week passwords. Moreover, diversity of IoT devices is also a reason for data insecurity. Therefore, there is high need of data to be encrypted before sending it to any network. Tamizharasi and Sultanah [11] discussed three types of IoT healthcare provider (Centralized, distributed and cloud based) architectures. Authors revealed that due to the distributed nature of electronic health records, centralized architecture does not provide better solution. However, distributed architecture supports hospital and clinical management systems. Authors also mentioned CP-ABE (attribute based) encryption algorithm in the paper as an appropriate technique to provide better data security. However, user attribute management is only major drawback of this technique. Ghanavati et al. [12] proposed a framework based on IoT and provide the facility of remote patient's health status monitoring. Connectivity of WBAN using smart phones 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 central place can be tampered easily. MM Hossain et al. [6] described about the security issues of IoT devices with reference to their less computing power. Hardware, software, and network level security limitations play an important role to protect IoT device data. According to 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 serious chance of data exploitation by malicious attackers.

Ahmad et al. [13] presented a framework using fog computing as an intermediary between the end user and cloud. This framework helped in sharing the healthcare information. Data privacy and security was preserved by introducing an integral component cloud access security broker (CASB). The purpose of this component was to implement different security policies on cloud. Fog computing acts as a secure gateway between users and cloud however with the increase in number of IoMT devices, the time for server response increases.

Baccarini et al. [14] proposed a distributed blockchain based smart contracts 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 et al. [15] proposed a blockchain protocol for engaging attribute based encryption and providing end-to-end privacy-preserving IoT ecosystem in decentralized networks. Security achieved by blockchain and attributed based encryption but costs computational overheads. In emergencies, this can lead to severe results. Yang et al. [16] proposed a secure and lightweight distributed IoT healthcare system. Data security was implemented using attribute based encryption with the facility of keyword search to tackle with the challenge of accumulated effective data retrieval mechanism. However, poor flexibility in revoking attribute is the major drawback of attribute-based encryption.

Liu et al. [17] presented an implementation design that used the emerging family of Elliptic Curve library for providing security at distinct levels in internet of things (IoT). The library provided the security with efficiency. Library has two implementation versions: one provided the high speed while the second one was the memory-efficient version. ECC provides security with low power consumption and less memory space.

Chung and Park [18] proposed a PHR open platform for providing healthcare services to manage chronic disease. Framework 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 sent wirelessly is secure and protected. Dynamic

security provided by Distributed object group framework (DOGF's) supporting components of object group.

Table 1: Research Matrix Table.

Research	Characteristics	IoMT	Centralized Security	Distributed Security	Authentication, Authorization
(Ahmad et al. 2016)	Security	Data protection	Data protection	-	Access Control
			Fog computing		
(Ghanavati et al. 2017)	Remote Patient Monitoring	-	-	-	-
(Rahulamathavan et al. 2018)	Privacy and Security	Data Security	-	Data Security	Trust, Access Control
(Yang et al. 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 et al., 2018)	Tracking Solution	Localization of Healthcare Center Assets through IoT	-	-	Security Holes
(Chen et al. 2016)	Security	environment data security	Cloud Storage	-	Access Control
(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

Proposed Methodology

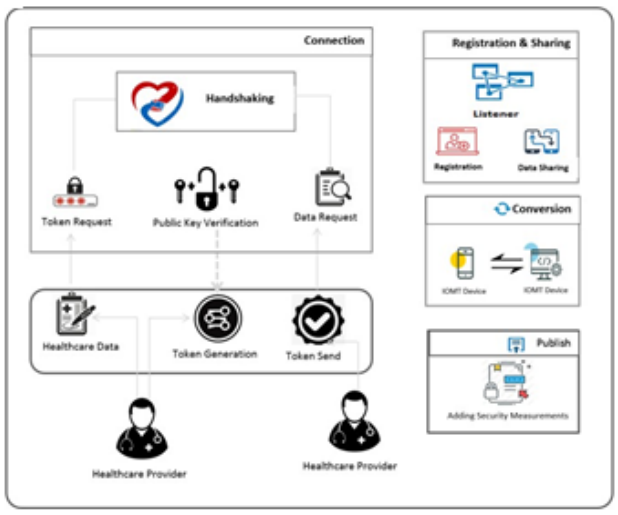

Figure 1: Architecture diagram of Distributed bases IoMT healthcare system.

Handshaking

Mainly there are two types of requests that handshaking deals with in algorithm 1. First, the request is made to get device information and to generate token using algorithm 1.1. Handshaking establishes the connection between IoMT devices using public key of the patient. The patient shares his public The proposed system (**Figure 1**) is a distributed framework for security of IoMT device data, which comprises of five components. 1) Handshaking is the entry point that sends request for data and connection between IoMT devices by sending and receiving tokens. 2) Listener validates the request and send data if encryption techniques are same on both sender and receiver side. Whereas, the control registration is also a sub part of listener, which timely generates registration request and update all the nearby devices.3) An additional security layer containing different cryptographic techniques 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) At the end publish sends data directly to the requesting device and apply HMAC/digital signature to validate the data coming from authentic user. Detail of each component is given in the following sections. The second request is made for data sharing (algorithm 1.3) (**Figure 2**).

Key (PK) and Universal resource identifier (URI) to healthcare provider from whom it may want to share his data. First, the request analyzes that it is either requesting for device token or data. If the request is for token: Request device information (algorithm 1.1), the response at the patient device made by validating the Public key (PK). A unique token is also generated

and forwarded to the requesting device in algorithm 1.2. If the request was: Request data information (algorithm 1.3), then the (response at the patient device is made by validating the token using algorithm 1.4. Message body in algorithm 1 (**Figure 2**) containing ST (security technique), RT request type) and token (s) sent to the requesting device as output to establish a secure connection **(Table 1)**.

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
```

Figure 2: Algorithm 1 Establishing Connection between IoMT devices.

Listener

It comprises of a sub-components named: Control Registration. It initiates a registration request (algorithm 2.1) (**Figure 3**) after a specific time interval on each IoMT device, which registers the new incoming device on the network. Therefore, all the devices on network send register request to its nearby devices by sending its URI and capability (Security technique). The registration is made on the basis of HOP count. IoMT device get registers if HOP count is low for receiving device. Therefore, all the devices on network have a list of nearby registered devices and their capability through which any user can send any type of request to its registered devices. Secondly, Listener component validates the incoming request in algorithm 2.2 (**Figure 3**) and share encrypted data if both IoMT devices are using same security technique. Input to this component is provided by the handshaking component in the form of message and token. This component validates the incoming token and checks for 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 same encryption technique. However, if there is a difference between both techniques or the device does not have capability to apply any encryption technique then it uses the distributed services. In distributed services, conversions are performed to apply required security technique by using the list of nearby registered 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
```

Figure 3: Algorithm 2 Listener.

Conversion

It verifies either the nearby device can apply required encryption technique for the requested IoMT device. Conversion request with data and token is forwarded to apply the required encryption technique. Conversion applies in algorithm 3 (**Figure 4**) if receiving device poses the required encryption technique or has capability to convert into required technique. Request is denied if available security technique does not exist. After applying the security technique, data is sent to the requesting device using publish method as an output.

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
```

Figure 4: Algorithm 3 Conversion.

Security layer

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). As IoMT are low power computing devices and some of them are unable to apply even simple encryption technique therefore distributed security services are used in proposed system. Attribute Based Encryption for high security and Elliptic Curve Cryptographic technique for low power computing devices are being used [16]. In 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 a poor flexibility in revoking attribute. Therefore, the proposed system presents a hybrid encryption technique, which is combination of ECC, and user defined attributes. The user has to provide the key as well as the user defined 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.

Publish

After applying the suitable encryption technique in security layer, output produced by encrypting the healthcare data in a format aforementioned at the time of request. After applying encryption, that system 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 not tampered. Therefore, the requested data authenticated and transferred securely to healthcare provider system.

Case study

A complete case study was designed to understand the whole flow of the proposed system. **Figure 5** illustrates the complete flow to transfer patients' data securely between different IoMT devices.

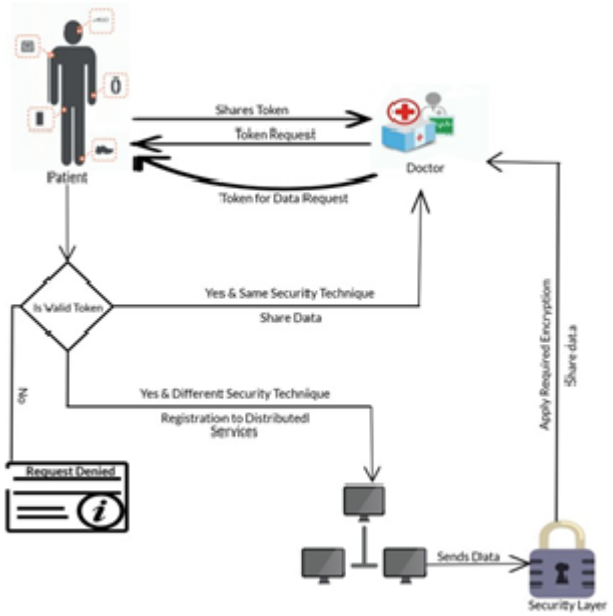

Figure 5: *Flow Diagram of* illustrates the complete flow to transfer patients' data securely between different IoMT devices.

When a patient visits a doctor, the doctor requires his healthcare readings those are stored in patient's IoMT device. At the first step, the doctor requests device information from 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. 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 for security technique in which data is requested. If both devices have 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 forward conversion request to the device. Now, control is transferred to the next device and the send encrypted data to the requesting node. To validate if the data is coming from an authentic node, the sender adds HMAC/ digital signature in the data showing the identity of the device. We added a security layer into the framework using the combination of lightweight Elliptic curve cryptography (ECC) and attribute. These attributes are mentioned at the time of data request. This is how the system can securely send data from patient's device to doctor's device.

Evaluation

Experimental setup: We developed two simulators to calculate the efficiency of the proposed system. 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 own local storage. For experimental design, we consider two types of devices: first type read the heartbeat rate and second device measure the blood pressure (systolic, diastolic). We simulated 400 instances of two types of IoMT devices to generate healthcare data (blood pressure, Heartbeat rate). The 20% of these devices do not have the ability to provide encryption. Hence, these IoMT devices requests 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 **(Figure 6)**.

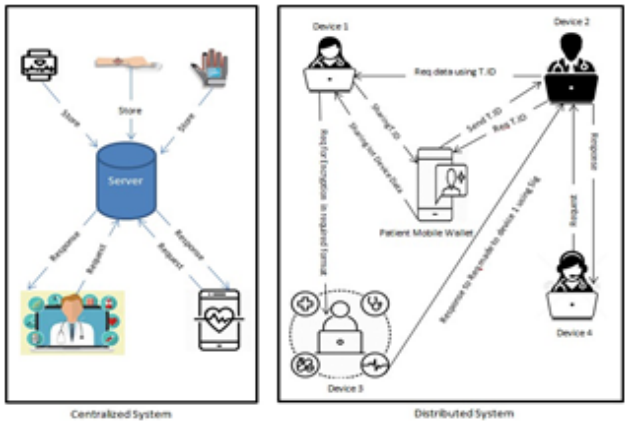

Figure 6: Centralized and Distributed System.

Experiment 1: In experiment 1, the 400 devices scenario simulated, and during the data transfer, the network traffic was monitored using the Wireshark. In centralized system, 80% of the requests were transferred in plain text and those were easily detected through the tool. However, in distributed systems, 20% requests were the vulnerable and readable. As number of requests increased, the data vulnerability also increases. The **Figures 7** and **8** shows the screen shots of a request that has been sniffed by weireshark during the centralized and distributed experiment.

Figure 7: Unencrypted Data Transaction on Network using Wireshark.

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 the **Figure 8.**

Figure 8: Encrypted Data Transaction on Network using Wireshark.

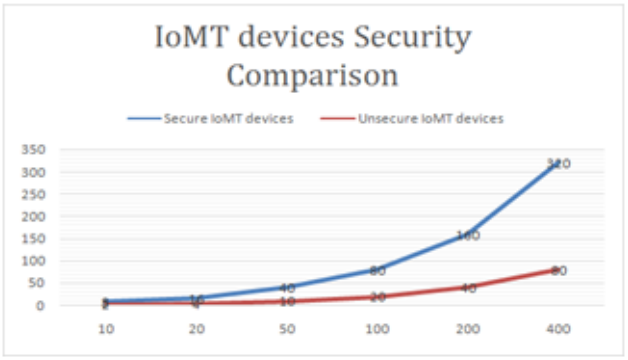

Figure 9: IoMT devices Security Comparison.

Figure 9 explains different 400 IoMT devices security comparison in our proposed system. It can be observed in the

figure that with the increase in 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.

Experiment 2: In the second experiment, we run the same scenario of 400 devices with 10,0000 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 showed in the **Table 2**. Data transfer is the time taken for 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 uses distributed processing by using encryption services from other devices on network. Response time for centralized system is different from proposed distributed system. Efficiency of both systems can be check**.** Results generated using combination of different devices. If we develop results using 10 different IoMT devices and less number of requests, the centralized system gives better results (**Figure 10**) than distributed system as with less number of data requests, central server performs well. However, in case of increased number of IoMT devices and data requests, central server's efficiency compromises and its increases the response time. As shown in **Table 2**, average data transfer time for 400IoMT devices in centralized system is 0.6069(ms) whereas it reduced to 0.406465(ms) in distributed.

Table 2: Comparison table.

		10 Device	20 Device	50 Device	100 Device	200 Device	400 Device	Average
Centralized	Data Transfer time (ms)	0.29	0.381	0.553	0.674	0.8055	0.9379	0.6069
	Access time (ms)	0.193	0.271	0.48	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

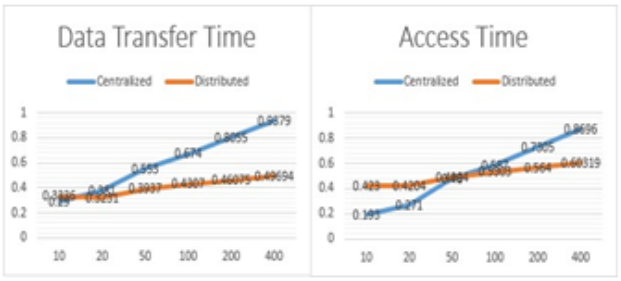

Figure 10: Data transfer time and Access time.

Results and Discussion

Healthcare data like blood pressure, heart rate, pulse rate and other collected through IoMT devices. Patients share their data to their doctors and health care centers using these IoMT devices. Proposed distributed architecture for IoT based E-health systems allows 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 combination of user defined attributes with Elliptic curve cryptography (ECC) [19,20].

In 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. So the data transfers in plaintext. Therefore, this gives chance to rise the obvious security challenges. The central feature of network results in security issues e.g. 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 **Figures 4 and 5** show the difference between the system with the same number of data requests. Access time also reduced from 0.52185 (ms) in centralized system to 0.5052(ms) in distributed system previous and proposed system. Data can be easily revealed and tempered in 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 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 provide a secure data transmission.

Security provided by the symmetric cryptography is low as it makes use of single public key that is easily accessible. Therefore, for providing strong 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 [16]. When it comes to CP-ABE and ECC cryptographic techniques, 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. While, Elliptic curve cryptography (ECC) is well suited for low power IoT devices, have small key size and can provide 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. But the single ECC encryption scheme has a poor flexibility in revoking attribute [16]. 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 while data decryption. Comparison in **Table 3** shows the security techniques and their proficiencies used in our framework. It describes the qualitative results from the literature.

Table 3: Comparison to 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. Results in **Table 2** show the comparison analysis. It can be observed in **Figure 7** that with less number of IoMT devices and data requests, response time for distributed system is larger than the centralized system but as 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 from other devices on network whereas the collective response time of 400 devices remained less than the centralized system. Reason for difference is due to the device level storage and encryption in distributed system. Each device stores data on its own storage. It is also due to the load on the server in centralized system which has to handle requests coming from different IoMT devices simultaneously. It shows that distributed architecture provides secure and efficient data transmission.

Conclusion and Future Work

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

References

1. Alsubaei F, Abuhussein A, Shiva S (2017) Security and privacy in the internet of medical things: taxonomy and risk assessment. In: 2017 IEEE 42nd Conference Local Computer. Networks Work LCN Work 6 : 112–120.
2. Ma Y, Wang Y, Yang JUN, MiaoY (2017) Big Health Application System based on Health Internet of Things and Big Data. IEEE Access 5: 7885–7897.
3. Alasmari S, Anwar M (2016) Security and privacy challenges in IoT-based health cloud. In 2016 International Conference on Computational Science and Computational Intelligence (CSCI): 198-201.
4. Oh S, Kim Y (2017) Security Requirements Analysis for the IoT. In: IEEE International Conference on Platform Technology and Service 1: 1-6.
5. Williams PAH, Mc Cauley V (2016) Always connected: The security challenges of the healthcare Internet of Things. In: IEEE 3rd World Forum Internet Things, WF-IoT: 30–35.
6. Hossain MM, Fotouhi M, Hasan R (2015) Towards an analysis of security issues, challenges, and open problems in the internet of things. In: Proceedings of 2015 IEEE World Congress on Service: 21– 28.
7. Alkeem, Shehada D, Yeun CY, Zemerly MJ, Hu J (2017) New secure healthcare system using cloud of things. Cluster Comput 20: 2211–2229.
8. Singh S, Kumar P, Seo S, Moon Y, Hyuk J (2017) Advanced lightweight encryption algorithms for IoT devices? survey, challenges and solutions. J Ambient Intell Humaniz Comput: 1-8.
9. Rabah K (2017) Challenges and Opportunities for Blockchain Powered Healthcare Systems: A Review. Mara Res J Med Heal Sci 1: 45–52.
10. Hossain MS, Muhammad G (2016) Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Comput Networks 101: 192–202.
11. Tamizharasi GS (2017) IoT-Based E-Health System Security? A Vision Archictecture Elements and Future Directions 655–661.
12. Ghanavati S, Abawajy JH, Izadi D, Alelaiwi AA (2017) Cloud-assisted IoT-based health status monitoring framework. Cluster Comput 20: 1843–1853.

13. Ahmad M, Amin MB, Hussain S, Kang BH, Cheong T, et al. (2016) Health Fog: a novel framework for health and wellness applications. J Supercomput 72: 3677–3695.

14. Baccarini AN, Griggs KN, Howson EA,Ossipova O, Hayajneh T, et al. (2018) Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42: 1–7.

15. Rahulamathavan Y, Phan RCW, Rajarajan M, Misra S, Kondoz A (2018) Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. 11th IEEE Internet Conference Advance Networks Telecommunication System: 1–6.

16. Yang Y, Zheng X, Tang C (2017) Lightweight distributed secure data management system for health internet of things. J Netw Comput Appl 89: 26–37.

17. Liu Z, Huang X, Hu Z, Khan MK, Seo H, et al. (2016) On Emerging Family of Elliptic Curves to Secure Internet of Things?: ECC Comes of Age. IEEE Transactions on Dependable and Secure Computing 14: 237-248.

18. Chung K, Park RC (2016) PHR open platform based smart health service using distributed object group framework. Cluster Comput 19: 505–517.

19. Bradley C, El-tawab S, Heydari MH (2018) Security Analysis of an IoT System Used for Indoor Localization in Healthcare Facilities. SIEDS: 147–152.

20. Chen S, Chiang DL, Liu C, Chen T, Lai F, et al. (2016) Confidentiality Protection of Digital Health Records in Cloud Computing. J Med Syst 40: 124.