Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 1659-1671
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/IJNAA.2021.5295

A secure biomedical data sharing framework based on mCloud

Akeel Sh. Mahmoud[a*], Nisreen Mohammed Mahmood[a]

[a] *Computer Center, University Of Anbar, Iraq.*

(Communicated by Madjid Eshaghi Gordji)

Abstract

Medical Clouds (mCloud) utilized various wearable devices and sensors for better care for patients by encouraging the perspective of the clouds. It gives a more versatile way to centrally and in real-time compare the patients' profiles in the conventional health-offline system. However, due to the lack of appropriate security measures in low-power computers, there are obstacles to data protection. The limitation made the data vulnerable to hacking 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 manuscript proposes a secure and faster-distributed method, which shares a patient's data by various devices connected to the mCloud with health caregivers without the need for the centralized server. The research harnesses the power of other locally available mCloud and related devices that have more computational capability. Our experimental results demonstrate that with the number increasing of mCloud 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 shows a decrease in the total response time from 0.6ms to 0.4ms utilizing the proposed distributed vs centralized system.

Keywords: mCloud(Medical Cloud), Health caregiver, Biomedical Data Transmission, Data Encryption.

1. Introduction

According to market research, the cloud-based healthcare market sector is poised to reach $120 billion by 2021, and the exponential rise has given birth to the Internet of mCloud. These days healthcare centers are equipping the patients with invasive and non-invasive mCloud devices to

*Corresponding author: Akeel Sh. Mahmoud

Email addresses: akeelab2000@uoanbar.edu.iq (Akeel Sh. Mahmoud[a*]), eng.nmsw@uoanbar.edu.iq (Nisreen Mohammed Mahmood[a])

Received: April 2021 *Accepted:* June 2021

collect different physiological parameters such as blood pressure, heart rate, and pulse rate [7]. These devices preprocess the received signal and transmit that to the central server through Wi-Fi services. 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 (utilizing the private and public cloud) is raising significant security issues and challenges [12].

Usually, the centralized systems provides data protection from unauthorized users through access control, encryption and data anonymity. 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 mCloud devices have serious security vulnerabilities that make encryption a fundamental challenge to mCloud [13]. The limited resources such as the low battery, small memory space and low processing power 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 [16]. 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 mCloud devices may have different security encryption techniques and it is not possible for the server to convert the data in all possible encrypted formats [23]. These security issues of mCloud devices are causing undesirable results in terms of trust deficit between the patient, hospital and insurance companies. The high hop-distance between the client and the central server, for example, causes patient data to be exposed to hackers through cloud transmission or integration with devices attached in a central framework [24]. 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 manuscript is 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 [29].

- How to provide device-level encryption for secure data transmission between the mCloud devices and other digital devices?
- How does the mCloud health system boost its efficiency?

The network of mCloud devices with different capacities and capabilities can collaborate with each other and perform the tasks more efficiently than a centralized system. The key feature of the manuscript is a distributed architectural proposal for e-health systems using mCloud that allow multiple devices to shake their hands, chat, turn and take resources to easily protect and move 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 manuscript [32].

2. Related Works

M. S. Hussain and Mohammed, 2016, [20] proposed to safely move patient data from cloud devices to healthcare practitioners via a cloud-based industrial healthcare system. This system protected the identities of the data utilizing watermarking and signalled enhancement before sending it to the cloud. Later research revealed that watermarking is an old data securing technique, that does not work when the opponent enhances his information on a supposed hidden key.

Alsobaee et al., 2017, [9], discussed different device layer attacks based cloud at the network layer. A taxonomy presented for patient data privacy and security in the cloud. Moreover, the risk

assessment method also proposed in the manuscript 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.

Alkeme et al., 2017, [8], introduced a cloud-based new healthcare system , It offers various essential safety criteria such as confidentiality, verification, transparency, privacy, honesty and non-repudiation. The authors explain that 70 percent of cloud systems pose severe security problems due to poor passwords and unencrypted network services. Moreover, the diversity of cloud and internet of thing devices is also a reason for data insecurity. Therefore, data encryption is essential before sending it to any network.

Three specific cloud care provider framework was explored in Tamezherasee 2017, [30]. (centralized, distributed and cloud-based). The authors found that central architecture does not provide a better approach due to the distributed existence of EHRs. The distributed architecture also facilitates applications for clinical and hospital management.

Ghanavate, Abewajy, Izadei [18] and Alilaewie, 2017, proposed a framework based on internet cloud infrastructure and provided the facility of remote patient's health status monitoring. Connectivity of WBAN utilizing 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 tamper easily.

M. M. Hossain et al., 2015, [19], described the security issues of medical cloud devices regarding their less computing power. Hardware, software and network-level security limitations play an essential role in protecting cloud device data. According to the authors, there are some security computations, which require remarkable computing resources. Therefore, cloud 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.

Ahmed et al., 2016, [5], presented a framework utilizing 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.

Baccarene et al., 2018, [11], a smart distributed blockchain contract for the generation and writing of records of all patient tracking activities in real-time using cloud-based smart devices on blockchain. In this method, the constraint is the regulation of transmission time. The device cannot then be used to deliver an emergency response, since delay increases response time. A distributed health care infrastructure is thus essential to handle many demands effectively.

Raholamuthavn et al. 2017, [26], introduced a blockchain protocol for engaging attribute-based encryption and providing end-to-end privacy-preserving cloud ecosystems in decentralized networks. Security achieved by blockchain and attributed based encryption, but it costs computational overheads.

Yung, Zhang and Tunge, 2017, [34], presented a secure and lightweight distributed healthcare system based cloud. Data security was implemented utilizing 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.

Lie et al., 2016, [22], implement a design that utilized the emerging family of Elliptic Curve library for providing security at distinct levels in cloud. The library has two implementation versions: one provided a high speed while the second one was the memory-efficient version. Elliptic Curve

Cryptography provides security with low power consumption and less memory space.

Chong and Parke, 2016, [15], proposed a PHR open platform for providing healthcare services to manage chronic disease. The platform collected the healthcare data and managed the records utilizing 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.

Volcanic et al2014 .'s [31] suggested a secure, soap-application protocol-based channel-based architecture. This manuscript offers a modern, scalable cloud security architecture that provides security (E2E) along with access control. It divides confidential trust realms that support primarily multi-diagram, asynchronous traffic and cache.

Chiang and Zhuang 2016, [14], presented a survey for highlighting new security challenges to the cloud. 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 cloud-based devices cannot allow extensive handling of remote credentials. Forcing a large number of devices to remotely authenticate will, even if possible, contribute to prohibitive costs and administrative difficulty. The existing security strategies are listed that several new safety issues in the evolving cloud will not be adequate anymore.

In order to provide safe entry, Scientist, Choudhury and Noll, 2011, [6] suggested a practical cloud-based architecture. Semantic ontologies use the proposed architecture elements. The authors added to the cloud's intellect with a practical architecture. Ontological overlays with a rule-based access system are used as semantic overlays. This ontology and M2M technology offer interoperability for safety and security.

The architecture that uses the ubiquitous existence of low-energy radio from Bluetooth to link cloud peripherals to the Internet was proposed in Zucharieh et al., 2015, [6]. The global smartphone network offers network infrastructure and mobility for low-power wireless devices that better use the opportunities provided by interoperability between heterogeneous clouds. On modern smart telephones, the proposed architecture serves as the key connection between low-capacitors and smartphones. They intend a two-pronged open-gate platform to develop frameworks for device phone interactions. As a temporary IP router, the first uses every smartphone as the usual IP end host. Second, a Bluetooth profile can be delegated on behalf of the user to the cloud.

The trust management scheme between cloud nodes is suggested by Saeed et al., 2013, [27]. The framework triggers pre-node activities to include various services that demonstrate the amount of faith that can be put in the node to perform the necessary tasks. Finally, a mutual service to the claimant node was offered only by the strongest partner. For false or malicious facts, its proposed framework effectively boosts the degree of contractual trust.

Alzaghuol, 2016, [10] has put forward a modern middleware web-center, interoperability and protection architecture, where health care providers depend in part (or in entirely). In cases where emergency facilities rely on the handwritten health record or use local, incapacitated electronic health records. Interoperability. Interoperability. The framework suggested aims to transform the alignment complexity from healthcare providers to the middle.

Table 1: Refers to Research Modeling Table

Research	Characteristics	mCloud 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 mCloud	Security with less response time	IoT Security	Encrypted Data Storage	Cryptographic data transmission	Trust access control

3. System Methodology

The architecture suggested (Figure 1) is a distributed structure for the cloud device data security, which comprises five modules. 1) Handshaking (Health Caregiver) is the entry point that sends a request for data and connection between cloud devices by sending and receiving tokens(Codes). 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 timer generates a registration request and update all the nearby devices.3) An additional security layer, containing different cryptographic techniques, is added to deal with lightweight mCloud devices.

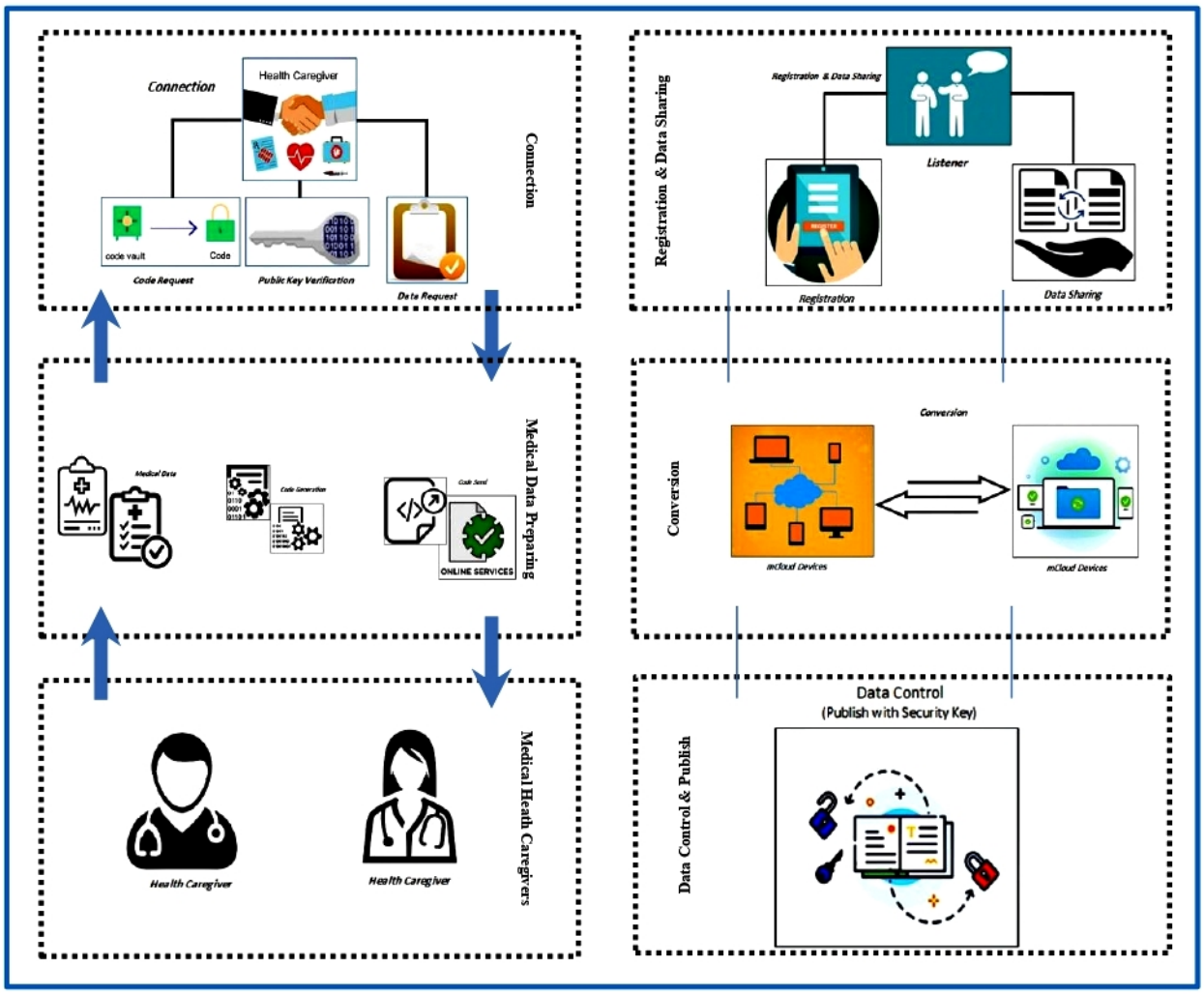

Figure 1: The infrastructure of mCloud health Caregiver system

Elliptic Curve Cryptography 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:

3.1. Handshaking (Health Caregiver)

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 Caregiver 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 Health Caregiver of source and requesting devices [4]. For the data sharing request (Algorithm 1.3), the response at the patient device is made by validating the token utilizing 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.

3.2. Listener

Control Registration, sub-module of the listener, initiates a registration request (Algorithm 2.1) after a specific time interval on each mCloud 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. mCloud device gets registers if the HOP count is low for the receiving device [33]. 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 mCloud devices are utilizing 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 [2]. Listener shares data to the requesting mCloud device if and only if both the systems are securing the data utilizing 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 utilize distributed services. In distributed services, conversions are performed to apply the required security technique by utilizing the list of nearby registered devices [25].

3.3. **Conversion**

It verifies whether the nearby device is capable of applying the required encryption technique for the requested mCloud 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 [1]. 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 utilizing the publishing method as an output [37].

3.4. **Security Layer**

The authentication layer is composed of multiple coding techniques such as symmetric encryption (DES, 3DES), Cipher text policy-based encryption attributes and Elliptic Curve Cryptography. The mCloud are low power computing devices and some of them are unable to apply even simple encryption techniques; therefore, distributed security services are utilized in the proposed system [35]. Attribute Based Encryption for high security and Elliptic Curve Cryptographic technique for low power computing devices are being utilized (Yang et al., 2017). In the proposed system, we are suggesting the combination of both techniques because the single Attribute based encryption utilize large private key size, whereas the Elliptic Curve cryptography has poor flexibility in revoking an attribute [21]. Therefore, the proposed system presents a hybrid encryption technique, which is a combination of Elliptic Curve Cryptography and user defined attributes. The user must have the data decryption key and attributes. Therefore, the suggested technique is the combination of CP-ABE and Elliptic Curve Cryptography. These attributes set by the mCloud device that sends its data [17].

3.5. **Publish**

After applying the requested encryption technique the conversion module forwards request to the publish module. The module transmits the data to the requested node directly [28]. To confirm the data comes from the node of the parent, 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 [3].

3.6. 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 mCloud devices. When a patient visits a doctor, the doctor requires his healthcare readings that are stored in the patient's mCloud 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. The doctor communicates with the devices to get the patient data utilizing 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 mCloud devices. These systems provide additional security layers that improve the protection of the content found in the data transaction. A patient mCloud 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 utilizing the combination of lightweight Elliptic curve cryptography 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.

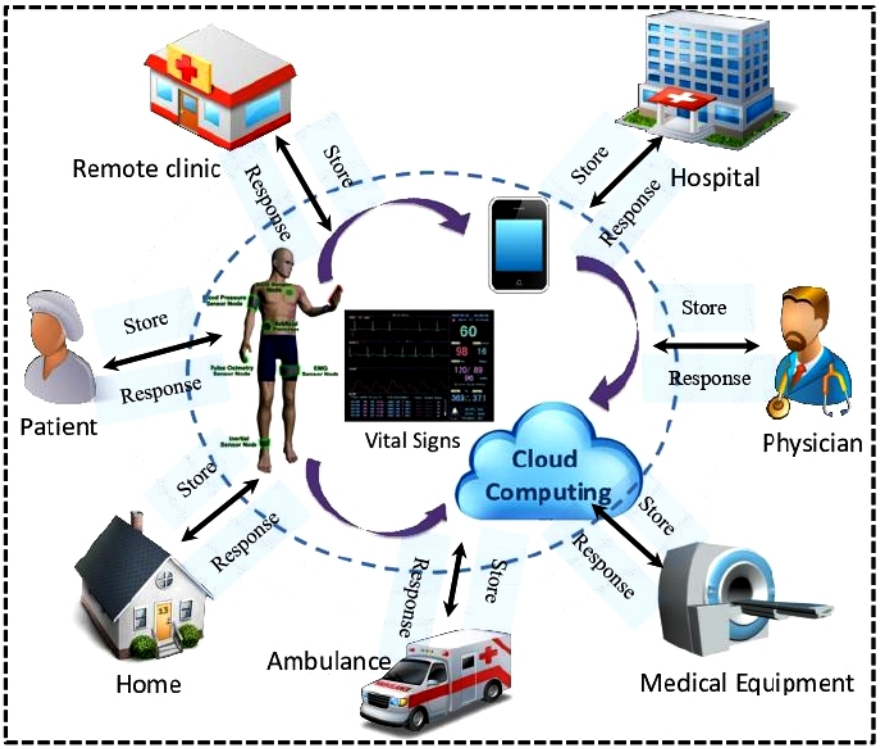

Figure 2: Infrastructure of Centralized System (Store and Response System)

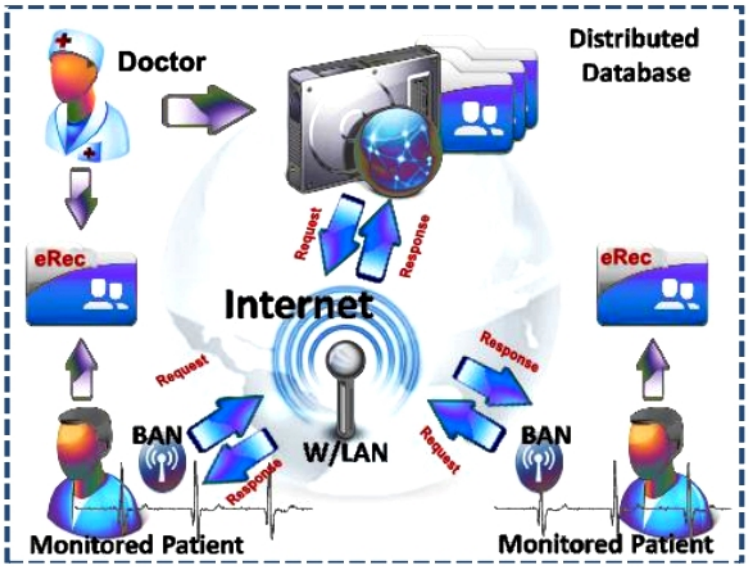

Figure 3: Infrastructure of Distributed System (Request and Response System)

4. Evalution

4.1. Experimental Setup

We developed two simulators to calculate the efficiency of the purposed 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 mCloud devices to generate healthcare data (blood pressure, Heartbeat rate). 20% of these devices do not have the ability to provide encryption. Hence, these mCloud 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.

4.2. Experiment No. 1

In this experiment, 400 devices scenario was simulated and during the data transfer, the network traffic was monitored utilizing 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 mCloud devices' security comparisons in our proposed system. It can be observed in the figure that with the growth of many mCloud 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.

4.3. 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 centralized and proposed distributed system is listed in Table 2.

Data transfer (Table 2) is the time taken for the patient's mCloud device to encrypt its data and store locally whereas access time is the time for doctor's mCloud device to get data from patient's device on the network. 20% of the total devices utilize distributed processing by utilizing encryption services from other devices on the network. Response time for the centralized system is

Table 2: Comparison table different from the proposed distributed system (Table 2). Findings generated utilizing a combination of different devices. If we develop results utilizing ten different mCloud devices and fewer requests, the centralized system gives better results (Fig. 7) than the distributed system. However, in case of an increased number of mCloud 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 mCloud 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 0.52 ms (in a centralized system) to 0.50ms (in a distributed system).

Table 2: Comparing Table between Centralized system and Distributed system

		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

5. Discussion

Healthcare data like blood pressure, heart rate, pulse rate and other collected through mCloud devices. Patients share their data with doctors and health care centers utilizing these mCloud 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 mCloud 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. A proposed additional protection layer for thin, lightweight computer devices. Proposed security layer comprised of a combination of user defined attributes with Elliptic Curve Cryptography.

In a centralized system, when the data moves between mCloud 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 security of transaction data content. 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 mCloud devices. This shows that the device level.

Security provided by the symmetric cryptography is low as it makes utilize of a single public key that is easily accessible. Therefore, for providing reliable security when we make utilize of simple asymmetric techniques; which provide security, but that is not enough to protect the patient's sensitive data in low power mCloud devices (Yang et al., 2017). When it comes to CP-ABE and Elliptic Curve Cryptography 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. Elliptic Curve Cryptography 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. Elliptic Curve Cryptography keys are a lot smaller than other forms of encryption such as RSA keys. The key power of Elliptic Curve Cryptography is half the main size, so an Elliptic Curve Cryptography key of 256-bit capability of 128 bit. A RSA key of 3,076 bits is also very solid. However, the single Elliptic Curve Cryptography encryption scheme has poor flexibility in revoking attribute (Yang et al., 2017). A purpose-built solution focused on privacy and security standards was designed to allow data exchange through healthcare systems. We suggested an Attribute based Elliptic curve cryptographic technique to secure mCloud device data. Poor flexibility in revoking attribute issue of Elliptic Curve Cryptography is handled by adding attributes. Therefore, a combination of Elliptic Curve Cryptography with attributes provides an extra security check during data decryption. Comparison in Table 3 shows the security techniques and their proficiencies utilized in our framework. Table 3, describes the qualitative results from the literature.

Table 3: Comparison of Security Properties encryption in proposed distributed architecture provides a secure data transmission

PROPERTIES	SYMMETRIC	ASYMMETRIC	CP-ABE	ELLIPTIC CURVE CRYPTOGRAPHY (ECC)	ELLIPTIC CURVE CRYPTOGRAPHY +ATTRIBUTES (ECCA)
SECURITIES	LOWs	MEDIUMas	HIGHcp	HIGHecc	HIGHecca
PRIVACIES	LOWs	MEDIUMas	HIGHcp	HIGHecc	HIGHecca
SIZE OF KEYS	LARGEs	LARGEas	LARGEcp	SMALLecc	SMALLecca
SECURITY ON SEVERAL LEVELS	NOT ACHIEVED	ACHIEVED	ACHIEVED	ACHIEVED	ACHIEVED

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 mCloud 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 utilizing 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 mCloud devices simultaneously. It shows that distributed architecture provides secure and efficient data transmission.

6. Conclusion and Future Work

In its features, this manuscript specifically proposed appropriate architectures and access management technology for a mCloud distributed healthcare environment. The proposed scheme includes a security layer that enables device-level encryption and ensures the integrity of content contained in transaction data. Different encryption algorithms have been applied according to the processing capacity of mCloud systems to overcome the issue of mCloud computer resource limitations. Since it uses a smaller key scale, elliptic curve coding has been shown to be a safer method for dealing with low-power computers. As an extra protection measure, we proposed using elliptic curve coding for attributes. The proposed system's usefulness for simultaneous data requests from various mCloud devices was also checked to determine the best overall response time. Our protection layer can be improved in the future to allow encrypted data transfer for more complex types of data, such as images and videos.

References

[1] A. S. Abdulbaqi, S. A. D. M. Najim, S. M. Al-barizinji and I. Y. Panessai, *A Secured System for Tele Cardiovascular Disease Monitoring.* In Computational Vision and Bio-Inspired Computing, Springer, Singapore, 2021, pp. 209-222.

[2] A. S. Abdulbaqi, S. A. D. M. Najim and R. H. Mahdi, *Robust multichannel EEG signals compression model based on hybridization technique,* International Journal of Engineering and Technology, 7(4) (2018) 3402-3405.

[3] A. S. Abdulbaqi, A. J. Obaid and S. A. H. Alazawi, *A Smart System for Health Caregiver Based on IoMT: Toward Tele-Health Caregiving,* iJOE, 17(07) 71, 2021.

[4] A. S. Abdulbaqi, E. S. Yousif and S. Al-din, *Virtual Environments Utilization for ECG Signals Analysis and Evaluation: Towards Heart Condition Assessment,* In IOP Conference Series: Materials Science and Engineering, IOP Publishing, November, 928(3), 2020, p. 032031.

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

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

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

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

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

[10] M. M. Alzghoul, *Towards Nationwide Electronic Health Record System in Jordan,* 2016, 650-655.

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

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

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

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

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

[16] A. Ekblaw, A. Azaria, J. D. Halamka and A. Lippman, *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, August 2016.

[17] M. H. Ellewe, A. M. Sagheer and A. S. Abdulbaqi, *A New Medical Images Encryption algorithm Based on Gold Code: Futures Trends Towards Telemedicine,* In IOP Conference Series: Materials Science and Engineering, IOP Publishing, 928(3), November 2020, p. 032032.

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

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

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

[21] M. N. Jain, *Security And Privacy Optimization And Service Provider Selection For Cloud Computing For Small And Medium Educational Institutions,* Turkish Journal of Computer and Mathematics Education, TURCOMAT, 12(10) (2021) 3753-3762.

[22] Z. Lie, X. Huang, Z. Hu, M. K. Khan, H. Seo and L. Zhou, *On Emerging Family of Elliptic Curves to Secure Internet of Things: Elliptic Curve Cryptography Comes of Age*, XX(XX), (2016) 1-12, https://doi.org/10.1109/TDSC.2016.257702 2.

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

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

[25] A. P. Oladeji and A. Olubunmi, *Data Offloading Security Framework in MCLOUD,* Journal of Computer Sciences and Applications, 5(1) (2017) 25-28.

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

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

[28] D. Sánchez and A. Viejo, *Personalized privacy in open data sharing scenarios*, Online Information Review, 2017.

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

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

[31] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon and R. Guizzetti, *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.2014.69 , 18975.

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

[33] M.Wolfson, S. E. Wallace, N. Masca, G Rowe, N. A. Sheehan, V. Ferretti and P. R. Burton, *DataSHIELD: resolving a conflict in contemporary bioscience-performing a pooled analysis of individual-level data without sharing the data*, International journal of epidemiology, 39(5) (2010) 1372-1382.

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

[35] E. S. Yousif, A. S. Abdulbaqi, A. Z. Hameed and S. Al-din, *Electroencephalogram Signals Classification Based on Feature Normalization,* In IOP Conference Series: Materials Science and Engineering, IOP Publishing, 928(3), November 2020, p. 032028.

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

[37] J. Zeng, Z. Long, G. Shen, L. Wei and Y. Song, *MCloud: Efficient Monitoring Framework for Cloud Computing Platforms*, In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, December 2017, pp. 409-419.