Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Security Enabled Response Delay Reduction in Healthcare Application Using Fog Computing

[1]Agnivesh Kumar Agnihotri, [2]Dr. Shashikant Gupta, [3]Dr. Basant Tiwari
[1]Research Scholar, Department of Computer Science and Application, ITM University, Gwalior
[2]Head of Department, Computer Science and Engineering, ITM University, Gwalior
[3]Associate Professor, Department of Computer Science and Engineering,Hawasa University,Ethiopia

Abstract
Owing to the Internet of Things' explosive growth in the last several years, wireless sensing technology has found a home in the healthcare industry, where up-to-date, accurate, and sound data forms the basis for all health system decision-making and is crucial for the creation and execution of health system policies. Fog & Cloud computing are new technological paradigm that provide on-demand availability of computing resources, especially storage and computing capability, without direct active management by the end-user. This paper proposes three-tier architecture for pervasively patient monitoring with security to patient data including confidentiality & integrity and fog-enabled data management that ensures less response delay toward patient treatment. For ensuring patient's data privacy, paper used ECIES based encryption/decryption method, that provide integrated scheme for confidentiality as well as integrity. For confirming reduced response delay, paper proposed fog enabled database management technique that provide data virtualization view and 'time/recency context aware' store/access method. The proposed architecture is simulated over Network Simulator-2 for implementing security algorithm and fog enabled 'time/recency context aware' store/access method. Simulated work is analyzed using various performance metrics like throughput, PDR, E-E delay, routing overhead and Hit/Miss ratio and compared against two scenarios named cloud only scenario and fog enabled scenario. Additionally, the efficiency of the suggested approach for protecting patient physiological data is examined in relation to security assaults such as Man in the Middle (MiTM) attack, chosen cypher attack, unforgeability, and non-repudiation.

Keywords: *Healthcare; Fog computing; Cloud computing; Physiological values; Patient' privacy, Reduced response delay; Data virtualization; NS-2.*

1. Introduction

A health information system (HIS) is a system that supports hospital functional management, collects, stores, manages, and transmits patient Electronic Health Records (EHRs), and provides an infrastructure to support policy decisions regarding healthcare data [1]. Comprehensive and consistent information is essential for the creation and execution of healthcare policy in all healthcare systems, traditional and electronic [2]. It also serves as the foundation for accurate decision-making.One of the main tenets of the healthcare system is the application of computing and communication technology, which enables the delivery of accurate and timely information to all stakeholders, including patients and healthcare providers. These technologies include client-server technologies, which offer an extensive database management system, wireless sensor technologies, IoT, & communication technologies for connected healthcare. The IoT&WSN are developing fields that integrate sensing, processing, and communication into one small device. By using IoT for patient monitoring in healthcare, new approaches to giving patients high-quality care are made possible. In the past several years, cloud computing has emerged as a new trend for patient EHRs administration data computation and storage as an online backend centralized system. Yet, network congestion, particularly in the healthcare system, frequently

prevents centralized cloud storage from offering real-time services and results in patient fatalities. CISCO proposed the Fog Computing infrastructure as a way to address the issue of network congestion and overcrowding. This infrastructure is an extension of cloud technology [3].

As demonstrated in Figure 1, fog computing is a distributed computing technology that functions as a bridge between cloud datacenters and IoT devices, such as medical sensors. Fog computing enables the closer integration of cloud computing resources and services with IoT devices and sensors by providing processing, networking, and storage capabilities. IoT devices are extensively distributed and have latency-sensitive, real-time service requirements at the edge of the network. The spatially centralized nature of cloud datacenters makes it difficult for billions of geographically dispersed IoT devices to meet their processing and storage needs. Consequently, poor Quality of Service (QoS), significant latency in service delivery, and network congestion are encountered. In a fog computing environment, network equipment can be located closer to IoT devices and typically includes routers, switches, set-top boxes, proxy servers, Base Stations (BS), etc. [4].

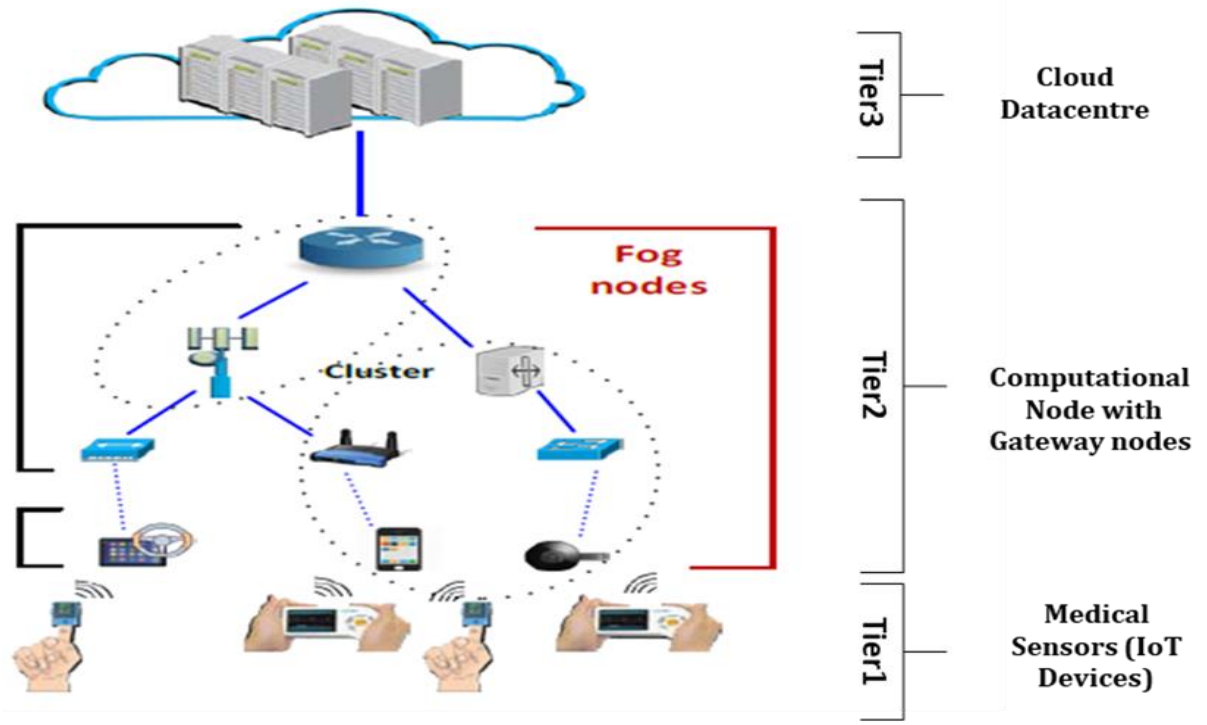

Figure 1: Fog based healthcare computing environment.

IoT devices can execute service-applications and come equipped with a range of processing, networking, and storage features [5]. Fog computing makes it possible to distribute Cloud-based services over wide geographic areas thanks to its networking components. Furthermore, mobility, scalability, interoperability, location awareness, and real-time communications are made easier by fog computing. Since fog computing may be used to reduce service latency, power consumption, network traffic, capital & operating expenses, content distribution, etc., it is a better and more useful technological choice for the healthcare services and domain.

By enabling patients to spend more time communicating with their physicians, electronic healthcare can increase patient happiness and engagement. It contributes to the transformation of healthcare by offering solutions that are affordable for both patients and medical professionals [6,7,8]. The most fundamental issues with these healthcare apps are data security and privacy, cost, accuracy and overflow of data, and device and protocol interoperability. Among these concerns, security, privacy, and prompt, accurate patient treatment are crucial elements that are taken into account in our work. The privacy of patients is a major consideration when using technology. Sensitive information that the patient might not wish to reveal could have a negative effect on their care. The integrity of this data must be guaranteed since the healthcare system encourages data interchange among its members in order to give patients better facilities. The effect of response delay in healthcare computing causing complicated health issues and even save or loss in human life [9]. So, data comes from any sensors to the main system or the system that utilize any physiological data must be reliable and time sensitive

to save the patient's life. Healthcare applications require extra security since private medical data needs to be shielded from fraud and unauthorized use for one's own gain [10].

This paper proposed an enhanced method that reduce or minimize response delay using three tire model. Further, this model also emphasizes on authentication, confidentiality and integrity issues using ECIEC (Elliptic Curve Integrated Encryption Scheme) algorithms. This will overcome the shortcomings of other traditional algorithms so as to get a better performance and to achieve the stringent performance to ensure above security issues in Fog computing healthcare application.

2. Related Works

Patients' data is sensed and sent to a base station for real-time data processing, storing, and decision-making in a HIS. Large-scale healthcare data processing quickly is a major problem for HIS. Numerous studies have been suggested about the use of fog-based systems for healthcare data processing, which gather, process, and send data to healthcare providers or storage devices for later use [11,12,13,14,15, 16]. Context aware computing, in which decisions are made in response to changing contexts, was also a part of this procedure. These fog-based frameworks increased the dependability of the HIS system by offering effective data processing techniques with less delay and speedy patient heath decision-making. Interoperability and delays are major problems with HIS systems. Different information processing and communication technology services are able to move and exchange data among many stakeholders who are configured with different technology devices with the best reaction time latency thanks to interoperability. The most recent communication technologies, such as 45G and 5G, are being used to handle this delay-sensitive and interoperability issue. A software framework built using Java and IDK services is being implemented [17, 18, 19, 20, 21, 22, 23]. The core function of HIS is to monitor patients' health in real time. Sensing, analyzing, diagnosing, and alerting patients and healthcare practitioners to illness are all included in this. Healthcare providers are provided in a quick, accurate, and dependable manner via the fog-based system. The fog-based system analyses physiological parameters associated with specific or general diseases to treat patients in a fast, accurate, and dependable manner. Real-time ECG monitoring, neurological monitoring, arthritic monitoring, and postural monitoring are among the studies [24, 25, 26, 27]. Because patient data in the HIS system is so sensitive and vulnerable to security breaches, it needs to be protected. The Health Insurance Portability and Accountability Act (HIPAA), which covers security & privacy rules for the use & applicability of protected health information (PHI), is supported by the US government. India and other developing nations are still pursuing this kind of initiative. Regarding the use, storing, and sharing of EHRs, the Medical Council of India has established certain rules and there is an information technology act [28]. Patient EHR availability, confidentiality, and integrity are examples of security concerns. EHR availability, confidentiality, and integrity. Unauthorized access to EHRsis linked to confidentiality concerns; unauthorized change of EHRs during transmission is linked to integrity issues; and unauthorized blockage of HIS services is linked to availability issues. A few of the studies that offered a security framework concentrated on protecting patient privacy, safeguarding the network from DDoS attacks, the function of certification authorities in ensuring the accuracy of patient data, and controlling access to EHRs, among other things [29,30,32,33,34,35,36].

3. Proposed Security Architecture, Setup and Algorithm

Proposed security protocol is based on Elliptic Curve Cryptography, where integrated version of ECC called ECIES has been used that provide security and privacy protections to a pervasive healthcare with ensuring integrity and confidentiality.This paper proposes Security Enabled Response Delay Reduction in Healthcare application using Fog based system. The layered architecture of proposed work is shown in figure 2 that is divided into three layers that are combinedly implemented on two sites namely Hospital Site and Cloud Site. Hospital Site implements Layer 1 and Layer 2 namely Sensing Layer and Fog implementation layer respectively. Layer 3 is referred as Cloud implementation layer which is implemented at Cloud site.

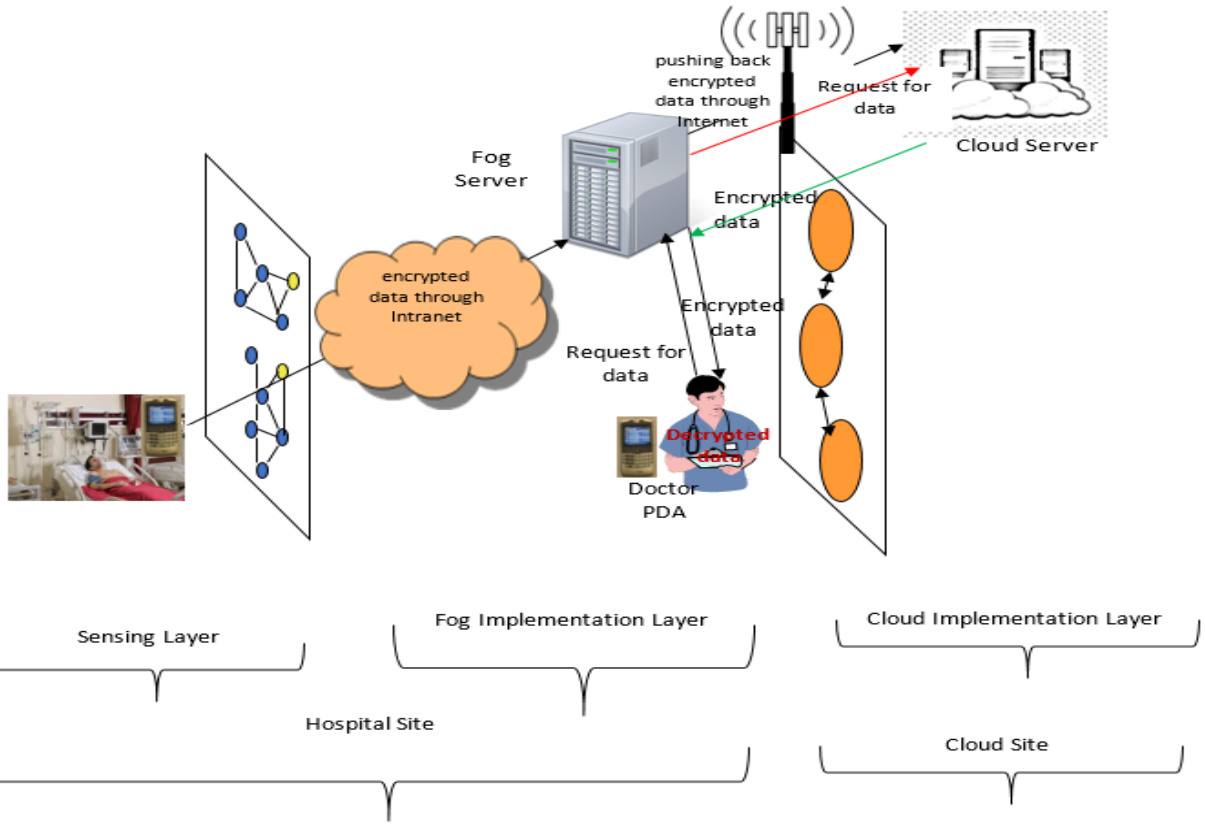

Figure 2: Proposed Architecture

At hospital site, sensing layer collect all the data using various physiological sensors implanted over patient body. These sensors sensed the data periodically and send it PDA device equipped near to patient, which collects all the data, encrypt it and send to the Fog Database implemented at the Hospital itself using intranet facility available at the site. The encrypted data is gathered and stored at the fog storage site. When a health care provider needs this data in an emergency, they first submit a request to the Fog database. This doctor has requested data from the fog server via the intranet facility using his PDA. The fog gadget now carries out the request and transmits information to the physician's PDA. The doctor's PDA decrypts this data. Whenever some extra data is needed by the doctor, that is not available at the Fog site, can be accessed by the doctor from Cloud site, where Cloud database isimplemented.

A variation of ECC, the ECIES is a public-key cryptographic technique that facilitates key exchange, digital signatures, and encryption.The ECIES, an integrated encryption system, employs the following primitives or operations:

A. Key Derivation Functions (KDF)

The KDF is used by the ECIES and the key agreement schemes. Keys are obtained via the KDF. The basic hash function construct, or ANSI-X9.63 KDF, is the KDF employed in this investigation.

B. MAC scheme

The MAC scheme is used by the ECIES. The receiver Database Server (Fog as well as Cloud Server) and the patient's PDA are the two entities intended to use MAC schemes. The suggested protocol makes use of the 128-bit key MAC feature of HMAC-MD5.

C. Symmetric Encryption Scheme

The Symmetric encryption scheme is used by the Patient’s PDA & recipient Database Servers (Fog & Cloud server), when patient’s PDA sends a message M to fog server and server recover M. The same process will execute when data is transferred between Fog Server to Cloud Server.In this context, symmetric encryption techniques are explained in terms of key deployment and setup processes, as well as encryption and decryption operations. When communicating, the patient's PDA and the receiver Database Servers (Fog and Cloud server) employ the following scheme:

Symmetric key cryptography (K_S) is used by the recipient database servers (Fog) and the patient's PDA to govern the encryption and decryption processes. When a patient's PDA transmits a message M to the fog server, it computes the cypher text C using the symmetric key KS and dispatches it to the fog server. When Fog Server receives C, it employs the same symmetric key KS to decrypt C in order to recover the message M. When data is transferred between the fog server & the cloud server, the same procedure is used.

The suggested work employs the XOR encryption system, wherein the message is encrypted by XORing the key & the message, and the message is decrypted by XORing the key and the ciphertext.

D. Selection of Domain Parameter

The numbers a & b must be entered into the provided elliptic curve equation, $y^2 = x^3 + axe + b$, where x, y, a, & b are elements in a Galois Field of order q, or GF (q), where q is a prime number, in order to select a specific ECC curve. Every option (a, b) produces a distinct elliptic curve. For the generation of values of a and b, system arbitrary select them and further based on these values particular elliptic curve is decided by the algorithm. The combination of x and y i.e. (x,y) gives us base point G. The x is found by taking a small random number. The value of y is given by $y = \sqrt{x3 + ax + b}$. Now system have a, b, G and it has to find the value of n by satisfying n x G = O i.e.,Point on the current elliptic curve at infinity. Now a, b, G, &n are decided and key generation process will start.

From the above basic ECC primitives, following function has been taken:

1. Setup
2. Key generation
3. Encrypt, and
4. Decrypt.

1. System Setup

In order to ensure security utilizing ECIES, Fog & Cloud server should carry out the following setup procedure:

I. The domain parameters of the elliptic curve over ρp have been determined, i.e., T = (p, a, b, G, n). These are composed of two parts, a and b, that indicate an elliptic curve E(Fp) defined by the equation, and an integer, p, that specifies the finite field Fp.

i. E: $y^2 = x^3 + ax + b \pmod p$,
a base point G (G_x, Gy) on E(Fp), a prime n which is the order of G.

II. Both Servers (Fog and Cloud) establish the KDF. For KDF, ANSI-X9.63-KDF with the option SHA-1 has been utilized in this work.

III. Then Servers establish the MAC scheme. In MAC scheme chosen, $k_M$denotes the key used by *MAC*, to produce tag. Proposed work used HMAC-MD5 MAC function.

IV. Now, server's symmetric encryption scheme has been chosen. Let *ENC* denote the encryption scheme chosen, &$k_s$denote the key used by *ENC* to produce cipher text. Proposed work includes X-OR Encryption Scheme.

Patient's PDA obtain the all above selections made by servers in an authentic manner, that are domain parameters T, the*KDF,* the *MAC*scheme, and *ENC*.

2. Key Generation

Patient's PDA, Fog Server and Cloud Server performthefollowingkeydeploymentproceduretopreparetouseECIES:

1. Servers establishanellipticcurve private and publickeypair $df_{dbs,}$ and $Qf_{dbs}$for Fog Server and $dc_{dbs,}$ and $Qc_{dbs}$for Cloud Server associatedwiththeellipticcurvedomain parameters*T*establishedduring thesetupprocedure.Thekeypairgenerated as follows:

Input:ECC DomainParameters T = (p, a, b, G, n).

Output:ECC keypair$df_{dbs,}$ and $Qf_{dbs}$for Fog Server and $dc_{dbs,}$ and $Qc_{dbs}$for Cloud Server relatedwith*T*between Fog Server and Cloud Server.

process: Generateanellipticcurvekeypairasfollows:

1.Randomlyorpseudo randomlyselectaninteger$df_{dbs,}$ anddc_{db}intheinterval 1 to *n*-1.

2.Calculate$Qf_{dbs} = df_{dbs}.G$. and Calculate$Qc_{dbs} = dc_{dbs}.G$.

3.Output df_{dbs}, $Qf_{dbs}$and dc_{dbs}, Qc_{dbs}

2. In the same way Patient's PDA generates in public and private key pair d_{pda} and Q_{pda}. Patient's PDA and DBS obtain in an authentic manner the elliptic curve public key of each other.

Next sub-section is proposing algorithms to make the communication between Fog Server and Patient's PDA as well as Fog Server and Cloud Server.

a. Encryption Operation

Patient's PDAencrypts messages 'M' using ECIES using the keys and parameters established during the setup procedure and the key deployment procedure as follows:

Algorithm: Encrypt(m)
Select a random number k ∈ [1, n- 1] and calculate R = kG Compute P (x, y) = k.Qf_{dbs} such that P ≠ 0. *IF P= 0 then it is invalid and go to step 1.* Execute Key Derivation Function (KDF) to derive a key i.e.,Kkdf= KDF(x). Parse the Kkdf into Ks and Km by shifting bits into Left and Right side. Encrypt M using established symmetric algorithm chosen at the time of setup i.e. $C = ENC (K_S, M)$ Execute MAC operation selected duringthesetupproceduretocomputethetag*D*: $D = MAC (k_M, C)$
Output: Cipher Text: Triplet (R, C, D) to Fog Server/Cloud Server

b. Decryption Operation

Fog Server decrypts cipher text using ECIES using the keys and parameters established during the setup procedure and the key deployment procedure as follows:

Algorithm: Decrypt (R, C, D)
Compute (X', Y') = d*fdbs*.R Execute Key Derivation Function (KDF) to derive a key i.e.,Kkdf = KDF(x'). Parse the Kkdf into Ks and Km by shifting bits into Left and Right side Execute MAC operation selected duringthesetupproceduretocomputethetag*D*: $D' = MAC (k_M, C)$ Check whether D'=D. If yes then go to step 6 else invalid D and stop the procedure. Decrypt C using established symmetric algorithm chosen at the time of setup i.e $M = ENC (C, k_S)$.
Output: Message M.

The above encryption/decryption operation is executed between Patient's PDA and Fog Server. The same operation is executed between Fog and Cloud Server using key pair generated between them, that are $df_{dbs,}$ and $Qf_{dbs}$for Fog Server and $dc_{dbs,}$ and $Qc_{dbs}$for Cloud Server.

c. Database Management and Querying

Since healthcare is a latency sensitive application where real-time streaming and processing response is very important concern and observations or monitoring is the vital target of application. The amount of data that is sent to cloud servers for processing, storing, & analysis is often less with fog computing. In a fog computing environment, smart devices situated at the network's edge handle data processing. In this lieu, fog database is implemented at the hospital site and it is near to access the data, but Fog database is limited in its size. this reduces the latency issue by enabling storage and computational resource close to the end-user with the benefit of fast processing especially at the time of emergency. As discussed in the proposed architecture in subsection 3.1, fog database is placed in between the patient's/doctor's PDA and the cloud database. It is used to hold recent/frequently used patient's data. This is done by storing the data that is frequently accessed by the doctors to monitor and observe the patient's condition to handle any emergency situation and hence it reduces the response delay.

Here, it is also important that how data is managed inside the fog and cloud database for healthcare application. For this, proposed work suggested following components of data management:

a) Data collection,

b) Data storage assessment at front fog site,
c) Data transmission to push back to cloud, and
d) Data searching and response to front end at doctor PDA.

a) Data Collection: In this component, fog database receives the encrypted data from sensors, decrypt it and store it to the fog database server. This data contains Patient_Id, Physiological Parameter Value, Date and Time of sensed value. For physiological parameters, Blood Pressure (BP), Heart Rate (HR), Body Temperature (BT) and Pulse Oximeter (PO) are considered. Following table shows one instance of Electronic Health Record (EHR):

P_id	BP	HR	BT	PO (%)	Time	Storage_Date	Accessed_Date	Recent Bit (1/0)
P001	80	70	101	100	05:05:23am	23/01/2020	--	0
P001	70	65	99	98	09:10:41pm	09/01/2020	24/01/2020	1
.	.	.	.	.	.	.		
.	.	.	.	.	.	.		

b) Data Storage Assessment at front fog site: This is internal component of fog device, that execute "Recent/Time-based Context Sensitive" data management algorithm takes care of size of database on the basis of time and date. The purpose of this module is to store recent data into the database. Recency of data is based on two criteria; Either data is stored with seven days (denoted by '0' bit) or data is recently accessed by the Doctor (denoted by '1' bit). This module will manipulate the recency bit by checking its accessed date. If accessed date is increased seven days, it will turn back to '0'. Whenever this module assesses the storage capacity of the database and find out the database of particular patient is older than seven days as well as its recency bit value is '0', it push-back this data to the cloud database.

c) Data Transmission to push back to Cloud: This module is fully responsible to push-back the data to offline backend and centralized database implemented at cloud after encrypting at fog site and that is further transferred over the internet and received by cloud site where this data is decrypted and further accumulated at the respective database.

d) Data Searching and Response to front end at Doctor PDA: This module is responsible for searching and response for required data, requested by the Doctor. This module gives the Data Virtualization view of data to doctor, by assuring that data will be replied to him/her, even either it is at the fog or not (i.e., at the cloud). When doctor want to access Patient's, he/she then contacts the Fog node and retrieves the data. He/She will never know about where the data is? This is the responsibility of module to provide in any condition. This module work with the Data assessment and storage module to check, whether is available at the fog or not. if data is available at the fog, it will return that data after encrypting, otherwise fog node.

Algorithm: Doctor querying for data

Doctor send Encrypted Message to Fog server with Patient-Id and required physiological parameters i.e. {Pid, phy_value}.
Fog device decrypt the Message 'M' and start searching of data in the fog database with K instances inside the database.

2.1. For every (pid^i, phy_value^i) i∈ K for patient do
Storage site matches pid^i,$Phy_value^i$with {Pid, phy_value} given by doctor
. If {Pid, phy_value} = = pid^i, phy_value^i then
Database device returns corresponding encrypted {pid^i,phy_value^i } to doctor.
Doctor executes the **Decrypt (**pid^i, phy_value^i**)**
Doctor accepts the patient data
Stop with successful Termination.
Else Go to Step-3
End if
2.2. End For
Fog sends Encrypted Message to Cloud server with Patient-Id and required physiological parameters i.e. {Pid, phy_value}.

Cloud server will execute the same step 2.1.1 to 2.1.2 with storing that data to fog database as per "Data Storage Assessment at front fog site" module and successfully stop the algorithm with guaranteed data access about required patient.

4. Result and Discussion

The outcomes of the suggested work's simulation procedure are compiled in this section. Two situations are used in NS-2 Version 2.31 simulation. First scenario implements security algorithm to ensure confidentiality and integrity of patient's data. Second scenario implemented for evaluating data accessing from cloud and Fog server with the concept of data virtualization to ensure response delay reduction. Each result has been discussed and compared with respect to both scenarios to prove the utility and improvement of proposed work (fog-based implementation) over old work (cloud-based implementation).

4.1. Cloud-Based Implementation

Cloud-based scenario shown in figure 3 deployed the patient's PDA, which receives the physiological values of BP, HR, BO and body temperature from patient's Body Sensor Network, where these sensors are implanted during medical treatment. These physiological values are transferred from Patient's PDA to cloud server after processing in fog device and which store in all the patient's data at cloud data center. Whenever, Doctor required the data, it request from cloud site and then cloud datacenter response to doctor query and send the respective data to doctor's PDA.

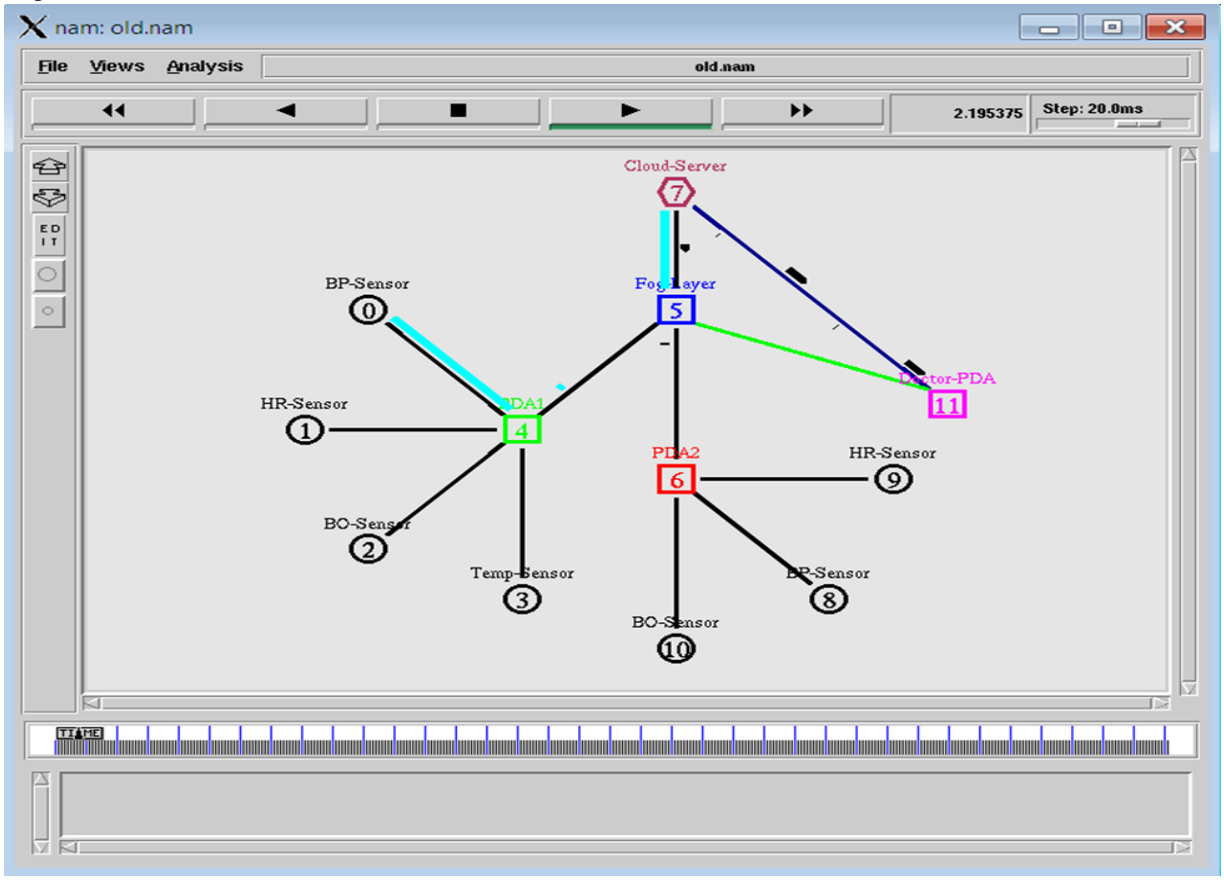

Figure 3: Cloud-based implementation with accessing data through cloud only

4.2. Proposed Fog-Based Implementation

The proposed fog-based scenario shown in Figure 4also deployed the same body sensors implanted over patient's body with PDA that transfer the data to fog site. Here an intermediate storage restricted database is implemented, where time/recency context data is stored to ensure the response delay reduction, while older data is transferred to centralized cloud server. The basic difference in previous scenario and proposed scenario is this, here, data is accessed only through the fog server with data virtualization view, while in previous scenario, data

is accessed on through the cloud site as shown in figure 3. Proposed scenario is useful for response delay minimization while receive secure data from the fog device

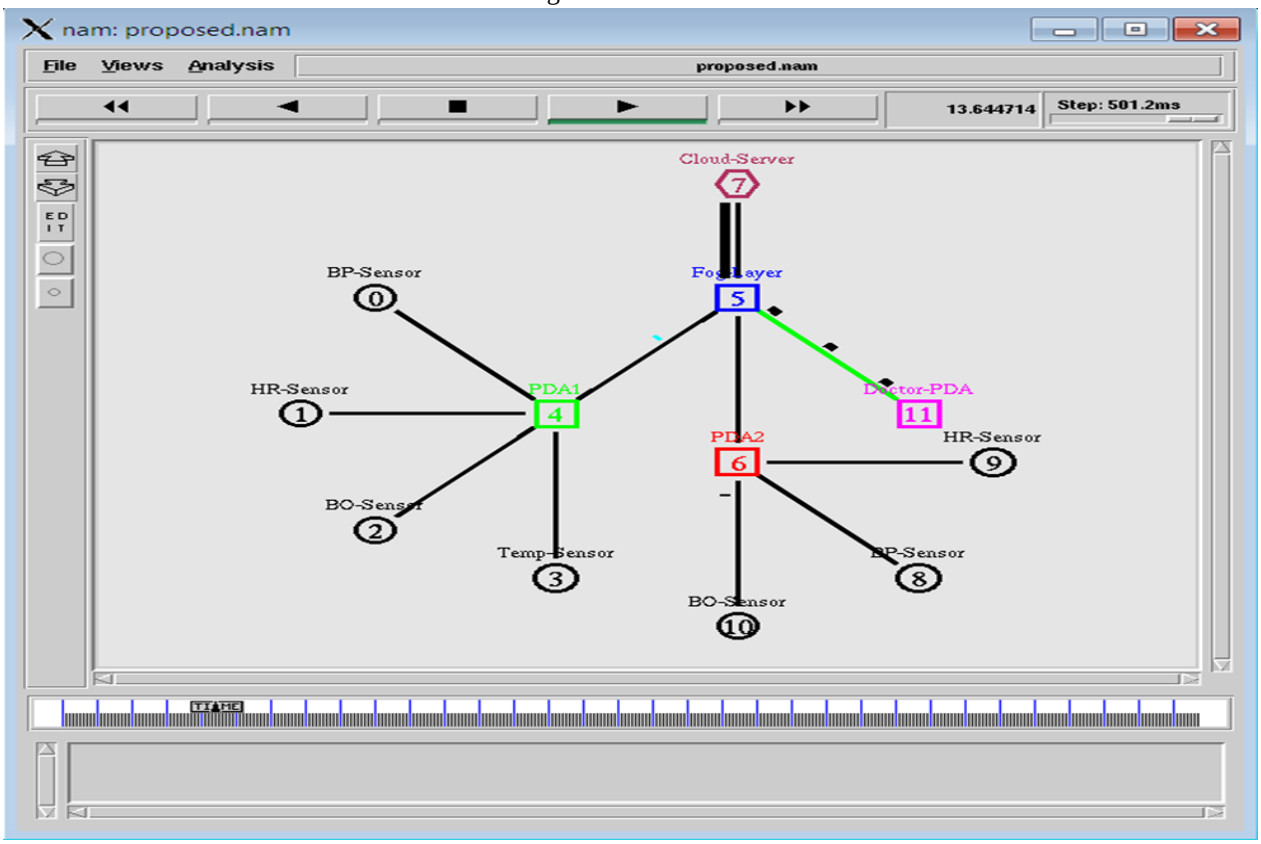

Figure 4: Proposed Fog-based implementation with accessing data through Fog only (Data-Virtualization View)

4.3. Simulation Parameter

This section describes simulation parameters like number of Cloud Server, Fog device, PDA, sensor type, and security mechanism etc. Table 1 below lists the simulation's parameters.

Table 1- Simulation Parameter

Devices & Protocols used	No. & Name
Cloud Server	1
Fog Device	1
Doctor PDA	1
Client PDA	2
Sensor Type (Per Patient) Blood Pressure Sensor (BP) Heart Rate Sensor (HR) Blood Oxygen Sensor (BO) Temperature Sensor (Temp)	 1 1 1 1
Simulation Time	100
Security Protocol	ECIES with SHA
Transport Layer	TCP, UDP
Traffic Type	CBR, FTP
Packet Size (bytes)	1000
Speed (m/s)	Random

4.4. Security Simulation

Proposed simulated encryption scheme is shown in following figure 5, where patient's PDA sends the data in encrypted form using ECIES algorithm with SHA. This data is stored at fog and cloud database after decryption that ensured the confidentiality and integrity as shown in following simulated result. Simulation is showing physiological parameter with real-time sensed value, its encrypted value and hash generated to ensure integrity.

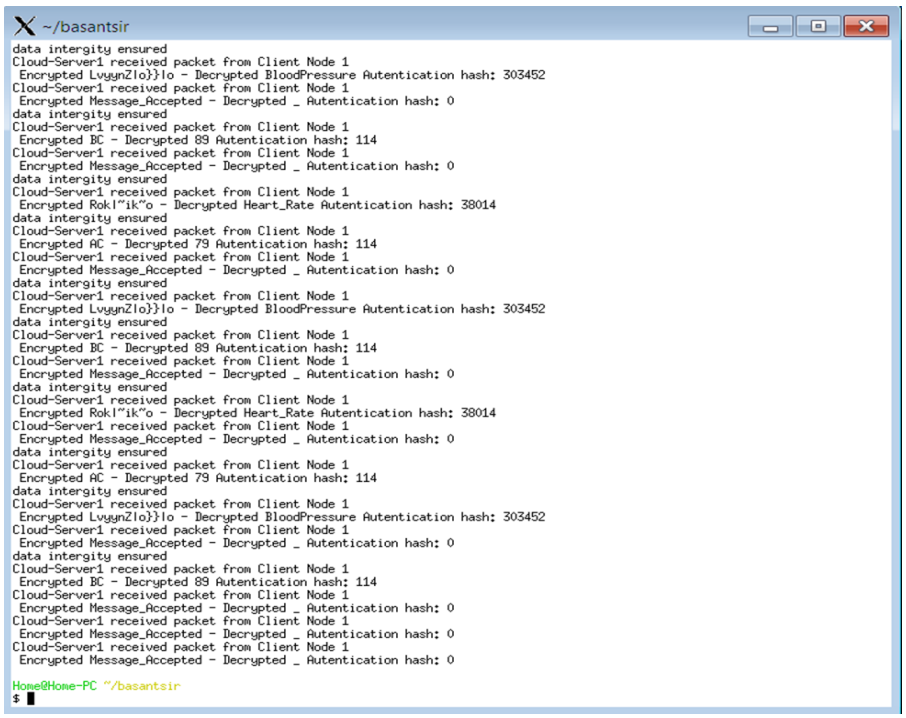

Figure 5: Encrypted data transmission simulation received at Fog and Cloud database

4.5. Throughput Analysis

Throughput is calculated with reference to accessing of data and measured per unit time (Kilobyte/second). The simulation results of both the scenarios (cloud and proposed fog) have been recorded for evaluation purpose. Following figure 6 shows throughput comparison in between data accessing only through cloud (scenario 1) and accessing data through cloud via fog i.e., data virtualization view (scenario 2).

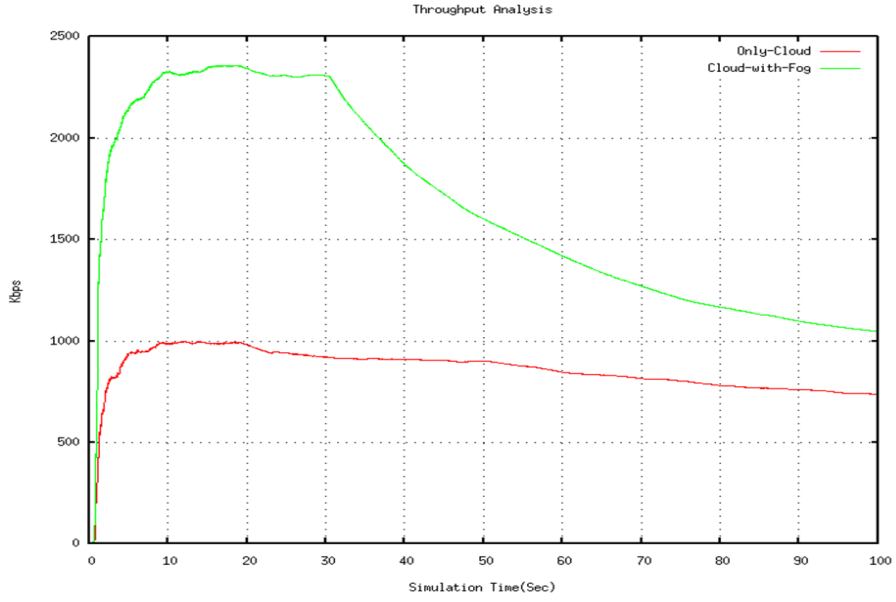

Figure 6: Throughput analysis between cloud only scenario and cloud via fog scenario

The Y-axis of the graph displays kilobytes per second, while the X-axis displays simulation duration in seconds. The comparison graph concludes that data accessing through data virtualization view i.e., accessing data from cloud via fog provide throughput as compare to only cloud device.

4.6. Packet Delivery Ratio Analysis (PDR)

PDR stands for proportion of data received relative to total data transmitted; a higher PDR indicates less data loss at the receiving end. Following figure 7 shows the PDR analysis and comparison. The comparison shows that cloud via fog scenario perform well as compared to packet delivery ratio from only cloud server scenario. This betterment is recorded because doctor receives the data directly from the fog device which store in local database and situated at nearby location and missing only data is called from cloud server.

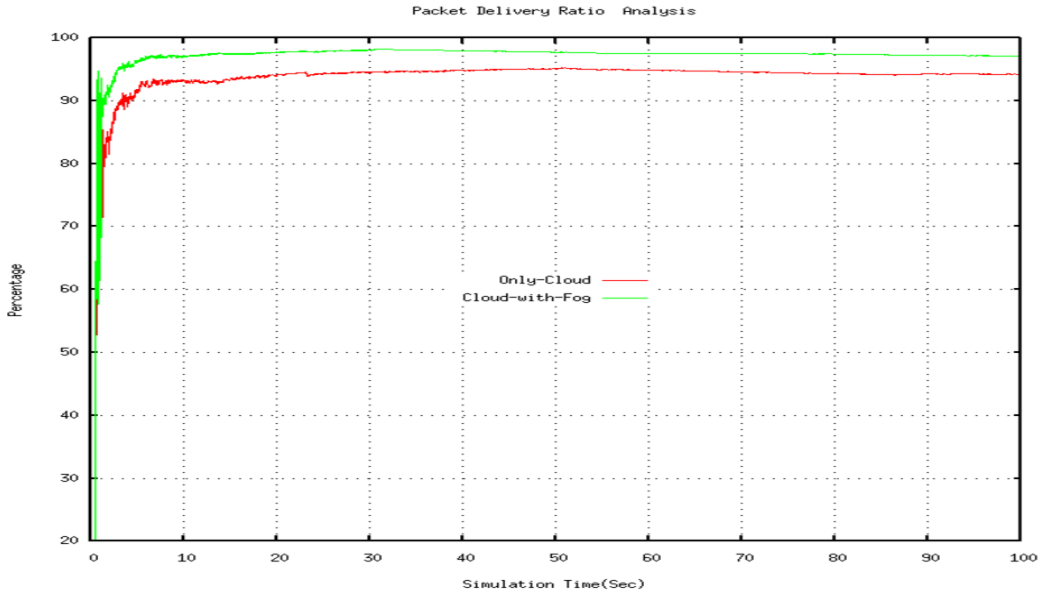

Figure 7: Packet Delivery Ratio analysis between cloud only scenario and cloud via fog scenario

4.7. End to End Delay Analysis (in Milliseconds)

The term "end-to-end delay" refers to the amount of time packets take to move from source nodes to receiver nodes. Queue latency, bandwidth, processing, and contention all affect end-to-end latency. When delay is higher it means network, performance is lower. The result graph shown in figure 8 shows that cloud via fog scenario record less end-to-end delay as compared to only cloud scenario. This results that proposed approach is better to reduce response delay after implementing Fog database in between Doctor's PDA and Cloud datacenter.

4.8. Routing Load (Overhead) Analysis

When data transmission is happened in the network, routing overhead for management of data transfer is accomplished by the network. For example, during data transmission, some control packets like ICMP, routing packet network error control packet etc. are also transferred to manage the network and to facilitate the data communication successfully, but at the same time, it increases the routing load and overheads of the network, that affect the data transmission capability. So, Routing load (Routing overhead) is calculated as ratio of total control packet out of actual data packet received by the receiver. Routing load is always lower when network bandwidth is maximally utilizing. The result graph shown in figure 9 depicted that proposed cloud via fog scenario recorded lower overhead as compared to cloud-only scenario. The reason of lower overhead in proposed solution is that most of the time data is accessed from local network at the same site using intranet facility, while in case of cloud only scenario, data is accessed through internet where bandwidth is shared among many users.

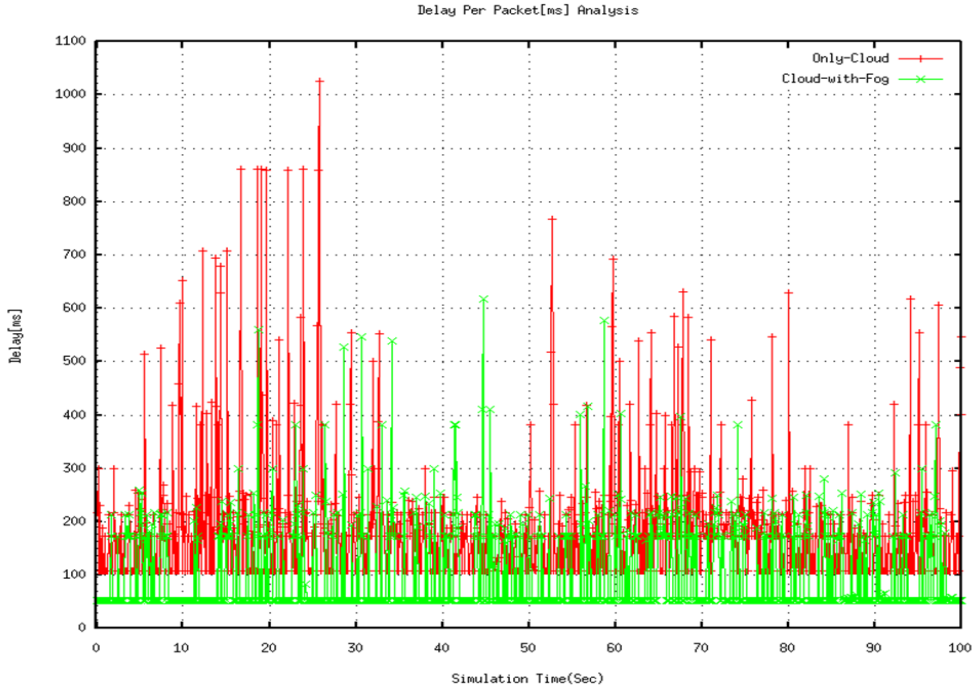

Figure 8: End-to-End delay analysis between cloud only scenario and cloud via fog scenario

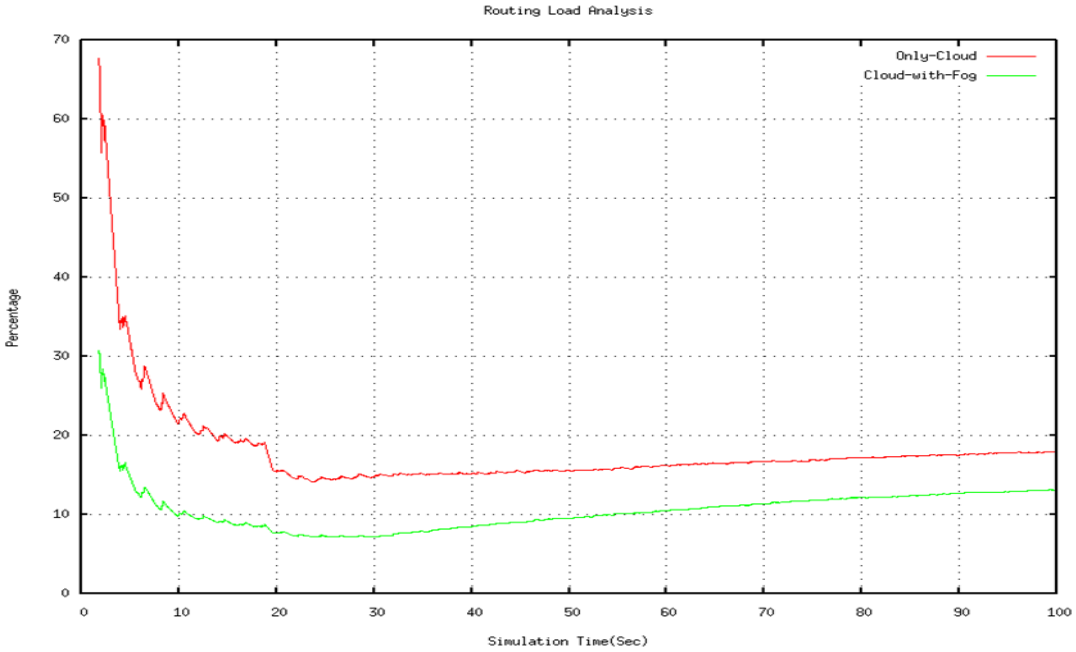

Figure 9: Routing Overhead analysis between cloud only scenario and cloud via fog scenario

4.9. Hit & Miss Ratio

The proposed work implemented Time/Recency context sensitive data storage at Fog site. In this sense, Hit and Miss Ratio become import concern and calculated with reference to fog database. Hit Ratio is the ratio between number of times data requested from fog server and it found in the fog database out of total number of requested generated. Similarly, Miss Ratio is the ratio between number of times data requested from fog server and it is not found in the fog database out of total number of requested generated. Hit Ratio is inverse of Miss Ratio and it affect the response delay. Following graph shown in figure 10 shows that Hit Ratio is better in proposed work and ensures reduction in response delay.

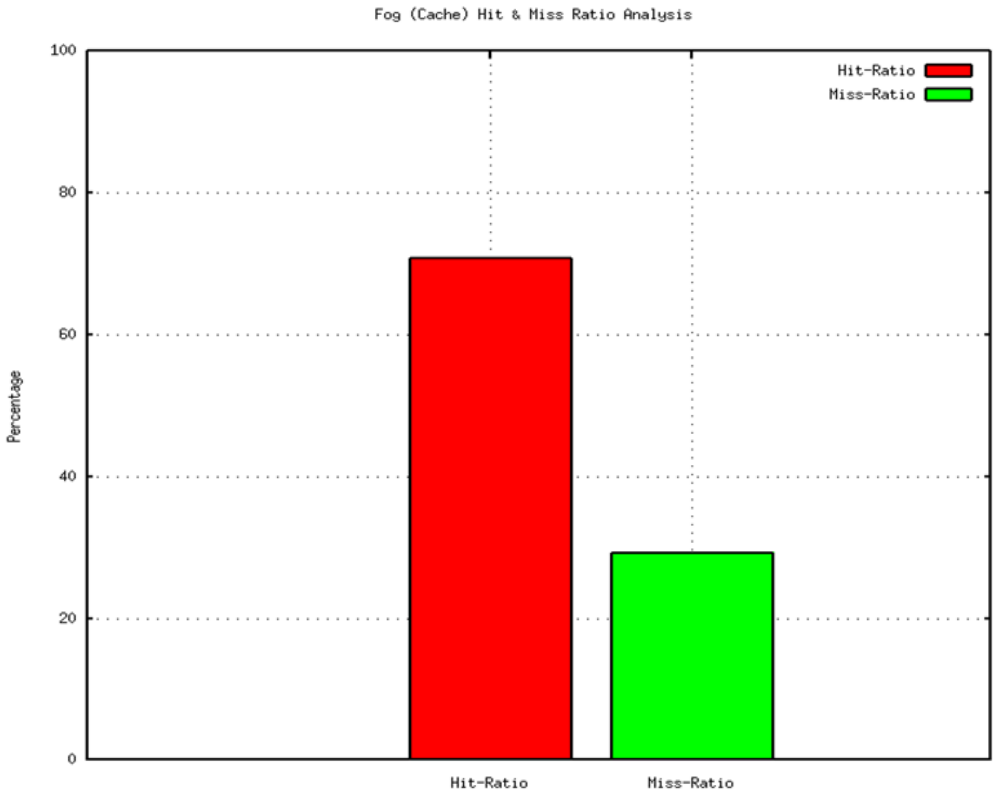

Figure 10: Hit & Miss Ratio analysis at Fog-site

4.10. Overall Network Analysis

The table 2 shows the comparative result between only cloud and cloud with fog and summarize the result with respect to all network dependent parameters such as total data receives from fog to doctor's PDA, from cloud to doctor's PDA, Hit and Miss ratio, Routing Overhead, average End-to-End delay &Throughput. The result table conclude that our proposed network provides better result as compare the Only cloud scenario.

Table 2: Result of overall network analysis for data accessing

Parameters	Only Cloud	Cloud with Fog
Data Receives from Fog Layer	0	3001
Data Receives from Cloud Server	2483	1241
Hit Ratio (Fog Cache)	-	70.74
Miss Ratio (Fog Cache Not Present)	-	29.26
Routing Load	18	13.2
PDR	94.16	97.18
Average E_E Delay (ms)	184.62	107.11
Throughput (in Kbps)	738	1046.78

1.11 Security Analysis

This section examines the security analysis of the suggested work in relation to security threats.

1.11.1 Man-in-the-Middle attack

On a network, an attacker watches as a session begins. Once a communication channel has been established, the attacker can use IP spoofing to pretend to be the authorised doctor & take control of the client computer, rendering it immobile. This assault is thwarted in this instance because the PDA transmits encrypted data rather than a message explicitly carrying his identification. Since he lacks the receiver's private key and the MAC code, the man in the middle is unable to decode the text.

1.11.2 Security against Chosen Cipher Text Attacks

The suggested plan is safe from the selected cypher text attack. The PDA uses the public key Q_{fdbs} from the Fog Database to encrypt every message that begins with "M." The trio (R, C, & D) is now selected & added to the fog database. A comparable technique is suggested for data transfer between clouds & fog. The suggested approach generates an arbitrary key pair using an arbitrary elliptic curve, so even if the attacker manages to obtain the chosen cypher text, he still requires the receiver's private key to build key pairs for deciphering, which he cannot find.

1.11.3 Confidentiality

Since symmetric encryption is implemented into our method, which is based on ECIES, it becomes difficult for an adversary to recover any information from the ciphertext. Our plan thereby ensures data confidentiality.

1.11.4 Unforgeability

The recipient database's (fog server or cloud server) private key, which is stored securely with the database, is needed to forge the message. Thus, the shared secret key generated during key generation is kept private, maintaining the feature of unforgeability. Furthermore, without knowledge of the PDA's private key, it is computationally impossible to produce a legitimate cypher text C provided by the PDA and claim that it came from the PDA.

1.11.5 Non-repudiation

The guarantee that someone cannot refute something is known as non-repudiation. That is, PDA cannot claim that it does not send encrypted text. By executing the verification process during the MAC verification process used in ECIES decryption, any trusted party or the recipient themselves can confirm that it was sent by the PDA.

1.11.6 Integrity

making sure that no unauthorized individual changes the information. Should an unauthorized user change the cypher text from C to C', the tag value during the decryption process will be determined to be something other than D. Integrity is guaranteed because this alteration was discovered during the verification phase (step no. 5 of the decryption procedure), when the recipient refused to accept the cypher text.

5 . Conclusion

In recent years' electronic healthcare has emerged as an effective technique for patient monitoring. But there are wide variety of challenging factors such as QoS and security of patient's physiological data. This paper presented an architecture that assures both the above requirements i.e., patient's privacy and reduced response delay. To ensure the patient's privacy, proposed work used the ECIES, an enhanced version of ECC algorithm, that encrypt the patient data before sending it to storage server and at the doctor's PDA at the time of accessing. This results in ensuring confidentiality of data and at the same time, by the same algorithm ensuring the integrity of patient's data, so that attacker cannot modify the data in transit as well as cannot disclose the patient's data. To assure the reduction in response delay from storage site, proposed work used Fog computing technology at the edge of the host network with storage capability that used to store recent data in the repository, where time/recency context sensing computing is used to assure recent data requirement. Here, we have used the concept of Data Virtualization from Doctor's point of view.

The proposed work is simulated in NS-2 simulator, and results are evaluated, analyzed and proved that proposed work is better over cloud technique on the basis of end-to-end delay, PDR and network overhead as far as response delay reduction is concerned. Since only one algorithm guaranteed both integrity and confidentiality, the suggested work maximizes security while using fewer computing resources to maintain integrity and confidentiality. In addition, it protects against a variety of assaults, including selected cypher, MiTM, unforgeability, & non-repudiation, making it an effective method of protecting physiological data from patients.

References

[1] M. Kumar and J. Mostafa, "Electronic health records for better health in the lower- and middle-income countries: A landscape study," Library Hi Tech. Emerald Group Publishing Ltd., 2020, doi: 10.1108/LHT-09-2019-0179.

[2] A. EGDAHL, "WHO: World Health Organization.," Ill. Med. J., vol. 105, no. 5, pp. 280–282, 1954, doi: 10.5260/chara.12.4.54.

[3] M. Pasha and S. M. W. Shah, "Framework for E-Health Systems in IoT-Based Environments," Wirel. Commun. Mob. Comput., vol. 2018, 2018, doi: 10.1155/2018/6183732.

[4] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A taxonomy, survey and future directions," Internet of Things, vol. 0, no. 9789811058608, pp. 103–130, 2018, doi: 10.1007/978-981-10-5861-5_5.

[5] P. Pagel and S. Schulte, "Fog Computing," Informatik-Spektrum, vol. 42, no. 4. Springer Verlag, pp. 233–235, 01-Aug-2019, doi: 10.1007/s00287-019-01211-z.

[6] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," J. Cloud Comput., vol. 6, no. 1, 2017, doi: 10.1186/s13677-017-0090-3.

[7] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Comput. Networks, vol. 144, pp. 17–39, 2018, doi: 10.1016/j.comnet.2018.07.017.

[8] Nasrullah Patel, "Internet of things in healthcare: applications, benefits, and challenges," 2019. [Online]. Available: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html. [Accessed: 22-May-2020].

[9] Y. K. Alotaibi and F. Federico, "The impact of health information technology on patient safety," Saudi Medical Journal, vol. 38, no. 12. Saudi Arabian Armed Forces Hospital, pp. 1173–1180, 01-Dec-2017, doi: 10.15537/smj.2017.12.20631.

[10] R. Priyadarshini, M. R. Panda, and B. K. Mishra, "Security in Healthcare Applications Based on Fog and Cloud Computing," in Cyber Security in Parallel and Distributed Computing, John Wiley & Sons, Inc., 2019, pp. 231–243.

[11] Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., et al. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641–658.

[12] Garcia-de-Prado, A., Ortiz, G., &Boubeta-Puig, J. (2017). COLLECT: COLLaborativEConText-aware service oriented architecture for intelligent decision-making in the Internet of Things. Expert Systems with Applications, 85, 231–248.

[13] Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for Healthcare 4.0 environment: Opportunities and challenges. Computers & Electrical Engineering, 72, 1–13.

[14] Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P. M., Sundarasekar, R., & Thota, C. (2018). A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generation Computer Systems, 82, 375–387.

[15] Sahni, Y., Cao, J., Zhang, S., & Yang, L. (2017). Edge Mesh: A new paradigm to enable distributed intelligence in Internet of Things. IEEE Access, 5, 16441–16458.

[16] Dupont, C., Giaffreda, R., & Capra, L. (2017). Edge computing in IoT context: Horizontal and vertical Linux container migration. In 2017 Global Internet of Things Summit (GIoTS) (pp. 1–4). Piscataway, NJ: IEEE.

[17] Mahmud, R., Koch, F. L., &Buyya, R. (2018, January). Cloud-fog interoperability in IoT-enabled healthcare solutions. In Proceedings of the 19th international conference on distributed computing and networking (pp. 1-10).

[18] Zhang, C., Cho, H. H., & Chen, C. Y. (2020). Emergency-level-based healthcare information offloading over fog network. Peer-to-Peer Networking and Applications, 13(1), 16-26.

[19] Yousefpour, A., Ishigaki, G., Gour, R., &Jue, J. P. (2018). On reducing IoT service delay via fog offloading. IEEE Internet of Things Journal, 5(2), 998-1010.

[20] Shukla, S., Hassan, M. F., Khan, M. K., Jung, L. T., & Awang, A. (2019). An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. Plos one, 14(11), e0224934.

[21] Mukherjee, M., Kumar, S., Zhang, Q., Matam, R., Mavromoustakis, C. X., Lv, Y., &Mastorakis, G. (2019). Task data offloading and resource allocation in fog computing with multi-task delay guarantee. IEEE Access, 7, 152911-152918.
[22] Khattak, H. A., Arshad, H., ul Islam, S., Ahmed, G., Jabbar, S., Sharif, A. M., & Khalid, S. (2019). Utilization and load balancing in fog servers for health applications. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-12
[23] Pace, P., Aloi, G., Gravina, R., Caliciuri, G., Fortino, G., & Liotta, A. (2018). An edge-based architecture to support efficient applications for healthcare industry 4.0. IEEE Transactions on Industrial Informatics, 15(1), 481-489.
[24] Vora, J., Kaneriya, S., Tanwar, S., Tyagi, S., Kumar, N., &Obaidat, M. S. (2019). TILAA: Tactile internet-based ambient assistant living in fog environment. Future Generation Computer Systems, 98, 635–649.
[25] Tanwar, S., Vora, J., Kaneriya, S., Tyagi, S., Kumar, N., Sharma, V., et al. (2019). Human arthritis analysis in fog computing environment using Bayesian network classifier and thread protocol. IEEE Consumer Electronics Magazine, 9(1), 88–94.
[26] Vilela, P. H., Rodrigues, J. J., Solic, P., Saleem, K., & Furtado, V. (2019). Performance evaluation of a Fog-assisted IoT solution for e-Health applications. Future Generation Computer Systems, 97, 379-386.
[27] Paul, A., Pinjari, H., Hong, W. H., Seo, H. C., & Rho, S. (2018). Fog computing-based IoT for health monitoring system. Journal of Sensors, 2018.
[28] Tiwari, B., & Kumar, A. (2015). Role-based access control through on-demand classification of electronic health record. International journal of electronic healthcare, 8(1), 9-24.
[29] Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., et al. (2018). BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1–6). Piscataway, NJ: IEEE.
[30] Liu, X., Deng, R. H., Yang, Y., Tran, H. N., & Zhong, S. (2018). Hybrid privacy-preserving clinical decision support system in fog–cloud computing. Future Generation Computer Systems, 78, 825–837.
[31] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50,102407.
[32] Vora, J., DevMurari, P., Tanwar, S., Tyagi, S., Kumar, N., &Obaidat, M. S. (2018). Blind signatures based secured e-healthcare system. In 2018 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1–5). Piscataway, NJ: IEEE.
[33] Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., &Sadoun, B. (2019). HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0. In 2019 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1–5). Piscataway, NJ: IEEE.
[34] Hayajneh, T., Griggs, K., Imran, M., &Mohd, B. J. (2019). Secure and efficient data delivery for fog-assisted wireless body area networks. Peer-to-Peer Networking and Applications, 12(5), 1289-1307.
[35] Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E., &Djaba, E. (2019). Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads. IEEE Internet of Things Journal, 6(2), 3925-3933.
[36] Awaisi, K. S., Hussain, S., Ahmed, M., Khan, A. A., & Ahmed, G. (2020). Leveraging IoT and Fog Computing in Healthcare Systems. IEEE Internet of Things Magazine, 3(2), 52-56.