The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

SECURITY ENABLED CLOUD-BASED ARCHITECTURE FOR HEALTH-INFORMATION SYSTEM

AGNIVESH KUMAR AGNIHOTRI[1], SHASHIKANT GUPTA[2] and BASANT TIWARI[3]

[1, 3] Dept. of Computer Science & Applications, ITM University, Gwalior, India.
[2] Dept. of Computer Science, Hawassa University, Hawassa, Ethiopia.

Abstract

Electronic healthcare (E-healthcare) is a combination of hardware, software, process, infrastructure, people, and protocol that is developed for the management of healthcare data including collection, storage, analysis, decision making, and transmission. It supports functional management of a hospital as well as provides an infrastructure that supports policy decisions over healthcare data. E-healthcare has grown decade by decade starting from 1960 to the present era and is divided into four-generation versions namely V.1.0 to V.4.0. E-healthcare in generation V.4.0 is dedicated to smart medical technology with cloud and fog-based computing systems including disease-oriented sensing systems, IoT, artificial intelligence, high-speed internet, and advanced internet protocols. This paper proposed a security protocol over a cloud-based system using an integrated version of ECC called ECIES that provides security and privacy protections to pervasive healthcare with ensuring integrity and confidentiality. The proposed methodology is simulated using Network Simulator-2 and analyzed using different performance metrics like routing load (Overhead), packet delivery ratio, end-to-end delay, and throughput under the scenarios of cloud-only and secured cloud scenarios. Further, the Proposed work is analyzed against various security attacks like MiTM (Man in the Middle), Security against Selected Cipher Text Attacks, Unforgeability and Non-repudiation, etc. Obtained findings indicate that the proposed method has a greater security level and reduced response delay with higher throughput. Finally, the paper concludes the proposed work and highlights the recommendation and future works.

Keywords: HIS, IoT, cloud computing, healthcare, medical sensors, ECIES

1.0 INTRODUCTION

Healthcare is a term used to provide qualitative treatment to maintain as well as improve the health of a patient against a specific disease. Patients are given Healthcare services in a hospital up to the home. From post-mid of the last century up to now, the healthcare industry has continuously evolved concerning hardware as well as software evolution [1]. This results in the emergence of various technologies for improving the lifestyle and healthcare of the patients with minimum cost and reduced time. The evolution of the healthcare industry includes its various generations that are classified from healthcare industry V.1.0 in the 1970s to healthcare industry generation V.4.0 in the current era [2]. Healthcare generation V.4.0 started around 2015 when wireless medical sensors became automated to take the preliminary decision about the health of patients and alert them. Intelligent sensing technology deployment becoming more advancing day by day that giving real-time monitoring and accurate decision-making about the patient without the restriction of time and place.[3].

Health Information System (HIS) [4] refers to a system that provides management of healthcare data including collection, storage, managing, and transmits a patient's Electronic Health Record (EHR), supports functional management of a hospital as well as provides an infrastructure that

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

supports policy decisions on healthcare data. HIS technologies in generation V.4.0 include Wireless sensors, IoT and communication technologies for connected healthcare, and Client-Server technologies for the comprehensive database management system. Sensing, processing, and communication are embedded together into a single tiny device in WSNs (Wireless Sensor Networks) and the IoT. Over the last few years, cloud technology becomes a new trend for data storage and computation of Patient EHR management as an online backend centralized system [5]. HIS generation V.4.0 utilizes the cloud-based technology, not only for storage of vast amounts of healthcare data but also provides a computing facility for process, analysis, and decision making in real-time with minimum interaction of healthcare providers. Cloud computing is used as utility computing for HIS, that have more computational power, a huge storage facility, and various networking resources. The Healthcare industry is now using cloud technology to increase efficiency, optimize workload, lower the costs of healthcare delivery and offer personalized care to improve results [6]. The cloud computing in HIS provides structured and well-organized sharing of healthcare data to all stakeholders, which results in the minimum risk of loss of EHRs. Some of the advantages of cloud computing in the HIS environment include (1) letting down operational expenses, (2) telemedicine capabilities (3) patient ownership of healthcare data, (4) high-powered medical analytics, and (5) ease of interoperability [7]. Although cloud technology becomes a new trend for data storage and computation of Patient EHRs management as an online backend centralized system, it possesses many security threats and privacy issues that are exploited by attackers such as tempering, jamming, denial of service, impersonation, forgery, spam., eavesdropping, man-in-the-middle and so on must be eliminated [8]. Another issue is Patient Privacy i.e patient privacy is a serious issue in HIS, which includes identity, data, usage, and location privacy of a patient. Thus, it is a thrilling issue in cloud computing since the patient's data is collected, stored, and transmitted through the network. Patient privacy includes identity privacy (like phone, address, UID, etc.), data privacy to preserve unauthorized and illegal usage, usage privacy to preserve patient's usual pattern, and location privacy to preserve patient's location information [9].

2.0 RELATED WORK

In HIS, the data of the patients is sensed and forwarded to a base station for data processing, storage, and decision-making purpose in real-time. Fast processing of huge healthcare data is a big issue in HIS. Various researches have been proposed regarding healthcare data processing using a cloud/fog-based system that collects, process, and transfer the data to the healthcare provider or storage device for further uses [10, 11, 12, 13, 14, and 15]. This processing also included context-aware computing in which decisions are made with the change of context [11]. These cloud and fog-based frameworks provided efficient data processing techniques with reduced delay and quick decision-making about patients' health that increase the reliability of the HIS system. Real-time patient health monitoring is the prime issue of HIS. This includes sensing, analyzing, and diagnosing disease and alarming patients and healthcare providers. Real-time monitoring in HIS includes policies and methods that help healthcare providers to monitor, diagnose and give treatment to patients. The cloud-based healthcare system provides accurate and reliable healthcare services to treat the patients by analyzing physiological values

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

related to particular or general diseases. Some of the research [16, 17, 18, 19, 20, 21, and 22] includes ECG monitoring, neurological monitoring, arthritis monitoring, and posture monitoring, and overall healthcare monitoring in real-time. Patients' data in the HIS system is extremely sensitive and HIS is always susceptible to security assaults, that's why it must be protected. The HIPAA ("Health Insurance Portability and Accountability Act") is endorsed by the US government and covers privacy & security rules for the consumption and revelation of PHI (Protected Health Information). India and other developing countries still working on such kind of act. Some guidelines are proposed by MCI ("Medical Council of India") as well as there is an information technology act regarding the utilization, storage, and sharing of EHRs [9]. Security issues include confidentiality, integrity, and availability of patients' EHRs. Confidentiality issues are related to unauthorized access of EHRs, integrity is related to unauthorized modification of EHRs during transmission and availability stated unauthorized blocking of HIS services. some of the research proposed by[23,24,25,25,27,28,29,30,31,32,33,34]provided a security framework that focused on maintaining patient privacy preservation during data transmission, preservation of network against DDoS attacks, the role of the certification authority in ensuring the patient data integrity, EHRs access control, etc.

3.0 SECURITY SOLUTIONS

For every system, security is crucial. In the case of healthcare systems, it is especially more crucial since these platforms deal with health information kept in Electronic Healthcare Records (EHRs).Privacy protection for patients is the primary objective of protecting healthcare systems. To ensure this, it is crucial to take precautions to stop any unwanted access to the system's EHRs in order. The security solutions of healthcare systems include the following two aspects that concentrate on protecting health data:

1. **Securing Medical-Sensor Communication**: The capabilities of individual medical sensors utilized in a BSN are consequently constrained by their very tiny form factors. Therefore, in the context of ubiquitous healthcare, complex, computation-intensive security mechanisms are required for protecting medical sensor transmission.
2. **Legislative Solutions:** Recognizing the significance of a legal framework for maintenance and protection of sensitive medical data kept as EPRs/EHRs. The obligations of data controllers and processors and the rights of data subjects are not clearly outlined under India's comprehensive data protection and privacy legislation. Even though provisions that can be used to this effect are scattered in various legal frameworks. This includes the MCI,Code of Ethics Regulations of 2002, Privacy and Right to Information Act of 2005, and Information Technology Act of 2000(India) u/s 3 addressesthe "authentication of electronic records" [22,35]. But these rules are not satisfactory nor up-to-date to address future technology innovations and contemporary privacy issues.

3.1 Proposed security protocol and Algorithm

This paper proposed a security-enabled cloud-based protocol for a health-information system based on Elliptic Curve Cryptography. Here, an integrated version of ECC called ECIES is

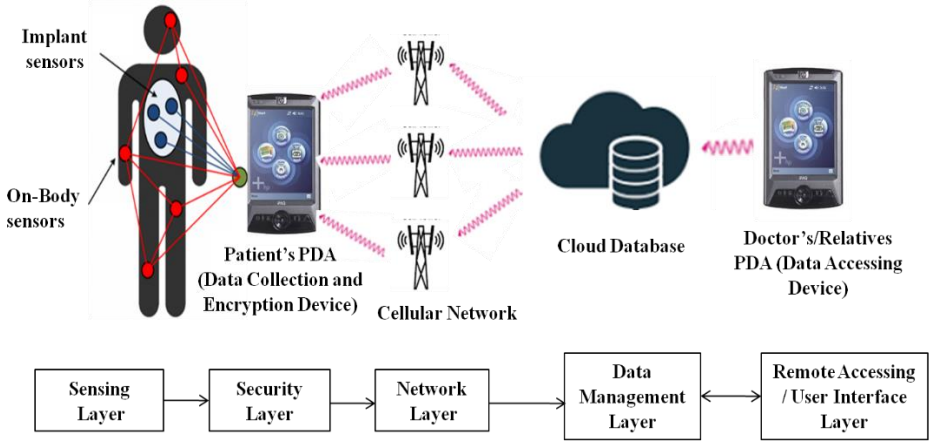
ISSN 1533-9211

DOI 10.5281/zenodo.7080841

used that provides security and privacy protections to pervasive healthcare with ensuring integrity and confidentiality. A public-key cryptographic mechanism that provides digital signatures, encryption, and key exchange is called ECIES ("Elliptic Curve Integrated Encryption Scheme"), which is a variation of ECC.

The general architecture of the recommended solution revealed in figure 1 is split into five layers. Out of them, the first two layers namely, the sensing layer and security layer are implemented at the patient's site. The sensing layer collects all the data using various physiological sensors implanted over the patient body. These sensors sensed the data periodically and send it PDA device equipped near the patient, which collects all the data, encrypts it, and sends it to the cloud database implemented at the data management layer shown in the figure using the cellular network. The cloud database receives a request when the healthcare professional needs this information at the time of emergency or normal situation. For this, the doctor request data by his PDA to the cloud server by a cellular/intranet facility. Then the cloud executes the request and sends data to the doctor's PDA. Communication within the system is fully encrypted i.e., data, as well as request/response, is encrypted within the network. When this data is received by the doctor, it is first decrypted by the doctor's PDA and further displayed on plain text using a user interface implemented as PDA.

Figure 1: Proposed protocol



The proposed security protocol first describes the initial phase where the Hospital sets up the physiological sensor network around the patient bed, and then the data collecting phase which summaries how a patient's PDA encrypts the gathered data. The data transfer phase between the Patient's PDA & Cloud Server using an internet facility outside the hospital describes how the system sends data to a storage site, followed by the query phase, which happens when a physician wants to retrieve data from the storage site.

The paper used ECIES for the encryption & decryption process. As its name suggests, ECIES is an integrated encryption method that makes the use of primitive's and functions. These include key derivation, MAC function, and symmetric encryption function/schemes to provide a strong security solution. One or more keys may be derived from a given secret value using

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

KDFs ("Key Derivation Functions"). The used KDF in this work is "ANSI-X9.63 KDF" which is the simple hash function design that is specified in ANSI X9.63 [51]. A recipient Database Server (Cloud Server) and a patient's PDA are the two entities that are intended to employ the MAC function. Here, the MAC functions are designed to make it difficult for an adversary to create legitimate tag and message pairings, allowing the scheme to guarantee data integrity and authentication. The symmetric encryption technique is utilizedvia the Patient's PDA and Cloud server, when the patient's PDA sends a message M to the cloud server and the server recover M. Proposed work uses the XOR encryption method, in which encryption contains XORing the key and message whereas decryption contains XORing the key along with the cipher text to retrieve the message. The proposed protocol derives the following primitives:

[51] B. Tiwari and A. Kumar, "Physiological Value-Based Privacy Preservation of Patient's Data Using Elliptic Curve Cryptography," Heal. Informatics - An Int. J., vol. 2, no. 1, pp. 1–14, 2013, DOI: 10.5121/hiij.2013.2101.

- System Setup
- Key generation
- Encrypt, and
- Decrypt.

A. System Setup

The cloud server must carry out the following setup process to prepare to utilize ECIES:

1. Each public-key cryptography system includes "arithmetic operations" on an elliptic curve over a finite field, which is specified by the elliptic curve parameters. The following are the domain parameters of elliptic curves over Fp:

   "T= (p, a, b, G, n)"

   Where, p specifies the finite field Fp, the selection of a particular ECC curve depends on values a and b in the given elliptic curve equation i.e., $y^2 = x^3+ax+b$ here x, y, a, & b represent element in a "Galois Field" of order q, namely, GF (q) where q indicates a prime number. Each selection of (a, b) produces a distinct elliptic curve. For the generation of values of a and b, the proposed protocol arbitrarily selects them, and further based on these values particular elliptic curve is decided by the algorithm.

   Now it needs value 'x' for the given ECC equation, which further derives value 'y'. 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 $y = \sqrt{x3 + ax + b}$

   Thus, protocol derived a, b, and based point 'G'. Now, protocol found the value 'n' by satisfying the equation n x G=O i.e. Point at Infinity on the present elliptic curve. Now proposed algorithm/protocol has a, b, G, and n.

ISSN 1533-9211

DOI 10.5281/zenodo.7080841

2. The cloud servers establish the KDF. This study used ANSI-X9.63-KDF using the SHA-1 option for KDF.
3. Then Server establishes the MAC scheme. In the selected MAC scheme, k M denotes the key that MAC uses, to create a tag. The HMAC-MD5 MAC function is a part of the suggested work.
4. Now, the server's symmetric encryption scheme is decided. Let ENC indicate the encryption scheme selected, and k_s signify the key utilized by ENC to create cipher text. The "X-OR Encryption Scheme" is part of the proposed work.
5. The patient's PDA obtains the selections authentically made by a server, which are the elliptic curve domain parameters T, the MAC scheme MAC, key derivation function KDF, as well as the symmetric encryption scheme ENC.

B. Key Generation

The patient's PDA and Cloud Server carry out the key deployment process listed below topreparetoutilize ECIES:

1. The cloud server establishes an elliptic curve private as well as public key pair $dc_{dbs,}$ and Qc_{dbs} for Cloud Server connected with the "elliptic curve domain parameters"created during the setup.These steps were taken to produce the key pair.

Input: Domain ECC Parameters "T= (p, a, b, G, n)".

Output: ECC key pair $dc_{dbs,}$ and Qc_{dbs} for Cloud Server related with T between PDA and Cloud Server.

Process: Generate the following key pairs for an elliptic curve:

1.Chose an integerdc_{db} at random or pseudo-randomly from interval 1 to n-1.
2.Calculate$Qc_{dbs} = dc_{dbs}$ .G.
3. Output $dc_{dbs,}Qc_{dbs}$

2. In a similar manner, the Patient's PDA creates in public as well as private key pair d_{pda} and Q_{pda}.The patient's DBSand PDAauthenticate each other using their elliptic curve public keys.

C. Encryption Operation

The PDA of the patients encrypts messages 'M' by ECIES using the keys & parameters created following setup & the key deployment technique described below:

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

Algorithm: Encrypt(m)
1. Choose a random number "k∈[1,n-1]" and compute R=kG 2. Calculate P(x, y) = k.Qc_{dbs} such that P≠0. If P=0 then the condition is invalid and go to step 1. 3. Execute KDF to derive a key i.e. Kkdf=KDF(x). 4. Parse the Kkdf into Ks and Km by shifting bits into the Left and Right sides. 5. Encrypt M using an established symmetric algorithm chosen at the time of setup i.e. $C = ENC (K_S, M)$ 6. Execute MAC operation selected during the setup procedure to compute the tag D: $D = MAC (k_M, C)$
Output: Cipher Text: Triplet (R, C, D) to Cloud Server

D. Decryption Operation

Cloud Server decrypts the cipher text with ECIES using the keys & parameters provided during the setup &key deployment procedures, as detailed below.

Algorithm: Decrypt (R,C,D)
1. Calculate(X', Y') = dcdbs.R 2. Execute KDF to derive a key i.e. Kkdf=KDF (x'). 3. Parse the Kkdf into Ks and Km by shifting bits into the Left and Right side 4. Execute MAC operation selected during the setup procedure to compute the tag D: $D' = MAC (k_M, C)$ 5. Verify that D'=D. If yes, go to step 6, otherwise invalidate D, and end the process. 6. Decrypt C using an established symmetric algorithm chosen at the time of setup i.e "M=ENC(C,k_S)".
Output: Message M.

4.0 IMPLEMENTATION

The proposed protocol is simulated in NS-2 Version 2.31 with the implementation of a security algorithm to guarantee the confidentiality and integrity of patient data. Here, two scenarios namely only cloud and cloud with security (Sec-cloud) have been simulated to check the efficiency of the proposed work. The simulated input parameter used is indicatedin following table 1.

ISSN 1533-9211

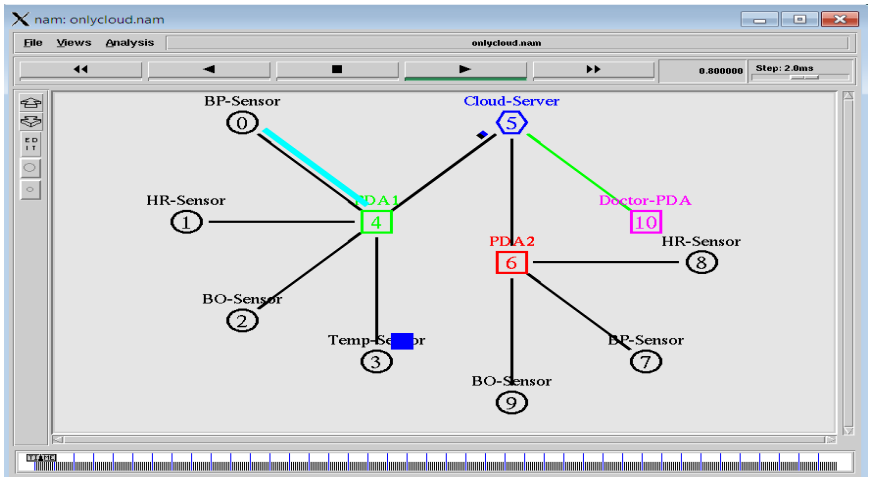
DOI 10.5281/zenodo.7080841

Table 1: Parameter for Simulation

Cloud Server	1
Doctor PDA	1
Client PDA	2
Sensor Type (Per User) • BP Sensor • HR-Sensor • BO-Sensor • Temp. Sensor	 1 1 1 1
Simulation time (seconds)	100
Security Method	SHA
Speed (m/s)	Random
Packet size (bytes)	1000
Traffic type	CBR, FTP
Transport Layer	TCP, UDP

NS-2 environment created for the execution of the proposed work is revealed in figure 2:

Figure 2: Simulated environment for proposed work



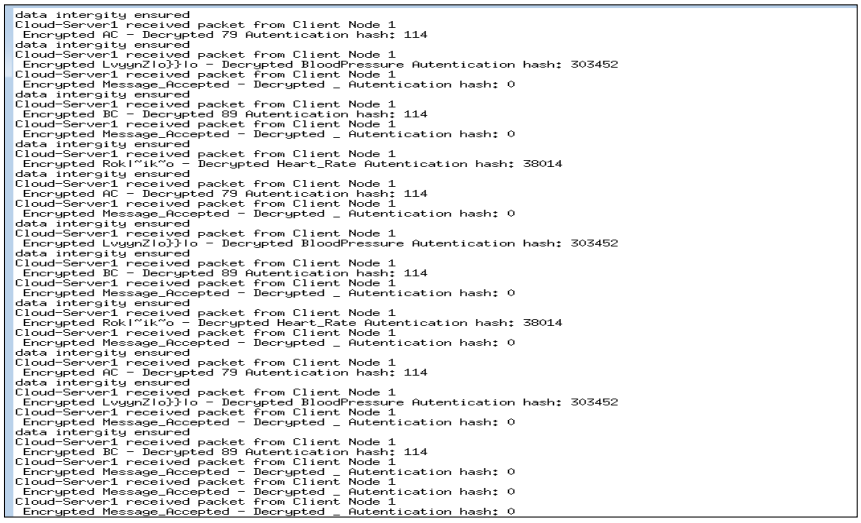
5.0 RESULT AND DISCUSSION

The proposed simulated encryption scheme is shown in the following figure 3, where the patient's PDA sends the data in encrypted form using the ECIES algorithm with SHA and stored cloud database after decryption that ensured the confidentiality and integrity as shown in the following simulated result. Simulation is showing physiological parameters with real-time sensed value, it encrypted value and hash generated to ensure integrity.

ISSN 1533-9211

DOI 10.5281/zenodo.7080841

Figure 3: Encrypted data transmission simulation received at Cloud database

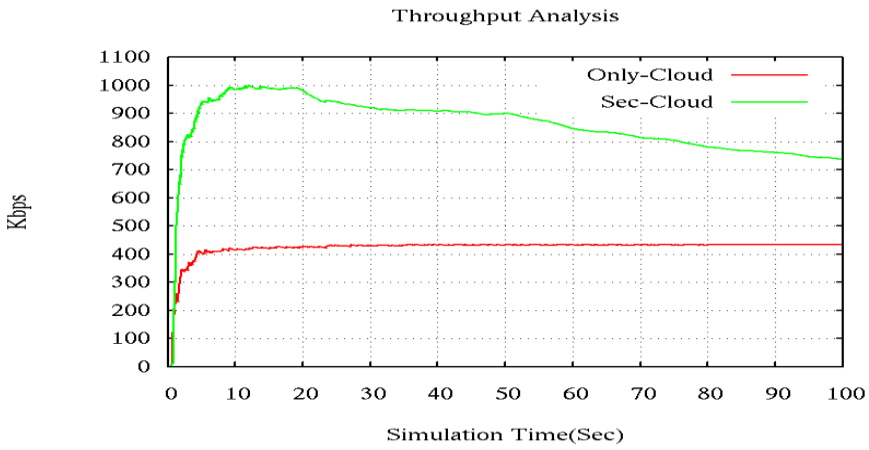


Further results are observed and recorded when particular data is accessed by doctors/relatives or other caregivers using his/her PDA. These results ensure the reliability and effectiveness of the algorithm.

5.1 Network Throughput Analysis

Throughput is calculated about accessing of data and measured per unit time (Kilobyte/second). For analysis, we have taken simulation results of both the scenarios (Only-Cloud and Sec-Cloud). The graph's X-axis signifiessimulation time in seconds and Y-axis signifieskilobytes/second. The comparison graph concludes that the proposed algorithm achieves 738 kilobytes per second throughput as compared to the only-cloud scenario where 433.06 KB throughput has been achieved. This data reduction is the result of various attacks.

Figure 4: Throughput analysis

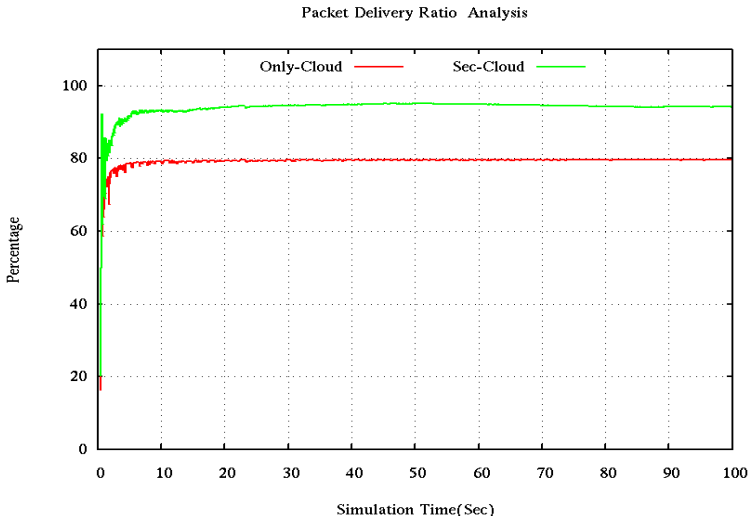


The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

5.2 PDR Analysis

PDR ("Packet Delivery Ratio")is a percentage ratio of data received out of total data sends, where higher PDR represents lower data loss at receiving end. Following figure 5 shows the PDR analysis and comparison. The comparison shows that Sec-cloud performs well as compared to the packet delivery ratio from the only-cloud scenario.

Figure 5: Packet Delivery Ratio analysis



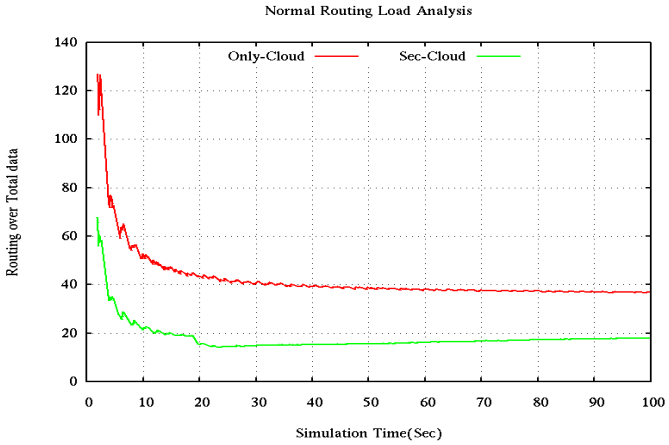
5.3 Normal Routing Load (NRL)

During data transmission in the network, routing overhead is calculated for the management of data transfer. 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. This affects the data transmission capability. So, Routing load (Routing overhead) is calculated as the ratio of the total control packet out to the actual data packet received by the receiver. Routing load is always lower when network bandwidth is maximally utilized. The resulting graph shown in figure 6 depicted that the proposed Sec-cloud scenario recorded lower overhead as compared to the only-cloud scenario. This figure shows that during 100 sec of simulation time, routing overhead is recorded as 18 in the Sec-Cloud scenario as compared to the Only-cloud scenario where routing overhead is achieved at 37.

ISSN 1533-9211

DOI 10.5281/zenodo.7080841

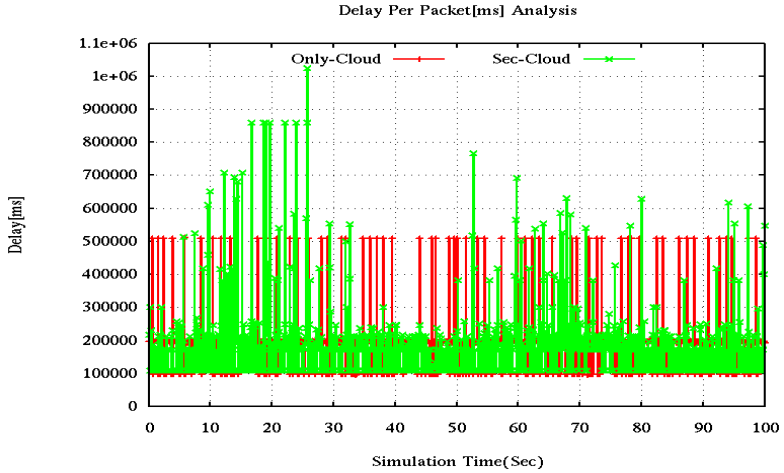
Figure 6: Routing Overhead analysis



5.4 Per Packet Delay or End-to-End Delay in [ms]

The time it takes for packets to transmit from the sender to the recipient nodes is known as the end-to-end delay. End-to-end delays are influenced by congestion, processing speed, bandwidth, and queue delay. When the delay is higher it means network, performance is lower. The resulting graph in figure 7 shows that the Sec-cloud scenario records less end-to-end delay than the only-cloud scenario. The figure shows 184.62 ms per-packet delay in the Sec-Cloud scenario as compared to the Only-Cloud scenario where a delay is recorded at 198.43 ms. This indicates the effectiveness of the proposed algorithm.

Figure 7: End-to-End delay analysis



5.5 Security Analysis

The security of the proposed algorithm against security attacks is examined as follows:

ISSN 1533-9211

DOI 10.5281/zenodo.7080841

5.5.1 MiTMattack

A network session opening is seen by an attacker. Once a communication session has been established between 2 parties, she/he may attack the client device to render it and then use IP spoofing to spoof the real doctor and take control of the session. This attack is stopped here because the PDA does not deliver the message comprising his identification directly, but rather in the encrypted version of the data. As a result, the man in the middle is unable to decrypt the text as he lacks the private key of the receivers and the MAC code that was utilized.

5.5.2 Security against Chosen Cipher Text Attacks

The suggested technique is secure against selected cipher text attacks. If the PDA wishes to encrypt any message "M", then he utilizes the cloud server's public key Qcdbs. The pair (R, C, and D) is now selected and delivered to the cloud server. If an attacker gets selected cipher text, he still requires the private key of receivers to produce key pairs for deciphering and he can't find it since the proposed work generate arbitrary key pair using an arbitrary elliptic curve.

5.5.3 Confidentiality

Since the proposed protocol is based on ECIES and incorporates symmetric encryption, it is challenging for the adversary to decipher the cipher text and retrieve any information. As a result, our system offers data confidentiality.

5.5.4 Unforgeability

The private key of the receiver (cloud server/Receiver PDA), which is kept safe with the receiver, is needed to forge the message. Thus, the Unforgeability property is protected by the confidentiality of the shared secret key produced during key creation. Unless the private key of the sender is known, it is computationally impossible to forge a valid "cipher text" C delivered by the sender (i.e., PDA to cloud server or cloud server to doctor's PDA) and claim that it is from a valid sender.

5.5.5 Non-repudiation

It is the certainty that something could not be denied. Therefore, the PDA is unable to claim that it does not send an encrypted text. Any trusted party or recipient himself may confirm that the message was transmitted by PDA by executing the verification method during the MAC verification process used in ECIES decryption.

5.5.6 Integrity

Assuring that information is not modified by unauthorized parties. If the cipher text was modified by an unauthorized party from C to C' and the tag value is computed as anything other than D during decryption. This modification is detected during the verification procedure (decryption process step number 5), and the "cipher text" was rejected by the recipient, ensuring its integrity.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

6.0 CONCLUSION

Electronic healthcare has developed as an effective technique for patient monitoring in recent years. This effectiveness is due to recent and available information and communication techniques. It includes wireless sensing technology, IoT devices, tiny medical sensing devices for sensing and communication, and cloud computing technology for processing and storage of physiological data.

This paper presented an architecture that assures. Patient's privacy. To ensure the patient's privacy, the proposed work used the Elliptic Curve Integrated Encryption Scheme (ECIES), an enhanced version of the ECC algorithm that encrypts the patient data before sending it to the storage server and at the doctor's PDA at the time of accessing. This results in ensuring the confidentiality of data and at the same time, by the same algorithm ensuring the integrity of patient's data, so that attackers cannot modify the data in transit as well as cannot disclose the patient's data.

The proposed work is simulated in an NS-2 simulator, and results are evaluated, analyzed, and proved that the proposed work is better over cloud technique based on end-to-end delay, PDR, and network overhead as far as response delay reduction is concerned. When security is concerned, the proposed work guarantees integrity and secrecy with improved security, by utilizing less computational costs, since only one algorithm assured both integrity and confidentiality. It also avoids different attacks like chosen cipher attacks, MiTM attacks, Unforgeability, and Non-repudiation, making it effective for securing patients' physiological data.

REFERENCES

1) Mosadeghrad, A. M. (2014). Factors influencing healthcare service quality. International journal of health policy and management, 3(2), 77.

2) Jain, R., Gupta, M., Nayyar, A., & Sharma, N. (2021). Adoption of fog computing in healthcare 4.0. In Fog Computing for Healthcare 4.0 Environments (pp. 3-36). Springer, Cham.

3) Tiwari, V., & Tiwari, B. (2019). A Data-Driven Multi-Layer Framework of Pervasive Information Computing System for eHealthcare. International Journal of E-Health and Medical Communications (IJEHMC), 10(4), 66-85.

4) Kumar, M., & Mostafa, J. (2020). Electronic health records for better health in the lower-and middle-income countries. Library Hi-Tech.

5) Pasha, M., & Shah, S. M. W. (2018). Framework for E-Health systems in IoT-based environments. Wireless Communications and Mobile Computing, 2018.

6) Ismail N. (2018), "How cloud technology is transforming the healthcare industry," Bonhill Group Plc, [Online]. Available: https://www.information-age.com/cloud-technology-transforming-healthcare-industry-123472352/. [Accessed: 22-May-2020].

7) Kamani V. (2019), "Five Ways Cloud Computing Is Impacting Healthcare," Jameson: Health IT Outcomes, [Online]. Available: https://www.healthitoutcomes.com/doc/ways-cloud-computing-is-impacting-healthcare-0001. [Accessed: 22-May-2020].

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

8) Tiwari, B., & Kumar, A. (2013). Physiological value-based privacy preservation of patient's data using elliptic curve cryptography. Health Informatics–An International Journal (HIIJ), 2(1), 1-14.

9) Tiwari, B., & Kumar, A. (2015). Role-based access control through on-demand classification of the electronic health record. International journal of electronic healthcare, 8(1), 9-24.

10) 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.

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

12) 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.

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

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

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

16) Vora, J., Kaneriya, S., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2019). TILAA: Tactile internet-based ambient assistant living in a fog environment. Future Generation Computer Systems, 98, 635–649.

17) Gia, T. N., Jiang, M., Sarker, V. K., Rahmani, A.M.,Westerlund, T., Liljeberg, P., & Tenhunen, H. (2017). Low-cost fog-assisted healthcare IoT system with energy-efficient sensor nodes. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 1765–1770). Piscataway, NJ: IEEE.

18) Vora, J., Tanwar, S., Tyagi, S., Kumar, N., & Rodrigues, J. J. (2017). FAAL: Fog computing-based patient monitoring system for ambient assisted living. In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1–6). Piscataway, NJ: IEEE.

19) Azimi, I., Anzanpour, A., Rahmani, A. M., Pahikkala, T., Levorato, M., Liljeberg, P., et al. (2017) HiCH: Hierarchical fog-assisted computing architecture for healthcare IoT. ACM Transactions on Embedded Computing Systems (TECS), 16(5s), 174.

20) Tanwar, S., Vora, J., Kaneriya, S., Tyagi, S., Kumar, N., Sharma, V., et al. (2019). Human arthritis analysis in a fog computing environment using Bayesian network classifier and thread protocol. IEEE Consumer Electronics Magazine, 9(1), 88–94.

21) 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.

22) Paul, A., Pinjari, H., Hong, W. H., Seo, H. C., & Rho, S. (2018). Fog computing-based IoT for the health monitoring system. Journal of Sensors, 2018.

23) Elmisery, A. M., Rho, S., & Aborizka, M. (2019). A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. Cluster Computing, 22(1), 1611–1638.

24) Rajagopalan, A., Jagga, M., Kumari, A., & Ali, S. T. (2017). A DDoS prevention scheme for session resumption SEA architecture in healthcare IoT. In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1–5). Piscataway, NJ: IEEE.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7080841

25) Chaudhry, J., Saleem, K., Islam, R., Selamat, A., Ahmad, M., & Valli, C. (2017). AZSPM: Autonomic zero-knowledge security provisioning model for medical control systems in fog computing environments. In 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops) (pp. 121–127). Piscataway, NJ: IEEE.

26) Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access, 5, 22313–22328.

27) 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.

28) Liu, X., Deng, R. H., Yang, Y., Tran, H. N., & Zhong, S. (2018). The hybrid privacy-preserving clinical decision support system in fog–cloud computing. Future Generation Computer Systems, 78, 825–837.

29) 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.

30) 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.

31) 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.

32) 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.

33) 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.

34) 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.

35) Mishra, N N; Parker, Lisa S; Nimgaonkar, V L; Deshpande, S N Privacy and the Right to Information Act, 2005. Indian Journal of Medical Ethics, [S.l.], v. 5, n. 4, p. 158, Nov. 2016. ISSN 0975-5691. Available at: <https://ijme.in/articles/privacy-and-the-right-to-information-act-2005/>. Date accessed: 22 May. 2022.