ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse331022021.pdf
https://doi.org/10.30534/ijatcse/2021/331022021

Enhanced Health-Care Protection Using Advanced Encryption Standard and Diffie Hellman Key Exchange Algorithm

Dr.A.Vijayaraj[1], Magesh Kumar N[2]
[1]Associate Professor, Information Technology, Vignan's Foundation for Science, Technology & Research, (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh-522213, India. satturvijay@gmail.com.
[2]Assistant Professor & Computer Science Engineering Vignan's Lara Institute of Technology and Science, Guntur, Andhra Pradesh-522213 , India. mageshkumarns19@gmail.com

ABSTRACT

In the modern world as technology develops, it is very crucial to secure, share and store the data. Especially, when it deals with medical data it is very important to secure that sensitive information. Sensitive information might be the pulse, temperature, or any disease-related symptoms. Such factors must not be shared unless or until with the users' permission. When any services or any user overcome the given act then the victim will be addressed in the court of law for the denial of service. Such activities must not be welcomed as in the world of modern technology; it is easy to secure the data as well as to share the data. Hence, it is significant to overcome privacy issues and security attacks. The co-factors associated with transmitting and securing data involves bandwidth and energy. Bandwidth and energy play a vital role during the transmission of data. Hence in this paper, we introduce a novel system of creating a portal for the patients who can enroll with their medical details and fix appointments with the doctor and get the prescription. First, the N^{th} Degree Truncated Polynomial Ring Unit (NTRU) method is used to encrypt the data collected where the private chats among the patient can be secured. Those data will be transmitted to the nearby cloud-let in an energy-efficient manner. Secondly, patients can communicate with other patients about their diseases where the disease based group can be created to share the information. Thirdly, patient's information is divided into tables and stored in the cloud for proper protection. As group chats and personal chats are involved, security is a must during communication and as an additional feature, the data are collected in a buffer format in the mobile, which paves way for reducing the bandwidth and energy consumption.

Key words: Cloud, Efficient energy, Bandwidth, Privacy, Security, Advanced Encryption Standard, Polynomial, patient, pulse.

1. INTRODUCTION

The ecosystem of connected objects that can be accessed using the internet can be defined as the Internet of Things (IoT). The 'thing' in IoT can be of any object. For example, a sensor that senses the heart rate where an IP address is suggested for every device used to transfer the data over the network. Often, IoT affects the decision process which may interact with both the internal state as well as the environment used. IoT helps in greatly reducing waste, cost and any data loss. It generally means empowering the computers. It helps in understanding the situation around us automatically in an independent way without any human intervention. They help in better security and improvement in analytics. The productivity cost among the organizations can be improved and helps in making smart decisions. Cloud increases the efficiency of the platform as well as help in the flexibility of operations performed.

2. RELATED WORKS

Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao and Long Hu [8] suggested a method for protecting and sharing the medical data. Generally, the medical record consists of the following stages such as collection, sharing and storage. When storing the data in the cloud it must be ensured that data are encrypted [9]. The data collected by the wearable device was encrypted and transferred to the cloud-let. Number Theory Research Unit (NTRU) algorithm was used to encrypt but supported only a single organization. Communications between patients are possible but the secure chat was in complexity [11]. This method provided high bandwidth and increased energy consumption. Hence, the method was not effective and energy-efficient.
Sanjay Ram M, Vijayaraj A [16] projected a scheme to create a reliable Computing surrounding for cloud computing scheme by incorporate the expectation work out the platform into Cloud computing scheme and pay consideration to the protection requirements in cloud computing surroundings. Rui Zhang and Ling Liu[14-19] suggested a reference model

for securing EHR, With the extensive use of Electronic Health Record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both the health-care industry and academic community[13]. Here, all the medical records are guarded using encryption techniques and it also maintains data integrity [15]. This model provides end-to-end verification using signature and user agreements. An EHR security reference model is created for both patients and health-care professionals, which enhances the three-component mechanisms such as collection, secure storage and secure usage [6-20]. This model prevents the user's identity.Yang.J.-J, Li.J.-Q, and Niu. Y[12] suggested a protocol for maintaining the confidentiality and integrity among data storage and sharing. The design works on Elliptic Curve Cryptography(ECC) and Sobol sequence, and the former work was based on pseudo-random sequence [1]. This protocol supports dynamic operations such as update, delete. The data provided are encrypted before storage using the RSA algorithm. It solves the problem of data leakage and data corruption [2]. The challenge-response protocol reduces the communication cost. Integrity is maintained without retrieving the original data.

Rongxing Lu, XiaodongLinandXuemin(Sherman)Shen[7] proposed a framework for checking and maintaining reliability under the users' sensitive information such as medical records during the mobile health-care called (SPOC) Secure Privacy-preserving Opportunistic Computing Transferring emergency health records may lead to privacy disclosure[5]. Hence, within opportunistic computing, only the patients with a similar disease will be connected and the framework provides access control based on the user. A Privacy-Preserving Scalar Product Computation (PPSPC) allows only certain medical users to participate in the framework and it does not reveal directly the symptoms of the user who are in an emergency [3]. To validate the proposed framework, a custom simulator is built and provides high reliability and reduces privacy disclosure. Quwaider.M and Jararweh. Y[10] employed a hybrid search for retrieving information about the patients. Here, the data is partitioned into plain text and ciphertext. The encrypted search can be based on two types which include Boolean and ranked search but these methods provided intolerable query cost and were not effective hence, the hybrid search came into existence to provide high reliability and to overcome the limitations and complexity during information retrieval [4]. The integration of access control and manipulation provides high reliability. Hee Jeong Cheong et. al [17] many positive results are created, such as enhancing the health care infrastructure, increasing the accessibility of patients to medical care and satisfaction, improving medical equity, improving medical quality, lowering costs, and rationalizing hospitals' business. From a national viewpoint, it is proposed that the initiative will increase transparency by addressing health system disparities and strengthen accountability by offering well-structured administrative health services. Yussuf Ahmed Syed Naqvi Mark Josephs [18] addressed the safety issues facing the healthcare industry in this paper and provided some of the reasons why this industry is vulnerable to cyber-attacks. It is an issue that impacts a whole sectors and not only is it specific to healthcare but when it concerns patient safety, the effect is even greater. There was a review of the limitations of medical technology, technology, and security culture. Finally, a cyber-security metric was proposed to enhance the safety of these networks.

3. EXISTING SYSTEM

In the existing system, cloud-assisted health-care data computing was very difficult to meet the users' demands and it was very hard to retrieve the data required by the user [8]. The medical process usually holds the three major steps which are data collection, sharing and storage. Various users may use the data available in the cloud in their convenient manner which may affect the retrieval process as well as increase the complexity among the network. This may increase congestion among the network and multiple users may not be able to retrieve the data simultaneously. The earlier system was proposed based on a single organization where the patient within the same hospital can use the data available. This system was not able to meet the demands requested by the user as the user rate increases far wide which increased the complexity while retrieving as well as sharing the data, there arrives the security problem. The system is proposed only to a single hospital and was unable to retrieve the real-time disease information and does not allow secured chats among the patients. This might cause sensitive information to be leaked which causes privacy and security problems. Group chats were enhanced but the complexity behind the social networks was higher. Transfer of medical data to the hospital server for every minute increased the bandwidth. Network traffic was higher and this required excessive energy.

4. PROPOSED WORK

Here, Bluetooth is used to retrieve the information from the kit which senses the body temperature as well as the heart rate of patients, the kit collects a maximum of five data where the sensor situated along with the Bluetooth device helps in sensing and the values are displayed in the mobile using the device which helps in exchanging the data. Once the values are collected, they are displayed in the service runner of the Tomcat server where they are found in an encrypted format. Bluetooth helps in using the radio waves generated. They are connected using fixed as well as mobile devices. Advanced Encryption Standard (AES) is a block cipher that tends to be symmetric and it is used to encrypt sensitive information such as medical data, bank data where the information might be lost due to technical errors or failures. It is easy to implement AES in both hardware as well as software and the key size of this algorithm helps in sending the large sensitive information. Diffie Hellman Key Exchange is used among the two parties who are in need to exchange their information.

The privacy issues among the two parties can be solved using this algorithm.

Diffie- Hellman Algorithm After the RSA algorithm[12], the Diffie-Hellman (D-H) algorithm was published. The D-H algorithm distributes keys safely over the free channel of communication[19]. Alice and Bob create a mutual hidden key and then constantly interact with each other. Details can be shared using an unsecure medium of communication. Eve or spy attacker does not comprehend the mutual.

PROPOSED ALGORITHM

1.Diffie Hellman Key Exchange:

Input: a, b, p, g, x, y, ka, kb

```
if(b==1)
return a;
else
return (pow(a,b));
```

Before encryption:

```
X=power(g,a,p);
Y=power(g,b,p);
```

After encryption:

Key generated:

```
Ka= power(y,a,p);  // Secret key for a;
Kb= power(x,a,p);  // Secret key for b;
```

Output: Secret key Generation ka, kb.

Let us consider a step-by-step example of the Diffie-Hellman key exchange steps:

1. Consider Alice and Bob as two parties; choosen the prime numbers as a primitive variable. P = 23 and G = 5 .

2. Alice select the integer **a** , theat is the secret key that transmits A to Bob. From the equation A= Ga mod P a = 4 , A = 54 mod 23 =4 4 A is obtained .

3. Likewise, Bob picks an integer **b** that is also a secreted key and then transfers B to Alice. B = Gb mod P. b = 7 , B = 57 mod 23 = 17.

4. S = Ba mod P. s = 177 mod 23 by Alice

   = 8,

5. Calculating s = Ab mod P , s = 47 mod 23

   = 8 by Bob.

Thus Alice and Bob distribute the similar hidden key s = 8 with the two parties. Both Alice and Bob now have the identical value s . Both values are hidden in the D-H algorithm and the others P, G, A, B values are public.

5. SYSTEM FRAMEWORK

The structure of the planned system can be described using the two important factors considered in the system where the bandwidth and energy are decreased as well as an encryption of the patient data.

5.1. Registration and symptoms matching

Patient registers personal details to a common web application that is explained in Figure 1: The application intermediates between patient and hospital applications. It contains multiple hospitals' patients' information. Due to this, the patient can easily register and get an appointment from the hospitals they need. During registration, the patient id generates automatically, the patient's information is about the name, email id, date of birth, age, place, guardian number. The patient enters his/her symptoms, it analyses all patient records in the portal and detects patients with similar symptoms. Once similar patients are identified from the patient's list, if the patient wishes to communicate then the patient can chat with those who have similar symptoms. The patient discusses their symptoms and disease, and then the treated patient suggests the hospital where they were treated. The personal messages are encrypted using the Diffie Hellman algorithm.

5.2. Disease based Group Creation and Data Sharing

After the patient discusses the symptoms with other patients. The application suggests doctors based on the patient location. The patient selects a doctor based on location or personal chat information and also fixes the appointment. While fixing their appointment they should specify their symptoms and then the doctor detects the disease based on their symptoms and provides them some medicine based on their disease. The doctor prescribes medicine to overcome their disease, if it is not possible, they can get treatment based on their locations from the efficient hospitals. During this treatment, patients add on disease based group. Patients with similar diseases can create a group to communicate and can even exchange their treatment information etc, it helps the patient to get their treatment with the best and efficient doctor.

5.3. Cloud Data Storage

The patients register their details to a common web application. Day-to-day, the medical information gets increased rapidly, so the application needs the cloud to store

the medical data. The usage of the cloud is easy because it retrieves the data when we are in need and helps in easy access. The medical data contains patient's sensitive information so data protection is more important. So, we use Advanced Encryption Standard (AES) to prevent the data. The application stores patient data in the cloud in two different tables. Patient information splits into two types is Electronic Identification (EID) and another is Medical Information (MI). Electronic identification contains patient personal information such as name, email, phone no, etc. MI contains patient's treatment information like medicine, disease. Electronic identification (EID) information is stored in ciphertext format and medical information is stored in plain-text format. If someone tries to change the details in the portal then the cloud always matches each data hash code if they do not match, then it could be understood that a malicious attacker has modified the data.

5.4. Client Data Encryption

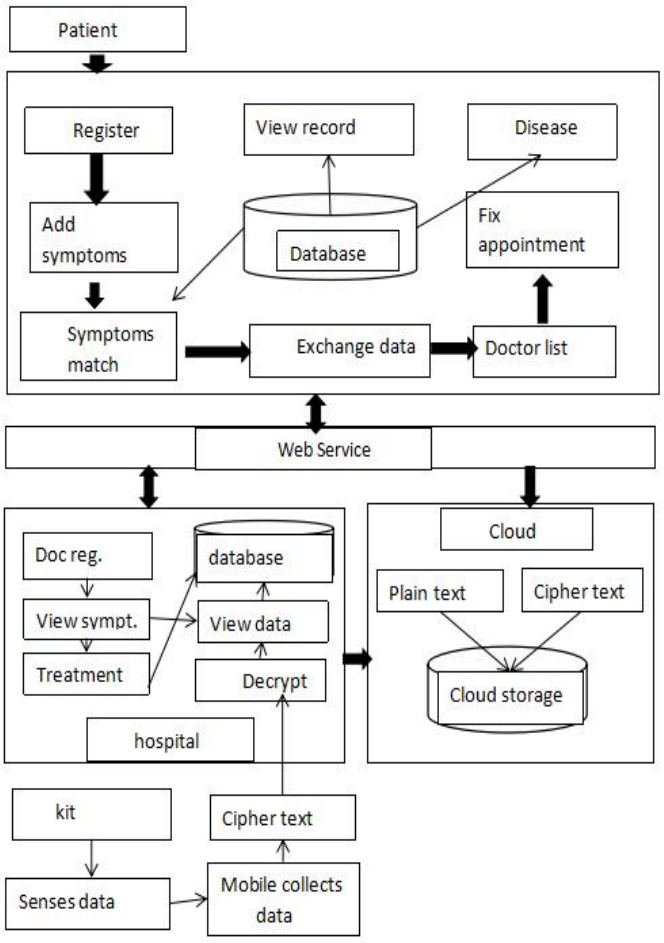

Figure 1: Architecture diagram -Health Care System.

During the treatment, the doctor monitors the patient body information such as temperature, heartbeat, etc. The kit will sense the data from a patient and transmits it to the patient mobile. Mobile and the kit is connected via Bluetooth. Mobile collects the patient information in an array format and stores it in a buffer after it fills it starts transmitting it, if in case of emergency then the data will be directly sent to the doctor and then message is delivered to the guardian number which is already registered, where the doctor prescribes the emergency medicine. The information is transmitted over a wireless network so security is more important. For securing the information, Diffie Hellman Key Exchange Algorithm is used. The information collected gets converted to ciphertext format and transmits to the hospital server. This reduces the energy consumption and bandwidth which are the co-factors that affect the network transmission. The doctor receives the encrypted data and decrypts it to view patient information. In case of any emergency, like an increase in temperature or abnormal pulse rate then the message gets transmitted from the patient mobile to the guardian informing the patient's health condition which could be better in assisting the patient during the abnormal condition.

Advantages

✧ As the data are collected in a buffer in an array format helps in reducing the bandwidth.

✧ The retrieval of data from the server helps in reducing the complexity which in a way reduces energy consumption.

✧ The portal created helps in coordinating multiple patients as well as sharing their information.

✧ The privacy issues can be rectified using the Diffie Hellman algorithm

✧ The malicious attacker who modified the data can be identified with their IP address.

6. CONCLUSION FUTURE ENHANCEMENTS

In this work, we have created a web portal where the patients from various hospitals can enroll with their details and this has been implemented by using a mobile application that helps in sensing the heart rate and to fix appointments with the doctor, where the group chats can be created based on the similar disease. The existing method used the application within a single organization and the coordination among patients was a drawback. Privacy protection and sharing the large medical record over the social network was a dynamic problem where sensitive information might be stolen by a third party. The information retrieval in the cloud was a bit difficult. Creating a portal for patients helped in coordinating patients among the various organization and the information could be shared among multiple patients who have enrolled in the application. Storing the patient health record in mobile in

an array format helped in reducing the bandwidth and excessive energy consumption. Sharing the medical record using encryption techniques such as Diffie Hellman and NTRU helped in reducing the communication cost. Algorithms helped in speeding up the process and used low memory cost. This method can be undertaken by any of the service providers and can be enhanced all over the world to avoid emergency deaths. Moreover, patient body details can be detected such as sugar levels, pressure which may lead to severe conditions. Medical imaging management could be added with this method to help the doctor to diagnose the patient in a better manner. Bio-metric of the patient could be added for further security along with strong encryption techniques.

REFERENCES

1. Cao.N,Wang.C,Li.M, Ren.M, and Lou.M, "**Privacy-preservingmulti-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems,** IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.
2. DongreK, ThakurR.S, Abraham et al.A, "**Secure cloud storage of data," in Computer Communication and Informatics (ICCCI),** 2014 International Conference on. IEEE,pp. 1–5, 2014.
3. He.K, Chen.J, Du.R, Wu.Q, Xue,.G andZhang.X, **"Deypos: Deduplicatable dynamic proof of storage for multi-user environments," .** 2016.
4. Hossain.M.S and Muhammad,.G, **"Cloud-assisted industrial internet of things (IoT)–enabled framework for health monitoring,"** Computer Networks, vol. 101, pp. 192–202 , 2016.
5. Hung.K, Zhang.Y, and Tai,.B, **"Wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society.** IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2.IEEE, pp. 5384–5387, 2004.
6. KaufmanL.M, **"Data security in the world of cloud computing," Security & Privacy,** IEEE, vol. 7, no. 4, pp. 61–64, 2009.
7. Lu.R, Lin.X, and Shen.X, "Spoc: **A secure and privacy-preserving opportunistic computing framework for mobile-health care emergency,"Parallel and Distributed Systems,** IEEE Transactions on, vol. 24, no. 3, pp. 614–624, 2013.
8. Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao,**"Privacy Protection and Intrusion Avoidance for Cloud let-based Medical Data Sharing",** IEEE Transactions on Cloud Computing,vol.pp,issue 99, 2016.
9. Pickard.K.T and Swan.M, **"Big desire to share big health data: A shift in consumer attitudes toward personal health information,"** in AAAI Spring Symposium Series, 2014.
10. Quwaider.M and Jararweh.Y, **"Cloudlet-based efficient data collection in wireless body area networks,"** Simulation Modelling Practice an Theory, vol. 50, pp. 57–71, 2015.
11. Xiang.W,Wang.G,Pickering.M, and Zhang.Y, **"Big video data for light-field-based 3d telemedicine,"** IEEE Network, vol. 30, no. 3, pp. 30– 38, 2016.
12. Yang.J.-J, Li.J.-Q, and Niu.Y, **"A hybrid solution for privacy preserving medical data sharing in the cloud environment,"** Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.
13. Yang.J.-J, Li.J, Mulder.J, Wang.Y, Chen.S, Wu.H,Wang.Q, and Pan.H, **"Emerging information technologies for enhanced health-care,"** Computers in Industry, vol. 69, pp. 3–11, 2015.
14. Zhang.R and Liu.L, **"Security models and requirements for healthcare application clouds," i**n Cloud Computing **(CLOUD)**, IEEE 3rd International Conference on. IEEE, pp. 268–275, 2010.
15. Zhao.J,Wang.L, Tao.J, Chen.J, Sun.W, Ranjan.R, Kołodziej.J, Streit.A, and Georgakopoulos.D, **"A security framework in g-hadoop for big data computing across distributed cloud data centers,"** Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.
16. Sanjay Ram M Vijayaraj A , "**Analysis of the characteristics and trusted security of cloud computing",** International Journal on Cloud Computing: Services and Architecture(IJCCSA). Vol.1, No.3, Pp. 61-69, November 2011.
17. Hee Jeong Cheong, Na Yoon Shin, Youn Baek Joeng, '**Improving Korean Service Delivery System in Health Care: Focusing on National E-health System' ,** International Conference on eHealth, Telemedicine, and Social Medicine , 978-0-7695-3532-6/09 $25.00© 2009 IEEE DOI 10.1109/eTELEMED.2009.51.
18. Yussuf Ahmed Syed Naqvi Mark Josephs , **'Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems'**,13th International Symposium on Medical Information and Communication Technology (ISMICT), 978-1-7281-2342-4/19/$31.00, 2019.
19. G.P. Biswas **"Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key",** IET Information Security, Vol. 2, No. 1, pp. 12– 18, 2008.
20. Kenji Imamoto **"Design and Analysis of Diffie-Hellman-Based Key Exchange Using One-time ID by SVO Logic",** Elsevier, Electronic Notes in Theoretical Computer Science 135 (2005) 79–94.