ZIBELINE INTERNATIONAL PUBLISHING

ISSN: 2616-5155
CODEN : MECJBU

Malaysian E Commerce Journal (MECJ)

DOI: http://doi.org/10.26480/mecj.01.2020.01.04

RESEARCH ARTICLE

CLOUD BASED E- HEALTH CARE DATA SECURITY AND PRIVACY BY USING ADVANCED ENCRYPTION STANDARD AND WATERMARKING TECHNIQUE

Daniya Jaffar[a], Ahthasham Sajid[a] *, Asma Jahangeer[b], Raja Asif Wagan[b]

[a]Department of Computer Science, Faculty of ICT, Balochistan University of Information Technology Engineering and Management Sciences , Quetta, Pakistan
[b]Department of Information Technology, Faculty of ICT, Balochistan University of Information Technology Engineering and Management Sciences, Quetta, Pakistan
**Corresponding Author E-mail: ahthasham.sajid@buitms.edu.pk , gullje2008@hotmail.com*

ARTICLE DETAILS

Article History:

Received 15 February 2020
Accepted 17 March 2020
Available online 24 March 2020

ABSTRACT

In 21st century technological word now has bring a tremendous change to health care system is widely used by doctor patients and researchers. Patients use wearable device such as smart eyewear, foot wear, smart watches, which is use by both patient to wear and by doctor to monitor patient condition remotely on cloud. This provides time savage fastest treatment facility but as this data is huge in amount it's very important to take care of security and privacy of the big data on cloud. Because the big data is not between patient and doctor it's on cloud were several third parties like service providers and other unauthorized user are also present and they can easily fetch patient's personal information for their own benefit. In this paper a novel approach based on advance encryption method and watermarking technique is presented to provide protection and security to e health data on cloud.

KEYWORDS

EHCR, AES Algorithm, Big Data, Image Watermarking, DOS.

1. BACKGROUND

Technology is revolutionized. Like other fields of life it's playing a vital role in Health care. Internet of things in medical and context aware devices made life of doctors and patients much easier than before, emergence of these technologies in healthcare reduce the cost, increase the performance and make healthcare more efficient than ever. But all the data of healthcare is shifted to cloud and it can be invade easily. Security and privacy of confidential medical data on cloud is a major concern (Sun and Wencheng, 2018). Risk of cyber crime on health care are higher, as compare to other organizations data on cloud. Criminals do cyber crime on cloud to take financial gain from personal information stored in hospitals database. Sometimes illicit upload personal data of individuals on public websites just to show flaws in e health security system. Other then this cyber attacks in e health care target famous political personalities to damage their reputation (Coventry et al., 2018).

2. INTRODUCTION

Technology is emerging day by day in every field of life from house hold work to large industries from educational sector to shopping mall. Man has developed technology to serve him 24/7. Like others fields of life technology is continuously emerging in health care system. Now health care system is known as electronic health care system as all the patient record is available online on cloud (Sun and Wencheng, 2018). Different wearable health care devices are developed for example smart watches, and jawbone are used to track fitness of patients calculates how much calories are burned per day. Most of smart watches give notification on cell phone one can integrates smart watch with smart phone. Similarly, smart glasses are developed to help visual impaired people. All the data from wearable devices and hospital record system is now shifted on cloud to facilitate patients even if they are at home or in any emergency condition. There are many benefits of EHRS for example doctors can remotely access patient condition and suggest suitable prescription it save time and Cost to travel its finishing paper based record from hospitals and many people like doctors, patients, hospital lab, account section now have complete information at a time due to cloud based pervasive system. There are some major problems along with these benefits (Abouelmehdi et al., 2018). Cloud services over big data is facing security and privacy concern from provider are third party who cannot be trusted completely and patient's personal data can be breach easily another scenario is malicious attack which results in form of data loss if doctor have no backup of patient record.

Similarly, insecure APIS, demand of service attack and account hijacking are some major problems. Another issue is server location most of cloud servers are located in United State but people from different countries of world use these servers which countries rule and regulation are applied that is not clear. Keep in mind that security and privacy are two different terms for example hospitals create unique secure system to share personal information of patient they don't use email or other such resources for confidential data and privacy is protect sensitive information about one personal or an organization. Security is independent variable it can be achieve without privacy while privacy depends on security (Chen and Min, 2016). Till now many techniques have been presented but no any technology is perfectly accurate 100% in term of security and privacy.
Many solutions have been presented thousands of researchers are working day and night to reach the level to secure data so that any

Quick Response Code	Access this article online	
	Website: www.myecommerecejournal.com	DOI: 10.26480/mecj.01.2020.01.04

Cite The Article: Daniya Jaffar, Ahthasham Sajid, Asma Jahangeer, Raja Asif Wagan (2020) Cloud Based E- Health Care Data Security And Privacy By Using Advanced Encryption Standard And Watermarking Technique. *Malaysian E Commerce Journal, 4(1) : 01-04.*

unauthorized user cannot access patient's confidential data. Frequently used technique is to encrypt specific file that contains patient's record before sending it to cloud. In this paper we will discuss some major attacks on cloud based data, the concept of security and privacy with the help of literature review and a solution for security and privacy of data on cloud, how the previously presented solution tried to solve the problem and at last we tried to present the solution of this problem with the help of advance encryption standard and watermarking technique.

3. PROBLEM STATEMENT

Placing critical data over the cloud environment most of the time individuals and organizations feel threaten to their privacy and security level. Deriving attention to the problem of electronic healthcare record in term of data privacy and security. To overcome various key challenges and attacks on cloud based medical record; Different encryption and decryption techniques to increase privacy and build trust level have been used independently early by the researchers. Watermarking technique as yet not been added to increase security level in the research community so in this paper image water marking will be used in combination with (AES) advance encryption standard technique to achieve high level security.

4. RELATED WORK

As discuss earlier several techniques have been proposed to secure patient's electronic data on cloud. Different researchers presented several solutions. Let's discuss them one by one (Alrawais and Arwa, 2017). Presented solution for secure data transmission by using cipher text policy attribute based encryption method (CP-ABE) along with digital signature based technique. Key is encrypting and decrypting on bases of attributes and key is provided to each fog node if it's satisfy the described policy (Zhang et al., 2015). Present's solution for big data management in e health care. Multilayer architecture has been presented. In first layer user data is collected in middle layer data integration is done with public resources. Unified API and unified interface are developed for developers and users respectively presented solution for privacy protection in cloudlet based data sharing where firstly data is collected from wearable devices and deliver to cloud by cloudlet (Chen and Min, 2016).

Trust model is created to check either client which are patients in this case want to share their data on cloud or not what is their trust level for sharing data on cloud. NTRU based encryption is done in this paper. Finally, collaborative ID is used to protect the whole system (Abouelmehdi et al., 2018). Presented a survey paper in which they studied several paper related to risk and challenges in e health care big data. They explained rules and regulations different countries follow for cybercrime and presented a solution based on anonymization and encryption. Author in this paper discusses life cycle of Big Data that starts with data collection phase data should be collected from authentic source and secure data from being stolen by other sources. After data collection data is transformation accords where first data is cleaned from duplication, missing data, noisy data and then it transformed.

By use of data mining algorithm third phase that is data modeling is completed. It's important to use an algorithm that provides data security. Finally, in last phase data is converted in to valuable knowledge and this phase is known as knowledge creation phase and information security and validity is basic focus of this phase (Fabian et al., 2015). Presented the solution to secure patients data inside the organization that how data can be share inside the organization securely by using multiple cloud service. Encrypted data from multiple cloud proxies is collected and distributed in parallel order. Cryptographic hash function is used to share data with external user and only limited data is shared with external user based on attribute based encryption. In future they address to work on key management and scalability of architecture in large organization (Ren and Yonglin, 2010). Present's solution for securing patients data from unauthorized access by mobile and ad hoc sensor network.

They discussed that patient's data can be collected from wearable and portable devices but these sensors network are ad hoc so data can be easily exposed to malevolent intruders and listeners. Along with data confidentiality utility of power consumption in sending message through ad hoc network is another issue thus in mobile health care system elliptic curve cryptography (ECC) with A symmetric key is used to protect the data with low consumption power. For encryption of patient information smart card is used it's kind of biometric for verification of patient's identity. Quality of privacy is examined by patients as they pretend an anonymous identity and multi agent's system is used the agent monitors user activity and check level of QOP that patient concern and negotiate patients request according to that (Balapure et al., 2017) .Presented review paper in which they reference different solutions some of them are in private cloud fine grain access control and attribute based encryption they also suggested to secure record of patient by encryption before sending data to cloud. Many issues have been highlighted such as flexible access of data, privacy exposure, as different keys are used so scalability of key and efficient user revocation.

Table 1: Related Work Summary

S.No	Author	Suggested Methodology
1	(Alrawais and Arwa, 2017)	Cipher text policy attribute based encryption method (CP-ABE) along with digital signature based technique is used.
2	(Zhang et al., 2015)	Performance of health care system can be increase by using technology. Multilayer architecture is presented. Data is collected in first layer, in second layer cloud driven platform is established and in third layer API are developed for users.
3	(Chen and Min, 2016)	To share patient's confidential information on cloud is sensitive. Number theory research unit method is used to encrypt data (NTRU).
4	(Abouelmehdi et al., 2018)	Survey paper that mentioned issues related to Big data its privacy and security concerns can be secure by encryption and anonymization method. Rules and regulations that countries applied are discussed.
5	(Fabian et al., 2015)	Presented solution for inter organizational data security for accessing data attribute based encryption is used and for sharing data cryptographic hash function is used.
6	(Ren and Yonglin, 2010)	Mobile and ad hoc sensor network are used to collect patient's data but sensor network are ad hoc data can be accessible to intruders. Elliptic Curve Cryptography with A symmetric key is used to protect data. Smart card is used for encryption.
7	(Sharma et al., 2018)	Issues are highlighted such that flexible access of data, privacy exposure, as different keys are used so scalability of key and efficient user revocation.

5. DISCUSSION

In this section we have highlighted in detail to differentiate between security and privacy level over data in cloud environment (Mousavi et al., 2014). Table 2 bellow reflects the comparison of same. In table 3 different attacks and challenges which could be launched over data in cloud has been discussed in detail.

Table 2: Difference between Security and Privacy

Security	Privacy
Security is protection of unauthorized access of data. Unauthorized users can be any person who is not registered with hospital EHR but want to access the record for personal sake or any burglar who can use hospitals information to forward the information to third party or extort individual.	Privacy mainly focuses on individual personal information. Privacy is hiding user's identity. For example there are two patients both are authorized user of hospital EHS but it's essential to maintain one's personal information from other authorized users.
Data availability, integrity and confidentiality are its security.	Protecting, securing and maintaining the confidential data is privacy.
A secure system without good privacy can be achievable.	A good privacy level without good security cannot be achievable.
Security refers safety to overall organization's asset and whatever it keeps.	Fair and legal use of individual personal information is sustainable privacy.

Table 3: Attack and Challenges on Clod based Data	
Ransomware	It's kind of malware that mostly attacks on cloud based collective data rather than individual pc and one cannot access their confidential data without paying heavy fee as an extortion.
Distributed Denial of Service Attack	Malicious act accused by cybercriminals they disturb flow of normal traffic on targeted server and fill it with flood of traffic cause a lot of trouble for health care staff who want to send email, prescription or other important information to patients. Real life scenario occurred in Boston children's hospital in 2014 and as result of the attack hospital spent $300,000 to recover the loss.
Brute Force Attack	Hacker use specific tools and technique and they developed software by the help of this software they break password or PIN and get access to personal accounts of people on web. It important for every user on internet to use secure password which cannot be disrupt easily.
Insider Attack	According to recent study it has been declared that almost 58% data of an organization is been threaten by insiders.
Other than above mention attack there are several problems that individual and hospitals are facing on cloud such as data breach, insecure application programming interface and many more.	

6. METHODOLOGY

In this research study we have initially encrypted data using AES algorithm and then the derived cipher text has been converted into image water marking. Over the communication channel water marking image would be forwarded to the receiver (Patient). At receiver (Patent) side for decryption process initially the water mark image been converted back to gain cipher text before applying decryption key to get plain text again (Azeez et al., 2019). Sub Sections 5.1, 5.2 and 5.3 will further elaborate this sub processes involved in this proposed methodology using figure 1 and 2 respectively.

6.1 AES Algorithm

This technique has been developed after brute force attack on DES in 1997 and successfully used till now to secure confidential data (Elhoseny and Mohamed, 2018). In AES symmetric block cipher is used with key size of (128-bit, 192 bit and 256 bit).

6.2 Encryption Process

In electronic health care system patient data is taken in plain text form after encrypting the data by using AES the encrypted patient's data is send for second step.

6.3 Image Watermarking

The encrypted data is embedded into an image for more security watermark is inserted on original image and encrypted information hides in the watermarked image. The flow of suggested method is presented in Figure 1.

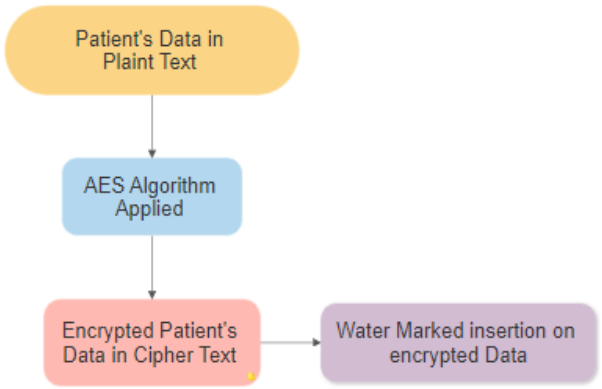

Figure 1: Patient's Data Encryption Process

6.4 Decryption Proces

On receiver end encrypted data is received first of all data is extracted from water marked image and then decrypted using the same key which is used for encryption. Flow of decryption process is presented by Figure 2.

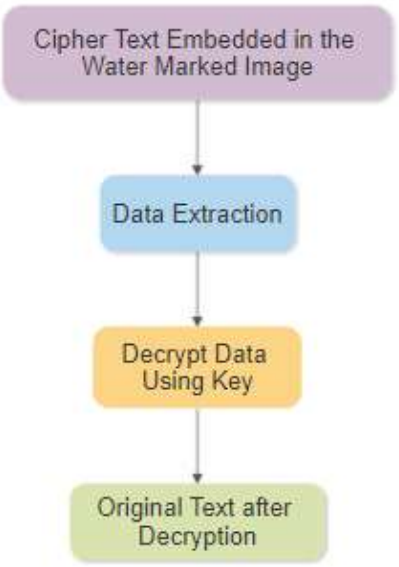

Figure 2: Patient's Data Decryption Process

7. CONCLUSION

In this paper we have discussed several issues such as patient's data security and privacy that are faced in health care industry when cloud services are used. Security and privacy of confidential patient data is on risk. To secure the data several techniques have been presented earlier in this paper we used combined approach first patient's data is encrypted using AES and embedded into watermarked image after that data is send on cloud and receiver in this case hospital staff and other authorized user can decrypt data as per their requirement and data remains safe from unauthorized access and being intrude.

REFERENCES

Abouelmehdi, Karim, Beni-Hessane, A., Khaloufi, H., 2018. Big healthcare data: preserving security and privacy. Journal of Big Data, 5 (1), 1.

Alrawais, Arwa, 2017. An attribute-based encryption scheme to secure fog communications. IEEE access, 5, 9131-9138.

Azeez, Ayofe, N., and der Vyver, C.V., 2019. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20 (2), 97-108.

Balapure, Ravindra, S., Khodke, P., 2017. Privacy Preservation Of E-Health Care System In Cloud, Exchange, 4 (3).

Chen, Min, 2016. Privacy protection and intrusion avoidance for cloudlet-based medical data sharing. IEEE transactions on Cloud computing.

Coventry, Lynne, Branley, D., 2018. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

Elhoseny, Mohamed, 2018. Secure medical data transmission model for IoT-based healthcare systems. Ieee Access, 6, 20596-20608.

Fabian, Benjamin, Ermakova, T., Junghanns, P., 2015. Collaborative and secure sharing of healthcare data in multi-clouds. Information Systems, 48, 132-150.

Mousavi, Mojtaba, S., Naghsh, A., Abu-Bakar, S.A.R., 2014. Watermarking techniques used in medical images: a survey. Journal of digital imaging, 27 (6), 714-729.

Ren, Yonglin, 2010. Monitoring patients via a secure and mobile healthcare system. IEEE Wireless Communications, 17 (1), 59-65.

Sharma, Sagar, Chen, K., Sheth, A., 2018. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing, 22 (2), 42-51.

Sun, Wencheng, 2018. Security and privacy in the medical internet of things: a review. Security and Communication Networks.

Zhang, Y., Qiu, M., Tsai, C.W., Hassan, M.M., Alamri, A., 2015. Health-CPS: Healthcare cyber- physical system assisted by cloud and big data. IEEE Systems Journal, 11 (1), 88-95.