International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

A Novel Survey to Secure Medical Images in Cloud using Digital Watermarking

Vaishali D. Kamble[1], Prof. Kanchan Doke[2]

[1,2]Bharati Vidyapeeth College of Engineering, University of Mumbai

---

Abstract - *Telemedicine has increased the number of ways in which healthcare can be delivered across places and countries instead of requiring the provider and recipient to be presenting the same place. Telemedicine is the process of exchanging the medical images between remotely located healthcare entities. The major obstacle telemedicine faces are providing confidentiality, integrity and authenticity to transmitted medical images. Radio Frequency Identification (RFID) system is one the solution to address this problem. A hybrid algorithm which combines encryption and digital watermarking in order to provide required authenticity and integrity. A cryptographic watermark and the patient's data are hidden in the cover image before being transmitted over public networks. To the receiver's end, the watermark image is handled by the extraction procedure in order to extract cryptographic watermark and the embedded medical data. The proposed algorithm was evaluated and tested using medical images of two different modalities.*

***Key Words*: Encryption, Decryption, Cloud Security, Cloud computing, Digital Watermarking, Private Key, Public key, Electronic health care, Cryptography, Medical Image, Security and Privacy.**

1. INTRODUCTION

Cloud computing is emerging as one of the most important technology of this decade. Various companies are investing millions of dollars in building infrastructure, services and application to make cloud computing easily accessible to consumers, businessman and organizations. It can be seen that how cloud computing will impact the healthcare business since it is diverse and complex it has several challenges such as protecting healthcare data, managing various information files, evaluating patient's details and diagnose various patients. The cloud security is nothing but the protection of data, various application and infrastructures involved in cloud computing. It protects with high level security such as protecting from unauthorized access. Weak access controls, susceptible to attacks affects the traditional IT and cloud system. The cloud security is the set of policies technologies and controls of deployed to protect the data. It is a sub domain of network security, computer security and information security. The cloud security allows to store the data at third party data centers. It works on two categories of security concerns such as security issues faced by their cloud providers and security issues faced by their customers. The providers must ensure that the infrastructure is secure and the client data and application must be protected. The users must take measure to fortify their applications and should use strong password. An efficient cloud security must recognize the issues related to the security management of cloud. The various security threats associated with cloud not only traditional threats such denial of service attacks, network eavesdropping and illegal invasion but also specific cloud computing threats such as side channel attacks and abuse of cloud services.

2. RELATED WORK

Pooja Prakash M, Sreeraj. R, Fepslin AthishMon, K. Suthendran [1] published in International Journal of Pure and Applied Mathematics (IJPAM 2018) "Combined Cryptography and Digital Watermarking for secure transmission of medical image in EHR system". In this paper, the medical image have been protected using encryption and digital watermarking techniques to protect the medical image from unauthorized users. Telemedicine is been rapidly in used therefore it is necessary to protect the medical image in healthcare.

Abdulaziz Hadeal [2] published in IEEE access (IEEE-November 2017) "Privacy of medical big data in a healthcare cloud using a fog computing". In this paper, the main focus is given to protect healthcare data in cloud using fog computing. Authenticated key agreement protocol is been proposed using bilinear pairing cryptography which will generate session key to securely communicate. The healthcare data are accessed and stored securely using decoy technique.

Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu [3] published in IEEE access (IEEE-2016) "Privacy protection and intrusion avoidance for cloudlet based medical data sharing". In this paper, a new novel healthcare system is implemented by using the flexibility of cloudlet. The function of cloudlet includes data sharing, privacy protection, and intrusion detection. During the stage of data collection, there is utilization of Number Theory Research Unit (NTRU) method to encrypt user's body collected by wearable devices. That data will be transmitted to the nearby cloudlet in an energy efficient

fashion. In next step, a new trust model also helps similar patient's to communicate with each other about their diseases. In third step, the user's medical data stored in remote cloud of hospital is been divided in three parts and protection is been done. In order to protect the healthcare system from the malicious attacks, a new collaborative intrusion detection system(IDS) method. It is based on cloudlet mesh which can effectively prevent the healthcare big data cloud from attacks.

Xin Yao, Yaping Lin, Qin Liu, Junwei Zhang [4] published in IEEE access (IEEE-2018) "Privacy Preserving search over encrypted personal health record in multi source cloud". In this paper, a new technique is been implemented known as CB-PHR system in which multiple data providers, such as hospitals and physicians are authorized by individual data owners to upload their personal health information to an untrusted public cloud. The health data are submitted In an encrypted form to ensure data security, and each data provider also submits encrypted data indexes to enable queries over the encrypted data. A new method is propose known as multi source order preserving symmetric encryption (MOPSE) scheme whereby the cloud can merge the encrypted data indexes from multiple data providers without knowing the index content.

Huaqun Wang [5] published in IEEE access (IEEE-2018) "Anonymous data sharing scheme in public cloud and its application in E-Health record". In this paper, a new technique is proposed a secure data sharing scheme to ensure the privacy of data owner and the security of the outsourced cloud data. The proposed scheme provides the flexibility of data while solving the privacy and security challenges for data sharing.

3. EXISTING WORK

1) Paper based system: Every test, medication and visit for a patient is manually recorded on paper. These records are called charts. Each division of the hospital has its own set of records.

2)File system: The complete patient record is maintained in a single file on the computer.

3.1 Disadvantage of Existing system

1) Slow data exchange

2) Scattered patient data

3) Patient data cannot be accessed by multiple departments within the hospital

4) Difficult data storage and retrieval

5) Space, Cost and Time

4. BLOWFISH ALGORITHM

Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR Xr
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

5. RFID IN HEALTHCARE SYSTEM

RFID (Radio Frequency Identification) is one of the automatic identification technologies more in vogue nowadays. There are wide research and development in this area which are trying to take maximum advantage of this technology. In the coming years many new applications and research areas will continue to appear. This type of sudden interest in RFID have brings about some concerns such as the security and privacy of those who work with and the use tags in their everyday life. RFID has been used to access control in different areas such as asset tracking to limiting access to restricted areas. The architecture and a prototype of a system uses distributed RFID over Ethernet and demonstrate how to automate an entire patient health record system by using RFID in an Hospital environment. The RFID systems used in educational institutions is not new. It is intended to show that how the use of it can solve daily problems in our university.

A hybrid technique which combines encryption and digital watermarking in order to provide authenticity and integrity. The original image two region known as ROI (Region of interest) and RONI (Region of non-interest). ROI defines the diagnostic region of image and RONI defines the rest of the image and has no or medical image diagnostic system. The image is then divided into 16x16 blocks. The remaining blocks are considered ROI blocks are not used for embedding. The RONI blocks are used for watermark embedding. On the receiver's side, the watermarked image is delivered to the extraction procedure in order to extract the cryptographic watermarks and the hidden medical data of patient. The algorithm consist of two procedure watermark embedded procedure and extraction procedure. By applying the embedding procedure, the cover image is segmented into ROI and RONI. It is the divided into 16x16 blocks.

6. SYSTEM MODULE

There will be three modules in this healthcare system such as Doctor Module, Patient Module and Hospital Admin Module.

6.1. Doctor module

1. Registration form: The doctors need to be register to access cloud based personal heath record system.
2. Login form: Only the authorized doctors can access PHR system. The process of authorization consist of username and password which is provided at the time of registration.
3. View History: Doctors can able to see previous medical history of the patient.
4. Upload Prescription: Doctors can upload the prescription online or they can consult to patient online.
5. View personal details: Doctors can able to see their personal details which was given by them at the time of registration.
6. Update personal details: Doctors can modify their personal details.

6.2. Patient Module

1. Registration form: Every patient need to register to access cloud based personal health record (PHR) system.

2. Login form: Only the authorized patient can access PHR system. The authorization process includes username and password which is provided at the time of registration.

3. View history: Patients can able to see their medical history.

4. Upload diseases: Patients can upload their current diseases online.

5. View personal details: Patients can able to see their personal details which was given by them at the time of registration.

6. Update personal details: Patients can modify their personal details.

6.3. Hospital admin module

1. Registration form: Hospital admin have to register their hospital on online cloud.

2. Login form: Login credentials are required to access cloud database.

3. Home page: Can able to see hospital staff information.

7. SECURITY ANALYSIS

In this process of identifying the security it is necessary to analyze the security of the healthcare system, backend network and hospital network. The different segments have several requirements and possess vulnerabilities that can be exploited by threat agents to launch attacks against the healthcare system. Quality of service, safety and security are key aspects in the deployment of a healthcare system. The identification of security related requirements, vulnerabilities and threats are keys to the to the development of trustworthy system. The identification of system assets, possible vulnerabilities and threats can help the associated system risks. From a system point of view transferring complete and accurate information from patient to the hospital is always necessary. Data security and patient's privacy are certainly the important challenges in the deployment of healthcare system. In order to highlight specific security requirements in healthcare system we analyse the system as a sequence of segments, identify related security requirements, vulnerabilities, threats and attacks of each segment and possible security solutions for identified issues.

8. ADVANTAGES OF HEALTHCARE SYSTEM

1. Patient Privacy:

The Health Information Portability and Accountability Act (HIPAA) establish national standards for electronic health care transactions and addresses security and privacy of health data13. Patient medical records are considered as protected health information under the federal and any changes or accessions of medical records must comply with HIPAA to maintain patient privacy. Medical information needs to remain accessible to the authorized persons. It must be inaccessible to unauthorized persons to prevent identity theft and compromise of confidential patient medical history.

2. Accountability:

Medical records includes physician orders as well as exam and test reports which are considered legal documents and it must be kept in unadulterated form. Doctors or other professionals may make errors, so it is important to maintain truthful, accurate information regarding patients.

3. Impact on Efficiency:

Medical records systems play a fundamental role in healthcare system. Because they communicate the patient's information between various professionals. A bottleneck in this critical process will slow down overall patient care; medical information flow is especially prone to delays because it involves personnel who must physically examine and transcribe data. Optimizing data management reduces costs by increasing throughput.

4. Privacy, Security, and Accountability:

The most serious concern with any system designed is to manage the confidential information securely and how securely the information will be protected.

9. CONCLUSION

In this paper, we have demonstrated through a proposed algorithm that combining encryption and watermarking techniques can provide secure transmission of medical images over vulnerable public networks. The algorithm is based on dividing the image into ROI and RONI regions and embedding three different watermarks in the RONI region. The watermarks were chosen and embedded in such a way to provide image integrity and authenticity, which are the two major requirements for secured medical image transmission. Based on the findings of this work, the proposed algorithm could open up a number of possibilities for the future work. For example, improvement on the quality of the extracted watermark bits can be achieved by applying different error correction schemes such as Hamming codes, turbo codes, Reed Solomon ECC code, and trellis codes. Another enhancement can be achieved by applying reversible watermarking techniques on the ROI region of the image.

ACKNOWLEDGEMENT

I would like to express our sincere gratitude towards my guide Prof. Kanchan Doke for the help, guidance and encouragement. This work would have not been possible without her valuable time, patience and motivation. I thank her for making my stint thoroughly pleasant and enriching. It was great learning and as honor being her student.

I am deeply thankful to Prof. D. R. Ingle, HOD of Computer Department and the entire team in the Department of Computer Engineering. They have supported me with scientific guidance, advice and encouragement. They were always helpful and enthusiastic and this inspired me in my work.

REFERENCES

[1] Ghosh Sudip, De Sayandip "A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using extended hamming code", International co and communication technology conference on electrical information (EICT, 2015).

[2] Maksuanpan S."A new simple digital image cryptography technique based on multi-scroll chaotic delay differential equation", 2013 5th international conference on knowledge and smart technology (KST).

[3] Pandey Smita "A novel approach for digital image watermarking using 5-DWT-SVD and stream cipher encryption with different attacks", 2016.

[4] Basu Abhishek, Chattopadhyay Avik "Implementation of a spatial domain salient region based digital image watermarking scheme", 2016 second international conference on research in computational intellengence and communication networks (ICRCICN).

[5] Khanna Anshul, Roy Nihar "Digital iamge watermarking and its optimization using genetic algorithm", International conference on csomputing, communication and automation (ICCCA2016).

[7] Yadav Awadhesh, Naskar Ruchira "A tamper localization approach for reversible watermarking based on histogram bin shifting", 2015 IEEE power, communication and information technology conference (PCITC).

[8] Akbarzadeh M. R, Ghofrani S. "Image Content Authentication and tamper localization using on semi fragile watermarking with the help of the curvelet transform", 2012.

[9] M. Chen, J. Yang, "A 5G cognitive system for healthcare for healthcare", Bigdata cognitive computation vol. 1, no. 1, p. 2. 2017.

[10] M. S. Hussain, G. Mohammad, "Toward end to end biometrics based security for IoT infrastructure", IEEE wireless common Mag., vol. 23, no. 5, pp. 45-51, Oct. 2016.

[11] W. Raghupathi, V. Raghupati, "An overview of health analytics", J. Health Med. Informat, vol. 4, no. 3, pp. 1-11, 2013.

[12] J. Bian, U. Topaloglu, " Towards large-scale twitter mining for drug-related adverse events", in proc. SHB. Maui, H1, USA, 2012, pp. 25-32.

[13] Foster I., Zhao Y., Raicu I. and Lu S., "Cloud computing and grid computing using the 360-degree compared", in Procedural Grid comptuting Environment Workshop, Austin TX, USA, Nov. 2008, pp. 1-10.

[14] Kaur M.and Bharti M., "Fog computing providing data security: A review", Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 1, pp. 832-834, 2014'

[15] Hajibaba M.and Gorgin S., "A review on modern distributed computing paradigm: cloud computing, jungle computing and fog computing", J. Comput. Inf. Technol., vol. 22, no. 2, pp. 69-84, 2014.

[16] Bonomi F., Milito R., Zhu J. and Addepalli S., "Fog computing and its role with the help of internet of things", in Procedural 1st Edition MCC workshop mobile cloud computing, 202, pp, 13-16.

[17] Rahman S. and El-Khatib K., "Privacy key agreement and secure communication for heterogenous sensor networks", J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858-870, 2010.

[18] Vikas S., Gurudatt K., Pawan K. and Shyam G., "Mobile cloud computing: Security threats", in Proc. Int. Conf. Electron. Common.. syst., Coimbatore, India, Feb. 2014, pp. 1-4.

[19] Patil D., Patil S., Koli N., "Secured cloud computing with decoy documents", Int. J. Adv. Comput. Sci. Cloud Compt., vol. 2, no. 2, pp. 43-45, 2014.

[20] Liu W., "Research on cloud computing security with their problems and strategy", in Proc. IEEE Conf., Yichag, China, Apr. 2012, pp. 1216-1219.