Volume 11, Issue 4, October 2024 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Enhancing Healthcare Data Security Using the RSA Algorithm: A Cryptographic Approach

Ishaan Kapur
Research Scholar
Amity International School, Saket
New Delhi, Delhi, India
Email: ishaankapur46@gmail.com

ABSTRACT

Security is the most important concern for transmitting medical images as it includes sensitive patient data. Security of medical data is very important to protect sensitive information when digital images as well as their relevant information is transmitted throughout public networks. It is worth framing the original model to ensure trustworthiness and safety of symptomatic data of patients which were received and transmitted. There are different ways to secure data. The "Internet of Things (IoT)" is forecasted to transform healthcare sector and could result in proliferation of "Internet of Medical Things (IoMT)".

This study proposes method to secure cryptographic data for patients in hospitals with "Visual Cryptography" and RSA (Rivest–Shamir–Adleman) model. It contains both public and private keys which are generated randomly. Medical data is encrypted with the private key, while public key is used during the process of decryption. The randomly generated public key is transformed into a text or image file with hidden "Visual Cryptography". The key can encrypt RSA public key with patient's mail to extract public key and restore medical data. With Visual Cryptography and RSA model, the proposed model can provide dual data security. This method is also usable when patient changes their hospital. In addition, transmission security is very important as compared to security of storage as a lot of infrastructures secure transmission protocols to avoid devastating security breach and avoid attacks like data loss and ARP spoofing.

Keywords:—*RSA model, visual cryptography, Internet of Things, Internet of Medical Things, ARP spoofing, data loss, medical data*

I. INTRODUCTION

Big data refers to a huge volume of data which is generated from different sources which need secure processing and storage. It consists of private data of the user or pervasive data from different digital devices. Storing data offers a lot of opportunities to improve revenues. A lot of "Sensitive Health Information (SHI) has become a patient-based model to exchange sensitive data. With an SHI service, a patient can manage, create and control their personal health records at once online, which have made retrieval, storage, and sharing medical data more efficient.

Every patient has complete control of medical records and share health data with different users, such as family members, friends, and healthcare providers. Because of high cost of specialized data centers in terms of maintenance and development, a lot of

SHI services are outsourced or offered by third-party service providers. These days, SHIs are stored in the cloud by Microsoft HealthVault (Vengadapurvaja et al., 2017; Stefano and Ricardo, 2016). Meanwhile, it can collect, analyze, and redistribute personal data of the patient for several health reasons. Figure 1 illustrates the scenario when health data is shared to improve the quality of services (Vengadapurvaja et al., 2017).

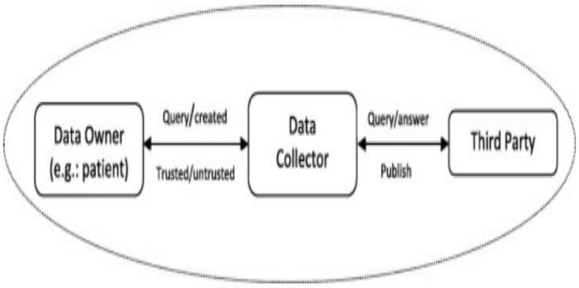

Figure 1: Scenario of sharing personal data for health purposes. Source – Sharma et al (2022)

With varied big data environment, users can use scalable distribution with internet connectivity. The data is shared in this environment and users don't know about the actual location of storage of data and they don't know other sources using and collecting data for their purposes (Kanika and Khan, 2017). There are different security and privacy concerns related to sharing mode which may affect its large-scale adoption. When SHI is stored in third-party and untrusted server, there might be risk for user privacy. When the "Health Insurance Portability and Accountability Act (HIPPA)" protects electronic and personal data and ensures sufficient protection, SHI data may be exposed by third-party storage server due to malicious acts.

Unauthorized users may access health data ahead of their privileges and rights. Hence, a promising and feasible approach should be developed to improve SHI security. In addition, it is possible to protect health data in two ways like protection by cryptography and policy. Hence, SHI should be protected and encrypted with complete control on the access. For sharing with third party, information owners should be able to tailor privacy policy as per the need. Visual cryptography was initially adopted by Naor and Shamir (1997). It is possible to split a secret image into shares in the stage of encryption. All the shares should be used to redesign the secret image in the decryption. Any n-1 shares cannot reveal the secret image.

The image for "Visual Cryptography" may be Grayscale, Binary, and Color in the initial image with all the n shares. In decomposition, each white pixel is decomposed into two white and two black pixels. The Rivest–Shamir–Adleman (RSA) algorithm is used by new devices to decrypt and encode messages. It is also known as "public key cryptography" as asymmetric cryptographic model. It belongs to the fact that it is not easy to find the factors of large composite. It is also a private and public key generator. RSA has both private and public keys. The public key refers to everyone as it can encrypt messages.

Messages encoded with public key can be decrypted only with private key. The private key remains secret. It is challenging to compute private key from public key. A cloud server stores the patient data in the hospital where security is very important. It offers secure and safe transmission as it consists of various manipulations for decryption and encryption. The system has a scope to provide ideal environment to deal with images. Every parameter of RSA and VC is implemented and minded to use this method in real-time applications like networks, distributed systems, and banking. Data security is focused to recenter search further to be used for multimedia security like video and audio.

II. Literature Overview

The "Wireless Body Area Network (WBAN)" is one of the most rising and growing field of "Wireless Sensor Network (WSN)". WBAN is a collection of body sensors that collect health data in real-time and transmit the same to medical server using wireless communication. Its cloud version can save lives in case of emergency as it provides real-time access to patient's health information. Since patient's data is highly sensitivity and private, it is worth having high-level security and protection to medical data over insecure public server. Nidhya et al (2021) proposed a secure architecture to monitor and access health data collected by WBAN. For robust security, they designed "Enhanced RSA (E-RSA)" authentication system. Along with master key, secret key is generated for the user. They have also considered some of the user attributes to secure the process of transmission of health data and also generated random value to generate secret key as per the concept of bilinear mapping. The simulation model explains how the proposed system efficiently preserve privacy and confidentiality to health data of patients in remote server.

The "electronic health record (EHR)" maintains patient's health data and cloud enables access to their data smoothly with huge storage at affordable costs. This way, organizations with EHR can transfer their data from local storage to cloud. However, there are different challenges to secure patient's data like data privacy, scalable access among various clouds, and access control. Gautam et al (2019) proposed an efficient and secure blueprint to secure confidentiality of data on the cloud computing storage. They carried out the proposed framework for confidential EHR data on cloud storage. In addition, this approach combines RSA and obfuscation to enforce authentication and confidentiality.

IoT has been one of the important solutions for data management when it comes to address concerns related to data security which can definitely improve overall storage, data collection, prediction of security breaches, maintenance, and taking corrective measures. Kavitha et al (2022) adopted a "deductive research approach, positivism research philosophy, and a descriptive research design" by collecting secondary data from scholarly articles, journals, and books. They have incorporated qualitative data analysis for the study. Given the pros and cons of IoT, AES, DES, RSA, and triple data encryption can be used in healthcare for data protection.

Internet of Things (IoT) network smoothly connects a lot of devices. Each device contains sensors to collect and generate data from its environment and sends the same to other objects through the channel. Transforming and storing this data is among the most challenging roles played by IoT and it is among the major concerns for all organizations adopting IoT technology. With communication, display devices, and storage, sensing equipment is benefitted with technological advances in healthcare. Al Shahrani et al (2022) proposed a "optimized hashing algorithm" with digital certificates to improve security. Health data are preprocessed and collected with normalization. They proposed "Discrete Decision Tree Hashing Algorithm (DDTHA)" with "Ant Colony Optimization (ACO)" hashes. The blowfish model is used for encryption and digital certificate is signed for authentication. Proposed system's performance is compared and evaluated with traditional approaches to prove system efficiency.

A lot of cryptographic models have been developed to ensure maximum security of message over the years during transfer over insecure mediums. It goes without saying that these models could curb the issue of insecurity of data and minimize cyber-attacks. Both symmetric and cryptographic models are secure. Osamor & Edosomwan (2021) focused on asymmetric models like "RSA Cryptographic model". They proposed a secure mode of data decryption and encryption by applying "scrambled alpha-numeric randomization" for clear knowledge of operational system of RSA model during decryption and encryption process. The "scrambled alpha-numeric randomization technique" adopts a different lettering sequence and numbering to every alphabet. It also adopts cryptographic syntax of message along with using American standard code for information interchange (ASCII)" encoding.

2.1 Research Gap

Various machine learning approaches have been used to protect healthcare data. This study fills much needed research gap by proposing a model to secure cryptographic data for patients' information in healthcare with visual cryptography and RSA model. With rapid advancement in digital imaging and internet technology, there are different ways to publish, create, and distribute images. Image-based validation and data security techniques provide ideal solutions to manage how private images and data are created to select people. Visual cryptography is a different type of cryptography that can encrypt handwritten texts, printed texts, and images, so human visual structure can only perform decryption.

2.2 Research Objectives

- To propose architecture for RSA encryption and decryption
- To discuss approach to preserve privacy of sensitive health data

III. Research Methodology

To fulfill the objectives above, this study is based on secondary data published in various articles and research papers related to RSA model in order to protect cryptographic data and proposed the RDA encryption and decryption architecture.

IV. Data Analysis

4.1 Architecture for RSA Encryption and Decryption

This section provides basic insight to the proposed architecture which is mainly categorized into five modules –

4.1.1 Management and Registration

The registration section of the hospital, patient registration on the Android app, and doctors on the official website consist of first module. This model considers healthcare system. First of all, the hospital is registered with needed details. The admin rejects or approves the hospital registered. The hospital can login only after approval. Later on, the hospital logs into the system. They can manage and add departments and register doctors in the hospital setting. After getting the doctor registered in the hospital, they can login with credentials. Doctors can manage symptoms and diseases of all patients. Appointments from patients are approved by the doctors and they can upload medical records in PDF or JPG format (Wilson and Abraham, 2022).

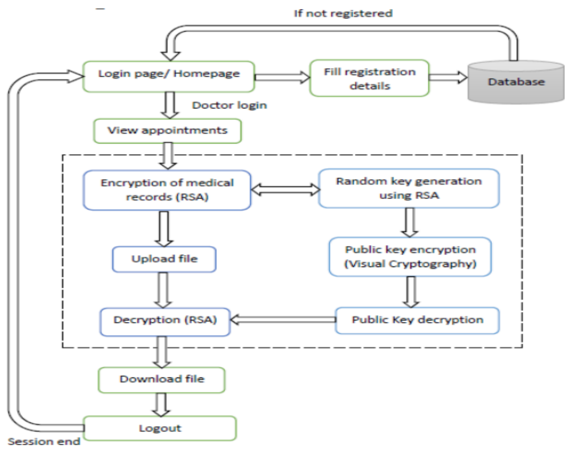

Figure 2: System architecture of model proposed Source – Wilson and Abraham (2022)

4.1.2 RSA Encryption and Decryption

Medical records like MRI, X-rays, lab reports, prescriptions, and CT scans, etc. are uploaded by patient or doctor that can be encrypted with RSA model before being stored in healthcare system to improve record security. RSA consists of both public and private keys which are generated randomly. Private key can encrypt medical data while “public key is used in the process of decryption. Patients can also upload medical data like lab reports, scan results, prescriptions, etc. Every time patients, doctors, and other authorized users wish to download the data, it should be approved by the patients as these medical records in the EHR are encrypted with RSA to secure records. Hence, it should be decrypted before authorized users can access records. RSA model is used by the system to decrypt medical records (Wilson and Abraham, 2022).

4.1.3 Encryption and Decryption of Visual Cryptography

Visual cryptography (VC) is an encryption method on text or images in which a visual system performs decryption. It encrypts image into various shares. After overlaying the printed shares together, human vision can decrypt the image. When it comes to upload medical record, a key is randomly generated. This private key can be used for encryption. The key is generated and encrypted by the file and stored in database of the hospital. Once medical record is downloaded, the cipher text and public key value is used for decryption, which is randomly generated and related to the record during upload. The public key can decrypt medical record and it is turned into text or image file with hidden VC. The key is randomly generated to encrypt the public key with VC and it is sent to email id of the patient to extract public key with VC decryption (Wilson and Abraham, 2022).

4.1.4 Patient module

Android studio is used as user interface by the patients. They can book and register appointments with Android app and they can choose their doctor and hospital after login. After selecting the hospital from the list, the patient can book an appointment from the selected doctor for their problem. Patients can also send complaints or suggestions to the healthcare department for doctor. It will be replied to and evaluated by the healthcare admin. The proposed approach is also applicable when patients choose another hospital. Other hospitals’ doctors can also get the medical history (like treatment plan, medication, scan results, and lab reports, etc.) of the patient by requesting them. After approval, the patient can provide the key on email id for doctors for downloading medical information. It is also the case when medical records are uploaded by the patient (Wilson and Abraham, 2022).

4.2 Approach to Preserve Privacy of Sensitive Health Data

Patient’s data may contain “sensitive health information (SHI)” as per the medical institutions and health societies. Patient’s SHI is a digital health record which is shared among several medical health institution worldwide for different reasons. It acts as a source of data for institution like pharmacy, hospitals, and labs (Yang et al, 2015). Any unauthorized access to SHI can increase privacy concern for a patient. To avoid data leak, a systematic approach has been proposed by Sharma et al (2022) –

4.2.1 System Model

The server is expected to be semi-honest, i.e., both curious and malicious (Sabrina, 2010). To be precise, the server attempts to get more hidden information in SHI data but it honestly follows the protocol overall. However, after submitting the data, patients don't have any control on it. Actually, they have lack of information on the actual location where data is stored. Additionally, a lot of users attempt to get information ahead of their rights. For instance, a pharmacy may need patients' prescription to improve their profits and for marketing purposes. They may conspire with other users for this purpose.

4.2.2 Patient's structure

It is assumed in this model that a registered patient has a unique SHI_id in the sensitive health information. Its data attributes can be categorized as health records, personal information, insurance data, hospital staff, and test reports (Figure 3). Sensitive health information is organized in a hierarchical manner for proper access-based decryption where authorized users get to know about sensitive health information of patients. An example has been used to give an insight to the proposed model. Suppose, Bob is a patient who owns sensitive health information in Hospital A. He creates F1, his SHI file on his first visit to the hospital. Along with health and general information, this file also consists of authorized individuals to access his data (Figure 3). Then, server stores the SHI and it is encrypted with proposed "Information Leakage Prevention Scheme (ILPS)".

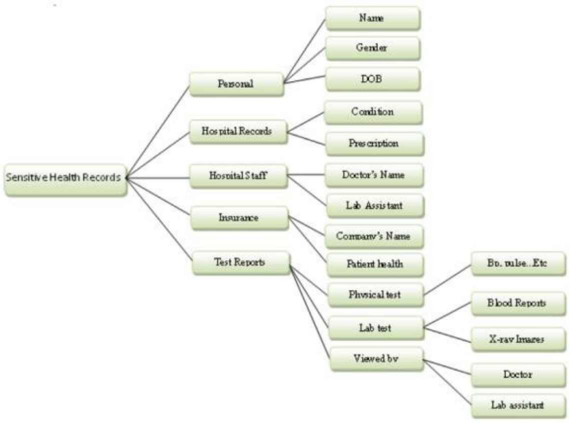

Figure 3: Overall Hierarchy of Patients SHI in proposed ILPS. Source – Sharma et al (2022)

The patient fully understands who can retrieve/decrypt their data in the proposed model. When creating patient's data, their technician, doctor, nurse, and family are involved. The proposed model can prevent leakage of SHI data and retain its confidentiality. The key is generated by patient's password and doctor's password in this scheme and password is mandatory after the treatment to get decryption key to access SHI of the patient. The proposed model is suggested for various users and domains.

- ***Actors*** – For secure patient-oriented SHI, the proposed model includes five important categories for individuals like personal domain, data owner, administrator, public domain, and big data server (Figure 4).
- ***Patient*** – Patient owns their sensitive health information in Hadoop. It consists of name, age, gender, family history, and disease.
- ***Personal Domain*** – Every patient has their own personal domain where they can trust their closed relatives like friends and family members. The patient offers access privileges as per the needs. Usually, the personal domain is small and it also reduces patient's burden.
- ***Public domain*** – In this domain, users don't have access rights over the SHI of the patient until patient allows. These entities are insurance company, hospitals, etc.
- ***Big data server*** – In this server, a lot of data can be stored easily, analyzed and processed. The SHI is stored in the server.
- ***Administrator-*** Each hospital is related to the administrator providing registration ID. During the first time visit at the hospital, the patient registers themselves for healthcare

services, create their profile, and get private key from the hospital, i.e., administrator." Whenever patient accesses the SHI, this private key is updated.

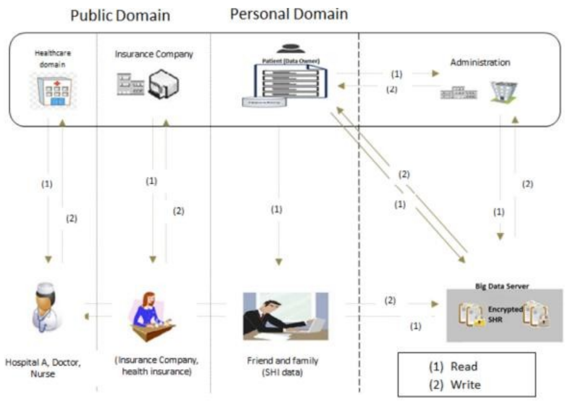

Figure 4: Proposed System Model to Secure Patient's SHI. Source - Sharma et al (2022)

V. Discussion and Conclusion

RSA consists of both public and private keys which are generated randomly. The private key encrypts medical data, while public key is used during the process of decryption. The public key was generated randomly and is turned into a text or image file, which is hidden, i.e., Visual Cryptography. Using VC, the randomly generated key to encrypt public key is sent to email id of the patient to gather public key with decryption. Finally, decrypted medical data is accessed with treatment plan, medication, lab reports, scan results, etc. Healthcare admin responds and evaluates feedback from the patients.

These could be either complaints or suggestions related to hospitals or doctors. Hence, dual data security is provided for medical records of patients with a combination of VC and RSA model. The proposed approach compares time complexity of "Elliptic Curve Cryptography" approach and RSA model for various file formats. As per the performance analysis, RSA takes a lot less time than ECC for decryption and encryption processes. Secure and instant diagnosis is needed in the world of healthcare. Transfer of images is a routine process and it is vital to find a productive approach to transmit on the network.

For safe transmission of images, there is a need to meet trustworthiness, authenticity, and privacy. Encryption is very effective for transmission and capacity. Data is not secured once sensitive data is decrypted. Messages are encoded on the encryption cryptography in a way that programmers are unable to read. Paired data or text data is preferred by the most popular encryption models. It is vital to ensure sensitive issue of security of data with advancement of e-commerce. It is worth framing the model for trustworthiness and safety of symptomatic data of patients which were received and transmitted. With a combination of VC and RSA model, dual data security can be provided for securing patient's data. Transmission security is very vital as compared to security of storage since a lot of infrastructures depend upon secure protocols to avoid security breach.

Safe transmissions are provided to avoid attacks like data loss and ARP spoofing. Hybrid or dual encryption is provided to improve data security and image uses VC. In an another approach, randomly generated key is transformed into an image using VC and it is split into patient's part and server's part. To retrieve data for the hospital or patient, the partitioned image should be uploaded to the server to offer generated key.

REFERENCES:

[1] Sharma, K., Agrawal, A., Pandey, D., Khan, R. A., and Dinkar, S. K. "RSA based encryption approach for preserving confidentiality of big data". *Journal of King Saud University-Computer and Information Sciences*, *34*(5), 2088-2097, (2022).

[2] Kanika, Agrawal, A., and Khan, R. A. "Security Integration in Big Data Life Cycle". In *International Conference on Advances in Computing and Data Sciences* Singapore: Springer Singapore, (pp.192-200). (2016, November).

[3] Vengadapurvaja, A. M., Nisha, G., Aarthy, R., and Sasikaladevi, N. " An efficient homomorphic medical image encryption algorithm for cloud storage security". *Procedia computer science*, *115*, 643-650, (2017).

[4] Naor, M., & Shamir, A. "Visual cryptography II: Improving the contrast via the cover base". In *Security Protocols: International Workshop Cambridge, United Kingdom, April 10–12, 1996 Proceedings 4* (pp. 197-202). , (1997) Springer Berlin Heidelberg.

[5] Nidhya, R., Shanthi, S., and Kumar, M. "A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm. In *Intelligent System Design: Proceedings of Intelligent System Design: INDIA 2019* (pp. 255 -263), (2021). Springer Singapore.

[6] Gautam, P., Ansari, M. D., & Sharma, S. K. "Enhanced security for electronic health care information using obfuscation and RSA algorithm in cloud computing". *International Journal of Information Security and Privacy (IJISP)*, *13*(1), 59-69, (2019).

[7] Kavitha, A., Rao, B. S., Akthar, N., Rafi, S. M., Singh, P., Das, S., and Manikandan, G. "A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT". *International Journal of Electrical and Electronics Research (IJEER)*, *10*(2), 270-275. (2022).

[8] Al Shahrani, A. M., Rizwan, A., Sánchez-Chero, M., Rosas-Prado, C. E., Salazar, E. B., and Awad, N. A. "An internet of things (IoT)-based optimization to enhance security in healthcare applications". *Mathematical Problems in Engineering*, *2022*(1), 6802967, (2022).

[9] Osamor, V. C., and Edosomwan, I. B. "Employing scrambled alpha-numeric randomization and RSA algorithm to ensure enhanced encryption in electronic medical records". *Informatics in Medicine Unlocked*, *25*, 100672, (2021).

[10] Wilson, B. and Abraham, J.. Medical "Data Security using RSA and Visual Cryptography". *International Journal of Science and Research (IJSR),11*(10) (2022).

[11] 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*, *43*, 74-86. (2015).

[12] Sabrina, F. "A novel resource scheduling algorithm for QoS-aware services on the Internet". *Computers and Electrical Engineering*, *36*(4), 718-734 (2010).

* * * * *