International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.186

Secure Data Transmission in Healthcare Monitoring Systems using Advanced Encryption and Decryption Techniques

Renjith P N
School of Computer Science and Engineering,
Vellore Institute of Technology Chennai Campus,
Chennai, India renjith.pn@vit.ac.in,
0000-0002-5109-7733.

Giridharaprasath M
School of Computer Science and Engineering,
Vellore Institute of Technology, Chennai Campus
Chennai, India
giridharaprasath.m2019@vitstudent.ac.in

Sudhakaran G
School of Electronics Engineering,
Vellore Institute of Technology, Chennai Campus
Chennai, India.
sudhakaran.g@vit.ac.in
0000-0002-0273-4185

***Abstract* — With the advancement of the Medical Internet of Things (MIoT) technologies, the accurate and continuous monitoring of the patients has become easy. A Smart Healthcare monitoring system is capable of monitoring different vital body signs such as blood pressure, heart rate, oxygen level and temperature. The sensors used in the monitoring system will capture the physiological signals and then the data can be sent to the cloud through IoT. Then the doctors or consultants can access the data from the cloud when needed to analyse the patient's condition. When sending the data to the cloud as such is prone to various attacks and can lead to misuse. So, it is advisable to use any of the techniques that are already available to prevent such attacks. One is, to encrypt the data that is being sent and then store the data. This type of system should follow certain rules to provide better security and also provide privacy to the data. This paper discusses the importance of encryption and decryption of data in a healthcare monitoring system. Healthcare monitoring systems are used to collect and analyze patient data, which is often sensitive and private in nature. Therefore, it is critical to ensure that the data is protected from unauthorized access or interception. The paper explores various encryption and decryption techniques that can be used to secure healthcare data, including symmetric and asymmetric encryption methods. Additionally, the paper discusses the challenges and limitations associated with the implementation of these techniques in healthcare monitoring systems. The study concludes that encryption and decryption of healthcare data is necessary to protect patient privacy and ensure the confidentiality of their sensitive information. Moreover, the study recommends that healthcare providers implement strong encryption and decryption techniques to ensure the security of patient data.**

Keywords—MIoT, Encryption, Decryption, healthcare monitoring, Unauthorized access

I. INTRODUCTION

The health care system has long struggled with issues like illegible diagnoses printed on paper, difficulty for healthcare professionals in accessing patient data, and a lack of resources (staff, time, and space) for patient monitoring. Hospitals and other healthcare centers have seen a significant increase in the use of healthcare monitoring systems, and many nations across the world are now very concerned about portable healthcare monitoring systems with emerging technology. The development of Internet of Things (IoT) technologies makes it easier for healthcare providers to move from in-person consultation to telemedicine. The health care delivery process will gain a lot from these technologies. These days, patient records are kept in digital form for subsequent use and easy access by anyone to assess the patient's condition. The storing of patients records in digital format is called Electronic Health Record (EHR). The electronic health record (EHR) or electronic medical record (EMR) is a computerised repository for data, diagrams, patient medical information, prescriptions, hospital or clinic records, radiological images, billing data, and other sensitive patient data. These records can also be shared among the health care providers and consultants with ease of access. However, there are a variety of security and privacy considerations that must be considered in order to promote and maintain essential medical ethical values and social expectations, even though these data are more practically useful than the traditional paper records.

The Electronic Health Records should follow certain security and privacy regulations and should ensure that the data that is being stored should be used for the right purpose and should ensure the privacy of the patient's personal information. Data security and privacy may be seriously jeopardised since they are sent electronically across the internet. Security is defined by the point at which access to someone's personal information is restricted and permitted for those with the required authorization. A person's right to decide for themselves when, how, and to what extent their personal information is shared or transmitted by others is referred to as their right to privacy. Sensitive information can be stolen via eavesdropping and skimming the sent data. Hackers gain access to the electronic health data information through data mining, which they may use to analyze patient data and spot trends and links. Using the data, they may classify and characterize the patients. Discriminatory and exclusionary consequences may result from this.

The use of lightweight, hardware-based authentication is one strategy that shows promise for data security. When the data is encrypted, others cannot access the data and make drastic changes to the data. In this way, it provides security and privacy of the data. The health care monitoring system usually consists of various sensors collecting data from the patient and all the sensors are connected to a microcontroller, where the data is converted to suitable format and stored for later purpose. The data that is being collected from the

sensor, are encrypted by the microcontroller and then only the data should be sent to the cloud to store the data. Without encrypting the data, hackers can get access to the data and can change the data. If the data is encrypted, the hackers cannot formulate the data, so they would not be able to change the data. So, we proposed a system where the data being sent from the sensor to the server is encrypted first and then sent to the cloud.

Encryption and decryption are two fundamental concepts in information security that are used to protect sensitive data from unauthorized access or interception. Encryption involves converting plaintext or readable data into ciphertext or coded data, using a mathematical algorithm and a secret key. The ciphertext can only be read by someone who possesses the secret key to decrypt the data. Decryption, on the other hand, is the process of converting ciphertext back to its original plaintext form, using the same algorithm and the secret key that was used for encryption. By encrypting data, sensitive information can be protected from unauthorized access or interception, ensuring its privacy and confidentiality.

II. Literature review

The first official encryption algorithm that was used was Data Encryption Standard (DES) [1] algorithm. Developed by IBM in 1975, Can be implemented in special purpose electronic devices, to provide cryptographic protection to binary coded data. This algorithm uses a single key for both encrypting and decrypting the data. The major drawback of this method is the small key size of 56-bit. This encryption algorithm is outdated as it became easy to break the encryption with the keys. So, to improve the existing method, Triple-DES [2] was developed. In this method, the data is encrypted three times using the same key, so it can improve the efficiency and makes it difficult to break the encryption. The major setback of this method is the processing time as the data should be encrypted three times.

In the year 1997, Joan Daemen and Vincent Rijmen developed a better and efficient encryption algorithm compared to the DES algorithm, which is called Advanced Encryption Standard (AES) [3] algorithm. It became the successor of the DES algorithm. In this method, different key sizes of length – 128 bits, 192 bits, 256 bits are used. Due to the increased key size, it makes it difficult to crack the encryption. Xin Zhou and Xiaofei Tang in their paper [4], talked about the implementation of the RSA algorithm, which is another Asymmetric encryption algorithm, that uses public key to encrypt the data and private key to decrypt the data. The public key is a product of two non-negative prime numbers. Their proposed method is easy to implement and difficult to crack the algorithm. Rajan and Geeta, in their paper [5] proposed a method to encrypt the data stored in files and can be shared with others. They used the RSA algorithm to encrypt the data. So that the data in the file is immune to any attacks and data leakage. The only drawback of their method is, they can only encrypt only one file at a time.

Mousa and Hamad [6], in their paper, talked about the RC4 encryption algorithm. RC4 is a stream cipher encryption algorithm. It uses a key of variable-length and also it encrypts one byte at a time. The data stream is simply XORed with the generated key sequence. This method is easy to use and fast, but it is an insecure algorithm.

Blowfish encryption algorithm [7] is a symmetric-key block cipher algorithm founded in the year 1993. It provides a successful rate of encryption at software level. But it was preceded by the AES algorithm [3] since it is similar to the DES algorithm [1]. It is an open source, non-patented and freely available for use and modifications. It uses the same key for both encrypting and decrypting the data. Blowfish is faster compared to other block cipher algorithms as it takes advantage of the built-in instructions imposed on the microprocessors for basic operations like bit shuffling. Blowfish algorithm found to be secure after several tests. Homomorphic encryption algorithm [8] is a type of encryption algorithm where the data can be used to perform computational analysis even if the data is encrypted. The patient's data that is being collected are sent to the cloud after encrypting to perform analysis on the patient using those data. There is no need to decrypt the data first to analyse the data, so it can prevent misuse of data, while storing in the cloud. But this process is slow since computation should be made on encrypted data.

Diffie-Hellman protocol [9] is an encryption algorithm where two users exchange a secret key among themselves and that key is then used to encrypt the message that they want to share among themselves. The protocol uses the multiplicative group of integers modulo p and g, where p is a prime number and g is a primitive root modulo of p. This protocol itself is limited to only the exchanging of the keys between the two users. Secure Hash Algorithm [10] is a cryptographic hash function algorithm which uses hash function to map the data of arbitrary size to a bit array of fixed size called hash value. It produces a message digest of larger hash value. The family consists of various versions of varying output size with increase in security and immunity to attacks. Currently SHA-3 is the latest version of the SHA family.

Searchable Symmetric Encryption [11] is an encryption algorithm, where it is easy to search over a collection of encrypted files even without decrypting the files first. With the encryption key and keyword that need to be searched, a search token is generated and using that searching is done. It is useful in implementing cloud storage servers, where the servers are unreliable and cannot be trusted. In this paper [12], they proposed a method to perform predictive analysis tasks on encrypted data. It is achieved by using a Homomorphic encryption scheme to encrypt the data and then the data can be used to perform analysis. As already said in [8] this method is incredibly slow and has performance issues. In this paper [13], they proposed a simple and efficient method to construct a Chosen-Cipher Attack (CCA) secure public key encryption scheme from an already existing Chosen-Plaintext Attack (CPA) secure Identity-Based Encryption (IBE) scheme. Their method produces an efficient and secure encryption scheme compared to the original approach. Identity-Based Encryption scheme [14] is a symmetric encryption, where the identity of the user can be found using unique information and is used as the public key for encryption. Then a Private Key Generator generates a private key, which is used for decrypting the data. The scheme is pre-defined by a set of four algorithms that form a complete IBE system. This method is secure and efficient.

Electronic Health Record Systems are used to collect the data from the patients. The data is collected by the IoT

devices that consist of various sensors, that are then sent to the cloud to store the data. But the system should follow certain security and privacy policies and the issues related to these systems is explained in the paper [15], along with various measures to follow to prevent security issues. In the paper [16] they talked about the challenges of protecting the patient's data stored in the electronic health record systems. Access control can be enforced to protect the data. Where the patient themselves can generate and store the encryption keys and can share the data to others to perform actions like searching for certain data in the records.

III. Problem statement

A healthcare monitoring system is a technology-based platform that is designed to collect and analyze patient data. It is typically used in clinical settings to monitor patient health status, track the progress of treatment plans, and provide insights into patient care. The system typically collects data from a variety of sources, such as medical devices, electronic health records, and patient self-reports, and uses algorithms and analytics to provide insights and feedback to healthcare providers. Healthcare monitoring systems can be used in a variety of contexts, such as in hospitals, clinics, and home health care settings. They are particularly useful in managing chronic diseases, such as diabetes, heart disease, and hypertension, where regular monitoring is necessary to ensure optimal patient outcomes. By providing real-time insights into patient health status, healthcare monitoring systems can help healthcare providers to identify potential health problems and take preventive measures to avoid complications. However, the use of healthcare monitoring systems also raises concerns about patient privacy and data security. The data collected by these systems is often sensitive and private in nature, and must be protected from unauthorized access or interception. This is where encryption and decryption of data comes into play, as an essential component of securing patient data in healthcare monitoring systems.

With the widespread use of healthcare monitoring systems, sensitive patient data is being collected and transmitted over networks. However, this data is at risk of being intercepted and accessed by unauthorized individuals, posing a serious threat to patient privacy and confidentiality. Thus, there is a need for effective methods of securing healthcare data to ensure its privacy and confidentiality. This paper aims to address this problem by exploring various encryption and decryption techniques that can be used to protect healthcare data in monitoring systems, and by analyzing the challenges and limitations associated with their implementation in this context. The data that is sent by the microcontroller, which is collected by sensors, needs to be encrypted in order to stop the hackers from accessing the data and using it for their own purpose and also to stop leakage of data. Before transmitting the information to the server, the data needs to be encrypted in order to be stored in the cloud and used for analysis. When the data is encrypted, the data cannot be easily used and the hackers cannot decrypt the data without necessary keys. When the data is encrypted using various keys, the keys should be protected at all cost. If the keys get leaked, then it can be used to decrypt the data and the data can be used for illegal purposes. The data can be encrypted and decrypted using a variety of techniques that are available.

In the Healthcare Monitoring system, Cyber-attack is a major concern. The data that is being sent and stored should be protected from intruders. The data may contain important information about the patients and important medical records which when leaked can cause consequences to the patient and the health care providers. So, it is important to safeguard the data. The hackers can steal the data using different ways. The health care providers should be able to provide various protection methods to protect their client's data. In this paper, we talked about various encryption algorithms that are available for using and made a comparison to find the best and efficient algorithm.

IV. Methodology

Encryption and Decryption is one of the methods that can be used to ensure the security and privacy of personal data that are collected from various sources which need to be kept safe from leaking and being misused or altered. There are various encryption algorithms available for use. Primarily it is of two types, based on how many numbers of keys are used to encrypt and decrypt the data. They are Symmetric and Asymmetric encryption algorithms. Symmetric encryption algorithm uses only a single key for both encrypting and decrypting the data. Whereas in Asymmetric two keys are used, one for encrypting, which is called a public key, and the other for decrypting, which is called a private key. These keys should be protected from getting leaked so that intruders cannot access the data.

The healthcare monitoring system usually consists of a microcontroller and various sensors to read the data. The sensors will read the data and send it to the microcontroller, which will convert the data to suitable format for processing the data. The server will create a key which can be used for encrypting and decrypting the data. Then the server will send the key to the microcontroller and using that, the microcontroller will encrypt the data and send the encrypted data back to the server. Now the server will use the same key or private key based on the algorithm used and will decrypt the data. The communication between the microcontroller and the server is achieved using socket programming. If an Asymmetric encryption algorithm is used, then the server has to create both the public and private key, and should send only the public key and keep the private key safe. Some examples of symmetric encryption algorithms are DES, AES, Salsa20 and an asymmetric encryption algorithm is RSA, which is discussed in this paper. Using a raspberry pi and a temperature sensor to read the patient temperature, the raspberry pi will encrypt the data and send it to the server.

In this paper, we have taken DES, AES, RSA, ARC2, Salsa20 and Blowfish encryption algorithms and recorded the time taken by each algorithm to encrypt and decrypt the data. We used Python as the programming language as it is easy to use and also has a cryptographic library that can be used for encrypting and decrypting the data. First, we implemented a simple encryption and decryption program for each of the above-mentioned algorithms. Then using the timer package library present in python, is used to find the time taken by these algorithms to encrypt and decrypt a large sized data and the findings are recorded. Then using the socket package library present in python, a simple server side and client-side communication is established where the server and client can send data back and forth. Using this program, first the server will open a port for clients to

connect to, and then will create a key for encrypting and decrypting and when a client connects to the server, the server will send the key to the client, then the client-side program will use that key and will encrypt the sample data. The encoded data will be sent back to the server, and the server will use the same key or a private key to decrypt the data. Just like before, the timer package is used again to find the total time taken for encrypting and decrypting the data. The timer starts when the client establishes a connection with the server, and will stop when the server decrypts the encoded data sent by the client.

The Raspberry Pi is a single-board miniature computer that can be used for a variety of purposes. It can read data from various sensors and also convert data received from the sensor to a suitable format using the package libraries available. The values from the sensor can be read and converted into the appropriate format inside the raspberry pi using the gpio module package in Python. In this example, the raspberry pi will act as a client, which will connect to an external server running on a computer. The raspberry pi will read the sensor values and using the key it received from the server, will encrypt the data and send the encrypted data back to the server.

V. RESULTS AND DISCUSSIONS

Some of the algorithms used in this experiment are no longer used in the real-world situations, and are taken into comparisons as new encryption algorithms are developed to overcome the issues and backdrops of old encryption algorithms. DES is no longer in use, as it uses a short key length, the data can be hacked with brute force attack. To overcome this, AES was developed, which uses long key length. AES is considered as the base standard algorithm for encryption, since it is very fast and secure. RSA is an asymmetric encryption algorithm that uses two keys instead of one key, to ensure more security. RSA is the most widespread and used encryption algorithm. From this experiment, we recorded that even though RSA is secure and reliable, due to the computational need to find the keys, it is a slow encryption algorithm compared to another encryption algorithm. Even RC2 is never cryptographically broken, but it is slower compared to AES. The only issue with the Salsa20 encryption algorithm is that it doesn't guarantee the authenticity of the encrypted data. We can overcome this issue by using Message authentication code to ensure the authenticity of the data. The Blowfish encryption algorithm uses key lengths of varying size, even though it is secure and fast, but a long key should be used to withstand a brute force attack. We plotted graphs to show the time taken by each algorithm to encrypt and decrypt the data.

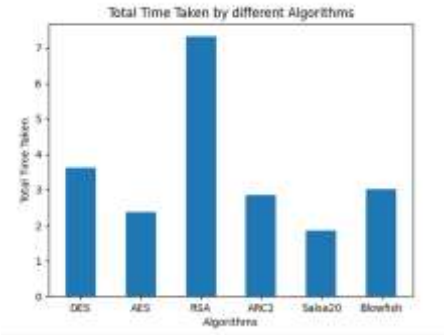

Fig.1. represent the time by algorithm during encryption

From this graph Fig 1, we can see the total time taken by each algorithm to encrypt the data on the raspberry pi and send the encrypted data back to the server and the server will decrypt the data. RSA takes the longest time, while AES takes the least time to encrypt and decrypt the data.

Time taken by different algorithms to encrypt and decrypt a large sized data. The RSA algorithm cannot encrypt large sized data. Again, AES takes the least time.

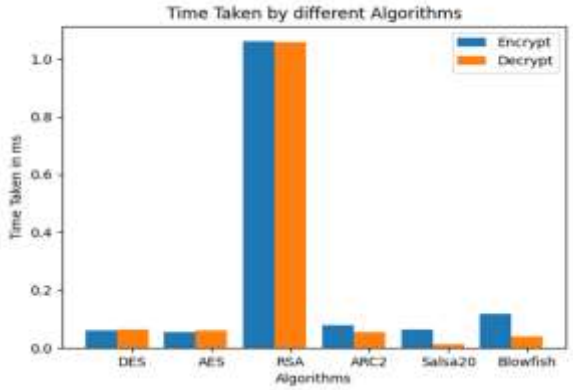

Fig.2. Represent the time by algorithm during decryption

The graph Fig 2, shows the separate time taken by the algorithm to encrypt and decrypt the data. RSA takes the longest time due to the computations needed to encrypt and decrypt the data. From this experiment, we can conclude that AES is one of the best algorithms to use, RSA is secure but is slower compared to other encryption algorithms.

VI. CONCLUSION

As we go into this new age of IoT, we can see the development of new technologies that can make our lives easier and can help us in a lot of ways, especially in real-time healthcare monitoring. If the security is exploited in this field, it can lead to huge problems. Especially when it involves life support. In conclusion, the importance of encryption and decryption of data in healthcare monitoring systems cannot be overstated. Healthcare data is sensitive and private, and thus needs to be protected from unauthorized access or interception. This paper has explored various encryption and decryption techniques that can be used to secure healthcare data, including symmetric and asymmetric encryption methods. Therefore, securing the data becomes important and comes to play in this scenario. Any breach in security in any of these systems or even intervention can lead to loss of life or any other serious consequences. Therefore, it is also important to implement error checking whether if the data is intervened by a middleman or the third person apart from sensor and server, with just encryption, there is no way the server or sensor can know that there is any intervention in data. With the help of error checking or intervention checking algorithms, one can assure an extra layer of security in these cases. Overall, this paper has provided valuable insights into the importance of encryption and decryption of data in healthcare monitoring systems. It is hoped that the study's findings will inform policy and decision-making in this area, and contribute to the development of more secure and privacy-conscious healthcare monitoring systems.

REFERENCES

[1] National Bureau of Standards - Data Encryption Standard, FIPS Publication, p. 46, 1977.

[2] R. Merkle, and M. Hellman, "On the Security of Multiple Encryption", Communications of the ACM, vol. 24, no. 7, pp. 465–467, July 1981.

[3] NIST, "Advanced Encryption Standard Call", NIST, 1997.

[4] X. Zhou, and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," In Proceedings of 2011 6th international forum on strategic technology, IEEE, .vol. 2, pp. 1118-1121, August, 2011.

[5] Rajan.S.Jamgekar, and Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA (IJESE)", vol. 1-(4), ISSN: 2319–6378, 2013.

[6] A. Mousa, and A. Hamad, "Evaluation of the RC4 algorithm for data encryption," Int. J. Comput. Sci. Appl., vol. 3, no. 2, pp. 44-56, 2006.

[7] Rajesh, M., &Sitharthan, R. (2022). Image fusion and enhancement based on energy of the pixel using Deep Convolutional Neural Network. Multimedia Tools and Applications, 81(1), 873-885.

[8] K. Munjal, and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," Complex Intell. Syst., 2022.

[9] Nan Li, "Research on Diffie – Hellman Key Exchange Protocol", IEEE 2 nd International Conference on Computer Engineering and Technology, vol. 4, pp. 634 – 637, 2010.

[10] Pazhani. A, A. J., Gunasekaran, P., Shanmuganathan, V., Lim, S., Madasamy, K., Manoharan, R., &Verma, A. (2022).Peer–Peer Communication Using Novel Slice Handover Algorithm for 5G Wireless Networks.Journal of Sensor and Actuator Networks, 11(4), 82.

[11] G. S. Poh, J. J. Chin, W. C. Yau, K. K. R. Choo, and M. S. Mohamad, "Searchable symmetric encryption: designs and challenges," ACM Computing Surveys (CSUR), vol. 50, no. 3, pp. 1-37, 2017.

[12] J. W. Bos, K. Lauter, and M. Naehrig, "Private predictive analysis on encrypted medical data," Journal of biomedical informatics, vol. 50, pp. 234-243, 2014.

[13] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," SIAM Journal on Computing, vol. 36, no. 5, pp. 1301-1328, 2007.

[14] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586–615, 2003.

[15] Chacko, Anil and Hayajneh, Thaier, "Security and Privacy Issues with IoT in Healthcare," EAI Endorsed Transactions on Pervasive Health and Technology, vol. 4, p. 155079, 2018,. 10.4108/eai.13-7-2018.155079.

[16] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," In Proceedings of the 2009 ACM workshop on Cloud computing security pp. 103-114, November, 2009.