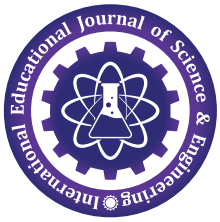
E-ISSN No : 2581-6195 | Volume : 2 | Issue : 6 | Nov-Dec 2019



RFID SECURITY IN HEALTHCARE USING HYBRID ENCRYPTION

Amanze, B.C.[1], Ononiwu, C.C[2], Nwoke, B. C[3]

ABSTRACT

A huge revolution has occurred in Radio frequency identification (RFID) technologies during the past decades. More vendors are involved and have invested in this technology which promises wholesale changes across a broad spectrum of business activities. Data security is a key area in RFID usage because the users of the system must be assured of their data's security. The increased focus on patient safety in hospitals has yielded a flood of new technologies and tools seeking to improve the quality of patient care. However, it is important to protect patient confidentiality as many medical conditions are stigmatized and disclosure could result in personal or financial loss. Encryption algorithms have been used since a long time to keep secret data safe from intruders. These algorithms are generally improved based on drawbacks of earlier algorithms. The focus of this paper is the implementation of a hybrid cryptographic algorithm. The algorithm is designed by amalgamation of two cryptographic algorithms AES and Elgamal. Performance evaluation of the existing and proposed algorithms was done on the parameters of security, encryption time and decryption time. Based on our analysis, the new hybrid encryption algorithm (CHE) has a better performance with respect to the security of patients' records and the confidentiality of their records is high.

KEYWORDS: RFID, Security, AES, Elgamal and Chamberlyn Hybrid Encryption Algorithm

1. INTRODUCTION

Radio frequency identification (RFID) technology is a non-contact, automatic identification technology that uses radio signals to identify, track and detect a variety of objects including people, vehicles, goods and assets without the need for direct contact or line-of-sight contact (as found in barcode technology) [1]. RFID is a growing trend in the healthcare industry, driven by a greater emphasis on patient safety than has ever been seen before. The increased focus on patient safety has yielded a flood of new technologies and tools seeking to improve the quality of patient care. Hospitals are complex institutions by nature and are constantly challenged to improve the quality of healthcare delivered to patients while trying to reduce the rate of medical errors and improve patient safety [2].

Precisely, identification is an important step in healthcare systems because each part of the healthcare system must be identified whether patients, devices or medications. Misidentification can cause fatal issues that may lead to loss of a patient's life [3]. RFID technology uses radio waves to transfer data and track any object that has a tag attached to it. The RFID system has three main components; the tag, the reader, and the backend server/database. The tag is usually placed on objects and has identification values such as secret key and an identifier stored in its memory. These values are also stored in the backend database/server and the tag can authenticate itself by sending and receiving its values to the server through a reader. The reader queries tags by sending radio frequency (RF) signals to ask the tag for their identification values is order to authenticate them [4].

The encryption technology is the basic safety techniques used in current e-commerce and banking websites which are of extreme importance. Information encryption technology cannot only meet the security requirements of confidentiality of information, but also avoid the leakage of the important information which is of high security especially in hospital and banking sectors. Therefore, encryption technology is the base of authentication technology as well as many other security technologies that are used todays [5]. Confidentiality of patient information has become a major issue in the storage and retrieve of healthcare data and biological samples. Some diseases, such as AIDs and depression are stigmatized and patients are often concerned that they could lose their employment or their insurance coverage if these conditions are revealed. Similarly, stored biological samples

[1,3] Department of Computer Science, Imo State University, Owerri, Nigeria
[2] Department of Computer Science, Imo State Polytechnic, Umuagwo, Nigeria

HOW TO CITE THIS ARTICLE:
Amanze, B.C., Ononiwu, C.C, Nwoke, B. C (2019). Rfid Security in Healthcare Using Hybrid Encryption, International Educational Journal of Science and Engineering (IEJSE), Vol: 2, Issue: 6, 08-10

Research Paper

can be used to identify future health risks, impacting a patient's chance of obtaining insurance. Therefore, it is critical that a patient's identity be protected in healthcare databases. At the same time, a medical record is dynamic and it is important that a healthcare team be able to unambiguously identify a patient when they need to retrieve or update the information in the database6. The purpose of this study is to encrypt the patients' record using a hybrid model which combines Advanced Encryption Standard and Elgamal algorithms.

1. AES encryption algorithm:

The Advanced Encryption Standard (AES), which implements the Rijindael cipher, is a symmetric block cipher that was developed as a result of a call by the United States National Institute of standards and Technology in 1997 for a secure cryptosystem to replace the then standard Data Encryption Standard algorithm which had become vulnerable to brute-force attacks.

AES is a symmetric algorithm. Therefore, it uses the same key for encryption and decryption. To allow for this phenomenon, all operations used in the encryption process must possess an inverse operation to exactly undo the transformations applied to the plain text in order to recover the plaintext message from the cipher text at the time of decryption. A field obviously contains the addictive and the multiplicative inverse of each of its elements and guarantees the existence of the inverse operation of any transformation applied to its elements. Thus, a field satisfies the requirements that will allow use of the same key in the encryption and decryption processes [7]. In AES, there are four transformations for one round.

- Sub Bytes - It is a nonlinear substitution in which each byte of state is replaced with the byte of S-Box in case of encryption and with the byte of inverse s-Box in case of decryption depending upon its value.
- Shift Rows – Each row is rotating according to row position from right to left. First row of state matrix remains unchanged, second row shifts by 1 bit to the left, the third row shifts by 2 bits to the left and fourth row shifts by 3 bits to the left. In case of decryption, shifting is to the right.
- Mix Columns – Performs mixing operation in which each byte is replaced by a value dependent on all 4 bytes in the column.
- Add Round key – Each byte of the state is combined with the round key using bitwise xor[8].

2. Elgamal Encryption

Elgamal encryption is an asymmetric key algorithm which is based on the public key exchange developed by Taher Elgamal in the year 1985. The system provides an additional layer of security by asymmetrically encrypting keys previously used for encryption. Elgamal encryption consists of three components; the key generator, the encrypting algorithm, and the decryption algorithm.

2. RELATED WORK

This section gives the overview of related work by various authors.

[12], found that RFID leads to gains in operational efficiency, organization wide quality and increased patient level accessibility. According to [10], hospitals are faced with confidentiality issues. For example there are fears that third parties could access private patient information such as drug use, therapy, diagnosis, and types of disease. [11], opined that prices are certainly a barrier to successful RFID implementation but as technology improves, these systems have become more affordable. New efficiencies can pay for a typical system in one to two years according to vendors. [13] Agrees that there are large cost efficiencies that can be realized with RFID. The wasted time spent searching for missing equipment and the expense of buying replacement equipment is a major cost to hospitals. [14] Found that managers believe the implementation of RFID in healthcare could lead to many benefits including improved patient care, improved patient security and safety, and improved organizational performance.

3. METHODOLOGY

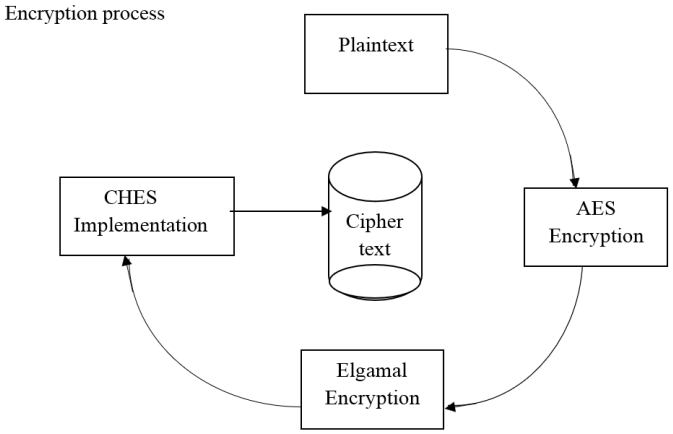


Figure 1: Block Diagram of Hybrid system.

4. IMPLEMENTATION/RESULTS

The implementation of this hybrid system shows that the time requirement for encryption is higher than the time requirement of AES and Elgamal.

1. Encryption Time

The time required to encrypt data is termed as encryption time of the cryptographic system. In the figure, X-axis contains data of different size for experiments and Y-axis contains time required. The encryption time of the AES, Elgamal and proposed hybrid system is given in below table:

Data Size (KB)	AES	Elgamal	Hybrid (CHES)
150	15	15	27
299	28	31	62
448	35	38	80
597	54	60	121
747	71	85	148

Table 1: Encryption for each algorithm

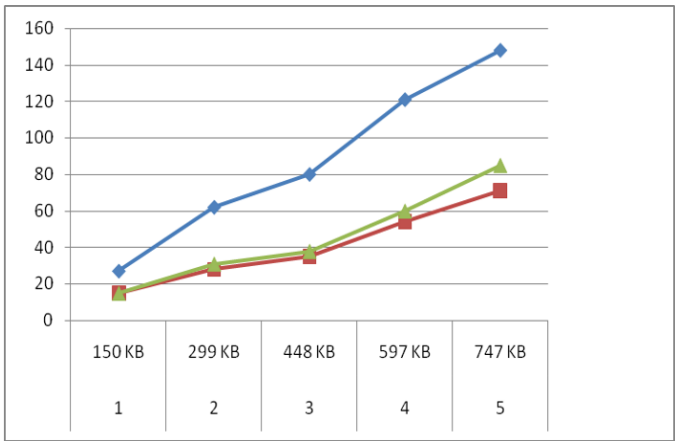


Figure 2: Encryption time for each algorithm

The diagram contains data of different sizes in X-axis by which experiments are conducted. Similarly Y-axis contains amount of time in microseconds. The results show proposed algorithm consumes more time compared to AES and Elgamal algorithm. According to mean performance, proposed Hybrid algorithm consumes more time with respect to AES and Elgamal algorithms.

2. Decryption time

The time to recover original data from cipher is known as decryption time[10]. The figure below shows comparative performance of AES, Elgamal and proposed Hybrid algorithm. The X-axis contains data of different size for experiments and Y-axis contains time required. The decryption time of the propose algorithm is higher compared to individual AES and Elgamal algorithm.

Data Size (KB)	AES	Elgamal	(CHE)
150	18	18	32
299	35	37	79
448	49	53	103
597	70	75	155
747	186	188	192

Table 2: Decryption Time for each algorithm

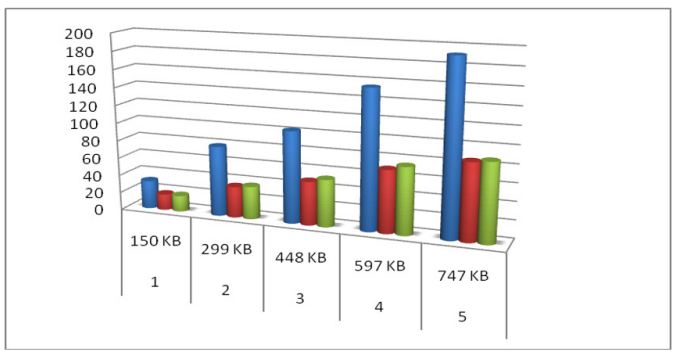


Figure 3: Decryption time for individual algorithms

The results as defined in the figure shows that the time taken by new Hybrid encryption algorithm for decryption process is much higher compare to AES and Elgamal algorithms. This makes the new Hybrid algorithm more secure since it will take a longer time to decrypt data.

6. CONCLUSION

Cryptography is performed to protect the intended data from hacking. In this paper, we discussed about AES, Elgamal and our proposed hybrid algorithm using AES and Elgamal algorithms. The proposed hybrid encryption algorithm has a better performance with respect to the security of patients' records and the confidentiality of that record is high. The new algorithm will ensure integrity of medical records of patients against potential hackers.

7. REFERENCES

1. O' Brien, D. (2006). RFID - Introduction and security considerations, Presentation at the ISS World, Washington, DC.
2. Aguilar A, Van der Putten, W and Maguire G: Positive Patient identification using RFID and Wireless Networks.
3. Lahtela A (2009). A short overview of RFID Technology in Healthcare. Systems and Networks Communications, ICSNC' 09. Fourth International Conference p. 165-169.
4. Song B, Mitchell CJ (2008). RFID authentication protocol for low-cost tags. In proceedings of the first ACM conference on wireless network security, 140-147.
5. Sushant S, and Gautam Borkar (2014). Hybrid Encryption system. International Journal of computer science and Information Technologies, Vol. 5 (6), 7563-7566.
6. Morse, R.E, Nadkarni, P., Schoenfeld. D.A., and Finkelstein, D.M (2011). Web-browser encryption of personal health information. BMC medical Informatics and Decision making, 11:70.
7. Sushant S, and Gautam Bortar (2014). Hybrid Encryption system. International Journal of computer science and information Technologies, Vol. 5 (6), 7563-7566.
8. Deore, P. and Chaudhari, T.; Hybrid Encryption for Database security. International Research Journal (9) Engineering and Technology (IRJET) Vol. 4 (11) 2017.
9. Kapoor, V., Yadav Rahul, (2016). A Hybrid cryptography Technique for improving Network Security". International Journal of Computer Applications Vol. 141 (11).
10. Wicks, A.V. (2006). Radio frequency identification applications in hospital environments. Hospital Topics 84 (3), 3-8.
11. Page, L. (2007). Hospitals tune in the RFID. Materials Management in Health Care, 16 (5), 18-20.
12. Revere, L.B. (2010). RFIDs can improve the patient care supply chain. Hospital Topics, 88(1), 26-31
13. Swedberg, c. (2009). Virtual health expects improved bed management from RFID. RFID Journal http://www.rfidjournal.com/article/view/7220.
14. Reyes, P.L. (2012), Accessing antecedents and outcomes of RFID Implementation in health care. International Journal of Production Economics, 136(1) 137-150.