Development of Radio Frequency Identification Database using Advanced Encryption Standard (AES) and Elgamal Encryption Algorithm (EEA) in a Health Sector

Amanze Bethran C[1]., Nwoke Bethel C[1] & Eleanya Mirian C[2]
[1]Department of Computer Science, Imo State University, Owerri
[2]Department of Statistics, Imo State University, Owerri
amanzebethran@yahoo.com +2347062523438
DOI: 10.56201/ijcsmt.v10.no5.2024.pg90.99

Abstract
The work proposed a hybrid encryption algorithm for security of database and protection in radio frequency identification system using an advanced encryption standard and elgamal encryption as a cryptographic primitive. The algorithm protects high-valued sensitive health records against malicious users. With the developed system, one can provide a proof for each record stored in the database of the RFID system because it is sufficiently robust to withstand replay attack, eavesdropping attack and backward traceability. All records are randomized and each tag has its own unique identification data. In the proposed solution, the database was secured using hybrid encryption standard. The system is user friendly and interactive. Security enhancement will be achieved with the new system. The software when deployed will assist health institutions to keep track of their patients' record easily. The New Hybrid Encryption algorithm takes much longer time compare to time taken by AES and Elgamal. Since the hybrid algorithm takes longer time for both encryption and decryption, it makes it more secure, since the higher the encryption processes the longer it will take for a hacker to break the encryption algorithm, since computing power is on the increase, speed will not be a problem in the nearest future and as such, in certain classified database, one cannot trade security with speed. This study will be useful in the protection of data stored in organizational databases. Data/information transmitted via insecure media will be received without interference or loss of data or information of any kind. It also reduces theft to its barest minimum. The hybrid security system will help individuals and organizations to protect their information from unauthorized user. Securing sensitive data from illegal access, theft and forging becomes a lesser challenge for different organizations, like security agencies, higher institutions and private sectors. This will make information stored or shared confidential. This study significant importance to Nigeria Police Force because it will forestall tampering of records but rather ensure its integrity.

Keywords: AES, EEA, Patients, Hospital

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 bar code technology). RFID technology can track the movement of objects through a network of radio-enabled scanning devices over a distance of several meters. The purpose of an RFID system is transmitting data from a portable device called a tag, to an RFID reader to execute a particular application based on the tag provided identification or location information (O' Brien, 2006). RFID technology has been in existence for decades and was originally developed for improving warfare technologies. The first application was developed by Britain as the Identify Friends or Foe (IFF) system, which was used to distinguish friendly aircraft from enemy aircraft during World War II (Landt, 2001). In the 21st century, with the development of RFID standards, decreasing prices and mandates from large organization such as Wal-Mart and the U.S. Department of Defense (DOD), RFID has become "the first important technology of the twenty first century" (Garfinkel& Rosenberg, 2005). Radio frequency Identification (RFID) is used in many applications such as in automation of automobiles, animal tracking, highway toll collection and supply-chain management (Garfinkel *et al*., 2005). Large organizations like Wal-Mart, Procter and Gamble, and the United States Department of Defense have deployed RFID as a tool for automation of their supply chains and in civil and mining operations for tracking of equipment (Jules et al., 2010). RFID technology is also used in infant management system. Furthermore, RFID security systems are deployed to locate wandering patients. (Saad & Ahmed, 2007; Atkins *et al*., 2010). RFID technology provides a quick, flexible and reliable way to electronically detect, track and control a different range of items. As well as these characteristics, the RFID has advantages which are not available with other identification technologies such as programmability and adaptation; it could achieve response times of less than 100*ms* even under harsh conditions (IIic & Notaros, 2010). The reduction in the cost of RFID and improvement in standardization is becoming widespread in business use and emerging as the successor of optical barcode. The main type of RFID tag is known as Electronic Product Code (EPC) tag which is standardized by an organization called EPC global Inc (EPC global, 2005). RFID is a technology to identify objects or people automatically. Security and privacy are very important in managing sensitive data and so, the stored data will be intelligible to only intended user thereby reducing the possibility of fraud. The retail industries will also derive benefits from this study because the protection and integrity of their database are assured.

STATEMENT OF THE PROBLEM

Data security is one of the main issues to be considered when the transmission is through wireless communication. The problems that necessitated this research are: eavesdropping, impersonation attack and the security of the back end database.

AIM AND OBJECTIVES OF THE STUDY

The aim of this project is to develop an Encryption Standard for RFID database. The objectives are to develop a system that can:

a. Provide a Hybrid encryption using Advanced Encryption Standard and Elgamal Encryption Algorithm to secure and validate the integrity of patients' database.
b. Provide a user-friendly, secured authentication and encryption to the users.

c. Evaluate the performance of the developed standard against other existing security algorithms to justify its development.

LITERATURE REVIEW

Reyes (2012) 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. Jhanwar and Barua (2009) came up with a hybrid public-key encryption scheme which is provably secure against adaptive chosen ciphertext attack. The scheme was constructed using Kurosawa-Desmedt paradigm. The security of the scheme is based on the Decisional Bilinear Diffe-Hellman problem. Wi (2010) designed a protocol for encryption of information on a web which makes it secure and hard to decrypt. This model used the substitution cipher in which each letter in the plaintext is replaced by some fixed number of position down the alphabet. This method is named after Julius Caesar who used this method to communicate with his generals. The result from this project is a data which is encrypted and decrypted to its readable form. Database encryption greatly affects database performance because each time a query runs, a large amount of data must be decrypted. Yang *et.al*, 2005 suggested that encrypting sensitive data only can provide the needed security without affecting the performance. According to Wicks (2006), 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. Page (2007), 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. Swedberg (2009) 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.

Dimitriou (2005) proposed a mutual authentication of both tags and the server. The general idea is that the server updates a tag's identifier if the tag proves its identity to the server and the tag updates its own identifier only when the server proves its validity to the tag. This protocol keeps both the server and the tag always in perfect synchronization. Though, this protocol protect against tag cloning, it is subject to tracking and denial-of-service attack. The response of the tag is static between two valid sessions and thus it makes the system susceptible to tracking and denial of service attack. In addition, if the server's response (that is, the server sends to the tag to prove its validity) does not reach the tag in a session, the tag becomes desynchronized with the server. John and Manimurugan (2012) in their research, focused mainly on the different kinds of encryption techniques that are existing, and framing all the techniques together as a literature survey. Their work includes extensive experimental study of implementations of various available encryption techniques. Also focused on image encryption techniques, information encryption techniques, double encryption and Chaos-based encryption techniques. Their study also extends to the performance parameters used in encryption processes and analyzing on their security issues. Mateescu and Vladescu (2013) came up with the hybrid approach of system security for small and medium enterprises by combining two different cryptography techniques which are Digital Signature algorithm and the RSA algorithm. Singh and Kaur (2015) in their research developed a hybrid approach for encrypting data on cloud to prevent DoS attacks. The new system was introduced to encrypt and decrypt the data before sending on cloud by using the two different techniques and was beneficial for simple data transfer and storing the data on a cloud. Agwara (2016) designed a hybrid encryption system that combines two symmetric encryption algorithms which were 3DES and AES together with hatching and salting techniques. The new hybrid system proved to be a more

secure system in keeping out attacks on information stored in the database. Nnabugwu (2018) designed a hybrid database encryption model that combines AES and RSA algorithms together with SHA512 and salting techniques. The new hybrid model provides integrity and authentication of the database.

METHODOLOGY ADOPTED

In this research, one proposed a solution to the existing system which consists in the implementation of a secure system based on Radio Frequency Identification wristbands with an RFID tag and mobile devices that allow for eliminating patient identification and rationalizing the use of time in patient care. The work involves substantial changes with respect to the traditional system. When patient identification is performed for the first time, an RFID wristband is assigned to him/her. Specifically, the NTAG21x ICs wristband, which follows the pattern set by the NFC Forum (association that regulates the NFC standards), is recommended here. This wristband will not be used to store any sensitive patient data. The only data stored on the wristband is an identifier assigned by the server. This identifier is generated through a process that will be discussed below. Such a generation takes into account the physical identifier of the wristband (similar to the Media Access Control (MAC) address number of computers) together with the patient record number. Note that this information will be written on the wristband in a completely secure way.

This wristband can be deployed both in the inpatient and emergency areas. It can be even assigned before the patient arrives to hospital, in the ambulance, where the identification and the writing procedures could be done through a mobile phone. The data stored in the wristband allow any member of the medical staff with the right permissions access to the patient record identifying the patient with the simple gesture of bringing a mobile device close to the wristband. The system prevents confusion when identifying patients and increases efficiency in the development of medical tasks. In addition, wristbands are fully recyclable, so when a patient leaves the hospital, its wristband is reset to be used by another patient. The system is designed to work with two separated servers, here referred to as the intermediate server and second server. On the other hand, the intermediate server manages access permissions to patients' data on the basis of medical staff shifts. On the other hand, the second server uses a Private Key Generator (PKG) to manage the information related to keys.

The use of two different physical servers is proposed to add a new security layer in the management of the keys. With this separation, different firewalls can be added to each server independently and different secure rules can be applied in the communications between them. Specifically, the limitation of the communication of the private key server to infra-communication (intranet communications) is advisable. In other words, the communication of the PKG with the extranet can be denied and just some interactions with the intermediate server can be allowed through, for example, an intranet. In this way, if the intermediate server is corrupted by an attacker, both the private key generator and the server keys should not be involved. Although having two servers is more expensive than having just one, we consider that this is a very low value when compared with the security that it brings to the proposed system. The protection of patients' data is a paramount objective in the healthcare environment. This is why security is one of the pillars of the described solution. In this work we applied a hybrid cryptographic encryption algorithm for protection of patient records.

The security of the communication between doctors and the intermediate server is based on an ElGamal encryption scheme that provides mutual authentication between doctors and the server through a PKG. Next, the details on how these security tools are used in the proposed framework are included. As aforementioned, when a patient arrives at a hospital, the first step

is the identification through his/her credentials. After that, an RFID wristband is assigned to him/her so that each patient is identified through an HMAC generated by the intermediate server by using the physical identifier of the wristband and the patient record number. If a patient does not have a medical record in the system, it is automatically created with some basic fields, such as name, age, state, etc. The system sends the physical identifier of the wristband to the intermediate server, and two 64-byte arrays denoted as ipad and opad are generated, where some default values are assigned to them during the initialization of the HMAC generation. New arrays denoted by ipadmsk and opadmsk are generated through a bit level exclusive OR operation on ipad and opad respectively, and the master secret key (msk). Then, with the physical identifier of the wristband Tag (idTag) and the Patient Record Number (PatRecN), the system uses a SHA3-512 hash function to generate the HMAC value. Firstly, the hash function is applied to the concatenation of ipadmsk, idTag and PatRecN. Secondly, the output of this hash function concatenated with the opadmsk is the input to another hash function so that the HMAC is the final result. This output is stored in the RFID wristband to be used as patient identifier. When trying to access a patient data, his/her RFID wristband must be read through a doctor's device, which sends the data obtained from the wristband, corresponding to the physical identifier of the wristband and the HMAC, to the server. The server verifies the authenticity of the bracelet and the doctor's access permissions. If the verification is positive, the authentication protocol described later is used each time a member of the medical staff needs to access to patients' data. Object-Oriented Analysis and Design Methodology (OOADM) will be used for the analysis and development of the credit card fraud detection system. PHP-MySQL and java programming language will used to implement the system. Confusion matrix was used to evaluate the performance of the system.

Justification of the Study

Today, as attack strategies which hackers use become more and more sophisticated, and the programs in which they attack become increasingly complex, which in turn increases the possibility that holes will be left open, encryption is becoming the last line of defense in database management system (DBMS) security. One might be thinking, what is the use of encryption in modern day database systems. That is, if the database administrator (DBA) has done his/her job (i.e. applying all the latest security patches, securing database information with least privilege access in mind, enforcing strong passwords, etc), then why do we need to add encryption on top of all that? The reason is that attackers can be clever and security patches are usually put out only after an attacker has exploited a new found weakness. Sometimes the database administrator overlooked some security weakness in their system; in order to secure such databases, care must be taken when implementing any cryptographic processes, especially when processing large amounts of data because encryption can incur considerable processing overhead. Moreover, one must consider the increased storage requirements, which are directly related to the cryptographic algorithm chosen, the size of the keys used, and the size of the unencrypted data (called plaintext or sometimes clear text). In this work, we used the Advanced Encryption Standard (AES) symmetric algorithm because of its speed and security since it is on record that AES encryption is very difficult to break and Elgamal encryption because of the challenges of data size and key length.

REQUIRED TOOLS AND AVAILABILITY

The computer system is divided into software and hardware. Both works together to achieve the desired goal in any application developed. In the web based security system developed, the following are required.

Hardware Requirement

Cryptographic algorithms are high performing secure engines that require considerable space in a design. When countermeasures are added to thwart security attacks, the space and memory requirements grow even more demanding. For these reasons, cryptographic algorithms have traditionally been embedded as proprietary designs in hardware on smart cards or 8 bit chips. Due to the speed required for a cryptographic process and the usage of large space of memory, the need to implement a high performance system becomes a major area of concern in actual implementation of the system. The following are the minimum hardware requirement for the system to be fully implemented in an organization

A Pentium M system with the following configurations

i. 2.4GHz of processor speed and above
ii. 80 gigabyte of hard disk
iii. 2 gigabyte of Ram and above
iv. 1024 * 768 screen resolution
v. Internet facility
vi. Printer
vii. Antenna, RFID Reader, Tag

Software Requirements

The following softwares are required for the application to be implemented in any system within an organization.

i.Microsoft SQL server 2005 express edition for storage of input data
ii.Microsoft.Net Framework 4.0 and above
iii.Window Installer
iv.Window Operating System (Client or Server)

PROGRAM DEVELOPMENT

Choice of Programming Environment

Visual web developer 2010 (VISUAL STUDIO 2010) was used as the web authoring tool because of its flexibility, bend ability and very easy deploying site. Microsoft SQL Server 2008 enterprise edition was used for designing the database that served as the back end for storing information because of its high maintenance and security tool. Visual Basic.Net was used as the Programming Language. VB.net is an elegant, flexible, simple, type safe, object oriented language that allows enterprise programmers to build a breadth of applications Vb.net also gives you the capability to build durable system level components by virtue of the following features:

a) Full COM/Platform support for existing code integration.
b) Robustness through garbage collection and type safety.
c) Security provided through intrinsic code trust mechanisms.
d) Full support of extensible metadata concepts.

The above reason was what motivated us to implement the system using the language.

Conclusion

The study provided useful protection of data stored in organizational databases. Data/information transmitted via insecure media received without interference or loss of data or information of any kind. It also reduces theft to its barest minimum. The hybrid security system help individuals and organizations to protect their information from unauthorized user. Securing sensitive data from illegal access, theft and forging becomes a lesser challenge for different organizations, like security agencies, higher institutions and private sectors. This make information stored or shared confidential. The study provided significant importance to Nigeria Police Force because reduce forestall tampering of records but rather ensure its integrity.

Acknowledgments
We would like to express our gratitude to the management of Imo State University, Owerri who has supported our research through TETFUND.

REFERENCES

Aissi, S., Al-Hamami, Alaa Hussein, Arabnia, Hamid, and Abuosba Khalil (2006). Proceedings of the 2006 International Conference on Security and Management, SAM'06: Foreword.

Alomair, B. &Poovendran, R. (2010). Privacy versus Scalability in Radio Frequency Identification Systems, *Computer Communication, Elsevier*, vol. 33, no. 18, pp. 2155–2163.

Atkins, A.S., Zhang, L., Yu, H., & Miao, W. (2009). Application of Intelligent Systems Using Knowledge Hub and RFID Technology in Healthcare Waste Management in UK and China International Conference in e-Business.

Banks, J., Hanny D., Pachano M.A. & Thompson L.G. (2007). RFID Applied, John Wily & Sons, Inc., Hoboken, New Jersey.

Burmester, M. & B. de Medeiros, (2007). RFID Security: Attacks, Countermeasures and Challenges, *Proceedings of 5th RFID Academic Convocation, the RFID Journal Conference.*

Deshpande, S. G.&Dahikar P.D., (2012). Strengthening of Data Security against its Attack, *International Journal of Advanced Networking and Applications3* (5) 29–35.

Dimitriou, T., (2005). A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks, Proceedings *of Conference on Security and Privacy for Emerging Areas in Communication Networks*.

Elminaam, D. S.A., Kader, H.M. A. & Hadhoud, M.M. (2010). Evaluating the performance of

symmetric encryption algorithms, *International Journal of Network Security*, *10* (3), 213- 219.

EPCglobal Inc. EPC^{TM} generation 1 tag data standards version 1.1 rev.1.27, 10 May 2005.

Garfinkel, S., Jules, A. &Pappu, R. (2005). RFID privacy: an overview of problems and Proposed solutions. *IEEE* Security and Privacy Magazine, 3(3): 34 – 43.

Garfinkel, S. & Rosenberg, B. (2005). RFID *Applications, Security, and Privacy*. Addison-Wesley.

Glover, B. & Bhatt, H. (2006). RFID Essentials. O'Reilly, Gravenstein Highway North, Sebastopol, CA, USA.

Jhanwar, M.P. &Barua R. (2009)., A Hybrid Public Key Encryption in Standard Model and A New Intractability Assumption, *Stat-Math Unit Indian Statistical Institute Kolkata, India*

Jignesh, R.P., Rajesh S. & Vikas K. (2012) Hybrid Security Algorithms for Data Transmission using AES-DES", International Journal of Applied Information Systems (IJAIS), *2*(2)

John, Justin M., Manimurugan, S., A survey on various Encryption Techniques. International Journal of Soft Computing and Engineering, Volume 2, Issue 1, March 2012.

Juels, A., Rivest, R.L. & Szudlo, M. (2010).*The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy.* In the 8th ACM Conference on Computer and Communications Security.

Kuppuswamy, P.& Al-khalidi, S. Q. Y. (2014). Hybrid Encryption / Decryption Technique Using New Public Key and Symmetric Key Algorithm, *Department of Management Information Systems, College of Commerce National Chengchi University & Airiti Press Inc.19*(2), 1–13.

Landau, S. (2004). Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard, *MathematicalAssociation of America Monthly* (February), 89–117.

Landt, J. (2001). Shrouds of time: The history of RFID, *An AIM Publication*, Pittsburg.

Mateescu, G., &Vladescu, M. (2013). A Hybrid Approach of System Security for Small and Medium Enterprises, *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems*, 656-662

Muhammad Iqbal, Andysah Putera Utama Siahaan, Riska Putri Sundari "Combination of

MD5 and ElGamal in Verifying File Authenticity and Improving Data security" International Journal for Innovative Research in MultiDisciplinary Field Volume 4, Issue 10, October 2018.

Nover, H. (2012). Algebraic cryptanalysis of AES: an overview, *International Conference & Workshop on Recent Trends in Technology*, 1–16.

O' Brien, D. (2006). RFID - Introduction and security considerations, *Presentation at the ISS World*, Washington, DC.

Okeke, S. (2014). The Study of the Application of Data Encryption Techniques in Cloud Storage to Ensure Stored Data Integrity and Availability, *International Journal of Scientific and Research Publications, 4*(10), 1-7.

Onyesolu, M.O. & Ogwara N.O., (2016). Information Security using a Hybrid Cryptographic Model, *International Research Journal ofComputer Science*, *11* (4), 15-22

Page, L. (2007). Hospital tune in the RFID. Materials Management in Health Care, 16 (15), 18-20.

Rabah, K. (2004). Data Security and Cryptographic Techniques-A Review, *Asian Network for Scientific Information Technology3*(1) 106-132.

Reyes, P.L. (2012), Accessing antecedents and outcomes of RFID Implementation in health care. International Journal of Production Economics, 136(1) 137-150.

Roussos, G. & V. Kostakos, (2009). RFID in Pervasive Computing: State-Of-The-Art and Outlook,*Pervasive and Mobile Computing*, vol. 5, pp. 110–131.

Saad, M.K. & Ahmed, S.V. (2007). Vulnerabilities of RFID Systems in Infant Abduction Protection and Patient Wander Prevention.

Singh, N., &Kaur, P. D. (2015). A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks. *International Journal of Database Theory & Application*, *8*(3), 145–153.

Song, B. & C. J. Mitchell, (2011). Scalable RFID Security Protocols Supporting Tag Ownership Transfer,*Computer Communication, Elsevier*, vol. 34, no. 4, pp. 556–566.

Sonia Rani, Harpreet Kaur "Implementation and Comparison of hybrid encryption model for network using AES and Elgamal "International Journal of Advanced Research in computer science Volume 8, No.3, March – April 2017.

Stallings, W. (2008). Cryptography and Network Security-Principles and Practices, Prentice Hall, Inc., 4th Ed.

Swedberg, C. (2009). Virtual health expects improved bed management from RFID. RFID Journal http://www.rfidjournal.com/article/view/7220.

Want, R. (2005). An Introduction to RFID Technology," IEEE Pervasive Computing, vol. 5.

Weis, S., S. Sarma, R. Rivest, & D. Engels, (2003). Security and Privacy Aspects of Low Cost Radio Frequency Identification Systems, (2003). *Proceedings of International Conference on Security in Pervasive Computing, Lecture Notes in Computer Science*, vol. 2802, pp. 454–469.

Wi, C. (2010). Implementation of hybrid Encryption Method using Caesar cipher algorithm, Unpublished master thesis, University Malaysia Pahang (UMP), Pahang, Malaysia.

Wiks, A.V. (2006). Radio frequency identification applications in hospital environments. Hospital Topics 84 (3), 3-8.

Yang, Z., Sesay, S., Chen Jingwen, and Xu Du (2005). A secure database encryption scheme. 49-53, 10.1109/ccnc.2005. 1405142.