IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 8, Issue.4, Apr 2020 E-ISSN: 2347-2693

Hybrid Encryption for Radio Frequency Identification in Healthcare System: Object-Oriented Analysis and Design Approach

Amanze, B.C[*1] ., Ononiwu, C. C[2] ., Eleberi, E.L[3] & Chilaka , U.L[4].

[1,3] Dept. of computer science, Faculty of Physical Sciences, Imo State University, Owerri, Nigeria
[2] Dept. of computer science, Faculty of Physical Sciences, Imo polytechnic, Umuagwo, Nigeria
[4]Dept. Computer science, Faculty of Physical Sciences, Federal Polytechnic, Nekede, Nigeria

DOI: https://doi.org/10.26438/ijcse/v8i4.4663 | Available online at: www.ijcseonline.org

Received: 13/Mar/2020, Accepted: 07/Apr/2020, Published: 30/Apr/2020

Abstract- 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. The aim of this study is to develop an Encryption Standard for RFID database. The objective is to develop a system that can: Provide a Hybrid encryption using Advanced Encryption Standard and Elgamal Encryption Algorithm to secure and validate the integrity of patients' database. The methodology adopted for this paper is the Object Oriented Analysis and Design methodology (OOADM). In this paper, five text files of different sizes were used to conduct four experiments, where a comparison of three algorithms Advanced Encryption Standard (AES), Elgamal Encryption algorithm and the new Chamberlin Hybrid Encryption Standard (CHES)was performed. Performance of encryption algorithm was evaluated considering the following parameters: encryption time, decryption time and size of encrypted file. Based on our analysis, the new hybrid encryption algorithm has a better performance with respect to the security of patients' records and the confidentiality of their records is high. The new algorithm will ensure integrity of medical records of patients against potential hackers. This thesis proposes 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. This 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. One recommend this work to Nigeria Police Force and higher institutions to enable them leverage on the digital technology to enhance security.

Keywords- RFID, AES, CHES, OOADM

I. INTRODUCTION

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message (Kuppuswamy & Al-Khalidi, 2014).

Hybridizing traditional method of Cryptography which includes symmetric and asymmetric, a new way of encrypting data will emerge which is more reliable and user friendly and difficult for breaking encryption (Deshpande & Dahikar, 2012). The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance. The hybrid cryptosystem is itself a public-key system, who's public and private keys are the same as in the key encapsulation scheme. In place of public key system we can use digital signature like message digesting function with symmetric key system to make hybrid crypto system. Note that for very long messages the bulk of the work in encryption/ decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value. For example, to encrypt a message addressed to user-1 in a hybrid technique user-2 does the following (Elminaam, *et.al.*, 2010; Gupta & Parvinder, 2013).

i. Obtains user-1 public key.
ii. Generates a fresh symmetric key.
iii. Encrypts the message using the symmetric key.
iv. Encrypt the symmetric key using user-1 public key. And send both of these encryptions to user-1.

To decrypt this hybrid cipher text, user-1 does the following:

i. User-1 uses the private key to decrypt the symmetric key.
ii. User-1 uses the symmetric key to decrypt the message.

II. REVIEW OF RELATED WORKS

Due to the important role that encryption techniques play in securing database systems, numerous algorithms have emerged with different techniques and performance. 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.

III. ANALYSIS OF THE EXISTING SYSTEM

In most current health systems, when a patient arrives at a hospital, the first step that the staff must do is to identify her/him. Patient identification is usually performed through the verification of a health identification card. Then, the patient is evaluated by a healthcare staff member who analyzes the information collected during admission and adds the results of new assessments if required. Afterwards, the patient may be seen by a specialist. Before each one of these actions, the process of patient identification must be repeated. This current system has several drawbacks. Doctors must check the patient record before assisting her/him. In order to do it, depending on the particular case, they can make such a consultation through printed documentation or by using a computer. If paper documentation is used, it is usually generated as a batch for a set of patients. For example, three medical records may be printed at a time so that a doctor can check and attend those three patients one after the other. Once they are attended, the doctor should leave the records and repeat the process with a new group of patients. This arrangement produces heterogeneous information because some data may be updated on computers while other data are kept in printed format. In addition, updates made by doctors are not changed in the central system in real time. In this approach, health workers have to deal with a lot of documentation, which leads to consuming considerable time and resources. On the other hand, each member of the medical staff has to visit several patients at each turn, which may generate wrong patient identifications, with serious consequences in some cases. However, security issues are important area of focus in every organization database. How to protect the security of an organization database and data is a major area of interest in this research work. There are many confidential data, classified information and medical records of patient in organization database, such as individual diagnosis medical reports of patients, medical records, government classified information, employee pay slip, user account, users password and so. These data are very important to the parties involved, so we must assure their security completely. From analysis gathered, Most Hospital that operate electronic system for keeping records of their patients records in the database stored all medical records in a plain text in the database of the hospital, such that a hack to such hospital database can expose patient medical records which are classified information. In this thesis, our major focus is on data security both in transmission and in storage.

Data Flow Diagram of the Existing System

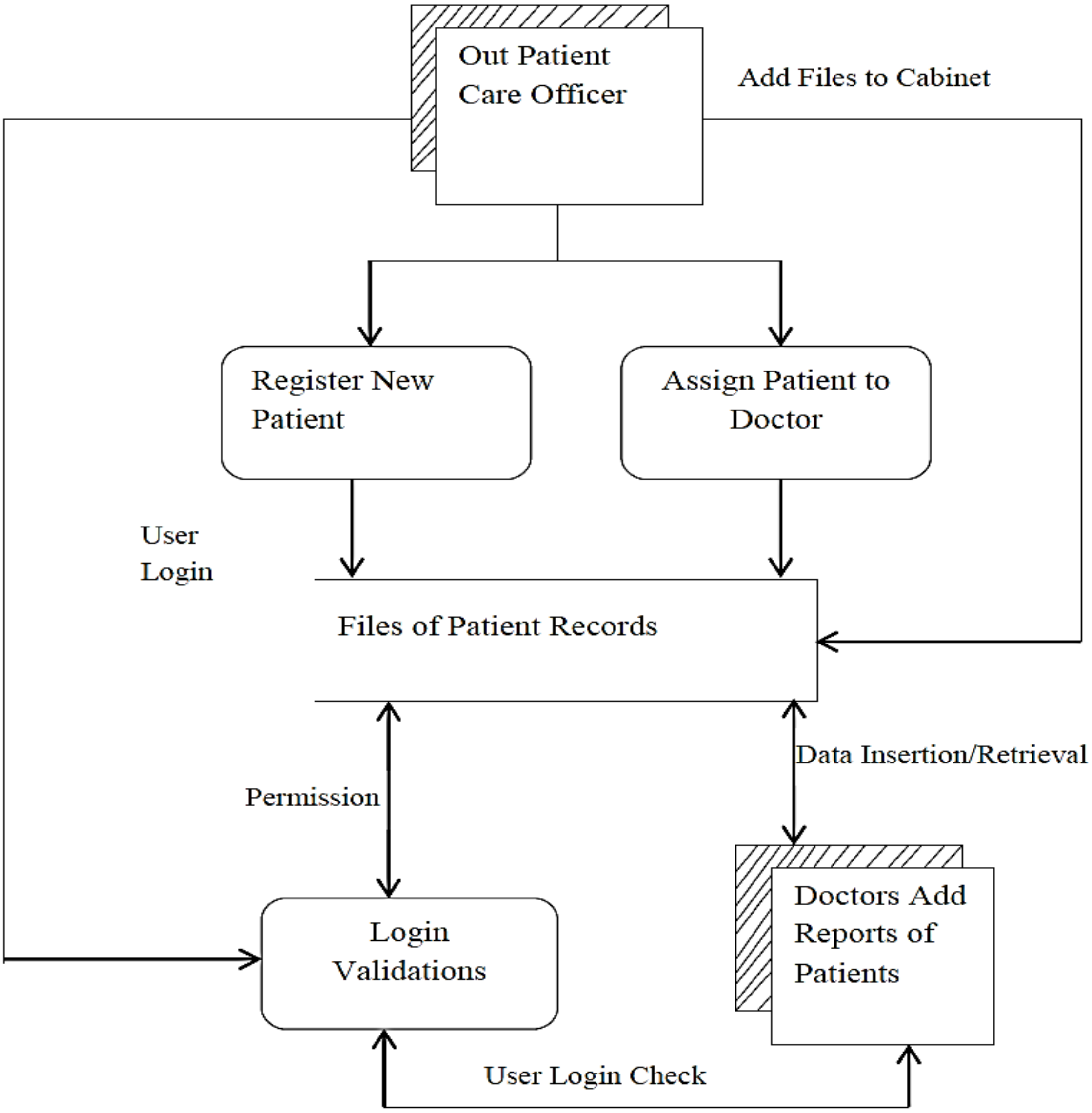

Figure 1 Data Flow Diagram of the Existing System

Advantages of the Existing System

a) It is easier for data management and direct querying using the database management system.
b) It is very fast during database operation such as insertion, update and retrieval of stored data.
c) It is very easy for the database administrator to manage data stored directly in case there were errors from the application point of view, the database administrator can easily update medical records at the back end without using the application itself.

Disadvantages of the Existing System

a) Potential danger to information resources

b) Weakness in application systems, network, business process or management procedures.
c) Medical Information can easily be compromise especially if an unauthorized users has a remote access to data stored in the database
d) Loss of Confidentiality and Integrity.

IV. ANALYSIS OF THE NEW SYSTEM

In this paper, one propose 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 misidentification 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 intra-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 generation of the HMAC can be seen in Figure 3.2. 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.

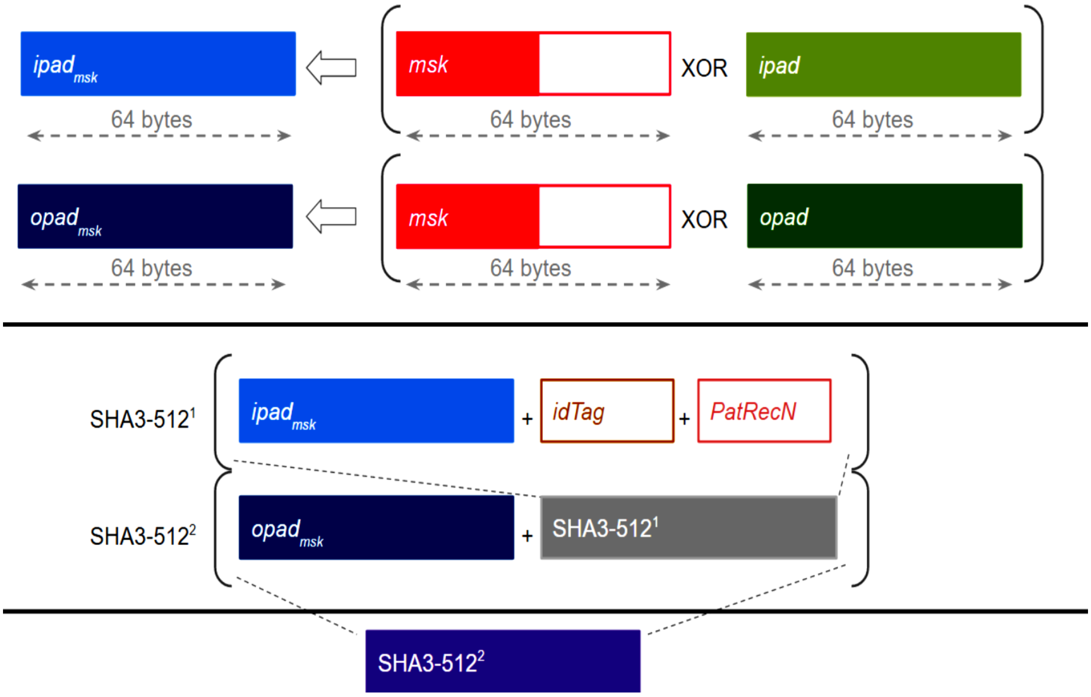

Figure 2 Keyed-hash message authentication code Generation

The protection of communications is achieved through an ID-based scheme. In this type of public key cryptography schemes, any text can act as a valid public key with a PKG. The main reason to choose this approach for the work is the simplification of management because in this way it is not necessary to define a public key infrastructure. Furthermore, an ID-based scheme was chosen because of its low computational complexity and its efficiency in terms of memory and usability. The description of all the steps of the communication flow during a medical record consultation between the participants in the system is included below:

1. A member of the hospital admission staff receives the basic patient's data.
2. This patient's information is sent to the intermediate server. The identification of the patient is analyzed at the server. If the patient is registered in the system, the server stores any new

information and the system sends the verification to the web application. Otherwise, the server generates new user identification and stores the corresponding data.

3. The assigning of a wristband to a patient starts with the reading of the physical identification of the tag idTag through an RFID reader.
4. The idTag is sent from the web application to the intermediate server, which links the idTag with the patient's medical record number PatRecN and sends these values to the PKG in the second server.
5. The PKG generates the HMAC value with idTag, PatRecN and the pre-calculated values ipadmsk and opadmsk. The HMAC value is sent to the intermediate server, which sends it to the web application.
6. The HMAC value is stored in the RFID tag of the patient's wristband.
7. When a doctor wants to identify a patient, he/she has to touch the RFID wristband with his/her mobile device to read both idTag and HMAC.
8. The stored values are sent from the mobile device to the intermediate server where the wristband is identified. The medical record is then loaded.
9. The intermediate server sends to the second server idTag, HMAC and PatRecN.
10. The PKG analyses and verifies the association, and the result of this verification is sent to the intermediate server.
11. If the HMAC verification is right, the server sends the medical record values to the mobile device where the doctor can read, edit or add data. The values corresponding to a patient can be modified until a new patient's wristband is read.

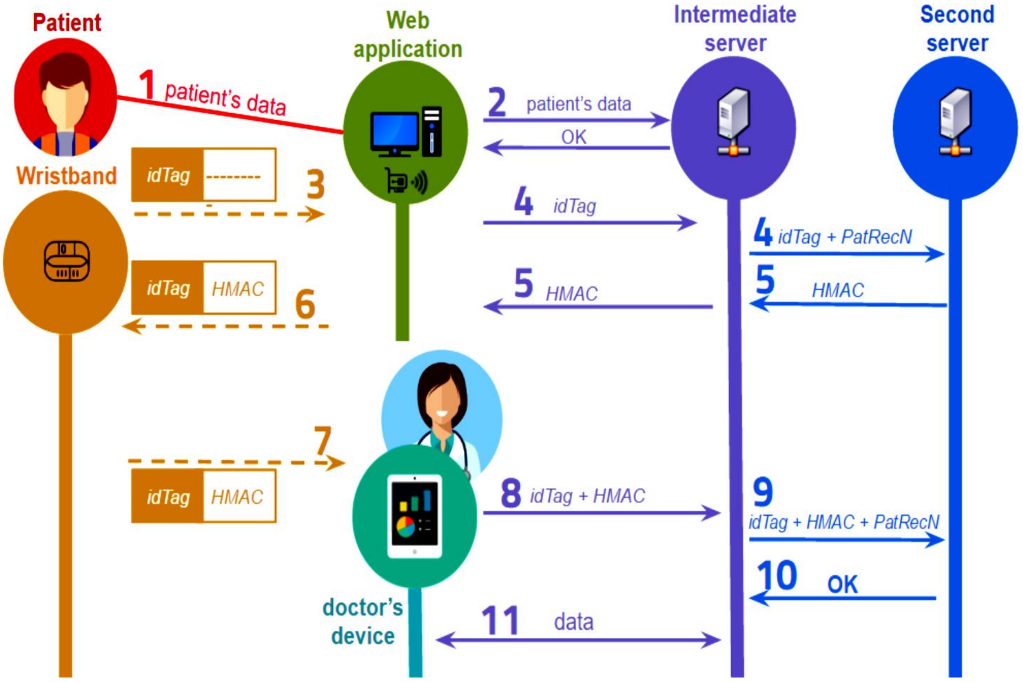

Figure.3 Medical record consultations

Communications between the mobile device of each member of the medical staff and the intermediate server are encrypted with an ID-based scheme. A crucial element of the work is the Private Key Generator in the second server because it is in charge of generating private keys for medical staff. The identifier used in the system for each member of the medical staff is the corresponding number of registered medical staff. Specifically, the system is adapted to a more secure infrastructure where the PKG and the intermediate server are separated.

As seen in Figure 3.4, on the one hand, there are different devices assigned to doctors, which are smartphones or tablets with RFID reader and Wi-Fi. On the other hand, each patient has an RFID wristband. The intermediate server is the controller of the communication between the medical staff and the PKG. In particular, the intermediate server has a public Application Programming Interface (API) for doctors' communication and other hospital computers and a private API for communication with the PKG. Finally, the PKG is in charge of the authentication and verification of each communication. This is why server keys are stored in the PKG. The protection of communications is achieved through an ID-based scheme. In this public key cryptography schemes, any text can be used as a valid public key. Specifically, the public key is usually extracted from some user's identity information, such as name, email or health identification.

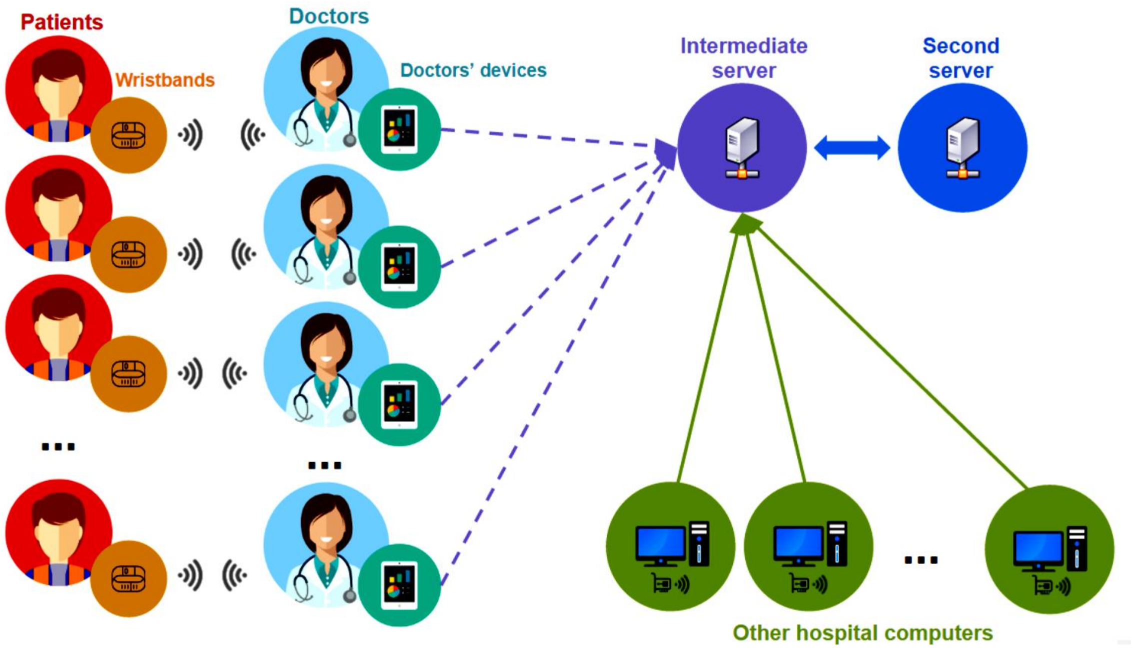

Figure.4 System's communication flow.

In the new system, mobile devices are used to manage patients' information. These devices have energy and computing capability limitations, so they should not depend on heavy cryptographic computations. Taking this into account, some protocols based on a client-server paradigm have been applied. One of the most used techniques to reduce the online cost is offline pre-computation. In the offline pre-computation used in this work, a few random values called ephemeral secrets are required to perform some operations in advance.

V. METHODOLOGY ADOPTED

The methodology adopted for this research work is the Object Oriented Analysis and Design methodology (OOAD). OOAD involves studying an existing system from the perspective of objects and similar objects are grouped as classes and their characteristics are handled as properties while their behaviors are treated as the actions or methods within the same bundle of object. This methodology was chosen because it is best used to handle a system where different objects exist. The methodology involves developers creating portions of the solution to demonstrate functionality and make needed refinements before developing the final solution. This technique can save considerable development time by reducing re-work as users see the product for the first time. It is an excellent way for the development team to confirm understanding of the requirements and ensure that the proposed solution is consistent with business expectations.

High Level Model of the New System

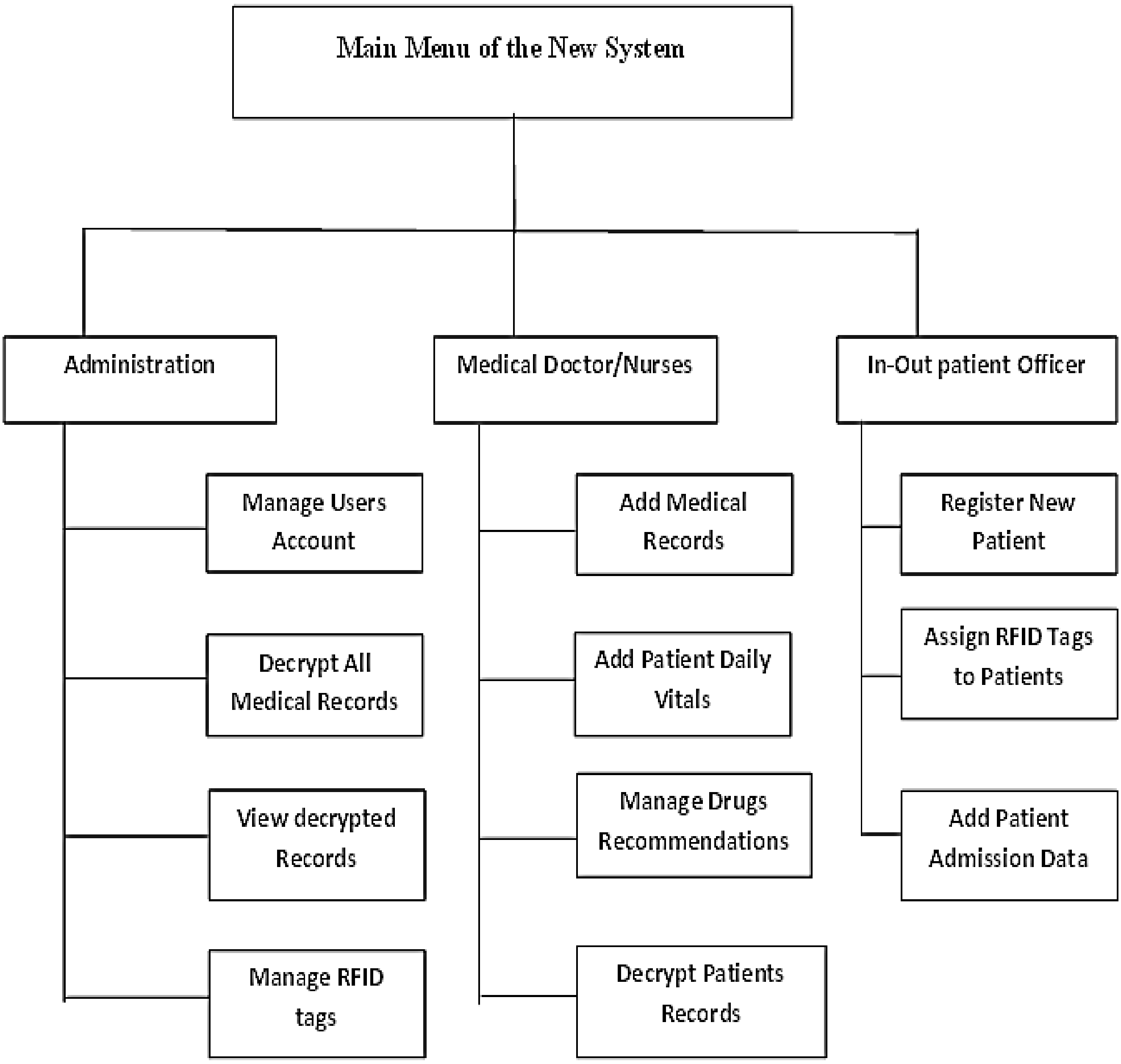

Figure.5 High Level Model of the New System

Overall Object Diagram of the New System

Diagram of the Hybrid Encryption Process

Figure 4.8 is a diagrammatic representation of the encryption. It shows the movement and conversion of data from plaintext to ciphertext.

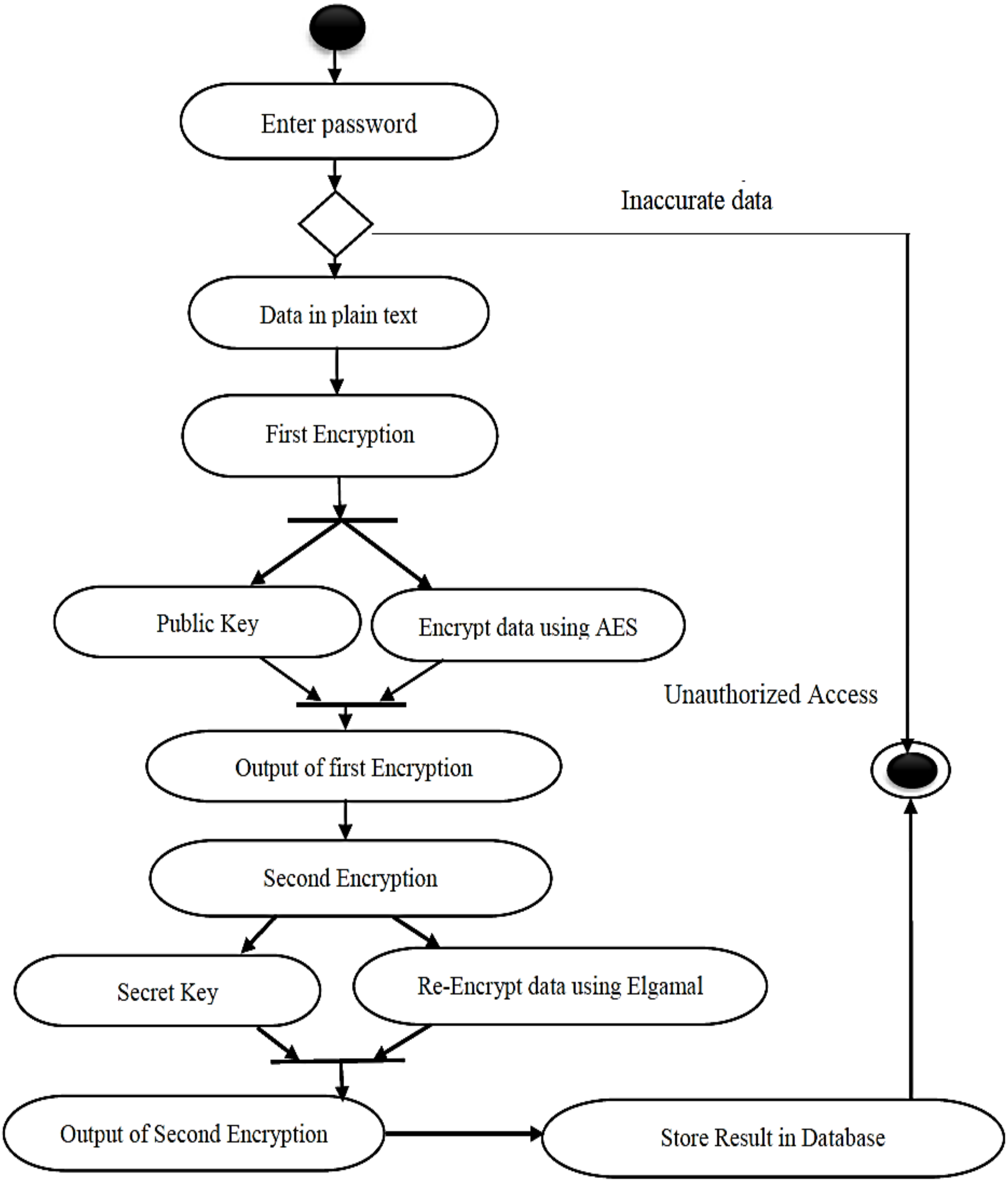

Figure .6 Hybrid Encryption Activity Diagram

Diagram of the Hybrid Decryption Process

Figure 4.9 is a diagrammatic representation of the various steps involved in the decryption of the encrypted records stored in the database.

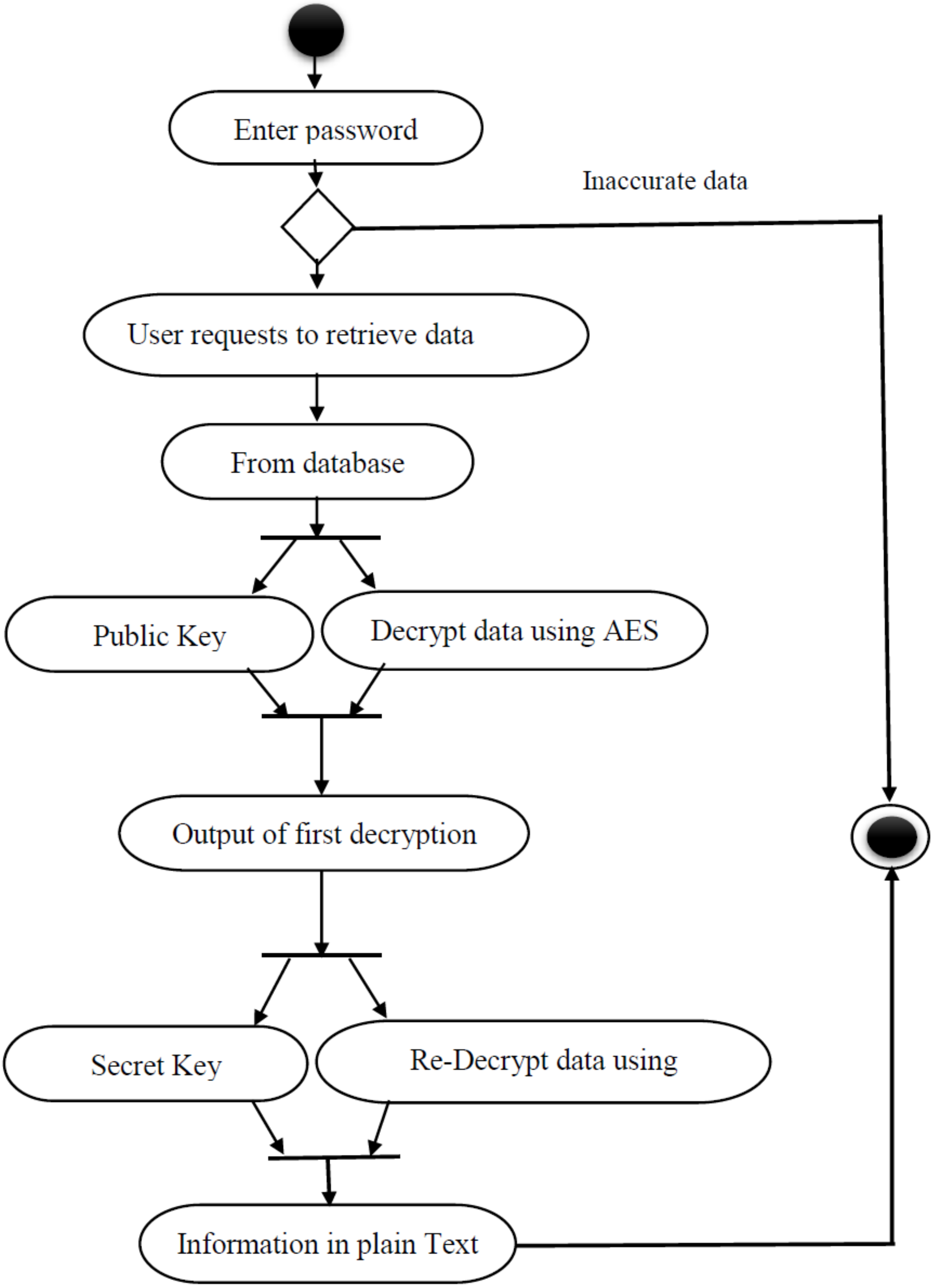

Figure .7 Hybrid Decryption Activity Diagram

Class Diagram of the Entire System

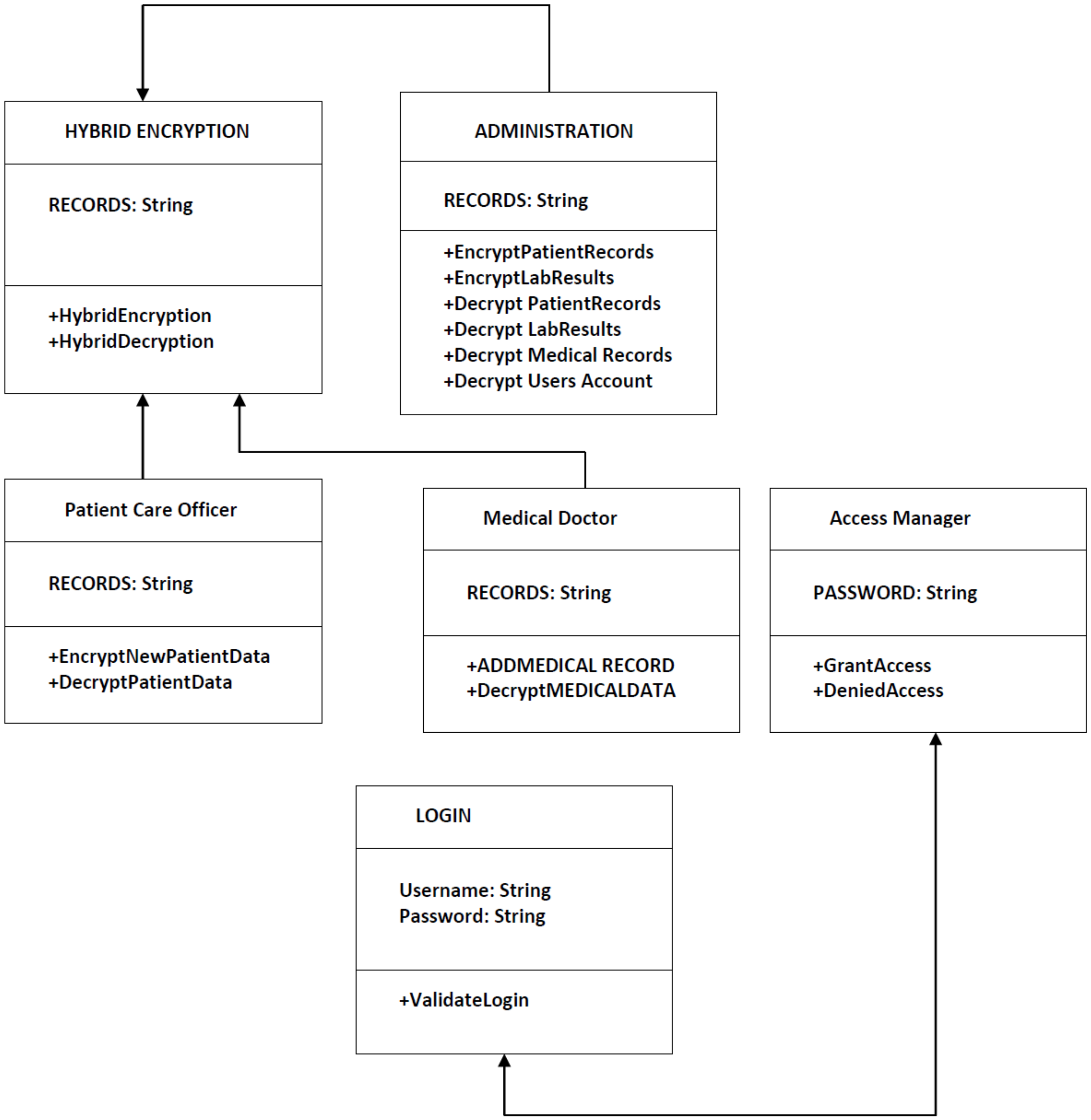

Figure .8 Overall Class Diagram of the Entire System

Sequence Diagram of the System

Figure 8 which can also be called event diagram describes the interactions among classess in terms of exchange of messages. It shows the flow of logic in the system and the sequential order of the flow

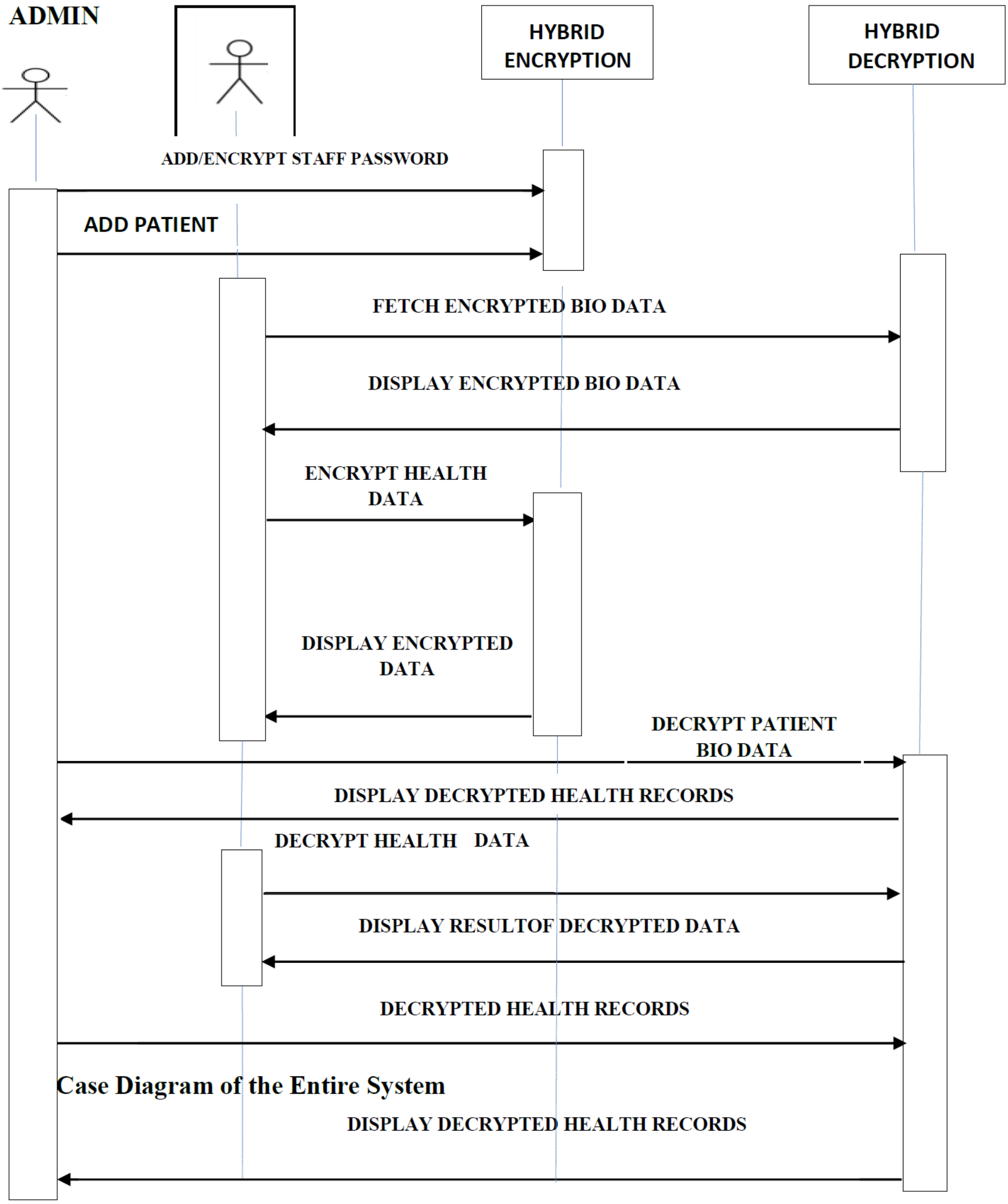

Figure .9 Sequence Diagram of the Entire System

Use Case Diagram of the Entire System

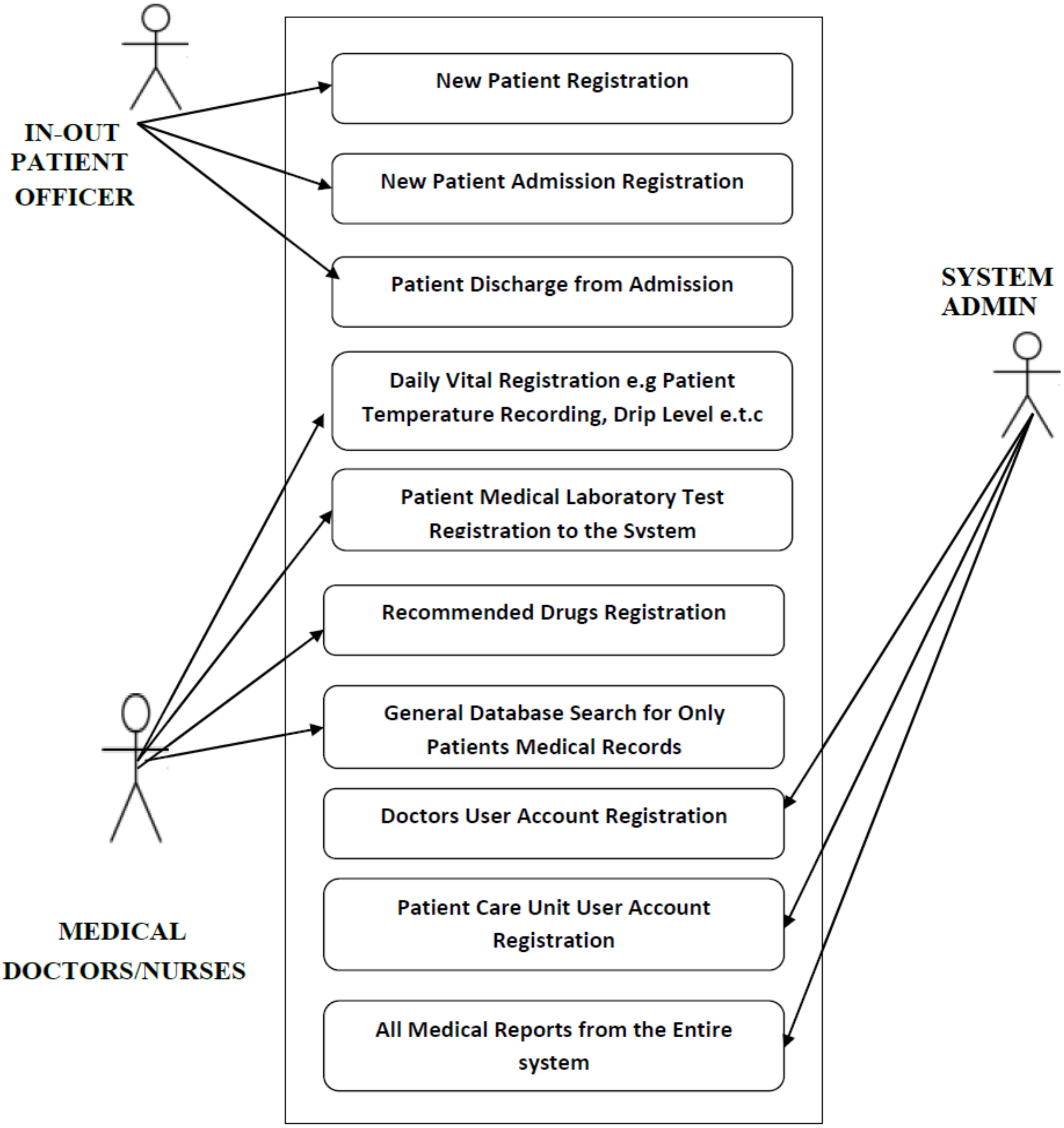
IN-OUT PATIENT OFFICER
New Patient Registration
New Patient Admission Registration
Patient Discharge from Admission
Daily Vital Registration e.g Patient Temperature Recording, Drip Level e.t.c
Patient Medical Laboratory Test Registration to the Svstem
Recommended Drugs Registration
General Database Search for Only Patients Medical Records
Doctors User Account Registration
Patient Care Unit User Account Registration
All Medical Reports from the Entire system
SYSTEM ADMIN
MEDICAL DOCTORS/NURSES

Figure .10 Use Case Diagram of the System

Algorithm

In this paper, several algorithms were used in the process of implementing a hybrid cryptographic system for database applications. The combination of the algorithms used gave rise to Chamberlyn Hybrid Encryption Standard.

Chamberlyn Hybrid Encryption Standard

State = X, Generate Random Keys k
1. Add RoundKey (State, Key k) [Initial Round, Add Round Key: each byte of the state is combined with a block of the round key using bitwise XOR]

```
2. For r = 1 to ($N_r$ - 1)
    a. Sub Bytes (State, S box) [Sub Bytes: a non linear substitution step where each byte is replaced with another according to a lookup table]
    b. Shift Rows (State) [a transposition step where the last three rows of the state are shifted cyclically a certain number of steps]
    c. MixColumns(State)  [MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.]
    d. Add RoundKey(State, Key r ) [Add Round Key]
    End

Final Round (no MixColumns)
1. SubBytes(State, S  box)
2. ShiftRows(State)
3. Add RoundKey(State, Key, Nr ) Y = State
```

Then Y is split into two 28 halves

4. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
5. The halves are recombined and subject to a compression permutation to reduce the key from. 56bits to 48 bits. This compressed keys used to encrypt this round’s plaintext block.
6. The rotated key halves from step 2 are used in next round.
7. The data block is split into two 32-bit halves.
8. One half is subject to an expansion permutation to increase its size to 48 bits. Output of step 7 is exclusive-OR’ed with the 48-itcompressed key from step 5.
9. Output of step 8 is fed into an S-box, which substitutes key bits and reduces the 48 bit block back down to 32-bits.
10. Output of step 9 is subject to a P-box to permute the bits.
11. The output from the P-box is exclusive-OR with other half of the data block. k. The two data halves are swapped and become the next round’s input.

Test Plan

In this paper, five text files of different sizes were used to conduct four experiments, where a comparison of three algorithms Advanced Encryption Standard (AES), Elgamal Encryption algorithm and the new Chamberlin Hybrid Encryption Standard (CHES)was performed. Performance of encryption algorithm was evaluated considering the following parameters: encryption time, decryption time and size of encrypted file.

4.10.2 Test Data

Table 4.10: show results of the encryption and decryption time for the following algorithm.

S/N	Algorithm	Packet Size (KB)	Encryption Time (Mill.Sec)	Decryption Time (Mill.Sec)	Data Size of Encrypted File(KB)
1	AES	150	15	18	199
	Elgamal		15	18	199
	HYBRID(CHES)		27	32	265
2	AES	299	28	35	397
	Elgamal		31	37	397
	HYBRID(CHES)		62	79	529
3	AES	448	35	49	529
	Elgamal		38	53	529

	HYBRID(CHES)		80	103	705
4	AES	597	54	70	793
	Elgamal		60	75	793
	HYBRID(CHES)		121	155	1058
5	AES	747	71	86	992
	Elgamal		85	88	992
	HYBRID(CHES)		148	192	1332

Actual Test Result versus Expected Test Result

Table 4.11 show details of Test Result against the Expected Result.

S/N	Algorithm	Packet Size (KB)	Encryption Time (Mill.Sec)		Decryption Time (Mill.Sec)		Data Size of Encrypted File(KB)	
			Actual	Expected	Actual	Expected	Actual	Expected
1	AES	150	15	17	18	20	199	201
	Elgamal		15	18	18	21	199	203
	HYBRID(CHES)		27	28	32	31	265	270
2	AES	299	28	29	35	36	397	400
	Elgamal		31	31	37	38	397	403
	HYBRID(CHES)		62	61	79	80	529	532
3	AES	448	35	37	49	51	529	534
	Elgamal		38	37	53	55	529	532
	HYBRID(CHES)		80	79	103	104	705	707
4	AES	597	54	55	70	72	793	799
	Elgamal		60	61	75	77	793	792
	HYBRID(CHES)		121	122	155	159	1058	1061
5	AES	747	71	72	86	89	992	994
	Elgamal		85	84	88	90	992	996
	HYBRID(CHES)		148	147	192	192	1332	1334

VI. CONCLUSION

Comprehensive review on RFID system was done. Research on subjects like radio frequency identification technology and standard, tags, readers' infrastructure and security issues has been done. In the proposed solution, the database was secured using chamberlyn hybrid encryption standard. The system is user friendly and interactive. Security enhancement was achieved with the new system. The software when deployed will assist health institutions to keep track of their patients' record easily. Therefore, one recommend it for use by higher institutions and Nigerian Police.

VII. RECOMMENDATIONS

RFID is very useful mainly in the warehouse management, distribution and retail outlet operations, goods shipment, goods receiving, and employee tracking. This research has shown that radio frequency identification can be applied in the hospitals and therefore, one recommend this work to Nigeria Police Force and higher institutions to enable them leverage on the digital technology to enhance security.

VIII. CONTRIBUTION TO KNOWLEDGE

This paper contributes immensely in improving the knowledge of the reader on:

a. Better ways of keeping track of patients' record in hospitals using RFID system
b. How to secure the database of RFID system using CHES based security.
c. The paper will serve as a reference point for people who may want to make further paper in this area.

REFERENCES

[1]. 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.

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

[3]. 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.

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

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

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

[7]. 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*.

[8]. 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.

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

[10]. Garfinkel, S., Jules, A. &Pappu, R. (2005). RFID privacy: an overview of problems and

[11]. Proposed solutions. *IEEE* Security and Privacy Magazine, 3(3): 34 – 43.

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

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

[14]. 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*

[15]. 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)

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

[17]. Juels, A., Rivest, R.L. & Szudlo, M. (2010).*The Blocker Tag: Selective Blocking of RFID*

[18]. *tags for Consumer Privacy*. In the 8th ACM Conference on Computer and Communications Security.

[19]. 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.

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

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

[22]. 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

[23]. 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.

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

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

[26]. 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.

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

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

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

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

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

[32]. Saad, M.K. & Ahmed, S.V. (2007). Vulnerabilities of RFID Systems in Infant Abduction

[33]. Protection and Patient Wander Prevention.

[34]. 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.

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

[36]. 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.

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

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

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

[40]. 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.

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

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

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