EMPIRICAL EVALUATION OF EFFICIENT ASYMMETRIC ENCRYPTION ALGORITHMS FOR THE PROTECTION OF ELECTRONIC MEDICAL RECORDS (EMR) ON WEB APPLICATION

Sunday Adeola Ajagbe[1*]
Research Scholar,
Computer Science Department
National Open University of Nigeria (NOUN), Abuja, Nigeria.
Correspondence email: *bright80@gmail.com
http://orcid.org/0000-0002-7010-5540

Ademola O. Adesina Ph.D[2]
Computer Science Department
Olabisi Onabanjo University (OOU), Ago-Iwoye, Nigeria.

John B. Oladosu Ph.D[3]
Computer Science and Engineering Department,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

ABSTRACT

The use of electronic medical record (EMR) system is gaining attention in the healthcare sectors around the world, and its acceptability threatened by the security of patients' information. Hence, the need to carry out study on efficient way(s) of protecting the information on EMR so that when even accessed it will remain incomprehensible except the approval is granted by the concern patient. The proposed solution for the protection of patients' information on electronic medical record EMR in this research was based on secondary data. Basically, one of the online database that were given particular attention was the software Open Medical System (OpenMRS). Experimental results obtained from three different asymmetric encryption algorithms show that Rivest-Shamir-Adleman (RSA) was the most efficient among the selected encryption algorithms based on the performance keys, and it was used to build an email notification system prototype for the protection of patients medical records. The set up implementation of a system prototype was carried out on EMR in this research was securely exchanged between local server and web server. It brings patients into decision making process on the management of their medical records by providing robust protection through email notification by informing the patient of any attempt to view/ access their medical records. It equally exonerates health care providers of any litigation that may arise as a result of access to their patients' medical records.

Keywords: Asymmetric Algorithms, Electronic Medical Records (EMR), Encryption, Paper-Base Medical Records, Protection, Web Application.

1. Introduction

The development in Information and Communication Technology (ICT) has made it possible to use electronic medical records (EMR) for more than record keeping but also to enable the storage, collection, sharing, and management of EMR among healthcare employees and other related healthcare institutions. The terms EMR and EHR sometimes cause confusion to some people. Although, an EMR contains the medical and clinical data gathered in one's provider's office, while an EHR includes more comprehensive patient information. Nevertheless, both are similar because they both do more than record keeping, and they are both products of health information system (HIS). It is also a means of reducing the workload and increasing the efficiency of health workers. There are other technologies employed in the health sector but EMR systems are recognized as one of the prime transformers of healthcare and a central element in Health Information Systems (Dzenowagis and Kernen, 2005).

The development and implementation of Electronic Medical Record (EMR) systems have been helpful in monitoring and facilitating the attainment of health-related aims and objectives. From a healthcare perspective, EMR systems improve the accuracy of patient care information recorded in health records, thereby enhance clinical decision-making, and improve accessibility of patients' healthcare information for continuity of care over space and time **(**Fitzpatrick and Ellingsen, 2013). From the administrative perspective, EMR systems also generate health care statistics, which are crucial in the management and planning of health services, thereby improving the quality of routine health data in health systems. From physicians' perspectives, the implementation and use of EMR have been reportedly beneficial in reducing waiting time of patients, reduced medication order errors, guide healthcare protocols and simplify generation of mandatory reports to higher authorities.

Information and Communication Technologies (ICT) are currently being implemented in healthcare settings and they are contributing immensely to the improvement of qualitative healthcare delivery. Although, these efforts have been concentrated on urban hospitals where criminal tendency is on the increase. Medical records, whether in paper or electronic form, serve multiple purposes within the healthcare sector. Their functions are to create basis for the historical record, support communication among providers, anticipate future health problems, record standard preventive measures, identify deviations from expected health trends, provide a legal record, and support medical research (Xiao-Ying and Peiying, 2016).

The adoption of traditional technique could be traced to the history of medicine which has many practical problems. The records may be inaccessible when in use by someone else or if misplaced; there may be missing data in the records due to oversight of the health worker; the data may be difficult to read (due to the poor handwriting of health workers); loss of medical record to inferno in case of fire outbreak. Moreover, the records increase in size over time and this may lead to loss of some sheets of papers; the effect of termite; space consumption in keeping number of files in shelf, if there is redundancy of data recording in different locations; and tedious process of data extraction for clinical research. One of the biggest and living examples of the shortcomings of paper-based records systems of patients' data was demonstrated by Hurricane Katrina (AL-nassar, Abdullah, Sheik and Osman, 2011). Hurricane Katrina destroyed the medical records of untold numbers of patients and bringing new attention to the need for electronic medical records EMR.

Medical diagnosis and record keeping are very important factors in the management of patients' health care. Patients' participation has also been identified as crucial to the management of their health, because patients' growing concern over the privacy and security of their personal and sensitive data stored on EMR has been a contributing factor to the slow adoption of this technology. The patient whose details of special illness like mental disorder, (psychiatric), HIV/AIDS, hepatitis got disclosed to third parties like employers, spouse or friends through EMR have experienced being sacked, divorced or stigmatized and eventually lost their life. Consequently, a relation to such victims would not be encouraged to be enrolled on EMR or ready to disclose the true state of his/her health because of the medical information of their relation that has been breached. Hence, the need to evaluate some way(s) to protect information on EMR, and consequently, the identification and use the best suitable encryption algorithm for protection of EMR on web application such that even if EMR of the patient(s) is illegally accessed, it will remain incomprehensible. The objectives of this study were to conduct empirical evaluation of the efficiency of asymmetric encryption algorithms for the protection of Electronic Medical Records EMR in web applications platform; and build a system prototype to notify the patient of an attempt to access his/her EMR database (through e-mail notification) with the aim of granting or denying access.

2. Literature Review

The history of medical record can be traced to the history of medical science. Medical records in those days used to be a paper-based but electronic medical records history is dated back around 1880s (AL-Nassar et al, 2011). A collection of a patients' medical information registered on paper sheets by health care providers is referred to as paper-based medical record. Paper-based medical record has been characterized by various degrees of limitations and short-comings, which include incomplete records, accessibility issues, illegible handwriting, fire outbreak, termites and storage capacity. In the comparisons of traditional paper-based medical records and electronic medical records EMRs, the quality and completeness of both records were analyzed. The uniqueness in these studies was the fact that same set of patients studied using traditional paper-based records were also studied using EMR system. The result showed potential advantages in quality and quantity from a procedural coding level when using an EMR if compared to a paper-based record for the same patient. Although, many hold the paper-based record as the gold standard, the study suggested the need to improve data capturing methodology (Stausberg et al, 2003).

Electronic Medical Records (EMR)

Electronic Medical Records (EMR) also has the ability to generate a complete patients' medical records all encounters as well as supporting other care related activities directly or indirectly; via interface, including quality management, evidence based decision support and outcomes reporting. Encryption-based electronic medical records (EMR) is less popular and that is why patients' privacy and security could still be violated, if patient controlled system, and encryption keys are not efficiently implemented and managed. EMR promises monolithic benefits if the mechanisms are tailored towards achieving privacy and security are not too cumbersome and can easily be managed by both the patient and healthcare provider without affecting the timeliness, clinician workflow and quality of healthcare service delivery (Hillestad et al., 2005; Omotosho and Emuoyibofarhe, 2014). Although, inside attacks are either continuously outnumbering or being the leading cause of external threats, most research still pays more attention to outsiders. The cost of privacy and security breaches is very high and difficult to recover for both the healthcare provider and patient (Appari and Johnson, 2010). For privacy reasons, patients at some point may be unwilling to disclose important information about their health status such as HIV and psychiatric behavior as their violation or disclosure may lead to social stigma, unfair treatment by employers, and at times irreversible damage to their social and professional reputation and sometimes leads to death (Omotosho and Emuoyibofarhe, 2014; Carroll, 2016).

Health Information Security

Technologies nowadays is emerging and dramatic transformation is shaping the world from isolated systems to ubiquitous Internet-enabled things. These things are capable of communicating with one another by sending data which contain valuable information.

However, this new world built on the basis of Internet, contains numerous challenges as regard to the security and the privacy of information. The rapid development of Internet-based computing allows numerous technologies to be developed and this equally calls for increasing demand for security of computer based information, because it is importance to ensure security and privacy in an emerging technological environment (Sahmim, and Gharsellaoui, 2017).

Health Information Security, (HIS) which also refers to security of electronic medical record, is a way of applying protection tools and measures of safeguarding health information on systems from any unauthorized person(s) to access or modify the information. This service has two components namely; Data security and System security. Data security covers measures to protect data and computed programs from undesired exposures and occurrences. On the other hand, system security involves protections associated with software, personnel, hardware and enterprise-wide institutional policies. Indeed, as healthcare organizations modernize and transfer their services to web-based applications, the information contained within them become more vulnerable for unauthorized access. If not properly secured, confidential information such as lab results, patient health data, treatment of life threatened diseases and billing information can fall into the hands of fraudsters and some unauthorized individual within that hospital premises or online. Therefore, security, confidentiality and protection of patient records must be upheld by securing user access to such critical details. (USAID, 2016).

Agbele, Februarie, Abidoye, Adesina, and Nyongesa, (2011) worked on how to ensure the security and privacy of information in mobile health-care communication systems. The work presented the sensitivity of health-care information and its accessibility via the Internet and mobile technology systems issue of concern in these modern times. The privacy, integrity and confidentiality of a patient's data are key factors to be considered in the transmission of medical information for use by authorized health-care providers. Mobile communication has enabled medical consultancy, drug administration, treatment, and the provision of laboratory results to take place outside the hospital. With the implementation of electronic patient records, medical information sharing amongst relevant health-care providers was made possible. However, the vital issue in this method of information sharing is security: the patients' privacy, as well as the confidentiality and integrity of the health-care information system, should not be compromised. Various ways of ensuring the security and privacy of a patient's electronic medical information in order to guarantee privacy and security of the information were examined. Although, encryption of algorithms was also considered, but the research was mobile based and not generic web-based and there was no significant role(s) for patient in the work (Agbele et al., 2011). Privacy and security are two important factors that must be considered when developing a patient centric EHR. Existing works have focused largely on security and less on how patient mastermind privacy control with the help of the healthcare providers (Omotosho, et al., 2017).

Encryption Algorithms

Encryption algorithms is the process of encoding or modifying a message to ensure that it becomes impossible to understand (incomprehensible) to anybody who cannot decode or know the key to unlock the message It is also referred to as cryptograph method. There are two distinct types of encryption or cryptography methods used for securing the information: Symmetric Encryption and Asymmetric Encryption (or Cryptograph Key). Figure 1 is the revised format of encryption and decryption principle.

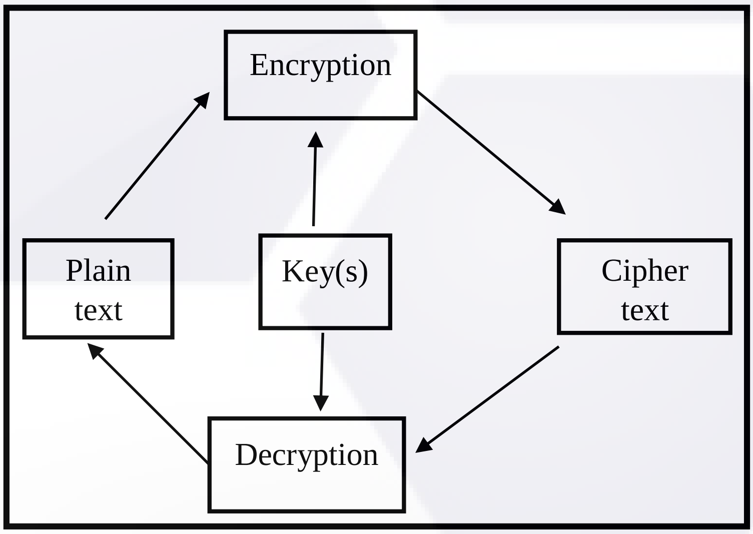


Figure 1: Encryption and Decryption System Principle

Source: Ajagbe 2019 (unpublished)

Asymmetric Encryption Algorithms

Asymmetric encryption algorithms (public key algorithms) uses different keys for encryption and decryption. Although, some schools of thought believe that the decryption key cannot be derived from the encryption key, and its implementation is based on digital certificate, but in actual sense, the decryption key can be generated from the encryption keys by extracting the decryption keys from the encryption keys using some software tool like Open Secure Socker Layer's (OpenSSL). One of the problems with private keys is exchanging them over the internet while preventing them from theft. Anyone who knows the secret key can decrypt the message. To overcome this, we have asymmetric encryption techniques, in which there is related pair of keys. (Shetty, Shetty and Krithika, 2014).

A public key is available to anyone who might want to send or receive message. A second, private key is kept secret by the owner only. This means that there is no need to worry about passing public keys over the internet. A problem with asymmetric encryption, is that it is slower than symmetric encryption. It also requires more processing power (battery) to both encrypt and decrypt the content of the message. In it, instead of a single key, every person has a pair of keys. One key, called the public key is known to everyone and the other one, the private key is known only to the owner. There is a mathematical relationship between these keys. Thus, if any message _m'is encrypted using any of the keys, it can be decrypted by the other key. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented (Bala, and kumar, 2015). Asymmetric algorithms are incredibly slow when compared with symmetric algorithms and it is impractical to use them to encrypt large amounts of data (RSA for instance). The main advantage of asymmetric encryption algorithm is the ability to transmit encryption keys or other data securely even when the parties disagree on a secret key in private. Most of these asymmetric encryption algorithms use different Hash Functions to compute messages. Figure 2 is the simplified version of asymmetric encryption principle

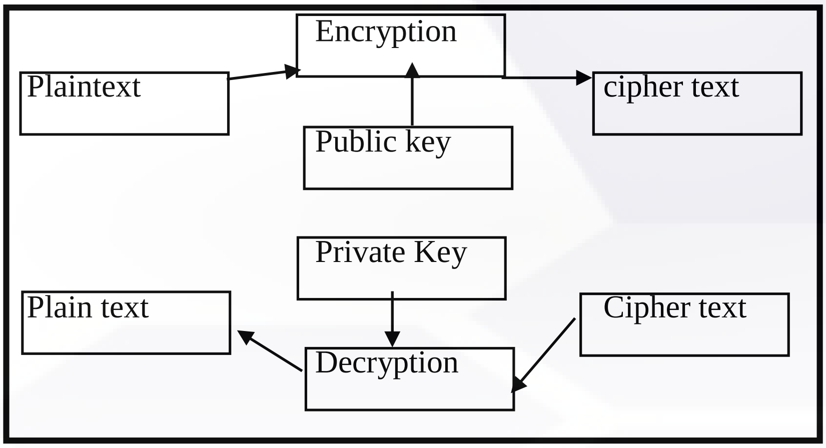


Figure 2: Asymmetric encryption principle

Source: Researchers

Digital Signature Algorithm

The National Institute of Standards and Technology (NIST) in August 1991, proposed the Digital Signature Algorithm (DSA) to United States Federal Government or FIPS for digital signatures for use in their Digital Signature Algorithm (DSA), specified in FIPS 186 adopted in 1993. A minor revision was issued in 1996 as FIPS 186-1 (Aayush, and Rekha, 2013) and the standard was further expanded in 2000 as FIPS 186-2. Digital Signature Algorithm (DSA) is similar to the one used by ElGamal signature algorithm. It is fairly efficient though not as efficient as RSA when consider for signature verification. The standard defines DSS to use the Secure Hash Algorithm (SHA-1) hash function exclusively to compute message digests. The main problem with DSA is the fixed subgroup size (the order of the generator element), which limits the security to around only 80 bits. DSA/DSS has limitation on hardware component because of the attacks can be menace to some implementations of DSA/DSS especially in electronic medical records environment. However, it is widely used and accepted as a good encryption algorithm. (Garfinkel and Spafford, 2002; Abood, and Guirguis, 2018).

Elliptic-Curve Cryptography

Elliptic-Curve Cryptography (ECC) is one of the public-key cryptography approach, it is based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for digital signatures, key agreement, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization. Public-key cryptography is based on the dintractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible: this is the "elliptic curve discrete logarithm problem" (ECDLP). The security of elliptic curve cryptography depends on the ability to compute a point multiplication and the inability to compute the multiplication given the original and product points. The size of the elliptic curve determines the difficulty of the problem (Garfinkel, and Spafford, 2002).

The major advantage of elliptic curve cryptography (ECC) includes its ability to use smaller key size for encryption, reducing storage and transmission requirements, i.e. an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key. The National Institute of Standards and Technology (NIST) of U. S. has endorsed and recommended elliptic curve cryptography in its operations, specifically Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature and Elliptic Curve Diffie–Hellman (ECDH) for key exchange. National Security Agency (NSA) of U. S. allows the use for protecting information classified up to top secret with 384-bit keys. Although, some argue that the US government elliptic curve digital signature standard (ECDSA; NIST FIPS 186-3) and certain practical ECC-based key exchange schemes (including ECDH) can be implemented without infringing them, including RSA Laboratories. (Bernstein, Lange, and Schwabe, 2012; Anton and Eliasson, 2017; Hanna and Sababa, 2018).

Rivest-Shamir-Adleman (RSA)

In 1978, Rivest-Shamir-Adleman (RSA) was designed, and it was named after the trio Ron Rivest, Adi Shamir and Leonard Adleman. This encryption algorithm uses a pair of keys, it is a public-key encryption algorithm and the standard for encrypting data sent over the internet. Like IDEA, RSA is also one of the methods used in our Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG) in relationship with security in Ubuntu and Launchpad programs. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break. This encryption algorithm has the advantage of being one of the most widely studied and used encryption algorithm method, and it is simple, well-tested and extremely elegant encryption technique (Singh and Supriya 2013; Abood, and Guirguis, 2018).

RSA is used as a baseline for the comparison of other encryption methods, it can be used both for encryption and for digital signatures. However, it is not as processing efficient or storage efficient as other encryption algorithms studied and requires the use of longer key lengths for equivalent security. At present, commonly used RSA key lengths include 1024 and 2048 bits. The basic principle of RSA security rests on the theory but poor implementation of tools that rely on protocol that is extremely difficult to factor the product of two large prime numbers into its constituent factors. Each individual in the RSA network must create two complimentary keys, commonly referred to as a public key and a private key, with each key able to decrypt messages enciphered using its compliment (Garfinkel, and Spafford, 2002; Singh, and Supriya, 2013). Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identify service provider. (Singh, Rashmi and Kumar, 2012).

Encryption on Web Platform

Private key should never be distributed since the private key assures that only the intended recipient can unscramble (decrypt) data intended for it. The recipient can freely distribute the public key without worrying since it is only used to scramble the data. It is included as part of the web browsers from Microsoft and Netscape. It is also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed web, Internet, and computing standards. RSA security depends on the difficulty of factoring the large integers. It is generally considered to be secure when sufficiently long keys are used (512 bits is insecure, 768 bits is moderately secure and 1024 bits is good, for now) (Bala, and kumar, 2015). The Mercury Mail package in xampp for windows is a great way to start sending emails from open EMR or any open source CMS program placed in xampp. Mercury Mail in openEMR has some benefits which include but not limited to: a). Easy to setup and integrated with xampp package b). The patient reminder mails (alert reminders) will be sent automatically c). Appointment reminders will be sent automatically using Batchcom/Automatic_notification via cronjob d). Secure.

3. Methodology

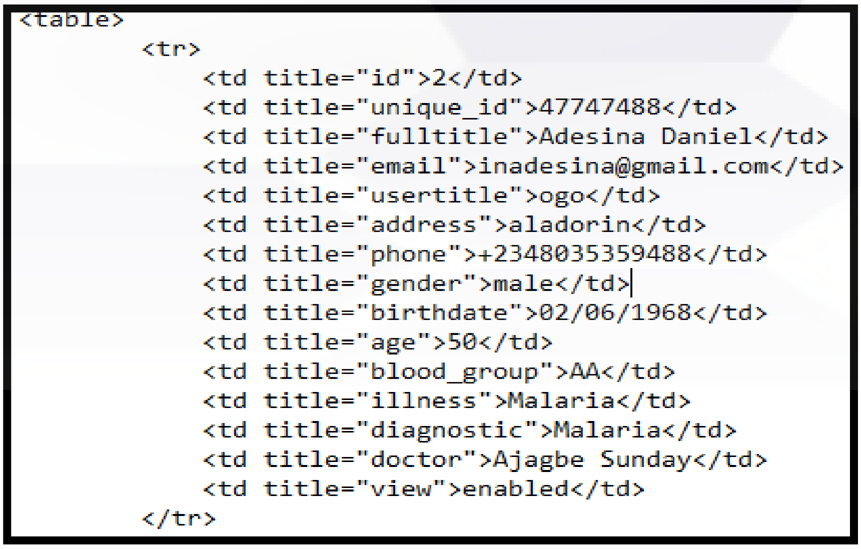
The review on confidentiality, privacy and security issues in healthcare delivery in this research was based on secondary sources. The information obtained from agencies/industry reports, conference papers, journals, and books were summarized in design and implementation of algorithm that will ensure confidentiality, privacy and security of patients' healthcare records on web-based application. Basically, one of the online databases that were given particular attention was the software open Medical record system (OpenMRS). The OpenMRS community is a worldwide network of volunteers from different backgrounds including technology, healthcare, and international development, working together to build the most flexible technology and world's largest platform to support healthcare delivery in some of the most challenging environments on the planet.

System Design

This section presents how the two distinct objectives in this research were addressed. The overall objective of this research is to ensure security of electronic medical record (EMR) system on web platform using efficient asymmetric encryption algorithms which is one of the most effective methods to secure patients' medical record from been attacked or accessed by both outsider and insider respectively. The specific objectives are: empirical evaluation of the asymmetric encryption algorithms in terms of processing time, memory, processor and battery consumptions, in order to determine the most suitable one for EMR on web platform context; and second objective focused on building a system prototype to notify the patient of an attempt to access his/her medical records on EMR database (through e-mail notification; The mail notification of the system prototype was developed using the Mercury Mail Configuration in Windows and xampp local server) in a more secure way, in which the patient may wish to give allow or deny access.

Source and Processing of Experimental Data

The anonymized data set of electronic medical records (EMR) available at https://wiki.openmrs.org/display/RES/Demo+Data was used. This is one of the most popular online open source medical records systems database. The data include electronic medical records of patients with their observations, demographics, vital sign, past medical history, progress notes, laboratory data, radiology reports, medications etc. The EMR automates and streamlines the clinicians' work flow. (Agbele et al., 2010). The EMR downloaded fromhttps://wiki.openmrs.org/display/RES/Demo+Data was pre-processed in HTML format and other necessary information which include unique id, full name, email, username, password, address, phone, gender, birthdate, age, blood group, illness, diagnostic and doctor were included to suit the research environment. Camargo et al (2015) also used the same database and was pre-processed to build patients medical record in XML for mobile platform. The figure 1 shows the sample of preprocessed data in database model of this research



```
<table>
        <tr>
            <td title="id">2</td>
            <td title="unique_id">47747488</td>
            <td title="fulltitle">Adesina Daniel</td>
            <td title="email">inadesina@gmail.com</td>
            <td title="usertitle">ogo</td>
            <td title="address">aladorin</td>
            <td title="phone">+2348035359488</td>
            <td title="gender">male</td>
            <td title="birthdate">02/06/1968</td>
            <td title="age">50</td>
            <td title="blood_group">AA</td>
            <td title="illness">Malaria</td>
            <td title="diagnostic">Malaria</td>
            <td title="doctor">Ajagbe Sunday</td>
            <td title="view">enabled</td>
        </tr>
```

Figure 3: An HTML example of electronic medical records
Source: Ajagbe 2019 (unpublished)

Specification of the Execution Environment

This research was conducted using the following specification experimental environment;

Hardware and Software

Intel Core 2 Duo Processor, 320GB Hard Drive, 3GB RAM on Packard bell machine, Operating system -Windows 10, Xampp, Apache Web server, Mysql database, PHP (Hypertext Preprocessor) programming language, HTML (Hypertext markup language), CSS (Cascading Stylesheet), Javascript.

Procedure for Asymmetric Encryption Algorithms

Procedure for asymmetric encryption algorithms was as follows;

i. Start
ii. Configure the encryption environment with the asymmetric encryptio algorithms (DSA, ECC, and RSA)
iii. Generate both the private and public key
iv. Save the private key to a file for reuse
v. Encrypt the patient's record with the public key.
vi. Save the patient record to the database
vii. Stop

Figure 4a: Procedure for Asymmetric Encryption Algorithms

Source: Researchers

Procedure for asymmetric decryption algorithms

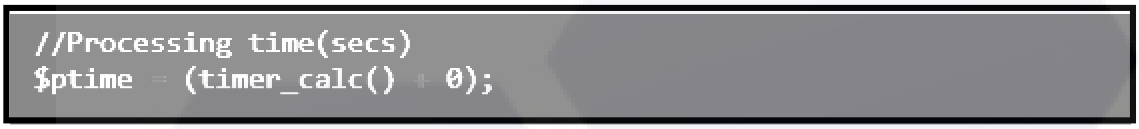
Procedure for asymmetric decryption algorithms was as follows;

i. Start
ii. Fetch the encrypted patient's record from the database
iii. Ask for record access permission from the patient
iv. Retrieve the private key from a file
v. Validate that the public key matches the private key.
vi. Decrypt the patient's record using the private key
vii. Send decrypted data back to the doctor
viii. Stop

Figure 4b: Procedure for asymmetric decryption algorithms

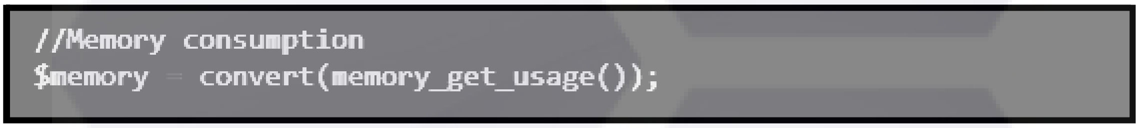
Source: Researchers

The research methodologies highlighted in Figure 4a and b were used for each asymmetric encryption decryption methods respectively. Encryption algorithms were evaluated using the following performance metrics; a). processing time, b). computing memory, and c). battery usage/ consumption. Pseudo code for the metric keys were show in the Figure 5a-c, it makes use of an external PHP library and file to aid their performance and optimum results of the metric keys.



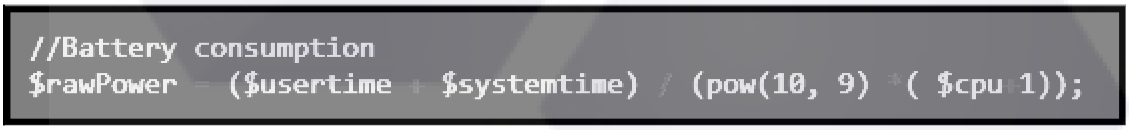
```
//Processing time(secs)
$ptime = (timer_calc() + 0);
```

Figure 5a: Processing time pseudo code
Source: Researchers



```
//Memory consumption
$memory = convert(memory_get_usage());
```

Figure 5b: Memory consumption pseudo code
Source: Researchers



```
//Battery consumption
$rawPower = ($usertime + $systemtime) / (pow(10, 9) *( $cpu+1));
```

Figure 5c: Battery consumption pseudo code
Source: Researchers

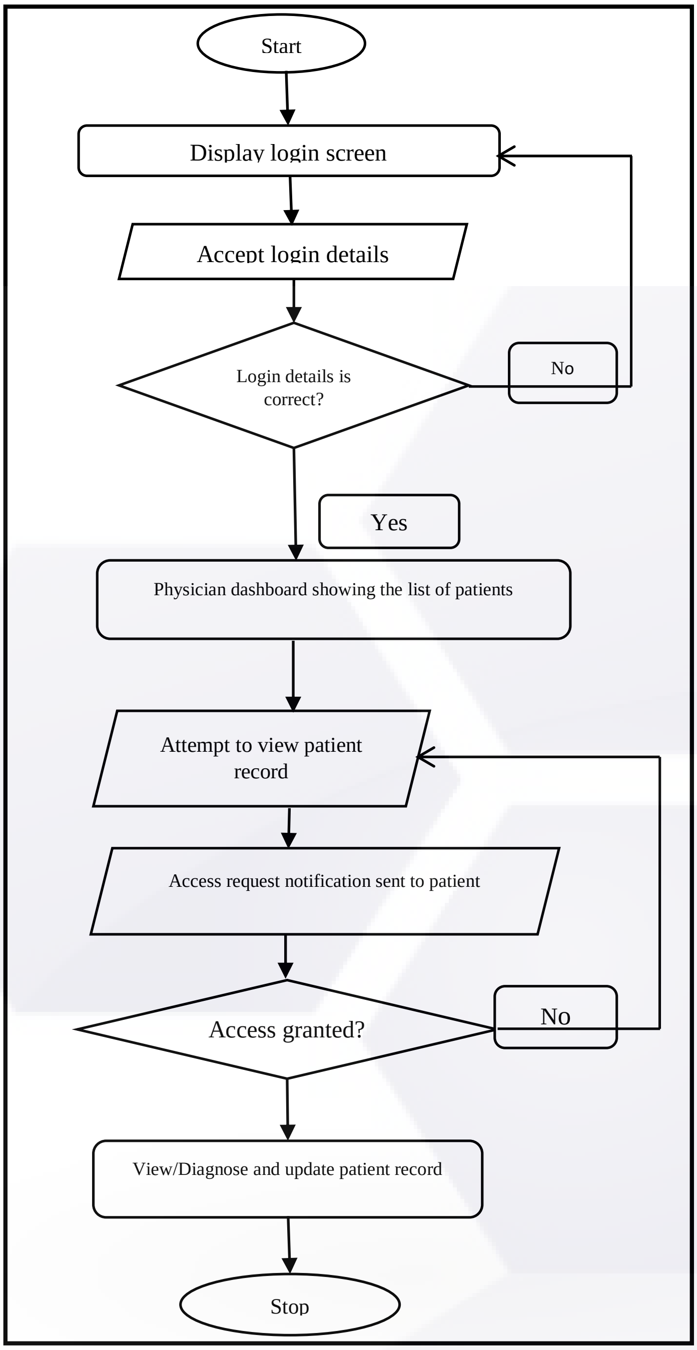

Start
Display login screen
Accept login details
Login details is correct?
No
Yes
Physician dashboard showing the list of patients
Attempt to view patient record
Access request notification sent to patient
Access granted?
No
View/Diagnose and update patient record
Stop

Figure 6a: Physician flowchart

Source: Researchers

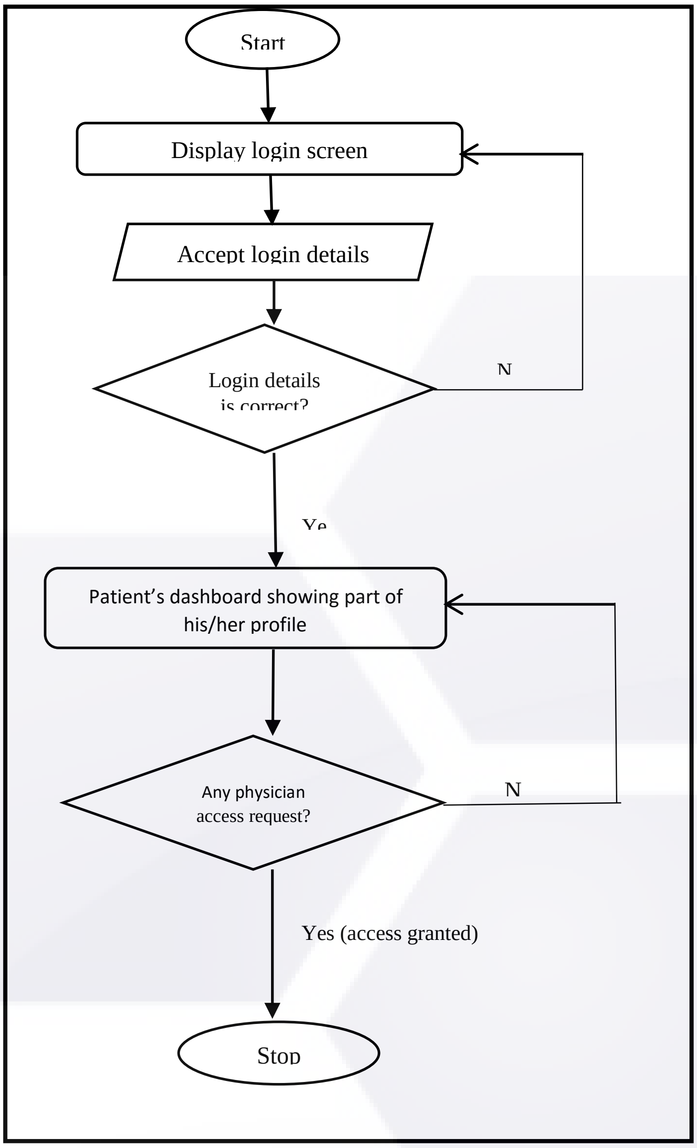

Start
Display login screen
Accept login details
Login details is correct?
N
Ye
Patient's dashboard showing part of his/her profile
Any physician access request?
N
Yes (access granted)
Stop

Figure 6b: Patient's flowchart

Source: Researchers

Figures 6a and b represent the flow chart of the system prototype from the beginning to the end of the process. Whenever a user is logged in, the system has different dashboard for the physician, likewise the patient. If the user is a physician, he/she will be redirected to the dashboard to access patients' list. When the physician attempts to access a particular patient's record, an email notification will then be sent to patient's email address for record access permission. When the patient checks the link in the email notification, the patient can then grant or decline access to patient’s information. The system ensures security of patient information on electronic medical record.

4. Results Analysis and Discussion

This section presents the obtained experimental results for each of the defined performance metrics and some details of email notification system prototype to ensure security of patients’ medical records. Three different asymmetric encryption algorithms were carefully selected for evaluation based on the reviewed works. Namely, Digital Signature Algorithms (DSA), Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). The efficiency was measured in terms of performance keys proposed by Camargo et al. (2015); Bala and Kumar (2015). The next section describes the performances and results of each of the encryption algorithms selected.

Performance Evaluation

These performance measures were calculated, increasing by 500 the number of electronic medical records (EMR) starting in 500 and ending in 5,000. For each performance measured a plot was generated including the seven selected algorithms and the combined one. Efficiency of each encryption algorithms were evaluated based on the following performance keys. For each performance metrics processing time, computing memory, and battery usage/ consumption. A plot was generated including the seven selected encryption algorithms.

Processing Time (Second)

Processing time is the time taken by the computer (in seconds) to encrypt a set of electronic medical records using each encryption algorithm methods. This can also be referred to as the execution time. The table 1 shows the experimental results of the research.

Table 1: Processing Time (Sec)

EMR	DSA	ECC	RSA
500	5.51	8.479	5.487
1000	5.432	6.845	9.028
1500	6.025	9.919	4.375
2000	6.504	10.38	10.458
2500	7.406	7.478	14.478
3000	8.24	9.113	6.546
3500	8.844	7.001	7.044
4000	9.5	7.727	3.664
4500	10.137	10.782	4.952
5000	10.617	7.372	6.529
Total	**78.215**	**85.096**	**72.561**

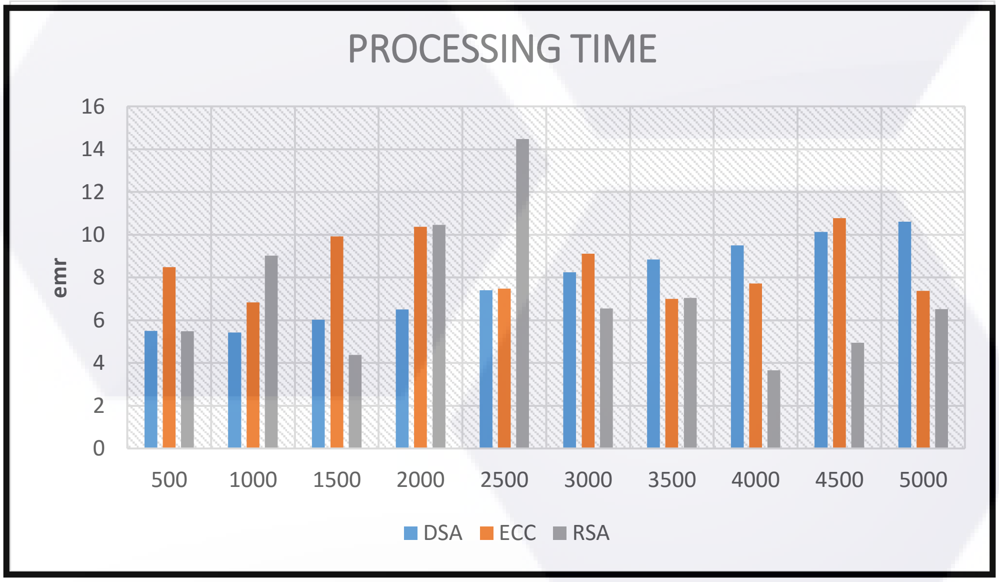


Figure 7: Processing Time (Sec)

Memory Consumption (MB)

The computing memory or main memory is one of the computer resources consumed (in Megabytses) to encrypt a set of electronic medical records (EMR) using each encryption algorithm methods, this can also be referred to memory consumption. Table 2 shows the experimental results of the research.

Table 2: Memory Consumption (MB)

EMR	DSA	ECC	RSA
500	2.08	3.65	2.08
1000	2.2	4.3	2.2
1500	2.33	4.95	2.32
2000	2.44	5.6	2.44
2500	2.56	6.26	2.56
3000	2.68	6.9	2.68
3500	2.8	7.56	2.8
4000	2.92	8.2	2.92
4500	3.04	8.86	3.04
5000	3.16	11.38	3.16
Total	**26.21**	**67.66**	**26.2**

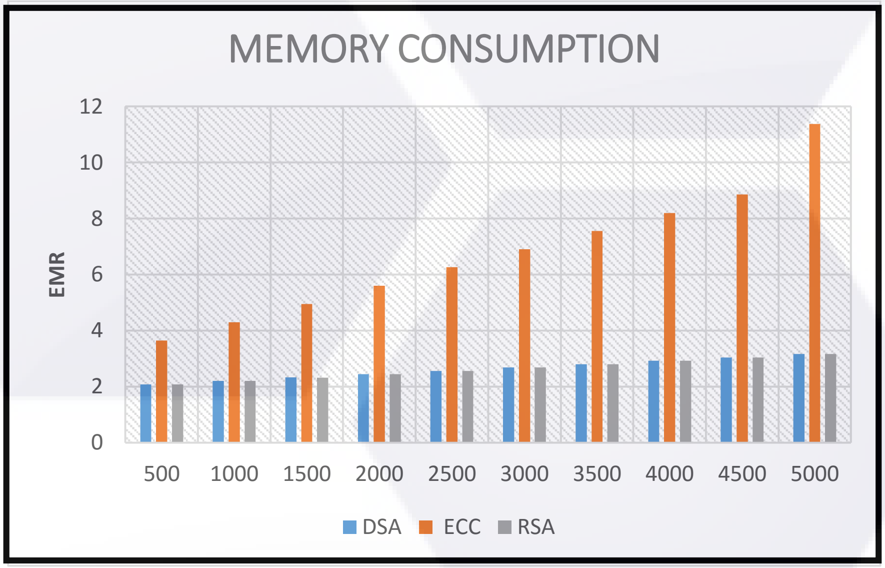


Figure 8: Memory Consumption (MB)

Battery Consumption

Battery usage is the percentage of battery consumption used by the computer to encrypt a set of electronic medical records using each encryption algorithm methods. It is measured in volts (V). table 3 shows the experimental results of the battery consumption during encryption of each algorithms

TABLE 3: Battery Consumption (V)

EMR	DSA	ECC	RSA
500	0.0034844	0.006344	0.004140625
1000	0.0040781	0.005359	0.006875
1500	0.0046406	0.00775	0.0034063
2000	0.0051406	0.008219	0.008140625
2500	0.0057967	0.0070469	0.0113594
3000	0.0064062	0.0052031	0.0051094
3500	0.0068906	0.0060156	0.00544
4000	0.007421	0.008453	0.00271875
4500	0.008	0.006756	0.003859375
5000	0.00828	0.0056719	0.00503125
Total	**0.0601382**	**0.0668185**	**0.056080725**

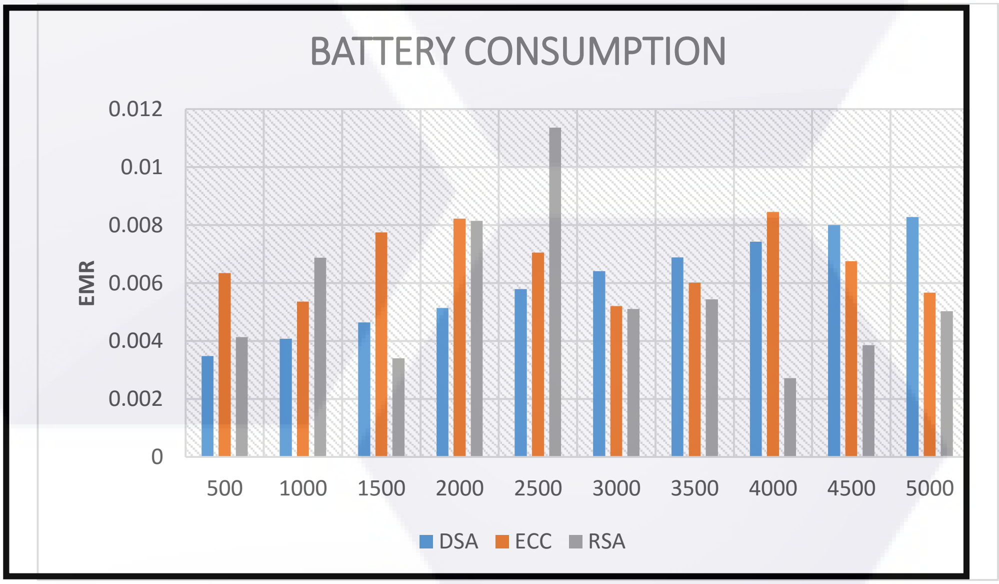


Figure 9: Battery Consumption (V)

Discussion

The results from tables 1, 2, and 3 show that RSA was the most efficient asymmetric encryption algorithms having spent **72.561** as processing time, **26.2** as memory consumption and **0.056080725** as battery consumption. In all, RSA consumed less computing resources during experimental evaluation. Hence, the most efficient encryption algorithms, RSA was then used to implement system prototype where sensitive and important medical information were protected/encrypted on a porous communications platform like web. This system prototype was successfully implemented after evaluation and proved to be one of the best methods to secure electronic medical record (EMR). The mechanisms provided by asymmetric encryption algorithms will make it extremely difficult if not impossible to break, because it makes the security stronger because large encryption keys provide more security.

5. Conclusion and future work

The use of Electronic Medical Records (EMR) system is gaining the attention of people in the health care sector around the world, and its acceptability is threatened by the security of patient's medical records. This study provides an evaluation of three distinct asymmetric encryption algorithms that were evaluated based on processing time, memory and battery consumptions as performance metrics. The results showed that RSA was the most efficient asymmetric encryption algorithms. The results of this research is in accordance with the study conducted by Fernández-Alemán, Señor, Lozoya, and Toval, (2012). Successful adoption of EMR is largely depends on privacy and security of the patient information, since the patient may encounter serious problems if sensitive information is disclosed.

Implementation of a system prototype was carried out on and it was securely exchanged between local server and web server. This was found to be a robust secured medical record system on web scenario and it has addressed the security concern raised by the new systems and guaranteed confidentiality, security and privacy patients' medical records. It brings patients into decision making process by informing the patient of any attempt to view their EMR. It's equally exonerated health care providers any litigation that may arise as a result of access to their patients' medical records. To the best of researchers' knowledge, this research work is one of the first initiatives to address security concerns to securely exchange electronic medical records under web platform and bring patient into decision making process in health management. This research has identified and utilized one of the methods to protect information of patient on EMR systems through asymmetric encryption algorithms. It is hoped that the proposed system will be implemented in the hospital in order to validate its practicability in a real life scenario. In addition, it is also expected that hybrid encryption algorithms will be studied based to determine its efficiency and effectiveness.

6. References

Abood, O. G., and Guirguis, S. K., (2018). A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications, 8(7)

Agbele, K. K., Februarie, R., Abidoye, A. P., Adesina, O. A., and Nyongesa1, H. O., (2011**).** Ensuring the security and privacy of information in mobile health-care communication systems. *S Afr J Sci. 2011;107*(9/10), Art. #508, 7 pages. doi:10.4102/sajs. v107i9/10.508

AL-nassar, B. A., Abdullah, M. S., and Osman, W. R. S., (2011). Overcoming challenges to use Electronic Medical Records System (EMRs) in Jordan Hospitals; *International Journal of Computer Science and Network Security, IJCSNS* .11 (8),51-58

American Health Information Management Association and American Medical Informatics Association (2007). Statement on the Confidentiality, Privacy, and Security of Health Records. *AHIMA Position Statement, December 2007*. www.ahima.org

Annapoorna, S., Shravya, S. K., and Krithika, K., (2014). A Review on Asymmetric Cryptography –RSA and ElGamal Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering.* 2(5), 98-105.

Appari, A. and Johnson, M.E., (2010) 'Information security and privacy in healthcare: current state of research', *International Journal of Internet and Enterprise Management*, 6(4),279–314.

Bala, T., and Kumar, Y., (2015). Asymmetric Algorithms and Symmetric Algorithms: A review; *International Conference on Advancements in Engineering and Technology* (ICAET 2015)

Basu, D., Bag, S. C, Dasb, A., and Razario, J. D., (2017). The importance of paper records and their preservation period in a Central Sterile Supply Department: An experience from an oncology center in eastern India. *Journal of Infection and Public Health, 10, 685–687. http://dx.doi.org/10.1016/j.jiph.2016.10.004*

Camargo, J. E., Sierra, D. F., and Torres, Y. F., (2015). Study of Cryptographic Algorithms to Protect Electronic Medical Records in Mobile Platforms. *Indian Journal of Science and Technology*, 8(21), DOI: 10.17485/ijst/2015/v8i21/60739

Carroll, R. (2016). *Aspen Valley Hospital Accused of Patient-Privacy Breach*, http://www. aspentimes.com/news/22463520-113/aspen-valley-hospital-accused- of-patient-privacy-breach

Dzenowagis, J and Kernen, G. (2005). Connecting for health: global vision, local insight. Report for the World Summit on the Information Society. *World Health Organization, Geneva*.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. A. O. & Toval, A. (2012). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics* 46, 541–562 http://dx.doi.org/10.1016/j.jbi.2012.12.003

Fitzpatrick, G., and Ellingsen, G., (2013). A review of 25 years of CSCW research in healthcare: contributions, challenges and future agendas. *Comput Support Coop Work 22*: 609-665

Garfinkel, S. I., and Spafford, G (2002). *Web Security, Privacy and Commerce*; 2nd Edition: O'Reilly Media Inc. USA. ISBN:0-596-00045-6

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. (2005) 'Can electronic medical record systems transform health care? Potential health benefits, savings and costs', *Health Affairs*, 24(5), 1103–1117

Hercigonja, Z., Gimnazija, D., and Croatia, V., (2016). *Comparative Analysis of Cryptographic Algorithms*, International Journal of Digital Technology and Economy, 1(2)

Omotosho, A., Emuoyibofarhe, J., and Meinel, C. (2017) 'Ensuring patients' privacy in a cryptographic-based-ehr using bio-cryptography', International Journal of Electronic Healthcare (IJEH), 9 (4), 227 54 https://www.inderscienceonline.com/doi/abs/10.1504/IJEH.2017.085800

Omotosho, A, and Emuoyibofarhe J. (2014); A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records. *International Journal of Applied Information Systems (IJAIS) 7(8), 11-18*

Nadeem, A. and Younus Javed, M. (2005). A performance comparison of data encryption algorithms. *Information and communication technologies, 2005. ICICT 2005. First international conference on. IEEE.*

Sahmim, S. and Gharsellaoui, H., (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review. *Procedia Computer Science* 112; 1516–1522

Singh, G., and Supriya, (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security; *International Journal of Computer Applications.* 67(19) 33-38.

Stausberg, J., Koch, D., Ingenerf, J., and Betzler, M. (2003). Comparing paper-based with electronic patient records: Lessons learned during a study on diagnosis and procedure codes. *J Am Med Inform Assoc YR. 10*(5), 470-477.

Xiao-Ying, Z. and Peiying, Z. (2016). Recent perspectives of electronic medical record systems (Review). *Experimental and Therapeutic Medicine* 11: 2083-2085, DOI: 10.3892/etm.2016.3233

Zriqat, I. A., and Altamimi, A. M., (2016) Security and privacy issues in ehealthcare systems: towards trusted services *(IJACSA) International Journal of Advanced Computer Science and Applications*, 7(9), 229-236

https://wiki.openmrs.org/display/RES/Demo+Data