Improving Security and Privacy for Health Information and Images

Islam Sami Abdulhameed
Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate Studies, Baghdad, Iraq. E-mail: ms201920528@iips.icci.edu.iq

Intisar Al-Mejibli*
Biomedical Informatics College, University of Information Technology and Communications Baghdad, Iraq. E-mail: dr.intisar.almejibli@gmail.com

Jolan Rokan Naif
Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate Studies, Baghdad, Iraq. E-mail: newjolan@gmail.com

Received September 11, 2021; Accepted December 10, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19164

Abstract

Recently, the wireless devices and information technology have been evolved greatly and used in many sectors such as health and military. Employing these technologies in health system require to transmitting the patient's information over the Internet. Hence, there is an urgent need to provide a high degree of security and privacy for patient information. This paper presents new encryption method to protect the information that are transmitted and stored in electronic health records (EHR) with maintaining its privacy. The proposal employs AES and ECC algorithms for security purpose and HMAC-SHA3 algorithm for privacy purpose. The suggested strategy was applied in different stages. ECC algorithm had been used to provides very fast key generation, and fast key agreement. A different key is generated for each session where both sender and receiver has the ability to generate the same private key. The obtained results show high level of security in both ends(Sender & receiver) as they have the role of encryption and decoding according to the query. The results were analyzed and tested according to the NIST test group and thirteen steps have been successfully passed.

Keywords

Security, Privacy, EHR, AES, ECC, SHA3, HMAC, NIST, Computer Network.

Introduction

Healthcare systems can be defined as technologies and automation intended to reduce the costs of managing large medical services and frameworks for future medical services

gradually across institutions, across borders and at the public level (Ruotsalainen, 2017). Figure 1 shows the healthcare system components. These systems have effectively contributed to maintaining the security of medical care. In addition, these frameworks have been described as a combination of private and general clinical wellbeing informatics, trade specifically, data presented or promoted through the Internet, and related developments (Section and Editorial, 2018). In other words, the term alludes to specialized progress as well as perspective, mindsets, and investment in global organizational thinking for better medical services at comparable, regional and global levels. In the stage where we deal with all of this, we determine that these systems are essential and perfect in our daily life and can save many lives by keeping the patient under constant observation in the emergency clinic through follow-up or clinical history of the patient (Gkoulalas-Divanis and Loukides, 2015).

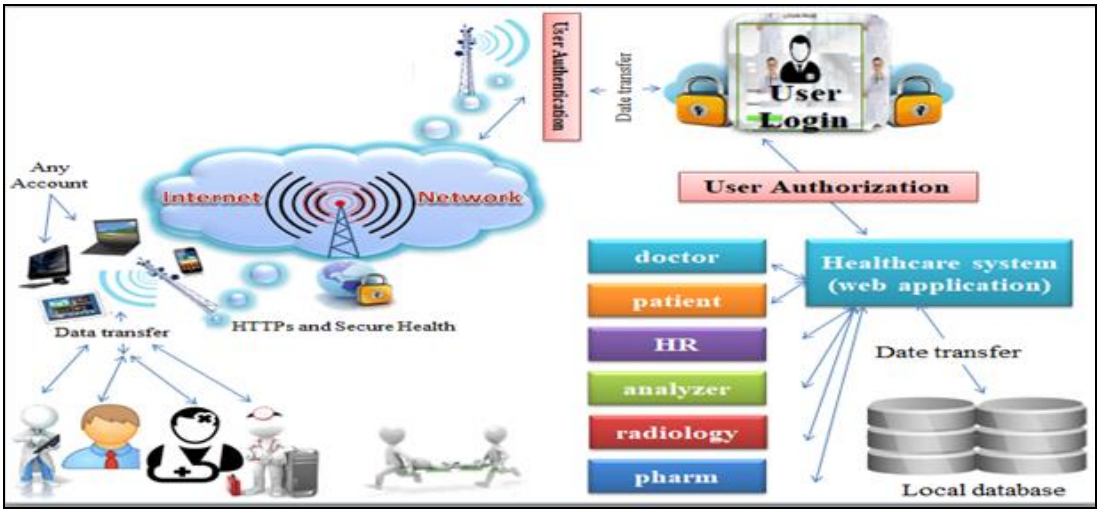


Figure 1 Healthcare system

Related Work

Many researches on data encryption techniques were suggested by researchers for use in data transmission in healthcare. We will focus on the two encryption algorithms, which are Elliptic curve cryptography (ECC) and advanced encryption standard (AES):

- (Hussein, 2019) proposed a cloud-based system for securely sharing and storing medical images. The proposed system relied on multiple encryption techniques to provide a high degree of safety for medical images to patients. lies through the transmission link and also when storing in the cloud, this is done using Elliptic curve cryptography (ECC), Advanced encryption standard (AES) and secure hash (SHA-3).

- (Jeba Nega Cheltha, 2018) suggested a way to protect sensitive images from unauthorized access using the RSA algorithm, ensure a secure provides very **fast key generation**, **fast key agreement** of public keys, honeycomb encoding technology is used, and noise in the encrypted image is corrected during transmission of the image over the communication channel.
- (Winnie, E. and Ajay, 2018) proposed system which is concerned with human temperature and creating a particular digital temperature sensor, DS18B20. Collected data is encrypted in the Fog Node using an advanced encryption standard (AES) algorithm and sent to the cloud. Therefore, the security of health data is improved through the work of computing in the cloud.
- (Lim *et al.*, 2018) suggested system that integrated security and privacy for medical information and images. It deployed an optimized version of SHA2 algorithm to create MAC with Java implementation. It used two similar MAC tags where the message is supposed to come to the patient from the doctor and means (authentication) and the message is supposed to be unmodified or tampered with or altered during transmission (message integrity). The authors concluded that data integrity and message authentication are essential components of the electronic communication of physician and patient messages.
- (Bansal and Agrawal, 2017) proposed a method of storing data safely and efficiently in cloud storage that requires less processing time and less CPU power by using the Elliptic curve cryptography (ECC) algorithm to increase integrity and security.
- (Gayathri *et al.*, 2017) presented a document, which is an extension of support for public keys in the encryption and decryption processes, including private keys. A combination of AES and ECC creates the private key. The AES key is usually 128 bits long with ten duplicates. However, this does not provide users with adequate security for their operations. To increase the level of security, the author apply 196-bit encryption with 12 iterations to generate round keys. This improve level of security for proposal users and maintain the confidentiality of user data
- (Mohammed, Slack and Naugler, 2016) proposed systems for encrypting electronic medical data that have demonstrated an application of the MD5 and SHA-1 algorithms to encode a message synthesized from private patient information.
- (Lee, Alasaarela and Lee, 2014) proposed a safe and effective system in which it relied on the ECC algorithm in key management to protect the health care system. Especially the patient's medical information, using private keys that were legally used to prevent the recurrence of attacks and also used the identification code, which is the SIM card number of patients' smartphones.

Component of Security

Must distinguish between authentication, authorization and access control because these are three terms that are important and difficult to understand sometimes; either they are defined as the same concept or the words are used interchangeably, and as a result, there may be confusion in these terms so that we will explain these concepts in more detail.

Authentication

It is a mechanism through which a person's data is verified, and it is often the first mechanism responsible for securing a specific system. It usually includes the digital form (username/password) and the physical form (ID/passport); It may also include other authentication mechanisms, such as a smart card, retina scanning, speech recognition, fingerprint scanning, and for authentication, the user must have created an account on a server that can be queried by the authentication method. (Azeez and der Vyver, 2019).

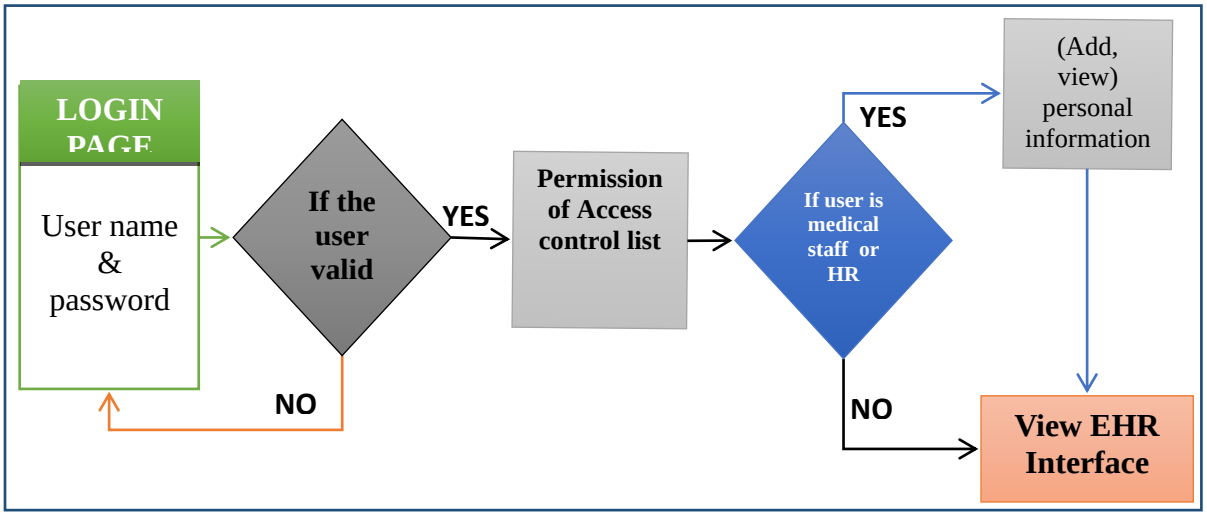


Figure 2 Authentication mechanism

Authorization

Authorization is a set of procedures that the user can perform after accessing a specific part of the system, and these procedures are set by the system developer according to conditional restrictions by the owner of the company or institution.(Azeez and der Vyver, 2019). Figure 3 shows the procedures that a user can perform based on his/her authorization.

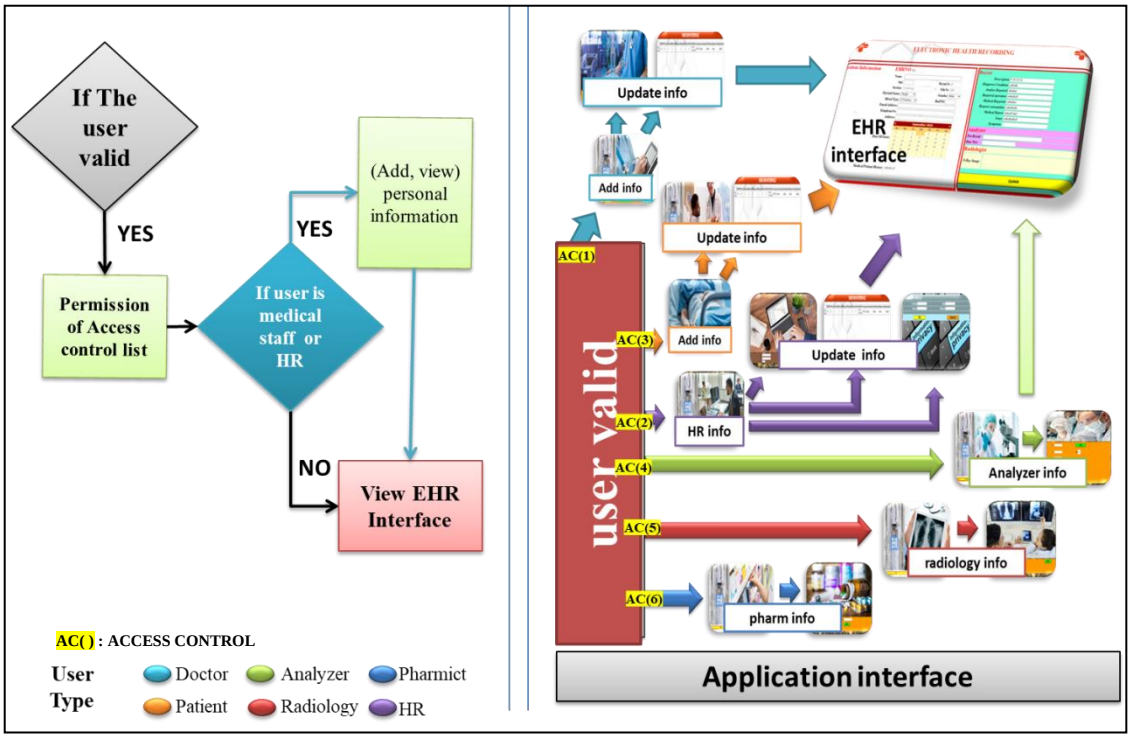


Figure 3 Authorization mechanism

Access Control

It is an additional step to help secure the system's main components; once the user's identity is confirmed, this process is performed to prevent data breaches. An example is controlling use to ensure the proper use of information in a particular system. This control is granted based on several conditions or follows a policy that was set in advance after granting access to information. For example under suggested scheme, whether the individual is an HR employee, physician, patient, laboratory analyst or radiologists, and each of them has a certain degree of authority, It means restricting this user from doing something that he/she may not be allowed to do (Gkoulalas-Divanis and Loukides, 2015).

Key Security Concepts

Federal Information Systems and Information Systems Security Categorization Standards (FIPS PUB 199) describes three security requirements and goals that determine the degree of safety for each category. (Stallings, Bauer and Hirsch, 2015).

Confidentiality (Stands for the Protection of Data and Confidentiality)

Maintain authorization restrictions for access to and disclosure of information, including protecting the confidentiality and proprietary information. This means that individual files

are locked and safe; confidentiality occurs when information is transmitted without authorization (Algarni, 2019).

Integrity (Covers the Integrity of the System and the Data)

Protection from any modification that occurs, whether tampering with information, making it incorrect, or destroying that information and the guarantee of the information are not rejected and ensure to valid it. Integrity can be lost when information has been illegally modified or destroyed. (Tchernykh *et al.*, 2019)

Availability

Ensure fast and reliable access to information and its use. It is considered one of the obstacles facing the user to access the information he/she needs in the system, and one of the essential things and principles to define security objectives is the use of the CIA triad, with some believing that information security needs other additional concepts. (Tchernykh *et al.*, 2019)

Techniques Used In Proposed Work

Cryptography is used to secure sensitive data, important information and protect information that sent electronically in the communication channels. The encryption system classified into two main types, symmetric and asymmetric. Symmetric encryption also known as private key encryption, the sender and recipient use the same key in the cryptographic and decryption processes. In contrast, asymmetric encryption is also called public-key encryption. In this type, the sender uses the recipient's public key to encrypt his/her message and uses private key for decryption [16]. In this paper, the two types of encryption were used, and the focus was on the AES algorithm and ECC.

Advanced Encryption Standard (AES) Algorithm

Advanced Encryption Standard (AES), which is popular today, is a symmetric block cypher that always uses the same key for encryption and decryption. Advanced Encryption Standard becomes new algorithm of U.S.'s In October 2000, as FIPS-197 in Federal and Register in December 2001, declared by two scientists Vincent Rijmen and Joan Daemen by the National Institute of Standards and Technology (NIST), it proposed to replace DES. AES is a non-Feistel cypher. AES divides its inflow into blocks of fixed size. Allows for a variety of key and block sizes. The size can be 128, 160, 192, 224, and 256 bits (multiples of 32 bits and from a minimum of 128 to a maximum of 256).

However, the default is that the input block size is always set to 128, and the key size is 128, 192, and 256. (Thorat and Inamdar, 2020)

Elliptic Curve Cryptography (ECC) Algorithm

ECC is an asymmetric cryptographic algorithm that implements all major capabilities of the asymmetric cryptosystems: encryption, signatures and key exchange. It relies on trapdoor functionality. It is considered one of the most secure algorithms and does not consume many mathematical operations. Its key size is tiny compared to other algorithms, for instance, a 112-bit key equivalent to RSA 512-bit key size. The use of these curves for coding was proposed independently at IBM and initially introduced in 1985 by Neil Koblitz from the University of Washington and Victor Miller, after which they have been widely used since 2005, taking an algebraic structure of elliptic curves on essentially limited fields and an approach to encoding the public key. Several fundamental and broad mathematical concepts to which elliptic curves belong, and these concepts create smaller, faster and higher efficiency cryptographic keys that can be used for these concepts. (Shankar, Tomar and Tak, 2015).For mathematical concepts of ECC, the set of all (X, Y) pairs satisfying the nonsuper singular elliptic curve equation:

$$y^2+xy = x^3 + a_2x^2 + a_6 \ldots\ldots (1)$$

They are called points on the elliptic curve E, where x, y, a_2, and a_6 are elements of the Galois FieldGF (2^n). The point addition (S=P+Q) and multiplication (R=k*P, where k is a constant) operations are defined such that both S and R are also points on the elliptic curve E. Further, it is impossible to find the value of K even if an R and P-value are found. This property forms the basic of the ECC algorithm. Elliptic curves are used in many different forms in cryptography, For example, secret key exchange uses the Basic Secret Sharing Algorithm (ECKAS-DH in [3]), The ECDH (Elliptic Curve Diffie–Hellman Key Exchange) is anonymous key agreement scheme, which allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel.

Assume that there are two parties *A* and *B* choose two **private keys(PK_a,PK_b)**, belonging to ***A*** and ***B*** respectively, where an ECC elliptic curve with generator point **G**, we can exchange over an insecure channel the values (PK_a * **G**) and (PK_b * **G**) (the **public keys** of ***A*** and ***B***) and then we can derive a shared secret: *secret* = (PK_a * **G**) * PK_b = (PK_b * **G**) * PK_a. The above equation takes the following form:

APubKey*BPrivKey= **BPubKey** * **APrivKey** = *secret*

The following explain the**ECDH** algorithm (Elliptic Curve Diffie–Hellman Key Exchange):

1. **A** generates a **random** ECC key pair: {**APrivKey**, **APubKey** = **APrivKey** * **G**}
2. **B** generates a **random** ECC key pair: {**BPrivKey**, **BPubKey**= **BPrivKey** * **G**}
3. **A** and **Bexchange their public keys** through the insecure channel (e.g. over Internet)
4. **A** calculates **sharedKey** = **BPubKey** * **APrivKey**
5. **B**calculates **sharedKey** = **APubKey** * **BPrivKey**
6. Now both **A** and **B** have the same **sharedKey** == **BPubKey** * **APrivKey** == **APubKey** * **BPrivKey**

keyed-hash message authentication code _ Secure Hash Algorithm (HMAC_SHA3)

A secure encryption message based on hash functions and the shared key authentication protocol with a secure exchange mechanism. It can effectively prevent data from being intercepted and manipulated during the transfer process. They preserve the integrity, reliability, and security of data and are currently used for better network security. It used by the hash function of SHA-512 and as an HMAC code. The HMAC method combines the message data with a hidden key and determines the outcome. The hash value is remixed with the hidden key and then hashed a second time512 bits in length is the output hash. An HMAC can be used to determine if, as long as both parties share a hidden key, has been tampered with, or has been tampered with. The sender determines the original data's hash value and sends it together with the hash value to the receiver; the receiver turn recalculates the hash value of the message received. The message would be authenticated if the initial hash value and the measured hash value match. If they do not matched, the value of the hash or data is changed. (Chen and Yuan, 2012).

Electronic Health Records (EHR)

EHR is a compilation in the digital electronic format of patient health documents, and these types of data are usually putting in the Electronic Health Records (EHR). Others defined the EHR as numeric charts containing detailed information of the patient's medical status [34] and can reside on multiple servers in the system. EHR has been increasingly popular in many world states in this time, such as Saudi Arabia (Aldosari, 2017), Jordan (Klaib and Nuser, 2019), the united states (Destino *et al.*, 2017), the united kingdom (Wilson and Khansa, 2018), Sweden (Hellberg and Johansson, 2017), and India (Powell, Ludhar and Ostrovsky, 2017). Many features exist of EHRs compared to standard handwritten health records or other types of electronic records. EHRs have evolved in many states to play the primary role in Health institutions and can depend on as an official document at present also, and it can be managed and update from any place

in the world by using specific authentication and permission to update information according to the person concerned (Tasatanattakool and Techapanupreeda, 2017).

"Outpatient Department" (OPD) is one of the hospital's departments, and it is the first point of contact among medical staff and patient in the hospital. When the patient goes to the hospital for the first time, he/she must go directly to this department, and the job of this section is to forward patients to the different hospital departments. "Admission, Transfer, and Separation for a patient" (ATS). (Graves, 2002).

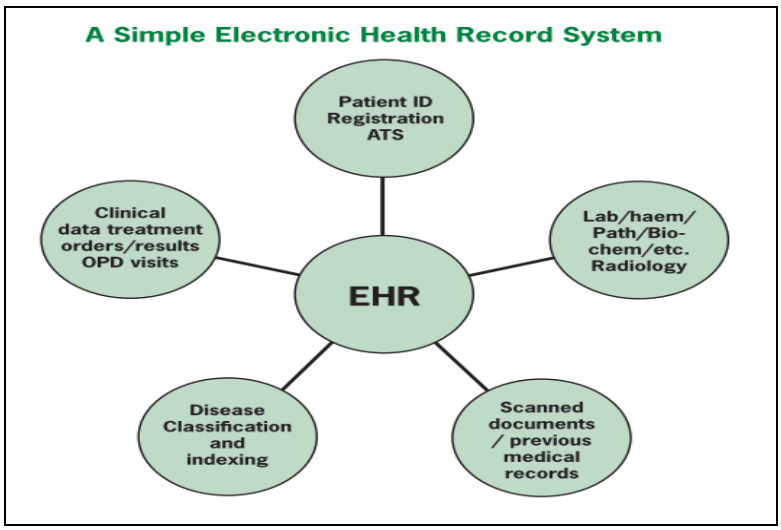


Figure 4 Simple Electronic Health Record. (Graves, 2002)

Proposed System

The used platforms in the proposed system are the Visual studio 2019 environment within the ASP.Net framework; the C # programming language to implement encoding and decoding and message integrity, and the Python programming language to examine the strength of the encryption. Also, the HTML language was used for building interfaces and the CSS style for coordinating the shapes and colors of the interfaces and SQL server language is used for database building.

In general, the health care system includes two components Server and Client. The proposal perform many operations in both sides as shown in figure 5. The block diagram of proposed system is shows in figure 6 where the client-side represents the interfaces, and the server-side represents the application with its database. The system is connected to several users including the medical staff, which consists of a doctor, radiologist, laboratory analyst, pharmacist and the patient. In addition to, the human resources officer. Each of these users has a username and password based on which he/she is granted

permission. Due to the granted permission, the privacy aspects of the system are implemented, where authentication, access control, and authorization are shown in figure 7.

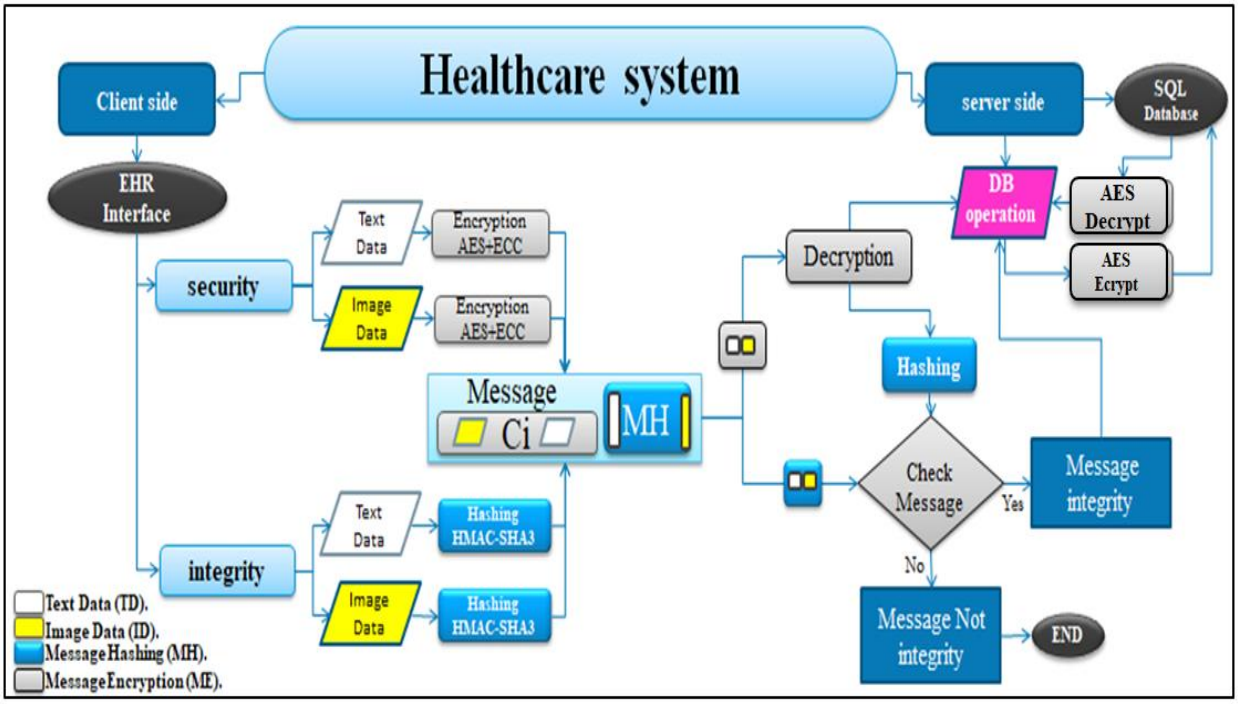


Figure 5 Flowchart of the proposed system

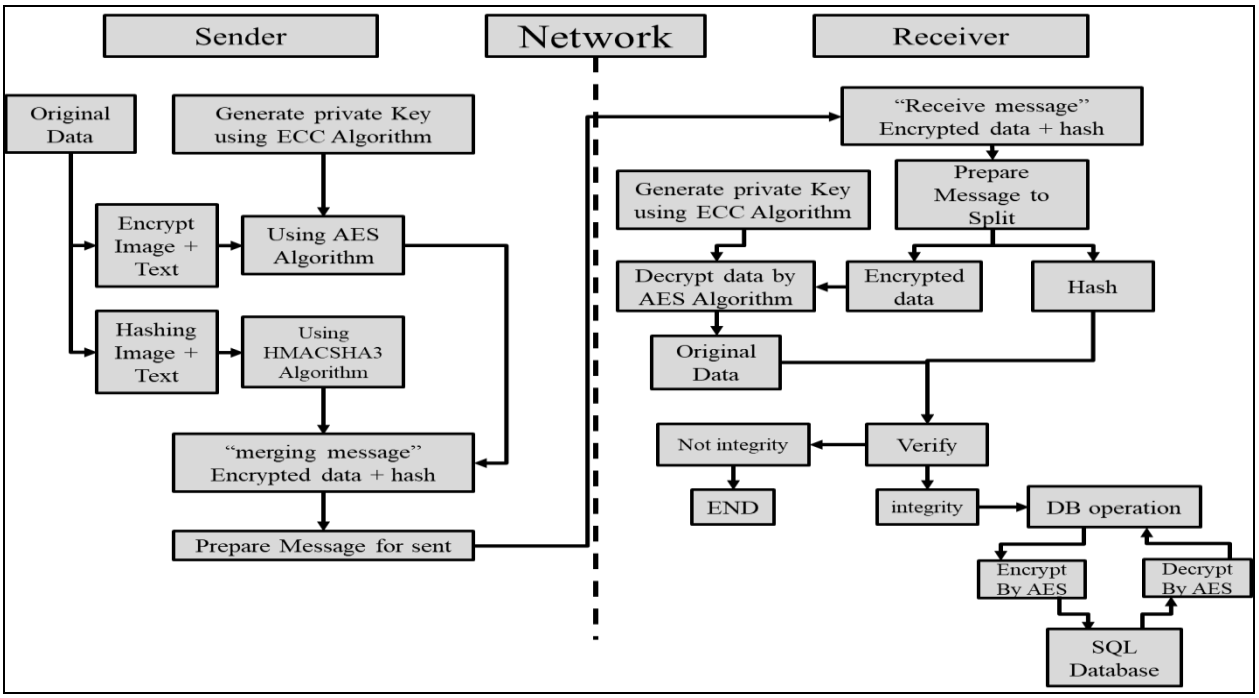


Figure 6 The suggested system's block diagram

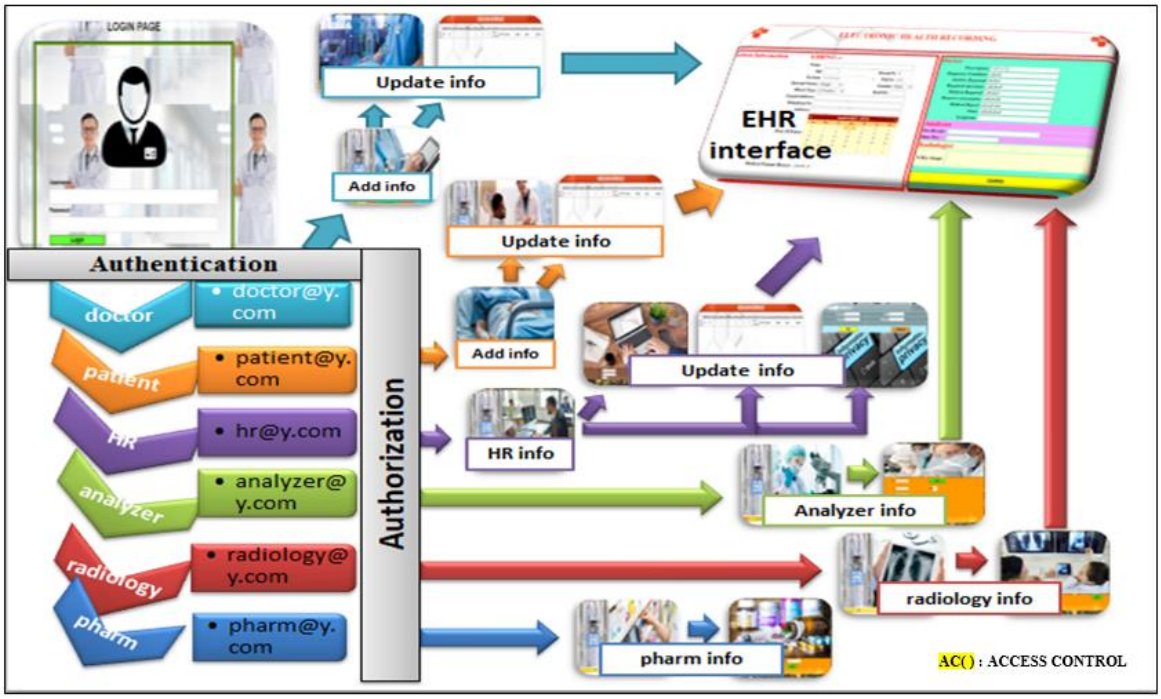


Figure 7 Authentication, Authorization, and Access control

- User Validation

Step 1: The human resources employee registers the patient by entering his/her username and giving him the patient code and password after logging in using the registered e-mail and specific password.

Step 2: The patient code is verified, and then it is transferred to the electronic health record page as shown in figure 8. Figure 9 presents the main interface of the electronic health record.

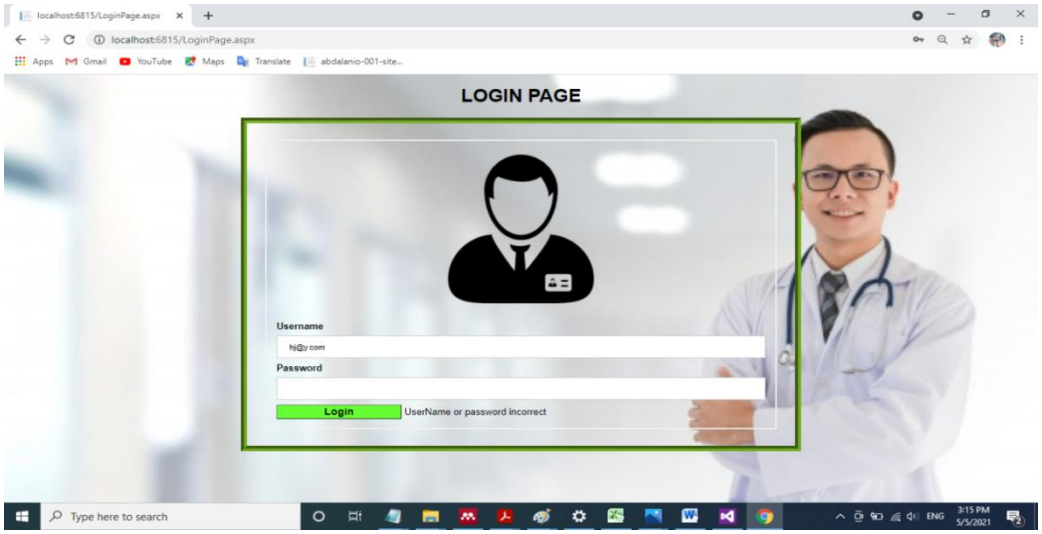


Figure 8 Login page of proposed system

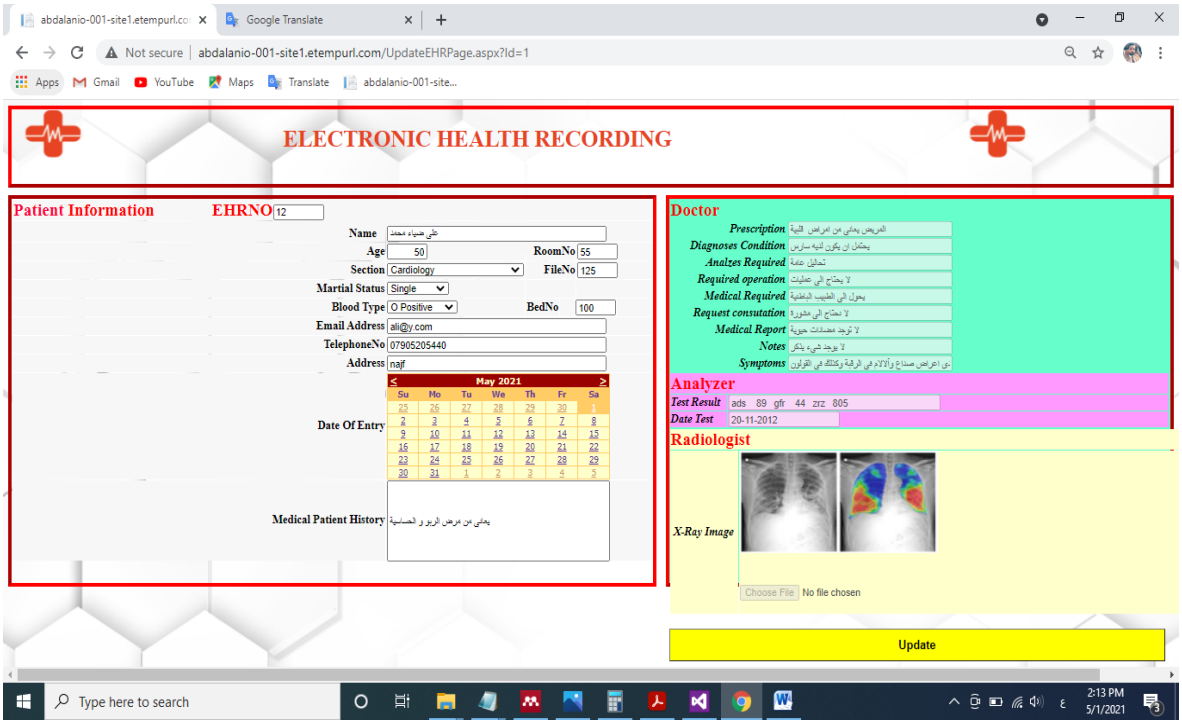


Figure 9 The main interface of the electronic health record

➢ Security and Privacy Phases

To complete the basics of proposed system, we worked on two critical aspects, the security and privacy.

1- Security Phase

We used two types of encryption techniques symmetric and asymmetric, to provide an intense, light, and fast method of security. For the symmetric encryption method, we used the AES algorithm with a key size of 128 bits and for the asymmetric encryption method, the ECC algorithm was used to generate private keys with more than 256 bits. To achieve data integrity the (HMACSHA3-512) algorithm is used hence; hash block of the transmitted original data is created.

- Encryption process:

The encryption process is done on both the sender side when sending and the receiver side when the data is received and stored in the database. The applied encryption method relied on the AES algorithm for data encryption, and ECC algorithm has been employed to generate the private key. In the applied encryption mechanism there is no key that travels with the message as in the traditional methods of Encryption. The mechanism of

generating keys is done by ECC algorithm that have curve (EC_BP256R1) on both sides sender and receiver at the same time and in the same environment specified in the system. When the Encryption begins, a key is generated on the sender side and the same key is generated on the recipient side where the generated key in both side is unique for each session. Encryption is done and the obtained encrypted data is combined with the hash code then the combination is sent. When the message reaches the recipient's side, it is decrypted directly using the key previously generated on receiver side for this session. After decrypting it and verifying the integrity of the data based on received hash code, it is encrypted again using the AES 128bit algorithm for the purpose of storing it as an encrypted form in the database.

- Decryption Process

The decryption process occurs at the receiver side and occurs in two cases, the first case when the message is received and the second case when the data is retrived from the database.Fo security purpos the data is stored in the proposed system in an encrypted form. In both cases, when the message is arrived to the receiver side that coming from the sender's side, the data is separated into a ciphertext and a hash, which is decoded by the AES 128 bit algorithm and based on the pre-generated key by the ECC 256bit algorithm.

2- Privacy Phase

Patient's privacy deals with how accessing his/her data. There will be significant patient data in the electronic health record that must be out of everyone's reach. The proposed system aimed to make each patient's data invisible to other patients. Figure 10 shows the flowchart of obtaining permission and ID number to determine each user privacy.

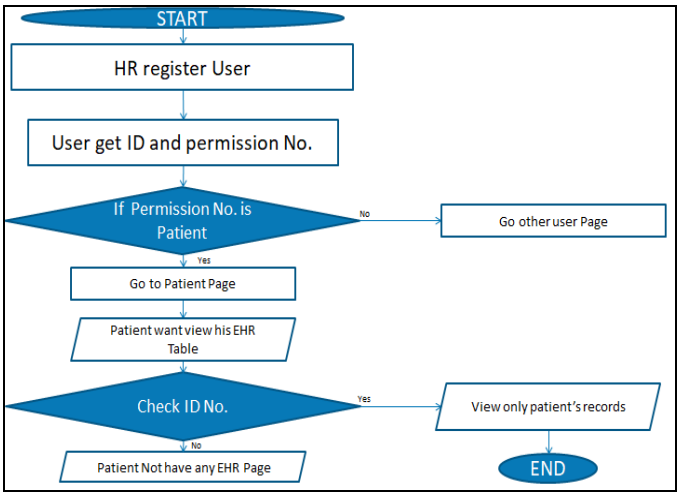


Figure 10 Flowchart of getting permission and ID number

Where when the patient is registered in the system by the human resources employee, the system provides the patient with two essential numbers that determine the patient's validity within the system; the first number is a permission number in the system, and is responsible for opening the patient to his/her personal page. The second number is unique ID number that given to each new user automatically where it is serial and unspecified. As shown in the figure 11, as for the matter with the medical staff, it differs somewhat, as the Human Resources employee also registers the medical staff and then they provided with two numbers from the system same as granted to patients as mentioned above.

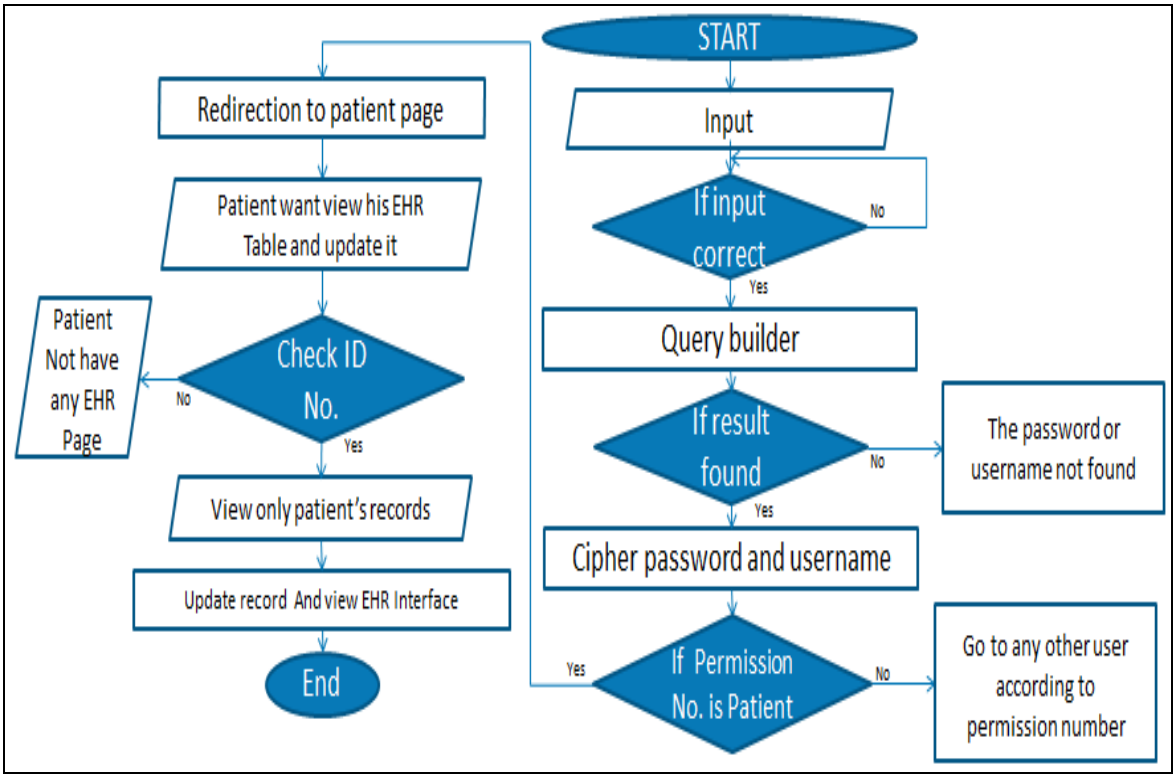


Figure 11 Privacy steps

Table 1 Access Control List

User	Privilege number
Doctor	1
laboratory analyst	2
Patient	3
Pharm	4
Radiology	5
HR	6

Table 1 shows the list of access control for each user type. The number shown in which is a permission number used to transfer user to his/her page according to the user's specialty, it is used to identify the doctor, analyst, or others Who supervised the treatment of the

patient, and this is done on the main page of the electronic health record. The human resource employee makes a choice of the medical staff ID from the list of the staff. Figure12 shows the patient's electronic health record with the ID number, as only his/ her record appears, and the same is the case with the rest of the patients.

Figure 12 shows adding a new electronic medical record for a patient and the process of giving him/her a personal ID number to be used by the medical staff who supervise his/her condition.

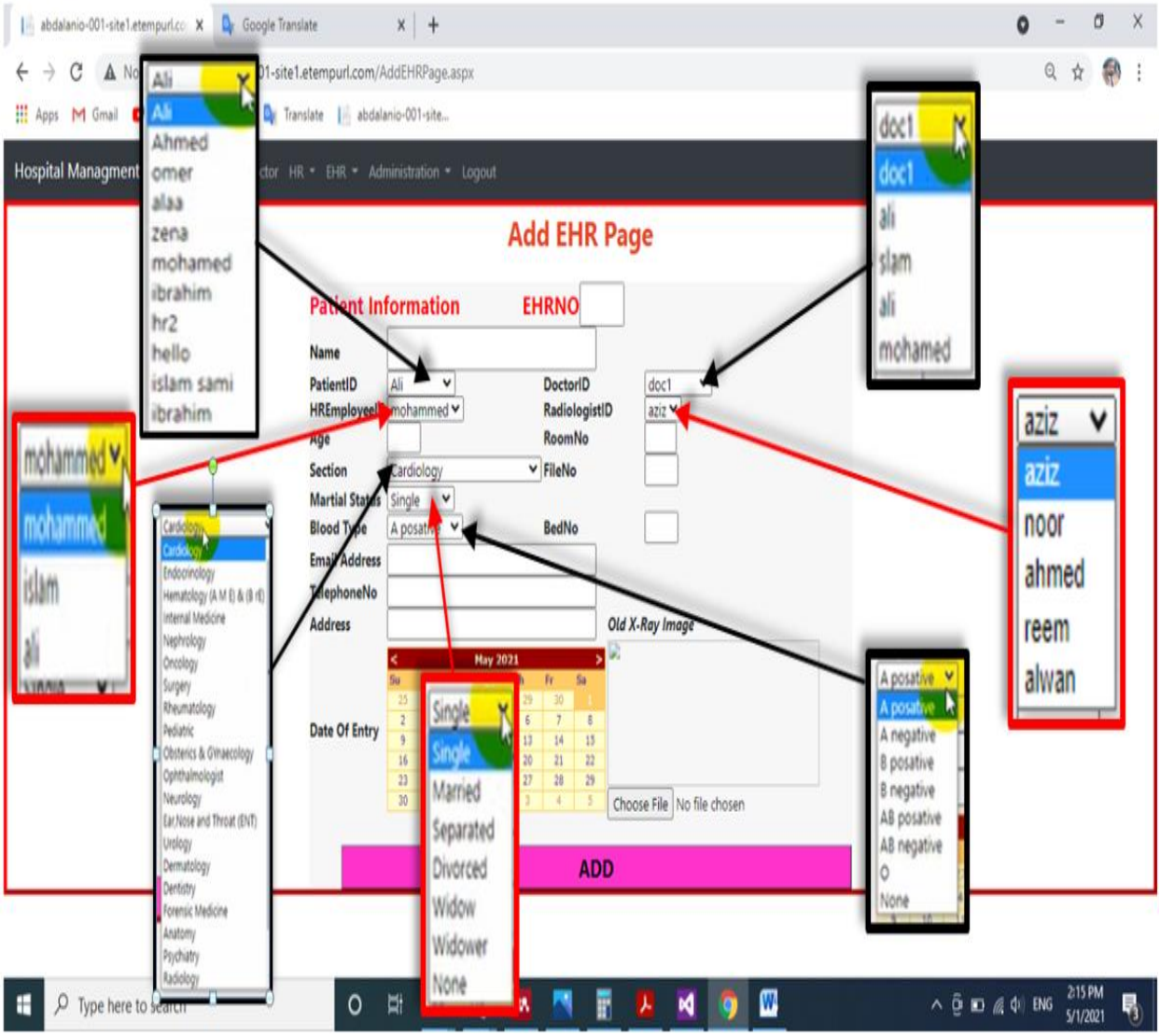


Figure 12: Adding a new electronic medical record for a patient

Results and Discussions

The proposed system implemented and evaluated on the smarterasp.net site. To evaluate the system Windows 10 Pro 64-bit operating system is used with Intel (R) Core (TM) i5-4200M,

2.50 GHz CPU, 8 GB of RAM (7.76 GB usable). The obtained results have been illustrated, analyzed, and discussed. Also, the tested and experiment using security NIST tests.

Time Execution

Different text data sizes were tested for a specific number of patients, and different medical image sizes were adopted according to the original size of the image.The used images arefrom radiology and sonar devices in health institutions as shown below. Moreover, the average time for all data was taken. Table 2, 3 and 4 shows the required execution time for (10, 25, 70), (100 Byte, 1KB, 2KB) and (10KB, 500KB, 1MB) data size respectively. Table 5 shows the required execution time for (83KB, 118KB, 263KB) image size.

Table 2 The Required Execution Time for (10, 25, 70) Data Size

Project Result: Windows 10 Pro, Intel(R) Core(TM) i5-4200M CPU 2.50GHz												
Patient .NO	**10 byte/ msec**				**25 byte/ msec**				**70 byte/ msec**			
	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify
Patient 1	0.0517	0.052	0.0177	0.0314	0.072	0.0933	0.0175	0.0124	0.1244	0.1898	0.0269	0.2808
Patient 2	0.0518	0.051	0.0177	0.0124	0.0808	0.0859	0.0176	0.0221	0.1422	0.1296	0.0175	0.3334
Patient 3	0.0519	0.082	0.0185	0.0394	0.0923	0.0889	0.0179	0.0085	0.169	0.1239	0.0347	0.4087
Patient 4	0.0522	0.0532	0.0192	0.0126	0.0744	0.0786	0.0188	0.0156	0.1717	0.1147	0.0341	0.3198
Patient 5	0.0529	0.0559	0.0175	0.0175	0.0874	0.083	0.019	0.0276	0.1732	0.1264	0.0255	0.3689
Patient 6	0.0531	0.0514	0.0173	0.0088	0.0849	0.0737	0.019	0.0085	0.1739	0.1674	0.0176	0.2407
Patient 7	0.0533	0.0492	0.018	0.0161	0.0645	0.0819	0.0191	0.0276	0.112	0.1437	0.0194	0.4298
Patient 8	0.0547	0.0547	0.0195	0.0314	0.0523	0.0755	0.0195	0.0276	0.1804	0.1423	0.0595	0.4967
Patient 9	0.0555	0.0516	0.0188	0.0314	0.0841	0.0853	0.0199	0.0124	0.1872	0.1056	0.0349	0.4252
Sum	0.4771	0.501	0.1642	0.201	0.6927	0.7461	0.1683	0.1623	1.434	1.2434	0.2701	3.304
Average	0.0530	0.0556	0.0182	0.0223	0.0769	0.0829	0.0187	0.0180	0.1593	0.1381	0.0300	0.3671

Table 3 The Required Execution Time for (100 Byte, 1KB, 2KB) Data Size

Project Result: Windows 10 Pro, Intel(R) Core(TM) i5-4200M CPU 2.50GHz												
Patient .NO	**100 byte / msec**				**1000 byte/ msec**				**2000 byte/ msec**			
	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify
Patient 1	0.5162	0.3889	0.0318	0.7262	1.0225	1.3286	0.1599	2.3654	1.3657	2.117	0.2499	4.0679
Patient 2	0.6696	0.3805	0.0195	0.8118	1.0369	1.2301	0.1098	2.34	1.4066	1.67	0.1652	3.2549
Patient 3	0.7697	0.3642	0.0336	0.7932	1.0462	1.4697	0.3378	2.5414	1.4405	1.0345	0.2779	2.4989
Patient 4	0.4322	0.4369	0.0382	0.7731	1.052	1.1758	0.13	2.2981	1.5704	1.2778	0.3309	3.1261
Patient 5	0.448	0.3337	0.0204	0.6454	1.0682	0.9982	0.1065	2.0146	1.6539	1.8469	0.4664	3.863
Patient 6	0.5162	0.3889	0.0318	0.7262	1.0695	1.7979	0.1166	2.9983	1.7113	1.7054	0.2618	3.7963
Patient 7	0.668	0.3769	0.0232	0.764	1.0846	1.4834	0.1646	3.1317	1.7256	1.483	0.3848	3.427
Patient 8	0.6696	0.3805	0.0195	0.8118	1.1829	0.9705	0.1064	2.2294	1.735	1.5476	0.6483	3.6249
Patient 9	0.7697	0.3642	0.0336	0.7932	1.397	1.0793	0.1083	3.5293	1.7784	1.6231	0.3679	3.3769
Sum	5.4592	3.4147	0.2516	6.8449	9.9598	11.5335	1.3399	23.448	14.3874	14.3053	3.1531	31.035
Average	0.6065	0.3794	0.0279	0.7605	1.1066	1.2815	0.1488	2.6053	1.5986	1.5894	0.3503	3.4484

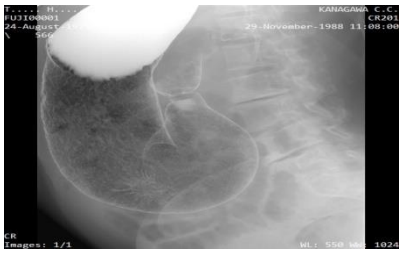
Table 4 The Required Execution Time for (10KB, 500KB, 1MB) Data Size

Project Result: Windows 10 Pro, Intel(R) Core(TM) i5-4200M CPU 2.50GHz												
Patient .NO	**10000 byte/ msec**				**500000 byte/ msec**				**1000000 byte/ msec**			
	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify
Patient 1	1.9354	1.0959	1.0621	3.9652	10.7168	13.0383	7.0763	14.4336	18.8733	23.4351	19.4872	31.7466
Patient 2	1.9987	2.4436	1.1132	5.1665	11.6755	15.5907	7.7174	20.351	19.7033	26.5072	20.9899	36.4066
Patient 3	2.0804	1.6694	1.2074	4.3211	10.0392	16.0758	8.0198	18.0784	19.9458	19.7492	28.1141	35.8916
Patient 4	2.2596	2.5078	1.2081	4.9129	12.6402	15.4353	6.2353	22.2804	20.4024	27.0113	22.863	40.8048
Patient	2.31	2.217	1.14	5.23	10.14	16.33	6.34	18.29	23.52	24.41	29.30	41.05

5	92	6	23	65	54	55	32	08	92	1	12	84
Patient 6	2.3492	1.6553	1.0951	5.5447	11.9754	15.526	7.7565	17.9508	24.4701	17.7591	22.9026	40.9402
Patient 7	2.414	1.1089	0.845	2.7758	10.9063	15.8908	7.9439	23.8126	23.2921	26.8247	22.9711	41.5842
Patient 8	2.8915	1.3058	1.1147	3.2189	10.8472	15.9233	8.0441	17.6944	24.3791	25.0467	21.1953	43.7582
Patient 9	3.8381	1.8426	1.5731	4.996	10.8616	17.8577	7.809	19.7232	25.4865	25.6046	21.033	36.973
Sum	22.086	15.8469	10.361	40.137	99.8076	141.673	66.945	172.61	200.081	216.348	208.85	349.16
Average	2.4540	1.7607	1.1512	4.4597	11.0897	15.7414	7.4383	19.1794	22.2313	24.0387	23.2063	38.7959

Table 5 The Required execution time for (83KB, 118KB, 263KB) Image Size.

Project Result: Windows 10 Pro, Intel(R) Core(TM) i5-4200M CPU 2.50GHz												
Patient .NO	**83 Kilo byte / msec**				**118 Kilo byte/ msec**				**263 Kilo byte/ msec**			
	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify	Encrypt	Decrypt	Sign	Verify
Patient 1	1.9985	2.4178	0.1132	2.6095	2.4578	3.9917	1.6736	4.1239	7.9877	5.7068	10.4658	5.8151
Patient 2	3.9511	2.8733	0.1109	3.0312	2.0498	2.499	1.3706	2.6716	8.9974	4.7971	9.4363	7.9496
Patient 3	2.9319	2.1365	0.1615	2.2699	3.3949	2.9781	1.3074	3.118	9.0654	8.0031	11.4377	6.2395
Patient 4	2.5802	2.4195	0.1355	2.5337	3.9709	2.0334	1.9183	2.1972	6.8781	5.773	9.6529	5.8995
Patient 5	2.4389	3.0891	0.122	3.3898	3.1396	3.819	2.9449	4.0687	5.9651	4.9998	11.1858	6.1028
Patient 6	3.6183	2.2438	0.1389	2.3826	4.0678	3.8134	2.9592	4.0259	6.1067	7.3576	9.2965	8.5307
Patient 7	2.627	3.0742	0.1634	3.1937	3.3312	2.3242	2.16	2.4393	7.9443	8.8835	9.1564	8.4154
Patient 8	2.7734	2.2592	0.2067	2.417	3.9549	2.3488	1.147	2.4554	5.5308	6.5782	10.0659	6.7552
Patient 9	2.7177	2.2756	0.1205	2.4115	3.7801	3.6591	2.1557	3.9986	9.8054	7.3408	7.5154	6.5951
Sum	25.637	22.789	1.2726	24.238	30.147	27.4667	17.636	29.0986	68.2809	59.4399	88.2127	62.3029
Average	2.8485	2.5321	0.1414	2.6932	3.3496	3.0518	1.9596	3.2331	7.5867	6.6044	9.8014	6.9225

Original Image			

NIST Test

The NIST "National Institute of Standards and Technology" used to analyze the randomness of the key generation of the proposed system by looking at 3 million bits generated in 11,719 lines, each line of 256 bits long. The strength of the generated switches, which has successfully passed 13 of the 15 tests, was proven after performing all the statistical tests for the NIST group, which are shown in Table 6.Figure 13 shows the random number test values.

Table 6 NIST test suite results

Test No.	Test	P-average	Result
1	frequency mono bit	0.12309626243355014	pass
2	frequency_within_ block	0.10272553542218647	pass
3	Runs	0.2736737671719827	pass
4	longest_run_ones_in_a _block	0.3339203469561405	pass
5	binary_matrix_+rank	1.0217149833352483e-107	fail
6	Desecrate_Fourier_transform(spectral)	0.48084432993305404	pass
7	non_overlapping_template_matching	0.3483880485598257	pass
8	overlapping_template_matching	6.0445816705986285e-15	fail
9	maurers_universalStatisics	0.9026949094979893	pass
10	linear_complexity	0.39971094795169193	pass
11	Serial	0.19538891279420326	pass
12	Approximate_Entropy	0.13057360499273662	pass
13	Cumulative_Sums	0.10893650836596228	pass
14	Random_Excursion	0.547215061932267	pass
15	Random_Excursion_Variant	0.1956193554239986	pass
The final result of the test		13/15 pass, 2/15 fail	

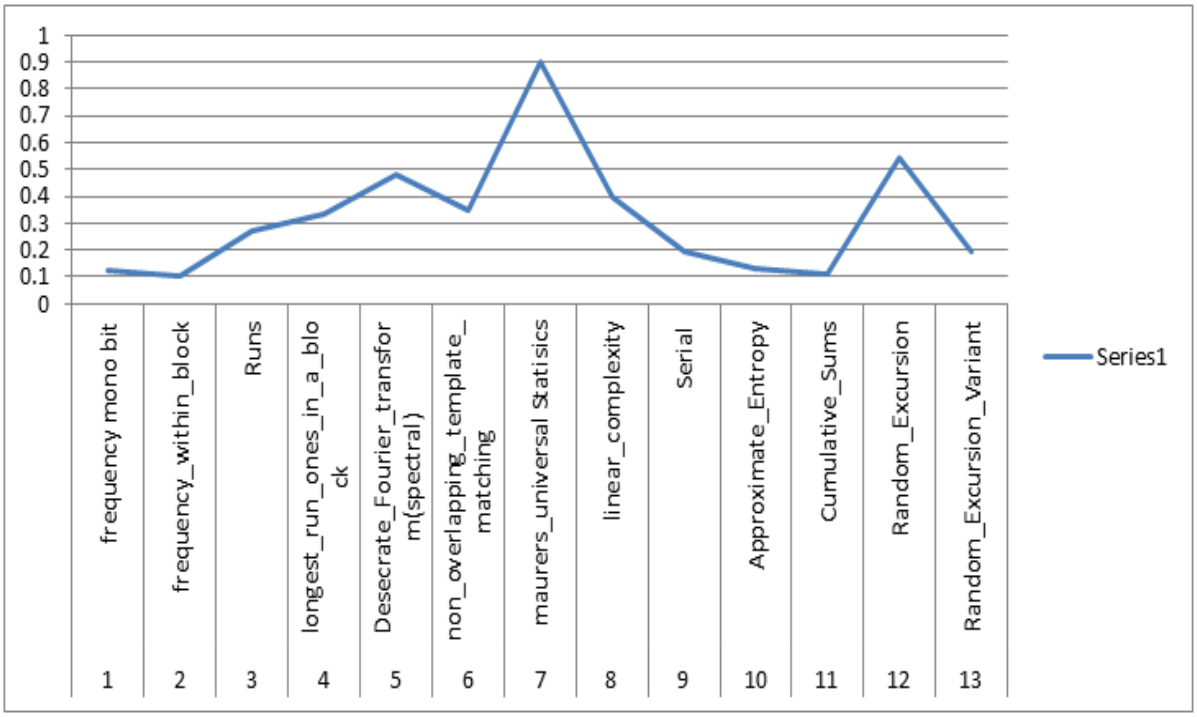


Figure 13 Random number test values

Conclusion

In the proposed system, a new, fast, efficient and secure strategy has been implemented to encrypt patient information through transmission and upon storage in an electronic health record form with maintaining their privacy. The proposal is based on algorithms (AES and ECC) for security and (HMAC-SHA3) for integrity. The experimental results obtained were promising in both the required execution time (encryption and decryption) and the level of security. Therefore, the proposal presents a suitable solution for the health care system because it deals with the vital information represented by the patient's information. The proposed system also added strength to the encryption despite the strength of the AES algorithm in Encryption. The problem of transferring the key in it is still the weak point of most encryption algorithm. The use of the ECC algorithm tackle this issue as it able to generate same key at both sides (sender and receiver). The generated key is unique for each session. The main aim of proposed system is to overcome the weak point in the AES algorithm through the mechanism, which is exchanging the private key throw transmitted message between sender and receiver. In addition, the key generation process for the ECC algorithm has passed a batch of NIST tests, proving that the key is random and unbreakable and this enhances the security of the system. Further, the proposed system used the (HMAC-SHA3) for maintaining the privacy of patient information. In general, The results showed that when the data size is

from 100 to 1,000,000 bytes, the required encryption time is ranged between (0.6 to 22.2) milliseconds and (0.3 to 24.0) milliseconds is required time for decoding the text data. Whereas for the medical image data (Real Test images used in Iraqi health institutions), the image size ranged (83 to 263) kilobytes, and the required encryption time ranged between (2.84 to 7.5) milliseconds and (2.5 to 6.6) milliseconds is required time to decryption.

References

Aldosari, B. (2017). Supportive care pathway functionalities of EHR system in a Saudi Arabian hospital. *Computers in biology and medicine, 89,* 190-196. https://doi.org/10.1016/j.compbiomed.2017.08.012.

Algarni, A. (2019). A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access, 7,* 101879-101894. https://doi.org/10.1109/access.2019.2930962.

Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal, 20*(2), 97-108. https://doi.org/10.1016/j.eij.2018.12.001.

Bansal, A., & Agrawal, A. (2017). Providing security, integrity and authentication using ECC algorithm in cloud storage. *In International Conference on Computer Communication and Informatics (ICCCI),* 1-5. https://doi.org/10.1109/ICCCI.2017.8117749

Chen, F., & Yuan, J. (2012). Enhanced key derivation function of HMAC-SHA-256 algorithm in LTE network. In Fourth International Conference on Multimedia Information Networking and Security, 15-18. https://doi.org/10.1109/MINES.2012.106

Destino, L.A., Dixit, A., Pantaleoni, J.L., Wood, M.S., Pageler, N.M., Kim, J., & Platchek, T.S. (2017). Improving communication with primary care physicians at the time of hospital discharge. *The Joint Commission Journal on Quality and Patient Safety, 43*(2), 80-88. https://doi.org/10.1016/j.jcjq.2016.11.005.

Gayathri, P., Umar, S., Sridevi, G., Bashwanth, N., & Srikanth, R. (2017). Hybrid cryptography for random-key generation based on ECC algorithm. *International Journal of Electrical and Computer Engineering, 7*(3), 1293–1298. https://doi.org/10.11591/ijece.v7i3.pp1293-1298.

Gkoulalas-Divanis, A., & Loukides, G. (Eds.). (2015). *Medical data privacy handbook.* Berlin, Germany: Springer. https://doi.org/10.1007/978-3-319-23633-9

Graves, T. (2002). A manual for developing countries. *Community Eye Health / International Centre for Eye Health, 15*(44), 64–64.

Hellberg, S., & Johansson, P. (2017). eHealth strategies and platforms–The issue of health equity in Sweden. *Health Policy and Technology, 6*(1), 26-32. https://doi.org/ 10.1016/j.hlpt.2016.09.002.

Hussein, N.H. (2019). Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3. *In 2nd Scientific Conference of Computer Sciences (SCCS),* 109-115. https://doi.org/10.1109/SCCS.2019.8852620

Cheltha, C.J.N. (2017). An innovative encryption method for images using RSA, honey encryption and inaccuracy tolerant system using Hamming codes. *In International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*, 796-799. https://doi.org/10.1109/ICCPEIC.2017.8290475

Klaib, A.F., & Nuser, M.S. (2019). Evaluating EHR and health care in jordan according to the international health metrics network (HMN) framework and standards: A case study of hakeem. *IEEE Access, 7*, 51457-51465. https://doi.org/10.1109/ACCESS.2019.2911684

Lee, Y.S., Alasaarela, E., & Lee, H. (2014). Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system. *In The International Conference on Information Networking (ICOIN 2014)*, 453-457. https://doi.org/10.1109/ICOIN.2014.6799723

Lim, C.K., Iipinge, V.J., Tan, K.L., & Hambira, N. (2018, November). Design and development of message authentication process for telemedicine application. *In IEEE Conference on Wireless Sensors (ICWiSe)*, 23-28. https://doi.org/10.1109/ICWISE.2018.8633289

Mohammed, E.A., Slack, J.C., & Naugler, C.T. (2016). Generating unique IDs from patient identification data using security models. *Journal of pathology informatics*, *7*. https://doi.org/10.4103/2153-3539.197203

Powell, A.C., Ludhar, J.K., & Ostrovsky, Y. (2017). Electronic health record use in an affluent region in India: Findings from a survey of Chandigarh hospitals. *International journal of medical informatics*, *103*, 78-82. https://doi.org/10.1016/j.ijmedinf.2017.04.011

Ruotsalainen, P.S. (2017). *Privacy, trust and security in two-sided markets*. In E-Health Two-Sided Markets, Academic Press, 65-89. https://doi.org/10.1016/B978-0-12-805250-1.00005-8

Abdulhameed, I.S. (2021). The Security and Privacy of Electronic Health Records in Healthcare Systems: A Systematic Review. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 1979-1992. https://doi.org/10.1109/ACCESS.2018.2885256.

Shankar, S.K., Tomar, A.S., & Tak, G.K. (2015). Secure medical data transmission by using ECC with mutual authentication in WSNs. *Procedia Computer Science, 70,* 455-461. https://doi.org/10.1016/j.procs.2015.10.078

Stallings, W., Bauer, M., & Hirsch, E.M. (2015). *Computer Security Principles and Practice*.

Tasatanattakool, P., & Techapanupreeda, C. (2017, December). User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy. *In 3rd IEEE International Conference on Computer and Communications (ICCC),* 1019-1024. https://doi.org/10.1109/CompComm.2017.8322697

Tchernykh, A., Schwiegelsohn, U., Talbi, E.G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36.* https://doi.org/10.1016/j.jocs.2016.11.011

Thorat, C.G., & Inamdar, V.S. (2020). Implementation of new hybrid lightweight cryptosystem. *Applied Computing and Informatics, 16*(1), 195–206. https://doi.org/10.1016/j.aci.2018.05.001

Wilson, K., & Khansa, L. (2018). Migrating to electronic health record systems: A comparative study between the United States and the United Kingdom. *Health policy (Amsterdam, Netherlands), 122*(11), 1232–1239. https://doi.org/10.1016/j.healthpol.2018.08.013

Winnie, Y., Umamaheswari, E., & Ajay, D.M. (2018). Enhancing data security in IoT healthcare services using fog computing. *In International Conference on Recent Trends in Advance Computing (ICRTAC),* 200-205. https://doi.org/10.1109/ICRTAC.2018.8679404