Mansoura Engineering Journal

Volume 46 | Issue 2 Article 2

6-8-2021

Towards a Secure E-Health System for Public Healthcare Sector in Egypt Using HL7.

Mona Mursi
is with Computer Engineering Dept, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt, monmursi@yahoo.com

May Salama
Computer Engineering Dept, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt, may.mohamed@feng.bu.edu.eg

Soha Galal
Computer engineering dept, Faculty of Engineering at Shoubra, Benha university, Cairo, Egypt., sohaemad@gmail.com

Recommended Citation

Mursi, Mona; Salama, May; and Galal, Soha (2021) "Towards a Secure E-Health System for Public Healthcare Sector in Egypt Using HL7.," *Mansoura Engineering Journal*: Vol. 46 : Iss. 2 , Article 2.
Available at: https://doi.org/10.21608/bfemu.2021.176376

Mansoura University
Faculty of Engineering
Mansoura Engineering Journal

Towards A Secure E-Health System for Public Healthcare Sector in Egypt Using HL7

Mona F. M. Mursi, *May A. Salama**, and Soha E. Galal

KEYWORDS:
electronic medical record; CDA; video consultation

***Abstract*—In this paper, we propose an eHealth system based on Health-level7 – Clinical Document Architecture targeting the public healthcare sector in Egypt. The System uses HL7, which is an international and well-recognized standard, to build electronic medical record while providing complete privacy and utmost security of patients' data. A novel property, that the system provides, is the online video consultation service which has become mandatory these days due to the widespread of COVID-19. Additionally, the system ensures the credibility of the physician's identity and practice through networking with the ministry of health and physicians' syndicate. The proposed system could also be accessible on an Android-based cell phone with all features fully functioning. Testing of the system's functionality and acceptability was conducted. It was noted that the system was well accepted by both parties; patient and physician. A comparison was carried out with other e-health systems highlighting the points of strength that the proposed system presents. The system has an extendable infrastructure that makes it flexible to integrate later with other systems.**

I. INTRODUCTION

In Egypt, the physician in public clinics deals with a huge number of patients. According to a research done by World Bank in 2018 [1], the number of physicians per thousand patients is 0.5. This makes it very difficult for physicians to manage and follow up with patients on a paper basis or in separate islands. The availability and feasibility to reach patients' medical records wherever and whenever it is needed is a key issue to enhance healthcare. The author in [2] highlighted that patients' satisfaction is a key factor to a successful health system. Many elements contribute to dissatisfaction such as commuting, waiting time, physician's interface with the patient and time allocated to the patient. The research in [3] showed the deficit in e-health for patients in the public healthcare sector in Egypt. Nevertheless, the outcome of [4] emphasized the readiness of health stakeholders to adopt an e-health system in Egypt.

The medical information and data in electronic form can be presented in different types depending on the scope and source as follows:

A. Electronic Health Record (EHR) which contains all types of information provided by clinicians who handle the patient's case. Those types could be laboratory reports, diagnosis, X-rays; or others. Patient's information could be accessed by authorized clinicians. EHRs exchange and share information with other healthcare providers, inside or across the country.

B. Personal health record (PHR) that contains the same information types as those of EHRs but patients do the management and access.

C. Electronic Medical Record (EMR) which is the digital version of the patient's paper records. EMRs are used by physicians, hospitals or clinics for diagnosis and treatment. EMRs facilitate tracking patients' data, monitoring patients

Received: (21 October, 2020) - Revised: (26 April, 2021) - Accepted: (19 May, 2021)

Mona F.M. Mursi is with Computer Engineering Dept, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt (e-mail: monmursi @ gmail.com).

****Corresponding Author:** May A. Salama., is with Computer Engineering Dept., Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt (e-mail: may.mohamed@feng.bu.edu.eg)).*

Soha E. Galal is with Computer Engineering Dept., Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt (e-mail: sohaemad@gmail.com).

(Ser. NO. BFEMU-2010-1058)

in order to improve their healthcare quality. EMR implementation is at the clinic, healthcare organization or hospital level.

The proposed system scope is to provide a medical record in electronic form that can be easily exchanged and edited for public hospitals in primary and secondary healthcare levels in Egypt. Health Level Seven (HL7) [5] is one of the most widely used standards for EMR structure. HL7 is considered the meeting point of healthcare and informatics. It avails a framework for data exchange, data sharing, data integration and retrieval through defining the way data is packaged and interchanged. This is done by determining the language, data type and structure of the data. Clinical Document Architecture (CDA) [6] is an example of forms that HL7 avails to be used in constructing the EMR. A CDA could hold various types of clinical information like Discharge Summary, Imaging Reports, Operative Note, Unstructured documents and more.

It can technically work with any other structure by editing database module only, leaving the control code untouchable which increases system edit ability, reliability and security.

Mobile view is a very important factor in building a new EMR. The system supports mobile view with all portal features. Functionality-wise, the system sets a flexible web view design through Module control view (MCV) system. The system mainly sets minimum static part of the web page and maximum on-load element creation depending on the required module. In other words, the system sets view depending on the database module using a programmed control.

The system also ensures the credibility of the physician's identity and practice through networking with the ministry of health and physician syndicate servers. This feature avoids completely any fake physicians or criminalized physicians from practicing.

A novel property that the system introduces is the online video consultation service. This service was very important to be incorporated due to the limited number of physicians in remote cities and the patients who must travel to the capital city to find a specialist to handle their diseases or simply patients who are physically incapable of traveling. Video consultation enables both patients and physicians to discuss the status and progress of their health through the video session instead of face to face. Moreover, this property is a necessity in the course of the COVID-19 pandemic since the patient and the people in contact with him are essentially isolated yet they need medical care. Physical contact between the physician and the COVID-19 patient puts the physician at great risk. Hence, video consultation while accessing the patient's EMR is a great asset.

In brief, the contribution of this paper is firstly, the use of the HL7 CDA structure in building EMR form as this is considered the first time this standard is used in Egypt. Secondly, ensuring the credibility of the physician by checking the Syndicate database for the validity of practice. Thirdly, the video consultation feature. All this is done through utmost data security standards and privacy.

The rest of the paper is organized as follows; Section II gives a brief about related work. Section III explains the proposed system. Section IV describes the security measures taken throughout the system. Section V exhibits the results and section VI concludes the work.

II. Related Work in Brief

Related work could be approached from two points of view; work done with HL7 and work done in the Egyptian healthcare sector.

A. *Related Work with HL7 Standard*

Li Xie et el [7] presented PHR system structure based on XML language, HL7 standard, Chinese Hospital Information and Digital Imaging and Communications in Medicine (DICOM). XML language allows integration with other HIS parts. The study shows a flexible system in sending and receiving patient's health information but without much focus on security. Qian Huang et el [8] showed a study of implementing a simple EHR model depending on HL7, XML, Java and XML for implementation and AES algorithm for security. Bruno M. et el [9] developed a security platform called DE4MHA which includes a set of algorithms like AES, RSA aiming to achieve confidentiality, Integrity and Authenticity for health care data exchange between patient and healthcare system through mobile phone taking into account battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. HL7 was used in [10] to build Fast Healthcare Interoperability Resources (FHIR) to exchange healthcare information. FHIR was constructed to enhance the exchange and integration of patient's data among different hospital services and radiology service. The research [11] draws a conclusive table presenting different researches using HL7 in constructing EMR, PHR and EHR.

B. *Related Work in the Egyptian Healthcare Sector*

In 2013, the authors of [12] , concluded that Egypt was very much behind in adopting EHR/EMR in hospitals that follow international standards. Few hospitals applied electronic systems but were very localized to their needs. In 2017, a paper was issued that briefed three trials of e-health implementation [13]. The first two were in cooperation with private companies and stopped for financial issues. They were to implement EMR. The first trial was not on the national level. The second trial had some technical and administrative barriers. The third trial was an accreditation program. There were two problems with this trial. First, no standard criteria were set to implement the medical record. Second, no mention of turning the medical records to EMR. The author in [2] proposed a password-based EMR system that had many vulnerabilities, among which the security method, integration and exchange of data among different entities and lack of mobile application.

It can be noted that although there were trials to transform into electronic records, there was no coherent approach to build a system on an international standard that could fit the different public healthcare entities. To the best of our knowledge, there was no work done on HL7 implementation for Egypt's healthcare system. However, a positive outcome of [4] emphasized the readiness of health stakeholders to adopt an e-health system in Egypt. It also revealed the concern of data privacy.

III. Proposed System

The proposed EMR system aims to provide a secure unified EMR that keeps patient’s basic and medical data from all public hospitals, clinics and primary care centers, located all over Egypt, into one centralized database belonging to the ministry of health (MOH). The stakeholders are: patient, physician, MOH and Physicians’ Syndicate. The overall system can be summarized by the class diagram, illustrated in Fig. 1 showing the relationship between the main entities.

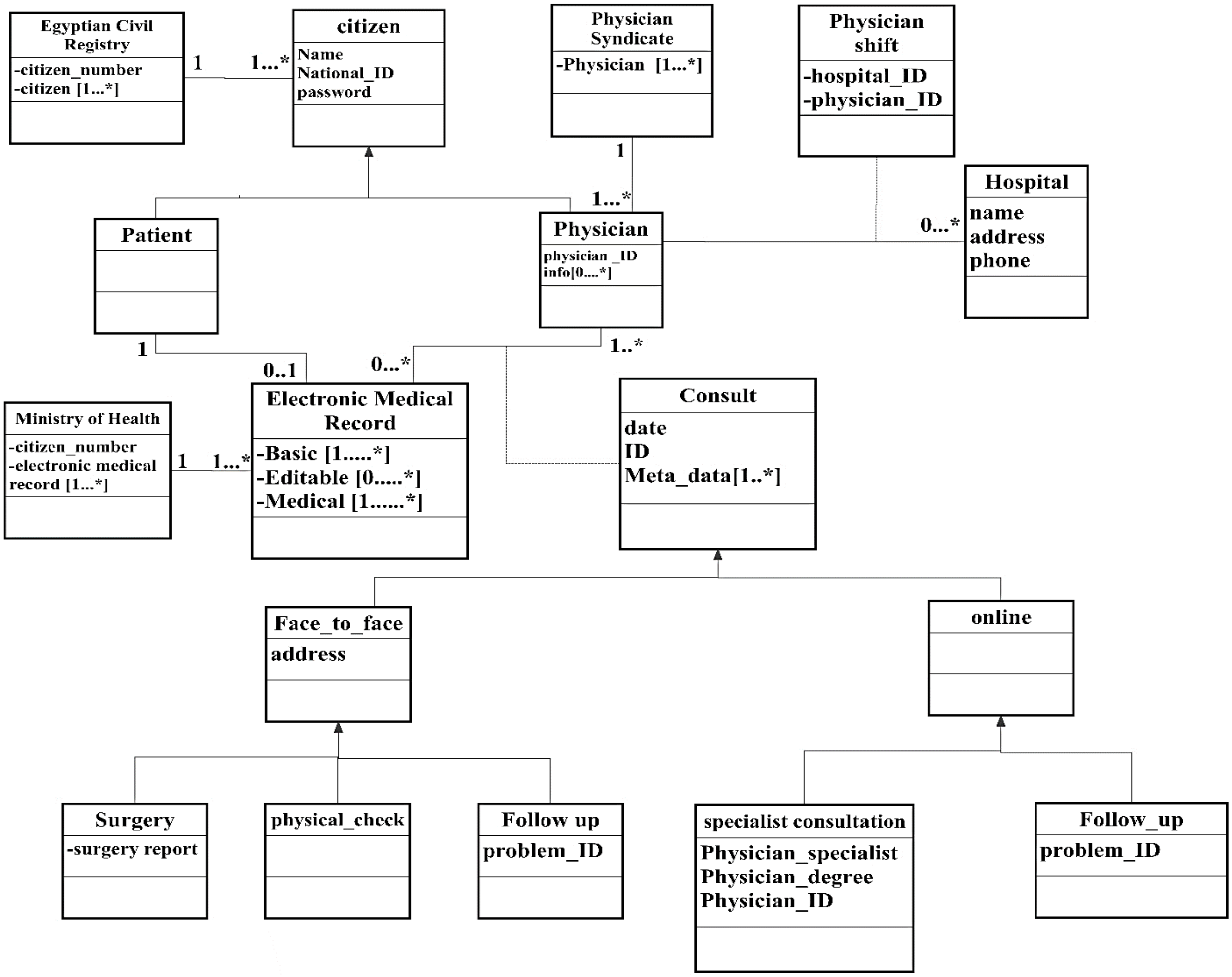


Fig. 1 Class diagram of the implemented system

The database consists of five main sets of tables as follows:

1. Basic Information Regarding:

a. Patient's information: national ID number, name, activation state (alive/dead), basic personal information.

b. Physician's information: national ID number, name, account activation state, specialty and basic personal information.

c. MOH employees’ information: employee national ID number, name, authorization level and basic personal information.

d. Physicians syndicate employee's information: employee national ID number, name, authorization level and basic personal information.

2. Hospitals' Information:

a. Hospitals' list: containing a set of Egyptian hospitals IDs, addresses and contact information.

b. Hospital- physician *information*: mapping between physicians and hospitals they work at.

3. *Patient Editable Information: patient's family medical history, next of kin ...etc.*

4. *Patient medical information: It is presented as a set of tables which can be read by the patient and physicians but the write access is only for the physicians, Data in those tables contain patient's medical problems, allergies, immunization ...etc.*

5. *Log Information: activities done by all who got access to the system database in details such as operation type, the time/date and the information accessed.*

6. *Online Medical Consultation Information: a set of information about consultation request from a patient to physician* and the date booked for the patient’s online consultation request.

Create, Read or Report, Update, and Delete (CRUD) are the different operations that are done by the system’s entities. Table I demonstrates the operations feasible for each entity.

TABLE I
CRUD OPERATIONS FOR EACH ENTITY

Entity	Operation	Resulting use case
Physician	Create	• Activate Account • Report Illness Case • Review/create statistics for his work • Book specialist online consultation • Book follow up
	Read	• Access Account • Access Conscious Patient's EMR • Access Unconscious Patient's EMR • View Online Consultation Requests
	Update	• Update Account information • Add Information to Patient's EMR • Set Dates for Online Consultation Requests • Temporary stop online consultation service
	Delete	• Permanently stop online consultation service
Patient	Create	-------------
	Read	• Search a physician • Access EMR.
	Update	• Evaluate Physician • Activate EMR • Update Editable Information • Forget Password
	Delete	-------------
Ministry of Health (MOH)	Create	• Add EMR • Create statistics
	Read	View Patient(s) Record(s)
	Update	Drop EMR
	Delete	-------------
Physicians syndicate	Create	• Add Physician Account
	Read	• View Physician(s) information
	Update	• Revoke Physician Account • Reactivate physician online consultation service
	Delete	-------------

To implement the system, the CDA and Database structures should be constructed first.

A. *CDA Structure*

CDA [6], [14] is an XML document with 2 divisions. The first is a Header that contains patient information, author, creation date, document type, provider and other related information. The second is the Body that contains information like admission details, diagnosis, patient details, medications and follow-up written as free text in one or multiple sections. It may optionally include coded entries.

CDA has three levels of document definition.

- Level 1 keeps the basic outline structure of the header and body. It allows using unstructured language or blocks inside the body and the header, thus, the patient can easily follow up.

-Level 2 uses structured XML-based sections in the body where a section is identified with a code.

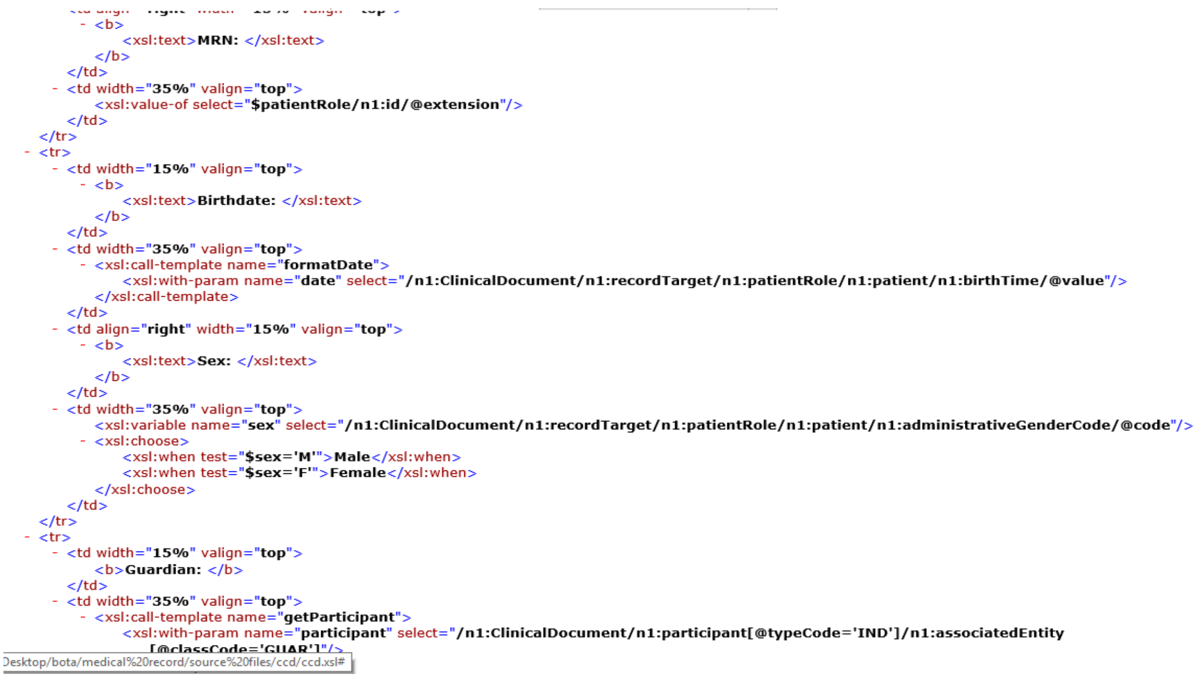
-Level 3 is the most complex as it should include a CDA header plus an XML body with narrative blocks and entries. These sections should be encoded.

The CDA full raw material is an XML file that should be converted into another form like pdf, doc, HTML to be readable by the human eyes. Hence, the first phase is to create an application capable of converting XML CDA into an HTML file. Fig. 2 illustrates an input CDA XML file fragment.

The HTML file contains a set of tags that indicates the style of the set of information and data. Therefore, another file is needed to indicate the style and structure of the HTML file. An XSLT style sheet is used along with XML to output the HTML file.

Once the GUI is built, the user can edit – based on his access level.

The Continuity of Care Document (CCD) is built on CDA using a set of templates and constraints to allow physicians to share medical information electronically with others.



```
      <td align="right" width="15%" valign="top">
      - <b>
          <xsl:text>MRN: </xsl:text>
        </b>
      </td>
    - <td width="35%" valign="top">
        <xsl:value-of select="$patientRole/n1:id/@extension"/>
      </td>
    </tr>
  - <tr>
    - <td width="15%" valign="top">
      - <b>
          <xsl:text>Birthdate: </xsl:text>
        </b>
      </td>
    - <td width="35%" valign="top">
      - <xsl:call-template name="formatDate">
          <xsl:with-param name="date" select="/n1:ClinicalDocument/n1:recordTarget/n1:patientRole/n1:patient/n1:birthTime/@value"/>
        </xsl:call-template>
      </td>
    - <td align="right" width="15%" valign="top">
      - <b>
          <xsl:text>Sex: </xsl:text>
        </b>
      </td>
    - <td width="35%" valign="top">
        <xsl:variable name="sex" select="/n1:ClinicalDocument/n1:recordTarget/n1:patientRole/n1:patient/n1:administrativeGenderCode/@code"/>
      - <xsl:choose>
          <xsl:when test="$sex='M'">Male</xsl:when>
          <xsl:when test="$sex='F'">Female</xsl:when>
        </xsl:choose>
      </td>
    </tr>
  - <tr>
    - <td width="15%" valign="top">
        <b>Guardian: </b>
      </td>
    - <td width="35%" valign="top">
      - <xsl:call-template name="getParticipant">
          <xsl:with-param name="participant" select="/n1:ClinicalDocument/n1:participant[@typeCode='IND']/n1:associatedEntity
            [@classCode='GUAR']"/>
```

Desktop/bota/medical%20record/source%20files/ccd/ccd.xsl#

Fig. 2 HL7 CDA XML file fragment

B. Database Structure

The database used consists of the following sets of tables:

Basic information about all stakeholders in the system; namely Patients, Physicians, MOH employees and Physicians syndicate employees.

Hospitals' information containing a set of Egyptian hospitals IDs, addresses and contact information. It also contains the mapping information between physicians and hospitals they work at.

Patient Editable information: which is the patient's family medical history, next of kin and other family information.

Patient medical information: It is presented as a set of tables that can be read by the patient and physician but the write access is only for the physician.

Log information: It is the activities done by all who got access to the system database in detail such as operation type, the time/date and the information accessed.

Online medical Consultation information: it contains a set of information about consultation request from a patient to a physician and the date booked by the physician for the patient’s request.

After constructing the structures, functionality will be implemented.

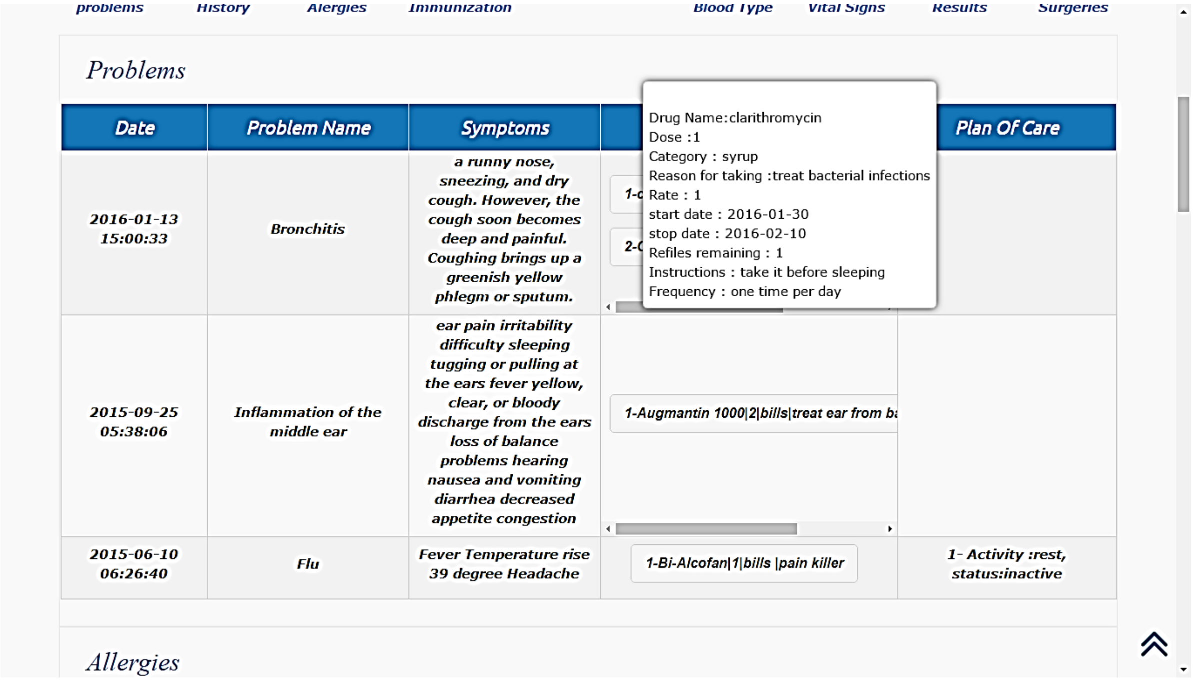
C. System Functionality Implementation

The main two participants in the system are the patient and the physician. After building the system each of them will deal with the system through a set of actions; each of which necessitates security implementation.

1) EMR access system implementation for the patient.

For a patient, to acquire an eligible EMR, he should send a one-time request to MOH to create an account with his credentials. Once created, the Patient can access his medical record whenever he wants and wherever he is through the web or smartphone after being authenticated by his national id and password. The Patient has a read-only privilege on his medical and basic data. However, he can edit his family medical history and next of kin information. Fig. 3 displays the patient’s EMR when requested by the patient.

For the first-time patient’s registration, a pre-check is done online, using the National id number, on the database residing on the MOH server to confirm that the applicant is an Egyptian citizen.



Problems

Date	Problem Name	Symptoms		Plan Of Care
2016-01-13 15:00:33	Bronchitis	a runny nose, sneezing, and dry cough. However, the cough soon becomes deep and painful. Coughing brings up a greenish yellow phlegm or sputum.	1-c 2-C	
2015-09-25 05:38:06	Inflammation of the middle ear	ear pain irritability difficulty sleeping tugging or pulling at the ears fever yellow, clear, or bloody discharge from the ears loss of balance problems hearing nausea and vomiting diarrhea decreased appetite congestion	1-Augmantin 1000|2|bills|treat ear from ba	
2015-06-10 06:26:40	Flu	Fever Temperature rise 39 degree Headache	1-Bi-Alcofan|1|bills |pain killer	1- Activity :rest, status:inactive

Drug Name:clarithromycin
Dose :1
Category : syrup
Reason for taking :treat bacterial infections
Rate : 1
start date : 2016-01-30
stop date : 2016-02-10
Refiles remaining : 1
Instructions : take it before sleeping
Frequency : one time per day

Allergies

Fig. 3 EMR view for patient

2) EMR access system implementation for physician

The role of the physicians’ syndicate is to keep track of the status of physicians; being authorized or not to practice. A physician should have a valid active work permit and account in order to practice. The physician sends a request to create an electronic account in the syndicate’s database. The syndicate employee reviews the physician’s data to verify it. If verified the account is created where the status is valid active permit. If the physician commits any violation, the account is revoked by the authorized employee and the system bans his name.

On the physician side, first, a pre-check is done with the physicians’ syndicate database to validate that physician. If valid, the physician can access a patient’s medical record. This access is committed only if the patient gives him access right through entering the patient’s national id and a password entered by the patient in the physician’s system. When the physician accesses a patient’s record, a new session begins where the physician can read or insert data but not update any previous data in the record. Whenever the patient leaves or the session ends, the physician can’t retrieve the patient’s medical record.

The physician can use the system to make some statistics about his work as the number of visits per day, patients with certain illnesses.

The techniques used on the client-side are HTML, Javascript and JSON while those used on the server-side are WAMP (Windows System Apache 2 PHP and MySQL).

The Client-side is on the patient and physician devices (desktop) while the Server side is the MOH database management system.

3) Mobile-based EMR system implementation

Implementing a mobile-based electronic medical record system increases the system availability for the users and communication ability in emergency cases.

The proposed EMR mobile system uses the same scenarios as those used in the web application. The security level is the same as is in web application except that the client-side is Android KITKAT instead of HTML and JavaScript.

4) Online Video consultation implementation

Online video consultation is a medical service that allows the patient to get in contact with the physician, face to face virtually, through a video call. This is very important in rural areas that lack the availability of medical specialists as well as for patients with movement hindrance or hazardous conditions. Not only that, but very important during the pandemic time when patients should be isolated and yet receive medical treatment to reduce the increase in infections.

Remote Video consultation aims to introduce a secure video communication session between physician and patient. The system proposes two scenarios; Follow up with the patient after an in-person visit and seeking second opinion consultation. Physician’s access to data is based on the Attribute-Based Access Control (ABAC) module that grants access based on a set of variable features editable by patient and physician.

IV. Security and Privacy

The proposed system provides authentication, confidentiality, integrity and non-repudiation. Fig. 4 shows the use case diagram of the basic mechanism and procedures for the proposed system.

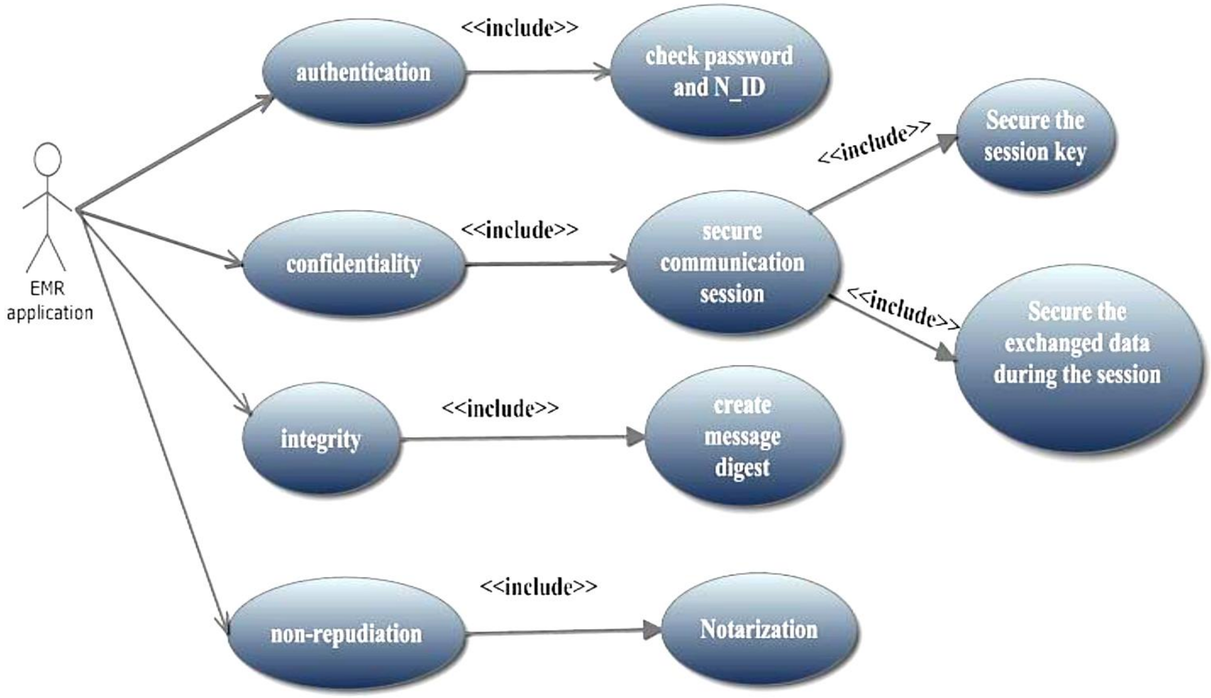


Fig. 4 Use case diagram for basic mechanism and procedures

A. Privacy

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) is a federal law that demanded the creation of national standards to assure the protection of sensitive health data of the patient against disclosure without his consent. Since currently there are no such Egyptian national standards, the proposed system uses HIPPA to set main privacy. All security aspects have been implemented in the proposed work to assure the privacy of patients’ data.

B. Access Control

There are several types of access control. Role-based access control (RBAC) where a group accesses classified data and performs a certain number of services based on the group’s role. Context-based access control (CBAC) in which the system sets data access based on the content and user role. Policy-based access control (PBAC) where a set of rules in a policy file indicates what a user can access and do. The proposed system uses Attribute-based access control (ABAC) module which is based on defining a set of features editable by the patient and physician. Access management is mainly controlled by patients except in very special cases like inpatient and statistical work.

MOH: The proposed system creates a new empty EMR for an Egyptian citizen in the database of MOH. MOH employee will sign in using his user name and password given by the system administrator. He is not authorized to visit any user's personal information. MOH employee can only register new users "Patients" by activating their EMR and deactivating their account using their national IDs if the patient is deceased. MOH employee can't reveal any patient medical information.

Patients: will sign in with a username and password that were set by him after signing up and his identity is confirmed by MOH. He can only access his medical records. Patients cannot add or delete their medical records' information. The patient is authorized only to edit emergency contact and family medical history. Patients can authorize physicians to access their medical records.

Physicians: will sign in by username and password that were set by him after signing up. A physician can access a patient's records if the patient allows the physician. This is done when the patient first enters his username and password. This will allow the physician to view/edit the medical record within 30 minutes, after that the physician will be automatically logged out and he won't be able to view or edit the patient's medical record. Physicians can add new records for the patient but cannot modify the contents of the existing medical records.

Physician Syndicate: Physician syndicate authorized employee will sign in by a given username and password from the system administrator. He is not authorized to visit any user's personal information. He can only register/ revoke Physicians by activating/ deactivating their accounts using their national IDs and physician ID number.

C. Login Authentication

It is established using powerful encryption and salted hash techniques on the user side and digital signature on the server. On a sign-in page, the user enters the User Name, National ID and password. A sign-in request to the server is initiated which in turn creates a new random salt and signs it by server RSA key to prove server identity. The server sends the signed salt to the client to verify it and extracts the salt then concatenates it with the password hash to represent the new salted password. The hash of the salted password is completed and combined with the inserted name and National ID. The result is plain text that is encrypted by the server's public key to create the ciphertext and then sent to the server. Fig. 5 shows the flowchart for the authentication process.

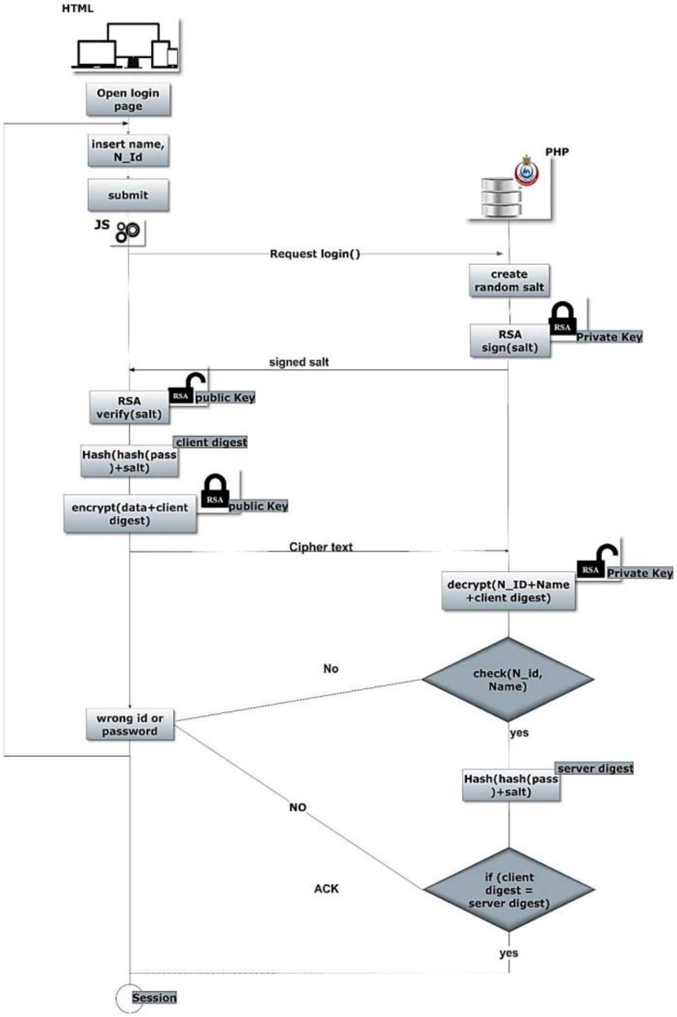


Fig. 5 Flowchart for the authentication process

D. Confidentiality on the Server-Side

It is achieved using AES 256 symmetric key encryption and protected through a secure OpenSSL connection between the main server and distributed database servers. Information exchange between the main server and users is done through a session secured by Asymmetric 1024 RSA for session key exchange and 256 AES for exchanged data. Each message should be digitally signed by the sender to ensure its authenticity and integrity. System digital signature uses SHA256 of the encrypted message as message digest then is encrypted both by sender private key. The system monitors all users' access and actions for auditing. All-access logs are kept on the MOHP side as a trusted third party between patient and physician to ensure non-repudiation.

After the session key is exchanged in a secure way between the user and the system, the second level of security begins by applying a symmetric key cryptography algorithm.

Two factors were used to choose the symmetric key cryptography algorithm; immunity against attacks and speed. AES is the last symmetric key cryptographic algorithm approved by the NIST in 2001 [15] based on its immunity to many attacks like brute force, statistics, linear and differential attacks.

Based on [16], the AES algorithm gave the best results in terms of speed and security in encryption and decryption operations in comparison to triple Data Encryption Standard (3DES), RC4, and Blowfish. Accordingly, the AES algorithm was chosen. So, the session key includes the AES randomly created key and IV algorithm specification and exchanged securely by using RSA at the beginning of each session. Each message is padded with one of the AES padding algorithms which is also sent along with the session key.

The two levels of security algorithms applied in the beginning and during the session ensure communication confidentiality.

E. System Integrity

The sender (client or server) sends a hash of the sent data along with the secured message through the secure timed session. On the receiver side, a new hash value of the message is created by the same hash algorithm used on the sender side. It is then compared to that of the sender side. If both are equivalent, then the message was not altered.

F. MOH Role

The main users of the system are the patient and the physician. Any operation involves MOH functioning as a third party to ensure non-repudiation of any user operations. For example, if a physician wants to view a patient EMR, the physician sends a request to the MOH server, not to the patient, and the server waits for the patient's permission to send the EMR to the physician. At the beginning of any communication between the user (patient or physician) and the MOH system, a check operation is applied to authenticate the user. This is done by comparing the national ID and the hash of the password inserted by the user against the one in the MOH database. The real password is never transferred in the system even with using secure channels, to avoid attacks that would violate the users' privacy. The hash algorithm used in the system is SHA 512.

G. Session Operation

At the start of each session, a set of session features called session key is exchanged between the system and the user. The direction and type of features are set based on the user's operation.

The session key includes very sensitive and important data related to the session security system. Therefore; it must be secured. RSA asymmetric key cryptography algorithm is applied to encrypt the session key. RSA is a very efficient algorithm and immune against many attacks like a chosen cipher. Although the RSA algorithm is not a fast algorithm when using a big amount of data, it works fine with the proposed system because it's applied only on the session key which includes a very small set of data.

All system stakeholders can insert and view data. In every new session, the client-side creates a random AES Key and IV work as a session key for one session only and shared by the server in a secure channel. Client-side encrypts session key by RSA public key and sends encrypted data to the server. The server decrypts ciphertext to get the session key to use in securing query result.

A data request is sent to the server. The Server applies the required query to the database. The query result is then encrypted by the session key and sent to the client-side. The Client-side decrypts the data and displays it. All the retrieved pages are database driven which means any change in the server database will reflect on the loaded page. Fig. 6 shows the retrieve process.

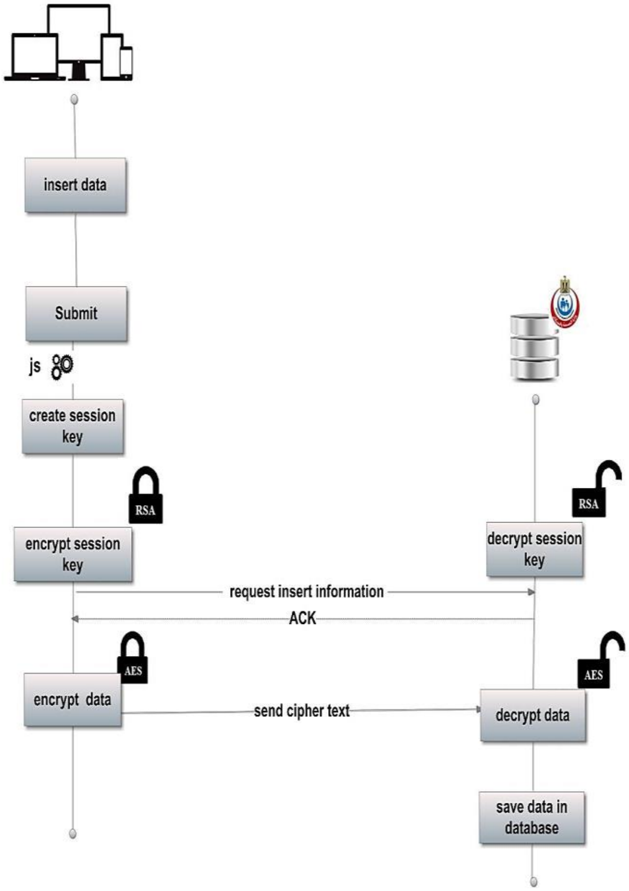


Fig. 6 Flow chart for retrieving data

The proposed security system makes EMR immune against impersonating attacks, such as man in the middle, through the PKI signing algorithm.

The whole authentication process is done by RSA algorithm with SHA1 signing algorithm and hashed salted password by SHA 256 function.

V. REMOTE VIDEO CONSULTATION

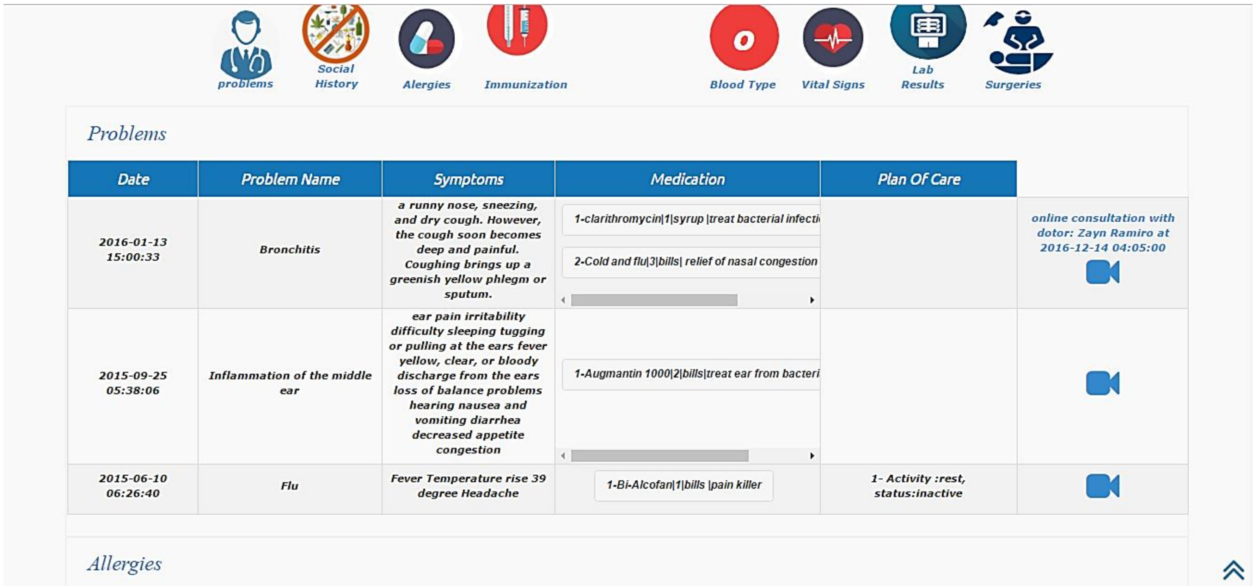
This service is no more a commodity. Other than being essential for patients who suffer from movement consequences or live distant from healthcare service, it is in high demand since the spread of the COVID-19 pandemic.

To implement this service, Web Real-Time Communication (WebRTC) is used. It is a collection of communications protocols and APIs that avails real-time communication over peer-to-peer connections. It requires no plugins and allows web browsers to request resources from backend servers as well as real-time information from browsers of other users. All security aspects are applied during the video session.

The consultation request could either be a follow-up request or a consultation request to a specialist. The request is saved in the database with a unique ID, patient ID, and physician ID.

The consultation request that the patient sends to the physician contains only the problem/complaint that the patient wants consultation on. The patient can upload tests, comments, and medical images that would help in the diagnosis and choose from already existing images In some cases, the physician would need to refer to the patient's medical record for more details. The physician can access the EMR only if he sends a request to the patient and the patient accepts. If so, the physician will be offered a one-time working link to view the patient's EMR.

Fig. 7 displays the screen for a specific problem selection to consult on which will be the only information in the EMR to be sent to the physician.



Problems

Date	Problem Name	Symptoms	Medication	Plan Of Care	
2016-01-13 15:00:33	Bronchitis	a runny nose, sneezing, and dry cough. However, the cough soon becomes deep and painful. Coughing brings up a greenish yellow phlegm or sputum.	1-clarithromycin|1|syrup |treat bacterial infecti 2-Cold and flu|3|bills| relief of nasal congestion		online consultation with dotor: Zayn Ramiro at 2016-12-14 04:05:00 📹
2015-09-25 05:38:06	Inflammation of the middle ear	ear pain irritability difficulty sleeping tugging or pulling at the ears fever yellow, clear, or bloody discharge from the ears loss of balance problems hearing nausea and vomiting diarrhea decreased appetite congestion	1-Augmantin 1000|2|bills|treat ear from bacteri		📹
2015-06-10 06:26:40	Flu	Fever Temperature rise 39 degree Headache	1-Bi-Alcofan|1|bills |pain killer	1- Activity :rest, status:inactive	📹

Allergies

Fig. 7 Selecting the problem for video consultation

VI. Results and Discussion

To evaluate the system, both patients and physicians were asked to operate the system and test its functionality. Tailored questionnaires were carried out for each party. Responses were calibrated on a 1-4 scale, where 1 is the best and 4 is the least.

A. *Patients' Satisfaction with the System*

A sample of 80 patients participated in the evaluation. The sample consisted of educated graduates and undergraduate students who work well with electronic devices, have good English knowledge and accept the idea of EMR. Comprehensive results with their breakdown on each scale value are shown in Table II. The last column shows the range of acceptance. Minimum acceptance depicts the total value of scales 1+2 while maximum acceptance represents the total value of scales 1+2+3.

TABLE II
PATIENTS FEEDBACK ABOUT THE SYSTEM

Feature Tested	1	2	3	4	Min- Max Acceptance
Functionality of the System	75%	15%	10%	0%	90-100%
GUI	50%	25%	15%	10%	75-90%
Extent to reach information	60%	20%	10%	10%	80-90%
Extent to edit information	60%	20%	10%	10%	80-90%
Time efficiency	55%	35%	5%	5%	90-95%
System will be effective in Egypt	45%	45%	5%	5%	90-95

The option of having Arabic language along with English was highly recommended.

B. *Physicians' Satisfaction with the System*

A sample of 50 physicians participated in the evaluation. The sample was biased towards fresh grads and young physicians who welcome working on electronic devices. The questionnaire was carried in three different public hospitals where each physician tried the system on a case of his choice. Results are shown in Table III. Physicians were concerned about two issues. The first was the training period and the second was the way history data of the patients would be input into the system. The results of the evaluation with the breakdown are presented in Table III.

TABLE III
PHYSICIANS' FEEDBACK ABOUT THE SYSTEM

Feature Tested	1	2	3	4	Min- Max Acceptance
Functionality of the System	65%	20%	15%	0%	85-100%
GUI	55%	30%	0%	15%	85%
Extent to reach his or patient's information	65%	20%	5%	10%	85-90%
Extent to edit his or patient's information	65%	20%	5%	10%	85-90%
Time efficiency	45%	30%	15%	10%	75-90%
System will be effective in Egypt	50%	30%	15%	5%	80-95%

C. Security Features Comparison

The system has been compared with other systems that were proposed during recent years in terms of security and privacy features.

It could be concluded that all security aspects have been taken into consideration and implemented. Login is established using encryption and salted hash techniques on the user side and digital signature on the server. ABAC module is used based on a set of variable features editable by patient and physician. Confidentiality on the server-side is achieved using AES 256 symmetric key encryption and protected through secure open SSL connection between main server and distributed database servers. Information exchange between the main server and users is done through a session secured by Asymmetric 1024 RSA for session key exchange and 256 AES for exchanged data. Each message should be digitally signed by the sender to ensure its authenticity and integrity. System digital signature uses SHA256 of the encrypted message as message digest then encrypts both by sender private key. The system monitors all users' access and actions to keep track of audit trials. All-access logs are kept on the MOH side as a trusted third party between patient and physician to ensure non-repudiation. Table IV illustrates the results.

D. Comparison between Proposed Work Portal and Other Operating Portals

It is worth noting that in the proposed work, Remote consultation avails a secure video communication session between physician and patient. Physician's access to data is ABAC.

The system supports mobile view with all portal features. Functionality-wise, the system sets a flexible web view design through Module control view (MCV) system.

Table V concludes the features comparison of the proposed portal with other portals.

TABLE IV
SECURITY FEATURES COMPARISON

Reference	Authentication	Access Control	Access Management	confidentiality	Integrity	Audit Log
Proposed system	Mutual authentication using salted hashed password with username and NID in encrypted form and on server side Digital certificate	ABAC	patient can control fully and selective sharing	AES 256	digital signature	encrypted log file
[17]	Certificate on smart card RBAC	PBAC	Patient	AES	NA	Access log
[18]	User name and password	PBAC	Patient control	Attribute based encryption (ABE)	NA	NA
[19]	NA	NA	NA	NA	NA	NA
[20]	ID based digital signature	RBAC	Professional	Asymmetric encryption	NA	Access record
[21]	NA	RBAC	patient	NA	NA	comply HIPPA
[22]	NA	RBAC	patient	NA	NA	access record
[23]	NA	RBAC	patient	Asymmetric encryption	Message authentication code HMAC	xxx
[24]	NA	policy	patient	Asymmetric key cryptography	NA	third party
[25]	digital signature	NA	NA	Asymmetric key cryptography	Digital signature	NA
[26]	Password with digital signature in zip file	policy	patient	AES 256	NA	NA
[27]	password	policy	patient	EL Gamal	NA	NA
[28]	NA	PASS access control	NA	NA	NA	PASS audit trial control
[29]	unique ID with digital certificate	ABAC	Policy-Based	ABE	NA	NA
[30]	login	RBAC	Policy-Based	NA	NA	audit log

TABLE V
PORTAL SERVICES COMPARISON

Portal	**Access control**	**Access management**	**Authentication**	**Remote consultation**	**Integrity**	**Mobile view / app**	**Audit trial**
Proposed work	ABAC	patient	Mutual authentication using a salted hashed password with username and NID in encrypted form and on server-side Digital certificate	Video consultation	Digital signature	Yes	yes
www.sundhed.dk	RBAC	Physician	Digital signature stored on code file or smart card with login by user ID and password	Email consultation	Digital signature	Yes	yes
infoway.com	RBAC	Profession	Smart card with login by user name	Telehealth program	Digital signature	Yes	yes
healthhub.sg	RBAC	Profession	Login bypass ID and password	Smart Health Video Consultation	Digital signature	Yes	yes

VII. CONCLUSION

In this paper, we proposed a comprehensive prototype for a secure EMR system adapted to the public healthcare sector in Egypt using the HL7 standard which is considered the cross point between healthcare and information technology. It is a worldwide standard that can be integrated into other systems. To the best of our knowledge, this is the first HL7 system to be proposed for the Egyptian healthcare sector.

Interviewing and answering questionnaires by the physicians and patients were used to collect data, evaluate and understand the requirements to adapt HL7 CDA for local use. A remote video consultation system was established and implemented to facilitate medical services across the country. This is necessary not only to reduce the patients' queues and waiting time in hospitals and clinics but most importantly to help COVID-19 patients receive medical treatment. Moreover, this service will facilitate medical care for patients who suffer from difficulties in moving. A standalone service was set to perform the remote medical consultation services with high concern of security aspects in consultation sessions.

On the audit side of the system, we faced many obstacles. One of the main obstacles was the pronounced difference in the work environment, system and problems in most hospitals although they are all under the umbrella of the Ministry of Health. In addition, shortage of computers and electronic resources in some hospitals and their absence in others were also a hindrance in the audit phase. The weakness in computer skills and the English language for most administrative and medical staff assistants made it more difficult during the various phases of system development.

Finally, installing a pilot system in a public health sector hospital was impossible as it required many authorizations that were beyond our capabilities. Hence, we couldn't conduct a real-time test to assess the performance on the right scale and identify weaknesses and strengths in a real-time environment. The testing was performed on a private level base.

REFERENCES

[1] T. W. Bank, "Physicians per (1000 people)," 2018. [Online]. Available: https://data.worldbank.org/indicator/SH.MED.PHYS.ZS. [Accessed 21 09 2020].

[2] H. Mohamed, "A model for computerization and implementation of electronic health records in primary health care in Egypt," Journal of Community Management, vol. 3, no. 1, p. 1017, 2020.

[3] M. Mursi, M. Salama and S. Galal, "E-Health in Egypt: A Brief Review," in Proceedings of the 5th International Conference on Digital Health 2015, Florence, 2015.

[4] M. Badran, "eHealth in Egypt: The demand-side perspective of implementing," Telecommunications Policy, no. 43, pp. 576-594, 2019.

[5] "HL7," HL7 International, 1987. [Online]. Available: www.HL7.org. [Accessed 03 October 2020].

[6] "CDA Release2," HL7 International, [Online]. Available: HTTP://WWW.HL7.ORG/IMPLEMENT/STANDARDS/PRODUCT_BRIEF.CFM?PRODUCT_ID=7. [Accessed 03 october 2020].

[7] L. Xie, C. Yu and L. e. a. Liu, "XML-based Personal Health Record system," in 3rd International Conference on Biomedical Engineering and Informatics, Yantai, 2010.

[8] Q. Huang and Q. Yin, STUDY ON ELECTRONIC HEALTH RECORD AND ITS IMPLEMENTATION, MASTER THESIS, School of Health and Society, 2012

[9] B. Silva, J. Rodrigues and F. e. a. Canelo, "TOWARDS A COOPERATIVE SECURITY SYSTEM FOR MOBILE-HEALTH APPLICATIONS," Electronic Commerce Research, vol. 19, p. 629–654, 2018.

[10] MAXHELAKU and A. Kika, "Improving Interoperability in Healthcare using HL7 FHIR," in 47th International Academic Conference, Prague, 2019.

[11] R. Saripalle, C. Runyan and M. Russell, "Using HL7 FHIR to achieve interoperability in patient health record," Rishi SaripalleChristopher RunyanMitchell Russell, vol. 94, 2019.

[12] A. Sharaf Eldin, D. Saad and S. Ghada.A., "Evaluation of Electronic Health Records Adoption in Egypt," nternational Journal of Engineering Research and Applications (IJERA), vol. 3, no. 1, pp. 1131-1134, 2013.

[13] S. Abd Elgaber, A. Abdel-Fattah M and M. Helal S, "A Roadmap to Implement EHR Nationwide in Egypt," Communications on Applied Electronics (CAE) , vol. 7, no. 6, 2017.

[14] R. e. a. Dolin, "HL7 Clinical Document Architecture, Release 2," Journal of the American Medical Informatics Association, vol. 13, no. 1, 2006.

[15] N. I. o. S. a. T. NIST, "Block Cipher Techniques," 2001. [Online]. Available: https://csrc.nist.gov/projects/block-cipher-techniques. [Accessed 03 October 2020].

[16] H. Agrawal and M. Sharma, "Implementation and Analysis of Various Symmetric Cryptosystems," Indian Journal of Science and Technology, vol. 3, no. 12, 2012.

[17] B. Elger and J. e. a. Iavindrasana, "Strategies for health data exchange for secondary, cross-institutional clinical research," Comput Methods Programs Biomed, vol. 3, 2010.

[18] S. Narayan, M. Gagne and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010.

[19] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in IEEE International Conference on Cloud Computing, CLOUD 2010, Miami, 2010.

[20] S. J and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems , vol. 21, no. 6, 2010.

[21] A. AL Faresi, D. Wijesekera and K. Moidu, "A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules," in Proceedings of the 1st ACM International Health Informatics Symposium, 2010.

[22] C. Ardagna, S. di Vimercatia and S. e. a. Foresti, "Access control for smarter healthcare using policy spaces," Computers & Security, vol. 29, no. 8, 2010.

[23] M. Jafai, R. Safavi-Naini and C. e. a. Saunders, "Using digital rights management for securing data in a medical research environment," in Proceedings of the tenth annual ACM workshop on Digital rights management, 2010.

[24] J. Jin, H. Hu and M. e. a. Covington, "Patient-centric authorization framework for electronic healthcare services," Computers & Security, vol. 30, no. 2, 2011.

[25] C. Quantin, D. Jaquet-Chiffelle and G. e. a. Coatrieux, "Medical record search engines, using pseudonymised patient identity: An alternative to centralised medical records," International Journal of Medical Informatics, vol. 80, no. 2, 2011.

[26] W. Jiana, H. Wen, J. Schollb and e. al, "The Taiwanese method for providing patients data from multiple hospital EHR systems," Journal of Biomedical Informatics, vol. 44, no. 2, 2011.

[27] P. Deshmukh, "Design of cloud security in the EHR for Indian healthcare services," Journal of King Saud University - Computer and Information Sciences, vol. 29, no. 3, 2017.

[28] G. Gazzarata, R. Gazzarataa and M. Giacominiab, "A Standardized SOA Based Solution to Guarantee the Secure Access to EHR," Procedia Computer Science, vol. 4, 2015.

[29] D. Chen and e. al, "Securing patient-centric personal health records sharing system in cloud computing," China Communications,, vol. 11, no. 13, 2014.

[30] J. Li, "A Service-Oriented Approach to Interoperable and Secure Personal Health Record Systems," in IEEE Symposium on Service-Oriented System Engineering, San Francisco, 2017.

Title Arabic:

نحو نظام صحة إلكتروني آمن لقطاع الرعاية الصحية العامة في مصر باستخدام المستوى الصحي 7

Arabic Abstract:

يقدم هذا البحث نظاما للصحة الإلكترونية يستهدف قطاع الرعاية الصحية العامة في مصر. تم بناء النظام المقترح على أساس المستوى الصحي 7 - هندسة الوثائق السريرية ، والذي.يعتبر معيارا دوليا ومعترفا به جيدًا ، لبناء السجل الطبي الإلكتروني مع توفير الخصوصية الكاملة والأمان الأقصى لبيانات المرضى. الخاصية الجديدة والمتميزة التي يوفرها النظام هي خدمة الاستشارات عبر الفيديو التي أصبحت ضرورية هذه الأيام بسبب انتشار كوفيد-19. بالإضافة إلى ذلك ، يضمن النظام مصداقية هوية الطبيب وممارسته من خلال التواصل مع وزارة الصحة ونقابة الأطباء. يمكن أيضًا الوصول إلى النظام المقترح على هاتف محمول يعمل بنظام اندرويد مع تشغيل جميع الميزات بشكل كامل. تم إجراء اختبار لوظائف النظام ومدى قبوله. ولوحظ أن النظام يحظى بقبول الطرفين ؛ المريض والطبيب. تم إجراء مقارنة مع أنظمة الصحة الإلكترونية الأخرى وتسليط الضوء على نقاط القوة التي يقدمها النظام المقترح. يحتوي النظام على بنية تحتية قابلة للتمديد تجعله مرنًا للتكامل لاحقًا مع الأنظمة الأخرى.