A Model for Exchanging Secure Information between Ophthalmologists

ArwaAlKowiter, TaghreedAlOtaibi, Khawla Al-Rajhi & NahedAlSahdi
Prince Sultan University
Riyadh,Saudi Arabia
arwa1990.aa@gmail.com, taghreed-d@live.com, k_alrajhi@hotmail.com & nahed-al9hdi@live.com

Norah Alhammad
Tamkeen Technologies
Riyadh,Saudi Arabia
norah.a.alhammad@gmail.com

***Abstract*—With a wide variety of eye problems and diseases, the need for discussion between ophthalmologists increasing day by day. Especially when ophthalmologist wants to communicate with each other's and discusses unclear conditions and symptoms remotely. It is difficult to share patient information and images which related to his condition with another ophthalmologist who works in another place securely. As we know there is a huge growth in data exchange technologies for medical data. In data exchange, security is one of the most important and essential issues for healthcare systems to protect patients' related information. We will facilitate the communication between ophthalmologists by enabling them to share patient information remotely and securely. Therefore, we developed a model by using peer-to-peer architecture to exchange patient information. Also we address the security which is the most important issue by applying three techniques: permission, encryption, and logs.**

***IndexTerms*—Ophthalmologist, Exchange model, Security, Peer-to-Peer, Encryption, Communication, Healthcare.**

I. Introduction

The rapid growth of information and communication technology has contributed to accelerate innovation in health information systems. Recently, all patients' related information include patient records, laboratory reports, pharmacy drugs are stored in hospitals system. Which make the exchange of patient information electronically is possible between doctors. Generally, doctors don't share their knowledge with other doctors in same position. But if there is a need for a consultation they consult higher position doctors. Where the higher position doctors are always busy and have a full schedule. Based on these circumstances the time and place issues are arising. Thus we come up with this project to develop exchanging patient related information model.

While developing the model the main issue we faced is how to protect patient information through exchanging process between one ophthalmologist to another. Also the information should be protected if it's accidently received by unauthorized doctor. Thus, to achieve a high level of security we search for many methods and techniques suitable for the model. Therefore, we decide to use three techniques: first, the sender doctor has to set the permission over the document for the receiver doctor. Second, the patients' documents are stored encrypted. Third, all the document usage among the exchange process are logged. So, the control over the document will be with the sender by setting the permission on side and seeing the logged data from other side. We present an approach to reach such a data control. Hence, we develop a model that helps ophthalmologists exchanging information securely.

The paper is structured as follows. Section one describes the literature review of papers that are explored during this research. Section two describes the developed model to exchange patient information with the main tasks of the system. Section three discusses the techniques and methods to secure the document. Section four addresses the transfer and management process of the document. Finally, Section five present conclusion and future work.

II. Related Work

Recently, many researchers have been conducted studies in different sectors such as: banking, social media, mobile services, and healthcare. In result they investigate and explore to get the best security approach that ensures the usability and integrity of the system to exchange information between different parties.

A. Banking Application

Elkhodr, Shahrestani and Kourouche are addressed security issues in their paper "A Proposal to Improve the Security of Mobile Banking Applications" [1] they proposed a confidence negotiation approach used to access mobile banking applications. This approach is combined with the Transport Layer Security (TLS) as the core protocol. The aim of this combination is to increase the security of mobile banking applications. Thus, led to obvious improvements in security compared to the old-fashioned identity-based only access control techniques. The proposed model is implemented as a mobile application. It indicates that the developed application is easy to use and deploy in normal mobile environments.

Also, there is other technique proposed by Vijayalekshmi and Rabara in "Fending Financial Transaction from Phishing Attack" [2] to help reducing the security concerns and face trust breaches in online financial scene. There are two types of phishing attack that target the personal profiles of online banking. Online banking allows customers to manage financial transactions on a secure website operated by their retail or

IJRS

virtual bank. The financial activities within bank can classify under three fields: Client-to-Client (C2C), Client to Bank to Client (C2B2C), and Bank-to-Bank (B2B). The proposed solution mechanism is a pre agreement of a session that specify the key by Transaction Enabling Key (TEK) to successfully between the client and bank server in the context of C2C or C2B2C. The B2B interaction requires a still sophisticated technique, like submitting the Service Right Certificate (SRC) taken by each actual bank website to the other counterparty during the online financial transaction. The submission of faultless SRC by the corresponding entities ensures the integrity of the website and henceforth the credibility of financial transaction is supported.

Zhao and Muftic describe their concept of Secure Mobile Wallet in "The Concept of Secure Mobile Wallet" [3]. The idea of the application is providing the possibility to execute various mobile financial transactions to the subscribers. Their approach stored and running the application in the Javacard SIM chip, called Universal Integrated Circuit Card (UICC). It involves several Javacard applets supporting several types of financial transactions such as; mobile banking, mobile payments, mobile commerce etc. It supports Over the Air (OTA) transactions based on Short Message Service SMS, General Packet Radio Service (GPRS), or mobile Internet protocols. Also, it supports Over the Counter (OTC) transactions based on Near Field Communication (NFC) or Bluetooth protocols. However, the users' messages and data stored in the application are handled and maintained using both, OTA and OTC protocols. In addition they used a set of symmetric and asymmetric cryptography to ensure high level of security.

Jager, Kramer and Thalheim have conducted a study "Secure Data Storage and Exchange with a Private Wallet" [4] to develop an approach which allows the owner to store and share his private data with other users. Also, the owner has a full control over the usage of his data. Therefore, they developed a model based on peer-to-peer network to exchange data between the owner and holder. To achieve a high level of security, they used permission, logs, and encryption to exchange the data.

B. Social Media and Mobile Services

Yuan, Korshunov and Ebrahimi assumed that photo storage and hosting systems of public social networks are untrusted in "Privacy-Preserving Photo Sharing based on a Secure JPEG" [5]. They proposed privacy-preserving photo sharing architecture based on secure JPEG as a solution for the problem of photo privacy protection by securing photos sharing on social media. They used scrambling as the privacy protection tool for photo as a solution. However, the proposed solution was uploading secured photos in social media servers while the process of protection, reconstruction, and photo viewing are done on the client devices. Each client devices are relying on different secret keys to enable hierarchical privacy protection.

Another research was conducted by Zhu, Yang and Ma "SecureSnaps: A New Forward Secrecy Cryptosystem for Self-destructing Messages in Mobile Services" [6] focused on mobile services of ephemeral communications where a message has a certain temporal constraint instead of being stored permanently in storage at client. For example, Snapchat became very famous due to function "burn after reading". Therefore, their users feel secure while it is not truly deleted it can be retrieved by certain applications. However, they mentioned the issue of popular ephemeral communications services that they depend on untrusted service providers. So they present SecureSnaps which have two main functions: "forward secrecy cryptosystem" and "self-destructing messages" by applying an approach called cryptographic counting control. They used this king of control to ensure that there is no one can recover past messages once these messages have been entered the "destroyed state" for more security.

Furthermore, Tung, Lin and Lee proposed Pandora Messaging in "Pandora Messaging: An Enhanced Self-Message-Destructing Secure Instant Messaging Architecture for Mobile Devices" [7]. Pandora Messaging is a secure instant messaging architecture includes a "self-message-destructing" for mobile environment. Also, it enables the users to set time, frequency, and location constraints which specify the time to destruct the exchanged message by deleting the ephemeral keys. In addition to encrypt the messages sent via the XMPP instant messaging they used ephemeral key.

C. Health Care

Sierra, Torres and Camargo have conducted a study "A Secure Mobile System to Interchange Electronic Medical Records in HL7" [8] to present a system prototype for interchanging electronic health records between a mobile device and a medical information system in a secure way. Also, they conducted an evaluation with four symmetric algorithms and results showed that the Advanced Encryption Standard (AES) algorithm was the most suitable in a mobile environment according to performance measures. After that, they have implemented a system prototype that ensures security to exchange electronic medical records between a medical record system (server) and a mobile device (client). The system prototype was developed for the Android platform, which offers a graphical user interface to access electronic medical records stored in an EMR.

Another research was conducted by Hembroff and Muftic "Secure Healthcare Information Exchange for Local Domains" [9]. They proposed Secure Healthcare Information Exchange for Local Domains (SHIELD) system designed to provide interoperability, scalability, security and flexibility to electronic medical data and document exchange. The designed system incorporates fingerprint biometrics and smart card technology within a distributed system that allows healthcare providers to accurately track patients and securely exchange the information. The security of the system is achieved by permitting each hospital to exchange medical data with other hospitals within trusted federation.

III. METHODOLOGY

The adopted methodology for developing a model to exchange information between ophthalmologists would be

IJRS

through analyzing the related work and some interviews. We use related works to collect several security algorithms and then choose the appropriate approach for our model that protects patient information while exchanging process. However, from the interviews we collected the needed information by ophthalmologists who will be in this situation the consultant. Based on the collected and analyzed data we developed our model. Figure 1 illustrates the methodology of developing the model.

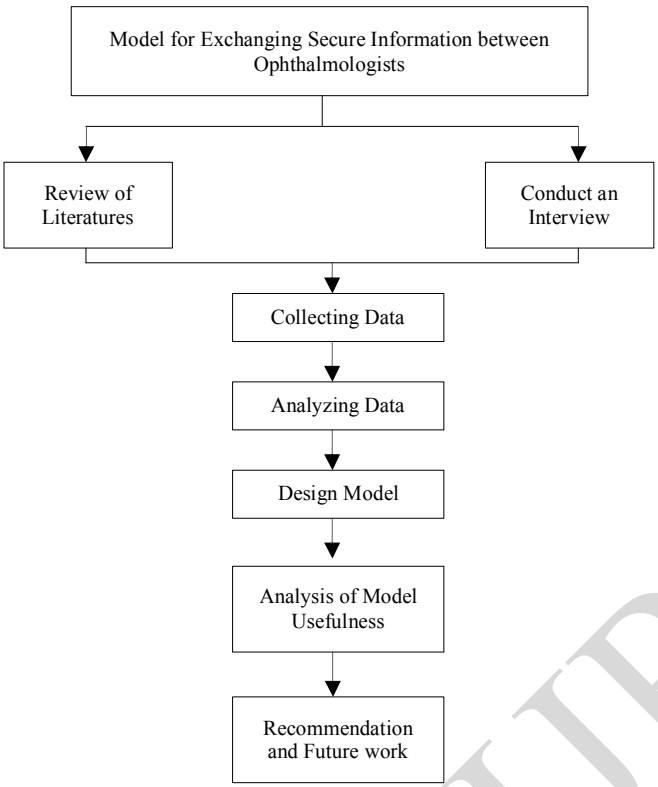


Fig. 1. Research Methodology

IV. Exchange Model

This section describes the model for exchanging patient related information between ophthalmologists. Normally, for each patient there is a document to hold his information in the hospital. This model use document management system (DMS) [10], which is used to track, manage and store documents. The DMS has many components that help to versioning, indexing and retrieval capability. However, the system works as an intelligent interface over the DMS [11].

On another hand, ophthalmologists communicate in a peer-to-peer network. These communications are secured by a hybrid encryption approach. Figure 2 shows the model for exchanging patient related information between ophthalmologists.

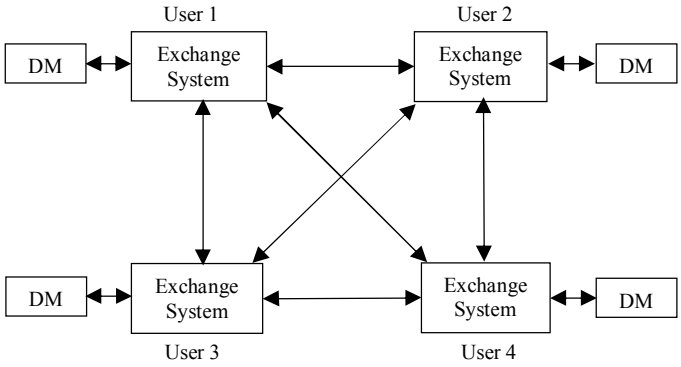


Fig. 2. Peer-to-Peer Exchange System Model

V. System Tasks Area

The exchange model is divided into multiple components to make the replacement of the components much easier. So, the implementation of the system will be modular. The following basic functional components will be implemented for the exchange system.

A. Sending Documents

Sending document function should make sure that the sending document is permitted and encrypted. After importing the document from DMS, the sender has to set the permission and the system will automatically encrypt the document and make it ready for sending. In addition, the DMS stores logs data such as: document id, sending date and doctor name. All these data are automatically generated by the system.

B. Communication

Communication function is important to secure the data while it transfers between the ophthalmologists. We choose the peer-to-peer network approach to exchange the data, because the exchange relationship is one to one. Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node (peer) to function as both a client and server. Using peer-to-peer brings some advantages like there is no need for full-time System Administrator. Every user is the administrator of his machine and can control his shared resources [12].

VI. Data Security

This section describes the data protection from destructive forces and from the unwanted actions of unauthorized users. To achieve this goal, we present three main aspects of the data security: permission, encryption, and logs.

A. Permissions

To protect the patient document from unauthorized users the sender has to set the permission over the document for the receiver. Usually Permission has three types: read, write, and

IJRS

delete. If the sender will send the document to different receiver he can set different permission for each one of the receiver [13].

B. Encryption

For secure communication there are two common approaches cryptography and steganography. The cryptography is the study of hiding information and it is used when communicating over an untrusted medium such as Internet, where information needs to be protected from other third parties. In the modern cryptography, there are three types of cryptographic algorithms used: Secret key (Symmetric key) encryption, Public-key (Asymmetric key) encryption and Hash functions. In this system we use hybrid of two types of the cryptography encryption which is Symmetric key and Asymmetric key. Symmetric key involves encryption methods where both the sender and the receiver share the same key used to encrypt the data. In Asymmetric key, two different keys are used but mathematically they are related [14].

For document encryption we choose Symmetric key encryption to take the advantage of speed. Also, to increase exchange security we choose Asymmetric key encryption to encrypt the key of Symmetric encryption. However, for encrypting the document by Symmetric encryption we can use any key length 128, 192 and 256 bits based on Advanced Encryption Standard (AES) [15]. But for encrypting the key of Symmetric encryption we use at least 2048 bits key long based on (RSA). RSA is created of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm [16].

Furthermore, to increase the security of encryption we can use steganography. Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention. Modern Steganography methods are called Digital Steganography. These modern methods include hiding messages within image, test or even video. Thus, we can hide the encrypted key (encrypted by Asymmetric cryptography) by Steganography.

For example: a 24-bit bitmap uses 8 bits to represent each of the three color values (red, green, and blue) at each pixel. The blue alone has 28 different levels of blue intensity. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used more or less undetectably for something else other than color information. If this is repeated for the green and the red elements of each pixel as well, it is possible to encode one letter of ASCII text for every three pixels [17].

C. Logs

When the sender sends a document he can't predict what the receiver does on that document. So, all the usage of the document should be logged on the database, this process enables the sender to track the sent document.

VII. Data Transfer and Management

This section describes how the data are transferred between ophthalmologists. Also, discusses the mechanism of storing and managing patient documents and how these documents could be retrieved.

A. Data Transfer

There are several ways to transfer the data between the ophthalmologists within the network. One of them Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are suitable for exchanging documents and for exchanging keys over the Internet and local network. TCP and UDP are suitable for transferring data from both computers and mobile devices. Figure 3 illustrates how the data is transfer from the sender to the receiver [18].

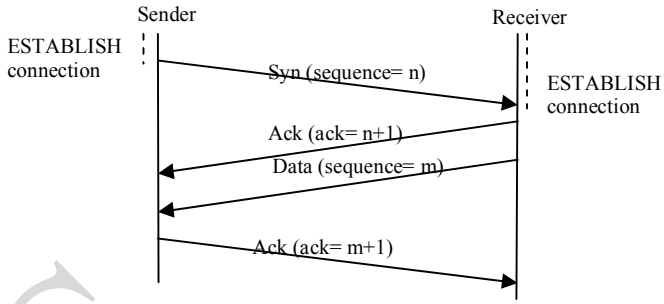


Fig. 3. Data Transfer Diagram

B. Data Management

To store data, every exchange system has its own database and every database gets the same database schema. Figure 4 shows the database schema as a Higher-Order Entity-Relationship Model (HERM) [19].

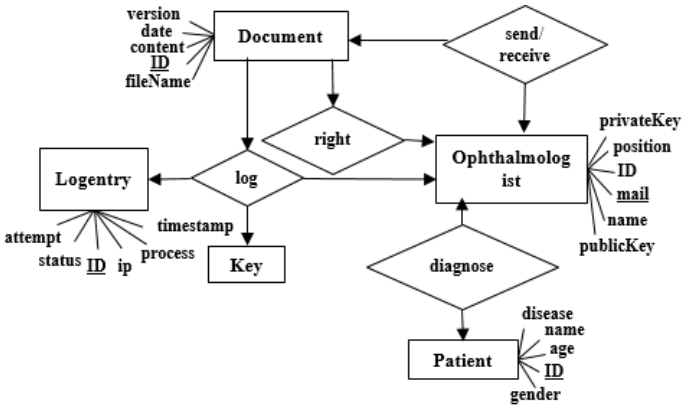


Fig.4. Entity-Relationship model

The main element of the database is document. A document contains many attributes which are document name, the content (patient information and the initial diagnosis), the date, the version number, and the priority. To ensure a high degree of flexibility the ophthalmologists can define the document priority based on the document importance.

The document can have one sender and many receivers. The sender is an ophthalmologist who has to diagnose the patient, set permission over document and send the document to the receiver. The document could have multiple keys with the corresponding permissions. Each key consists of encrypted key and the rights of the receiver document. The receiver is also an ophthalmologist who will receive the documents and he might respond to the sender based on his rights. Furthermore, the log contains many log entries. Each log entry provides: information about the affected document, the IP address of the device (on which action was performed), the number of attempts, the actual process, the status (successful or not), and the activity point in time. It is very important to guaranty that the document actions has been logged.

There is essential information that is never change under any circumstances such as: document ID and the user email. But the other attributes it might be changed.

VIII. Conclusion

Based on the difficulties that the Ophthalmologist faced in order to communicate with each other we developed our model. The model allows ophthalmologists to communicate in a peer-to-peer network. Using peer-to-peer network to transfer the document does not guarantee the security. To ensure that the document is secured we applied three techniques: permission, hybrid encryption, and logs of the document usage. All the documents transferred by using TCP and UDP which is suitable for transferring data from computers or mobile devices. However, the patient document, encryption information and logs are stored in database.

As a future work we intend to implement the model and distribute the system to hospitals. Taking feedbacks from ophthalmologists if there is a need for some modifications to the system. To be more useful and beneficial we will expand the system to include other doctors from different specializations.

Acknowledgment

We are greatly thankful to the faculty of Software Engineering department in Prince Sultan University, Especially Prof. AjanthaDahanayakefor her guidance, valuable comments, and support in overcoming the hurdles in the completion of this research.

References

[1] M. Elkhodr , S. Shahrestani and K. Kourouche, "A proposal to improve the security of mobile banking applications," in *ICT and Knowledge Engineering (ICT & Knowledge Engineering)*, IEEE, 2012.

[2] S. Vijayalekshmi and S. A. Rabara, "Fending finanicial transaction from phishing attack," in *Trendz in Information Sciences & Computing (TISC)*, Chennai, 2010.

[3] H. Zhao and S. Muftic, "The concept of Secure Mobile Wallet," in *Internet Security (WorldCIS)*, London, 2011.

[4] O. Jäger, F. Kramer and B. Thalheim, "Secure Data Storage and Exchange with a Private Wallet," in *New Trends in Database and Information Systems II*, Switzerland, Springer International Publishing, 2015, pp. 59-70.

[5] L. Yuan , P. Korshunov and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure JPEG," in *Computer Communications Workshops (INFOCOM WKSHPS)*, Hong Kong, 2015.

[6] Y. Zhu , L. Yang and D. Ma, "A New Forward Secrecy Cryptosystem for Self-destructing Messages in Mobile Services," in *Mobile Services (MS)*, New York, NY, 2015.

[7] T. Y. Tung , L. Lin and D. T. Lee, "Pandora Messaging: An Enhanced Self- Message-Destructing Secure Instant Messaging Architecture for Mobile Devices," in *Advanced Information Networking and Applications Workshops (WAINA)*, Fukuoka, 2012.

[8] D. F. Sierra , Y. F. Torres and J. E. Camargo, "A Secure Mobile System to Interchange Electronic Medical Records in HL7," in *Computing Colombian Conference (9CCC)*, Pereira, 2014.

[9] G. C. Hembroff and S. Muftic, "Secure Healthcare Information Exchange for Local Domains," in *Pervasive Computing Technologies for Healthcare*, London, 2009.

[10] S. Khan , U. Rani , B. V. Prasad, A. K. Srivastava, S. Selvi and D. K. Gautam, "Document management system: An explicit knowledge management system," in *Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2015.

[11] F. Kramer and B. Thalheim, A Private Wallet App for Secure Data Storage and Exchange, Switzerland: Springer International Publishing,2015.

[12] C. Nagel, J. Glynn and M. Skinner, "Peer-to-Peer Networking," in *Professional C# 5.0 and .NET 4.5.1*, Indiana, John Wiley & Sons, Inc., 2014, pp. 1433-1445.

[13] M. Moniruzzaman and K. Barker, "Delegation of access rights in a privacy preserving access control model," in *Privacy, Security and Trust (PST)*, Montreal, QC, 2011.

[14] R. Anderson, A Guide to Building Dependable Distributed Systems, cambridge: WILY, 2008.

[15] K. Sowmya Nag , H. B. Bhuvaneswari and A. C. Nuthan, "Implementation of advanced encryption Standard-192 bit using multiple keys," in *Research & Technology in the Coming Decades (CRT 2013)*, Ujire, 2013.

IJRS