www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7846-7849

Security Issues in Health Care

Sonia K Savant, Prof. Aruna S. Nayak
M Tech Computer Science
BVB College of Engeneering
Hubli-India
Computer Science Department
BVB College of Engineering
Hubli-India
sksavant14@gmail.com
arunan@bvb.edu

.

Abstract-----Information systems in healthcare is found to play a very crucial role in today's scenario as more and more patient data is accumulated and it has become extremely crucial for correct and early diagnosis leading to early and effective treatment. Hence the issue of security of patient data is increasingly gaining popularity. Implementing security techniques in health centers is very much necessary to provide the controlled access, confidentiality and integrity to the patient records. This paper presents a method using cryptographic means to improve trustworthiness of medical images, and healthcare information without compromising its quality to the end user. It also analyzes the security measures that have been implemented to provide the controlled access in the current project using MD5 algorithm and identifying its limitations to provide probable solutions.

Keywords-HealthCare, Security, Cryptography, MD5.

I. INTRODUCTION

Health is considered to be one of the most basic need of any human being and also the right to health is one's fundamental right[1]. The health care industry is historically generating large amount of data, driven by record keeping and health images. These types of records are very much important for any patient, since it helps the patient in diagnosing his disease.

This large amount of data is stored, processed and managed at each hospital. These activities at each hospital are considered to be most sensitive because anything wrong in these activities may affect the health and treatment procedure of a patient. In this regard it is necessary to secure the records of a patient because lack of proper controls, procedures, and policies may tempt unauthorized users to access and use patient information in an inadequate fashion, weakening the credibility of healthcare information. Today all the hospitals are moving towards storing the records on computers instead of paper work.

Traditional paper based medical record systems fail to keep up with the increasing demands placed on a healthcare industry. The solution is electronic medical record system that allow doctors to store the patient records[2]. Even though the healthcare providers automate their medical records, clinical systems, and medical imaging protecting the privacy of patient information is becoming increasingly challenging, because of the increased interconnection which enable around the clock patient information access for physicians as well as new methods of communication between providers, payers, and patients. The expanding scope of interconnected network between hospitals, clinics, suppliers, and other external parties is changing the characteristics of security in healthcare industries. Hence healthcare organizations are facing more security threats that increase the risk of inappropriate access to patient information. In this constantly evolving environment the various security measures such as firewall, antivirus, and intrusion detection are no longer providing the required level of granularity and safety.

Therefore security is considered to be as one of the major issue which plays a very important role in the health care fields in order to provide services like information integrity, authenticity, confidentiality.

So many healthcare organizations are working with their business partners to implement security and privacy to their healthcare records [3]. This paper describes the challenges of security and privacy in the healthcare environment. Various technologies that can be used to provide and improve the security, the limitation of current project.

II. DEFINITION OF SECURITY

The definitions of security

1) The state of being free from danger or threat.

2) The state of being secure is the degree of resistance to, or protection from harm.

3) The safety state against criminal activities such as terrorism, unauthorized access and theft.

III. CONSIDERATIONS ON SECUITY

The points that should be taken into account when dealing with information security.

A. *Security is not strictly technological issue[1]:* The best systems can render useless due to non-ethical users and hence only providing good security to any environment not only completely dependent on systems but also on people.

B. *Security is an evolving process:* security must be evolved continuously as the advancement in business rules[1].

IV. HOSPITAL MANAGEMENT SYSTEM

Hospital management system is a hospital information system, which addresses the major functionalities of hospital. It includes patient treatment, storing the patient records, and management of patient information. Once after storing the patient records it also provides the controlled access to the patient data. The main aim of this system is to make all activities in a systematic manner and to reduce the manual work.

The objectives of hospital management is to,

1. To computerize the patient details and hospital details.
2. To maintain the records effectively.
3. To manage the status of staff and doctors availability.
4. To provide timely availability of information
5. Deliver the services at a reduced cost.
6. To provide 24*7 availability of information.
7. To provide effective patient centric services.

The good management system will enhance the care quality and gives the better clinical outcomes. In addition it also improves the financial performance of the hospital, presents better solutions to all the problems in health care industry. Each hospital management software at each hospital has its own modules which integrates all these modules together so that these can work together and give better results. The integration of all these modules leads to availability of updated information at one desk. Information about appointments, bed availability, and schedules of doctors.

V. PATIENT PRIVACY AND SECURITY OF MEDICAL INFORMATION

Patient privacy is the right of patient to determine the extent to which their information is shared with others [4]. It includes confidentiality and integrity of data. The security of patient data is very much necessary since it has a direct impact on the quality of patient data. security is a means of providing controlled access to data, so as to take care of who and what each person at hospital is accessing and also the time at which the patient information is accessed since because delay in accessing the patient records may adversely affect the patient treatment.

VI. TECHNOLOGIES USED TO SECURE THE MEDICAL INFORMATION

Technical and administrative safeguards are in place to provide the privacy, security of patient information. These technologies provide safety through isolation, allowing physical access only to authorized persons, data backup and maintaining copies.

Technical safeguards include firewall, virtual private networks, secure socket layer, and encryption techniques. Each Electronic medical record must include the following components within their system security policies and procedures: authentication, availability, confidentiality, data integrity [6].

Authorization includes assigning rights and privileges to users to access certain resources.

Authentication is the process of verifying the identity of a user to a system that can be accomplished using login password.

Confidentiality is the process of preventing the third parties from accessing and viewing the records.

Data integrity is verifying that the data arrived is same as that it was sent.

VII. CRYPTOGRAPHY

Many hospitals today are moving from paper based records to electronic health care records. These automated processes help the doctors in diagnosing the diseases. A malicious person can easily collect the data if these records are available electronically. **Cryptographic mechanisms** are a suitable means to reduce or to eliminate the risks and to enhance the security of open distributed systems.

Cryptography is the art of transforming an intelligible message into one that in unintelligible and then retransforming the message back to its original form. This user and data authentication can be achieved through cryptography by so called **digital signatures.**

Digital signature is the most widespread method for data integrity and authenticity [1]. Using Digital signature it is very difficult to produce the original data without secret key. It is implemented using pair of keys. One is the private key, owned and used only by the signer, and the other is the public key, which may be published for anyone to check the validity of the signature. . It is important to stress that the public and private keys are related to each other, but a third party will not be able to derive one key from the other.

Encryption is done using private key and decryption is done using decryption key[1]. The data to be signed is hashed and the result is encrypted with the private key of the signing party, producing the digital signature, the public key of the signing entity is used to decrypt the signature, retrieving the hash generated at the signing time. Then, the original data are rehashed, generating another hash, which is compared to the retrieved one. If both are equal, then it can be said that the data are undamaged and authentic.

The users, e.g., physicians, nurses, and patients have to be equipped with cryptographic facilities. Every user must hold some kind of **personal, physical device** which is capable to hold his personal keys and to produce his digital signatures or to encipher his messages for him. Such personal devices can be smart-cards, advanced cards, handheld pen-computers, etc. In this cryptography can be used in healthcare centers to provide the security to the patient records at each level.

Consider the current project below in which the MD5 algorithm has been used to provide the security to the passwords and not the records. So in the following section ill deal with current project, its limitations comparison of MD5 and Cryptography.

VIII. CURRENT PROJECT

This project is all about developing the software **"GUNASHEELA IVF CENTER"** for Gunasheela hospital in Bangalore[5]. This software is specifically for IVF center at Gunasheela Hospital. The main objective of this project is to reduce the paper work used in the process of IVF and to escalate the notifications and to alert the doctors about their patients.

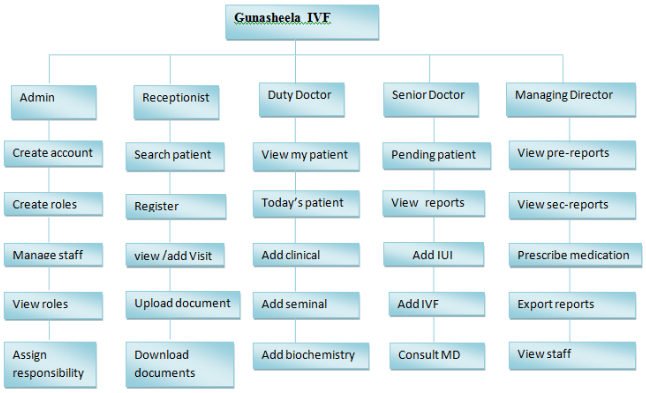

Fig. 1.Features of proposed system

There are five main modules in this project, such as Admin, Receptionist, Duty Doctor, Senior Doctor, and Managing Director. These five modules are not fixed but we can even create many Roles as per the requirement. To make this project generic we have set of responsibilities, and these responsibilities can be assigned to any Roles. Thus in case of emergencies the Admin can assign the responsibilities as per the need. So that if the particular Doctor is unavailable his tasks can be performed by other level doctors. i.e if the count of Duty Doctors are less on a particular day then the Senior Doctor or Managing Doctor can perform the tasks of Duty doctor this is possible only if Admin assigns the responsibilities to whom he want.

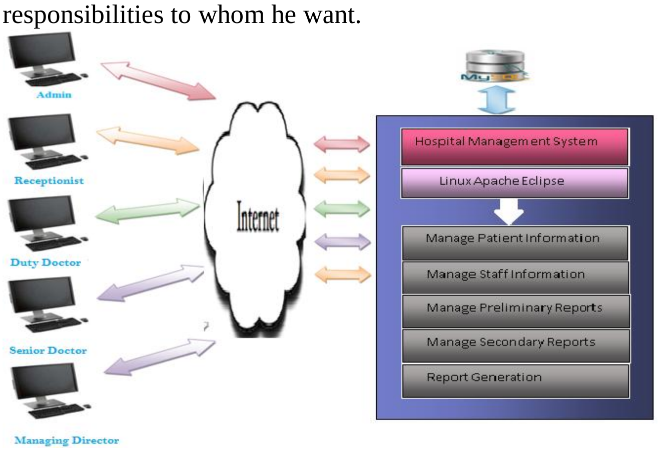

Fig. 2.Architectural Design

We have even given the mail facilities to send the notifications of pending patients to Duty Doctors and Senior Doctors. But sometimes the doctors don't require the mail notifications then they can easily disable this facility, and they'll get the notifications only when they login onto the system.

IX. FLOW OF EVENTS

Patient visits the hospital goes to the Receptionist, if the patient visit is first visit then the Receptionist will collect all the records of a patient such as name, Date of Birth, Email, Address and also spouse details. Once after the registration Receptionist will give the **Information Folio Number** to patient. Each patient is uniquely identified by Information Folio Number. Then the Receptionist will perform the add visit operation and assigns the Duty Doctor to the patient. If suppose the patient visit is more than one i.e second or further visit then the receptionist performs the search patient and assigns the Duty Doctor to the patient, Receptionist can also upload and download documents of a patient.

Once after the assignment of a patient to a Duty Doctor, the Duty Doctor will get notification of a pending patients when he logins. Duty Doctor the first level doctor performs the preliminary tests. He performs the Clinical Examination, Seminal Assay, and Biochemistry test. The Seminal Assay and Biochemistry tests can be performed only after Clinical Examination. So the Duty Doctor first performs the Clinical Examination and adds the details such as patient history, Last Month Period, Husband Blood Group, Wife Blood Group, Patient Weight, Height, and assigns the next level doctor Senior Doctor. The entry of Last Month Period, History Blood Groups are all one time entry only on the first visit the doctor enter these details and can edited only by the Duty Doctor who tested it. But the weight, Blood Pressure, Clinical Examination Description and assignment of senior doctor are entered each time when the patient visits and can be edited on that day. Once after the Clinical Examination the seminal assay and Biochemistry are performed by the Duty Doctor but are not mandatory.

Once after the assignment of a patient to a Senior Doctor, the Senior Doctor will get the notification of a pending patients when he logins. Senior Doctor the second level doctor performs the secondary tests. On the first day the doctor decides whether to do Intrauterine insemination or In vitro fertilisation test for the patient, based on the secondary test decided by the doctor on the first day the subsequent entries will be done as per the test decided. Once after the addition of details sometimes the secondary doctor can send the patient to Managing Director for further medication.

The next higher level is Managing Director, there is only one MD. The main activities of MD are, can view the details of any patient and staff, can also view the doctors details of each patient on a particular date ,can export the details of all the patients, the details of staff in PDF format.

X. SECURITY MEASURES

The security measures undertaken in this project is MD5 algorithm[4]. This algorithm is used in this project to provide the security to the staff passwords. The Admin creates the roles, the mail goes to the staff when his account is created by the Admin. In the mail there is a link which redirects to change password page. Then the staff enters his own required password, this password will be saved in the database in tblStaffProfile in encrypted format by using MD5 algorithm.

XI. MD5 ALGORITHM

This algorithm takes the input encrypts it and produces the output. This algorithm produces the 128 bits of output called as message digest[6]. Each message digest is uniquely generated.

In this current project as soon as the staff gives the required password, we are making a call to a function with a parameter as our entered password. This function converting the password into 128 bit code and stores it into the database. In this way here the security is provided to the passwords of staff. But the limitation of this current project is its not providing the security to the records of patient.

XII. LIMITATIONS OF MD5

1. The use of MD5 algorithm is to provide the authentication in hospitals may have risk because it may reduce the performance in high bandwidth systems. Thus causes performance degradation.

2. MD5 can be broken easily and is no longer secure to be used in healthcare centers.

3. MD5 is significantly slower than CRC.

XIII. COMPARISON BETWEEN MD5 AND CRYPTOGRAPHY

1. Digital signature is publicly available function which takes the Plain text and a secret key to produce a value that serves as the authenticator. But the hash function generates the hash value from a plain text which serves as authenticator[7].

2. The MAC authentication technique involves the use of a secret key to generate a small fixed-size block of data, known as cryptographic checksum or MAC that is appended to the message. But in MD5 it produces the encrypted hash data and is checked for authentication.

3. In Digital signature the generated MAC will be **MAC = CK(M),** but in hash function it takes variable size message M and produces the hash function H(M),a hash function does not use any key[7].

4. A hash function is much faster to compute since no key is involved in the computation, but a MAC provides better authentication in an unsecure channel.

CONCLUSION

This paper is telling all about the Hospital Management Systems. As the world is evolving today, the hospitals are now switching towards the technology and computers to store the records than using the paper work.

The move of hospitals towards technology has benefits but it also has some disadvantages in terms of security. So only, this paper is telling about the importance of security in hospital to store and retrieve the records of patients, the technologies used to provide the security, the importance of cryptography. This paper is also giving the description about the project "Gunasheela IVF Center", its security measures, the description about MD5 algorithm and limitations.

REFERENCES

[1] Providing Integrity and Authenticity in DICOM Images: A Novel ApproachLuiz Octavio Massato Kobayashi, Sergio Shiguemi Furuie, and Paulo Sergio Licciardi Messeder BarretooHarley .

[2] Security and Privacy System Architecture for an e-Hospital Environment

[3] Security and Privacy for Healthcare Providers White Paper: Best Practices Series for Healthcare

[4] Security of electronic medical information

[5] Report on Software for Gunasheela IVF Center

[6] MD5 algorithm by Harley Kozushkoarl

[7] Computer Networks & Computer Security Mar 15-18, 2004LecturerKartikKrishnaney