A Model of a Secured Smart e-Health System

Mohammad Tauhidul Alam
IT Operation & Communication Department
Bangladesh Bank
Dhaka, Bangladesh
tauhidul.alam@bb.org.bd

Prof. Dr. Md. Liakot Ali
Institute of Information & Communication Technology
Bangladesh University of Engineering & Technology
Dhaka, Bangladesh
liakot@iict.buet.ac.bd

Abstract— Health care system is one of the vital sectors in each country for its national interest. This paper presents a model of e-health system which covers all medical entities like patients, doctors, nurses, medical technologist, pharmacist, healthcare organizations, pathology labs, pharmacies etc. The model also introduces e-Health Card (Smart Card) for each patient for authentication and better e-health service. The work incorporates two important aspects of the proposed e-Health system: (i) the development and deployment of a medical information management system where user’s authentication is performed by NID (National Identification Number) through smart card and (ii) the privacy and security concern of the proposed system which is implemented by Role Based Access Control (RBAC) to access patient’s medical record with audit logs and by Encryption Algorithm to Exchange of medical documents. "NID" is a 17 digit unique identification number provided by LGED (Local Government & Engineering Department), a government organization of Bangladesh. This proposed model will provide an easy to carry and access facilities everywhere in the country.

Keywords— e-Health System, Smart Card, Medical Record, NID, RBAC, Encryption, Security.

I. INTRODUCTION

Healthcare is one of the fundamental human rights in any country. People have to go to the hospital or private doctors for medical checkup and treatment. Depending upon the situation doctor may suggest the patient to admit in the hospital or to have medical tests for further investigation of the disease. To get the medical tests done patient has to go to the diagnostic centers. Again patient may go to a different doctor or hospital for different diseases or even for the same disease. Each time the patient goes to a different place, he has to give his personal details like name, father name, age, gender, address, etc. which is troublesome and sometimes prone to error. Some hospitals have a system to maintain patients’ medical records but it is limited within the treatment facilitated by those hospitals only. To present the overall medical history to the doctor the patient has to maintain his own medical record. Most of the cases the medical record is maintained in paper format which can be easily misplaced lost or exposed to unauthorized parties. Another important issue is checking the authenticity of the medical staff like doctors, nurses, pathologists etc. It is important for hospitals to verify the background of the medical staff while recruiting to avoid fraud cases. It is also important for the patients to check the profile of whom he will get the treatment. Sometimes medical staff is blacklisted due to his mistreatment of the patient. This information is also crucial for both medical centers and patients to make the health care system a reliable one. Adoption of Information and Communication Technology (ICT) with the health care system is a demand of this day for increasing the efficiency of medical information management [1]. A broad range of e-Health applications have emerged to enable patient, nurse, doctor, and administrator to efficiently access relevant information, enhance the quality of patient care and reduce health care errors [2, 3-4]. Since e-Health services are usually cloud enabled where ubiquitous access to healthcare data are considered essential for effective treatment, Electronic records of the patients frequently need to be exchanged among different health care institutions [4]. So the system is exposed to all kinds of security threats. Again electronic records are more vulnerable than paper based documents. So it has introduced various securities and privacy concerns [3, 5-7]. But all these above issues at health sector still not integrated in a common framework in a secured manner to give quality e-health service to the patient. Our goal is to solve this problem.

II. RELATED WORK

In [1] the author tries to represent e-Governance scenario in health sector of uttarakhand, India and find out the scope for application of ICT in health care services for uttarakhand. In [2] authors introduce an e-health framework based on service oriented computing paradigm. It integrates information sources in order to cater to the information requirements in rural areas which are developed around a layered concept. This approach enables one to provide better visualization of distributed information services and a mean of integrate them to one stop information access. In [3] author proposed Aadhaar number (a
twelve digit unique identification number) for authentication for Indian e-health system. In [4] the author presents development and integration of an electronic Health Systems in Scotland. In this paper bottom up approach is used to implement e-health system. A portal based e-health system has been developed for local health care organizations and gradually expands it to national role. Role Based Access Control (RBAC) has been implented to access the patient’s medical record but there was no clear indication about authentication or identifications of medical entities (patients, doctors, and nurses etc.). Also there was no security technology used for medical document exchange. The authentication of the medical entities can be done by smart card technology where all necessary information of the entities will be stored and security on document exchange can be done by encryption algorithm. In [9] a smart card based healthcare information system is developed. Two smart card software modules are implemented that run on patient and healthcare professional smart cards, respectively. But maintaining software/hardware at both patient and healthcare professional side is very much costly. So Two smart card software module can be converted to one which resides at healthcare professional side to authenticate the patient through smart card and patient can access their medical record from cloud. In [6] the authors have proposed a security framework based on Service Oriented Architecture (SOA) for e-health service. The authors illustrated advanced authentication technique for better data protection and the applicability of different encryption algorithms combined with optimum key length which gives a cost-effective solution for secure e-Health services. AES encryption algorithm may be used for higher security and fastest speed. We have also analyzed the existing medical system of Bangladesh Bank (BB) and Bangladesh University of Engineering & Technology (BUET), Bangladesh. The employees of Bangladesh Bank take health service from doctors and nurses within organizational domain. A manual filing system is maintained for each employee. Internal doctors of BB use desktop based software to give prescription to the employee. As the software is desktop & intranet based rather than internet based, so employees only can view the prescribe medicine through intranet within BB, but they can’t see their profile and medical history outside of BB. Employees also take health service from external doctors and healthcare organizations. But those external doctors can’t see internal doctor’s prescription through online and vice versa. Almost same scenario exists for BUET. Our proposed model will help both organizations to make interoperable platform to manage a secured digital medical system.

III. PROPOSED E-HEALTH MODEL

The objective of this paper is to design an e-health model which provides an integrated secured framework for all medical entities (Patients, Doctors, Nurses, Medical Technologist (MT), Pharmacist, Healthcare Organizations, Pathology Labs, and Pharmacies etc.) to reduce the health care errors and to afford central medical information management by ensuring authenticity, integrity, and confidentiality.

A. System Design

The proposed e-health system is a combination of hardware and software which includes the security and authentication process. The hardware part consists of smart card and card reader. The software is divided into two modules: (i) web based module for core information management system (ii) smart card module for issuing e-health card and authentication. Authentication is performed by NID, Privacy is ensured by Role Based Access Control (RBAC) and the security of the system is enhanced by Encryption Algorithm to exchange medical documents and by Access Log. Web based module along with the central database will be hosted at Data Center (DC) or Cloud and smart card module & smart card reader will be installed at healthcare service points. Fig. 1 depicts the basic architecture of the e-health system.

![Fig. 1. Basic e-health Architecture](image)

B. Hardware Design

Each patient will be issued a contactless smart card as e-health card from a central authority. To give priority e-health service for old and persons with disabilities we have introduced color code for e-health card. We have used white card for general people, blue for old and green for disable people. The patient will only need to carry the e-health card to get medical assistance from anywhere in the country. To authenticate the e-health card, smart card reader will be installed at the service points like hospital, diagnostic centers, private doctors’ chamber etc. For the design Mifare classic 1K (MF1SS03x) is used as smart card which includes mutual three pass authentication (ISO/IEC DIS 9798-2) [10]. The memory of the card is divided in
16 sectors and each sector is further divided into 16 byte. Data read and write from/to these bytes as hexadecimal code. Individual set of two keys per sector to support multi-application with key hierarchy and also increases the security. ACS 122u USB NFC Card Reader is used as card reader for the system [11]. Though the mentioned card reader is used for the system any other card reader capable of handling Mifare classic 1K card can be used.

C. Software Architecture

The software communicates with the hardware, authenticates medical staff or patient’s identity, process patient’s medical information and preserves medical record. The software is the combination of web based module and smart card module. The web based module is implemented with WAMP (Windows, Apache, MySQL and PHP with Ajax) technology and the smart card module is implemented by C# (.Net framework). Both modules access the common e-health database (ehsystem).

1) Core Web Based Module: This is the main module of the proposed model. It is divided into nine different processes. As doctor involves many of the processes, a Data Flow Diagram (DFD) is drawn for doctor entity as in Fig. 2 which is used to describe different processes.

a) Verification and Registration Process: The central admin is responsible for performing the verification and registration process of all medical entities. At first, each user (human) must be registered as a patient. As each patient is uniquely identified by NID, so NID verification from National Database (NDB) is performed before registration. After proper verification and registration, each patient will get a login ID and password for web access. After registration as a patient, medical professionals (doctor, nurse, medical technologist, pharmacist) can be registered themselves at e-health system as a professional after proper verification from their respective authorities. Similarly e-health service points (Hospital, Diagnostic Center and Pharmacy) are uniquely identified by Registration Number. So they are verified through their respective registration authorities before registering as a service point at e-health system. Fig. 2 describes verification & registration process for a doctor. In Fig. 2 Doctor is an external entity which provides his details information to ‘Registration Process’. After registering as a patient, this process verifies doctor’s professional registration Number from BMDC (Bangladesh Medical & Dental Council) database. BMDC is the registration authority for doctors in Bangladesh. After successful verification, doctor’s professional information is written to ‘doctor’ table and provides a web access password to the doctor. Other entities follow the same procedure for registration.

b) Login Process: Each medical entity will get a password during registration process. This password and Login ID are used to login into e-health system. Professional password of a user is different from his patient password though his Login ID is same. Fig. 2 shows the login process of a doctor into e-health system and his login information is written to “central_access_log” table. Other entities follow the same procedure for login.

c) View Patient’s Medical Record Process: This process use different tables of patient as indicated in Fig. 2 to visualize the medical record of patients to the doctor where patient’s pathology report come from “patient’s web directory” at unencrypted form through ‘File Decryption Process’. Patients can also view their medical record through this procedure.

d) e-prescription process: Doctor can check the list of patients who are assigned to him. Doctor uses this process to give e-prescription to the patient. Fig. 2 illustrates the e-prescription procedures. In this process doctor can read patient’s personal, medicine and pathology information from different tables and write prescribed data to different tables as indicated. The patient may get the printed form of prescription from the doctor or the operator. A short form of e-prescription is written to patient’s e-health card using card module.

e) Patient Pathology Test Process: Pathology Labs use this process to authenticate a patient by his e-health card through smart card module, to view his pathology test given by doctor and to assign a Medical Technologist to perform the test.

f) Upload Pathology Report Process: Medical Technologist at pathology lab uses this process to upload patient’s pathology test report to temp directory and forward it to doctor for checking.

g) Check Pathology Report Process: Doctor uses this process to check patient’s pathology test report forwarded by medical technologist. After checking doctor transfers report from temporary directory to “patient’s web directory” at encrypted form through ‘File Encryption Process’ and update the patient’s pathology table. Fig. 2 illustrates this procedure.

h) File Encryption/Decryption Process: File Encryption is a sub process under ‘check pathology report’ process. After checking the test report forwarded from Medical Technologist, the doctor encrypt the test report and put it to patient’s web directory. File Decryption is a process under ‘view patient’s medical record’ process used by doctor and patient to view their pathology report at unencrypted form. Fig. 2 illustrates the file encryption/decrypt process.

i) Patient Admission Process: Hospitals/Clinics authenticate a patient by his e-health card through smart card module, admit the patient and assign a doctor to him through this process.

2) Smart Card Module: Smart Card module is another important module of the proposed model. This module is designed to issue a patient’s e-health card, identify a patient through this card and to store patient’s personal & medical information.
into this card. This module is used by central admin, healthcare organizations or private doctors and pathology labs. Fig. 3 depicts the smart card module interaction among different medical entities. Here central admin uses this module to issues an e-health card to the patient after successful registration in the e-health system through Patient’s web registration process. Medicals, Doctors use this module to identify a patient, to send patient into a queue of e-prescription Process of the web based module. Doctor checks the patient and gives an e-prescription. The patient’s medical record is stored at e-health DB and short form of e-prescription is stored at patient’s e-health card. Pathology labs use this module to identify a patient and send patient into a queue of Patient Pathology Test Process of the web based module for pathology test.

Figure 2: DFD for Doctor Entity

Patient’s Web Registration Process

Healthcare Organization / Private Doctor’s Chamber

Smart Card Module

Write patient’s medical history to card

Queue of patient for Doctor’s Web e-prescription process

Queue of patient for Patient’s Web Pathology Test process

Patient’s e-health Card

Patient’s e-health Card

Card Reader

Issue an e-health card to patient

Pathology Lab

Write patient information into card

Authenticate patient’s NID

Send Patient to Queue

E-health Card

© IEOM Society International 2177
IV. SECURITY DESIGN

We have secured our e-health model by implementing different layers of security. It includes: (i) Smart Card Security (ii) Authenticity & Access control mechanism (iii) Document Exchange Security (encryption algorithm) and (iv) Central Access Log.

E-Health card will help the authorities to verify patient’s identity and enable medical staff to check his medical record. This e-health card may be stolen and the thief may try to tamper or duplicate the e-health card. But each e-Health card has a hard coded non-editable unique identification number. Along with the built-in defensive mechanism a cryptographic function is implemented to enhance the security. This card also contains the NID of patient. Both NID and non-editable unique card identification number has been used to authenticate a patient. Hence though the thief can tamper the NID, he can't change the card number coded by manufacturer. So any attempt of tampering will not be successful.

Each entity is registered at our e-health system in authentic way as the proper verification is performed from their respective authority. Fraud medical entities are identified and filtered through this e-health system. So it will reduce corruption at health care system. Access control is another security concern of this system. Patient’s medical record contains sensitive data of the patient. Only limited person should access to patient’s medical record to keep the privacy. Role Base Access Control (RBAC) has been used to access control. There are different entities of the e-health system which plays different roles. A user may play multiple roles (i.e. a doctor or a nurse is also a patient). Table I describes the role based access control (read/write permission) to the patient’s medical record and e-health card.

<table>
<thead>
<tr>
<th>Medical Entity</th>
<th>Role</th>
<th>Read/Write Permission (patient’s web medical record)</th>
<th>Read/Write Permission (patient’s e-Health Card)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient or Doctor or Nurse or</td>
<td>Patient</td>
<td>Read (only his medical record) +</td>
<td>No</td>
</tr>
<tr>
<td>Medical Technologist or Physician</td>
<td></td>
<td>Write (only update personal information)</td>
<td></td>
</tr>
<tr>
<td>Doctor</td>
<td>Doctor</td>
<td>Read +</td>
<td>Read (NID &amp; card No) +</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write (Add new record)</td>
<td>Write (only medical history)</td>
</tr>
<tr>
<td>Nurse</td>
<td>Nurse</td>
<td>Read (only see prescribed Medicine &amp; Health status of assigned patient)</td>
<td>No</td>
</tr>
<tr>
<td>Medical Technologist</td>
<td>Medical Technologist</td>
<td>Read (see prescribed Pathology Test) +</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write (upload test report &amp; update record for assigned patient)</td>
<td></td>
</tr>
<tr>
<td>Pharmacist</td>
<td>Pharmacist</td>
<td>Read (Only see prescribed Medicine)</td>
<td>No</td>
</tr>
<tr>
<td>Hospital</td>
<td>Hospital</td>
<td>Read (General Information) +</td>
<td>Read (NID &amp; Card No) +</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write (Add admission record for visiting patient)</td>
<td>Write (only medical history)</td>
</tr>
<tr>
<td>Pathology Lab</td>
<td>Pathology Lab</td>
<td>Read (see prescribed Pathology Test) +</td>
<td>Read (NID &amp; Card No)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write (upload test report &amp; update record for assigned patient)</td>
<td></td>
</tr>
<tr>
<td>Pharmacy</td>
<td>Pharmacy</td>
<td>Read (Only see prescribed Medicine)</td>
<td>Read (NID, Card No &amp; prescribed medicine)</td>
</tr>
</tbody>
</table>

The major documents which are to be exchanged among different medical entities are patient’s medical reports. These documents should be exchanged securely. In our e-Health system all reports of the patient are encrypted before uploading to the patient's web medical directory. To observe a better security performance a cryptographic algorithm is needed to provide security function. To deliver a low cost and high quality of e-health service, both security and performance are required. A high level of confidentiality, integrity and availability must be maintained when the e-health service must be promptly provided. Again a secure algorithm slows down the process and degrades the system performance. Therefore, a trade-off between security and system performance needs to be considered carefully. So AES encryption algorithm is used which is optimum (Key size=128, 192 & 256 bit, Block Size=128 bit, speed=Fast (use byte substitution, row shifting, column mixing & key auditioning), Rounds=10, 12 or 16, crack able=Not possible) [5]. In our proposed system we used AES Rijndael-128 algorithm (key size=128) to encrypt and decrypt a file. To implement file encryption and decryption process we have used PHP Zend Framework 1.11.0 [13].

Sometimes people die or lose their organs for wrong treatment due to negligence of medical staff. Most of the cases suspected medical staff is unidentified due to the non-transparency of the system. So finding out medical staff who gives wrong treatment is a major concern. Medical staff gives health service through this e-health system and a central access log is
maintained to trace all kind of access information of each medical entity. Thus suspected medical staff will be identified at the
time of event or immediately after the event through this access log.

V. DEVELOPMENT AND TESTING

The proposed model has been developed at the Computer Lab of Bangladesh University of Engineering & Technology
(BUET) and tested at the medical center of BUET. This medical center has the facility of patient treatment, diagnostic test and
pharmacy. Doctors, nurses, medical technologists and pharmacists are also available at the medical center. Teachers and
Students have played the role of patient. The testing of this model has been applied on two hundred users (students, teachers,
doctors, nurses, medical technologists, pharmacists). The web based module with database server has been placed at BUET
data center and card module has been placed at BUET medical center. BUET administration has played the role of central
admin to verify & register users and to provide e-health card. Medical center has authenticated patient through e-health card
and provided e-health service. The following snapshots describe the testing output.

Fig. 4 shows the main page (web module) of the e-health system where central admin is logging to system to perform his
task. Each medical entity can login and can perform their task through this page.

Fig. 5 shows the issuance of e-health card for a patient through card module by central admin after successful registration
in the system through web module.

Fig. 6 shows the authentication and admission process of a patient through e-health card whenever he goes to a health
service point (BUET medical center) for treatment.
Fig. 7 shows that doctors can view patient's medical history with pathology test report (unencrypted format) before prescribing new medicine.

Fig. 7. Doctor views patient’s medical history before giving new prescription (Web Module)

Fig. 8 shows that doctor gives e-prescription to the patient assign to him.

Fig. 8. Prescribe Patient by a Doctor (Web Module)

VI. CONCLUSION

The proposed model is an effort towards facilitating information services to all medical entities and introduces an e-Health Card (Smart Card) for the general people, which can improve the total health care system. We have introduced colored e-health card for old and disable person to give priority e-health service. In our proposed model we have developed a centralized e-Health system with all medical entities to give faster service to the patient by replacing paper based medical record by web based medical record(e-Prescription, e-test report etc.) where the privacy of patient has been ensured by role based access. It also saves time, money and physical stress of the patient by delivering pathology report to the patient’s web medical record. Web medical records and reports have been secured by encryption. Fraud hospitals, clinics, pathology Labs, pharmacies, doctors, nurses are identified through the registration process which reduces corruption and abuse of medicine at health sector.
The proposed model also finds out the medical staff who gives wrong treatment as quickest possible time from central access log. So it will make the medical staff more responsive to their patient and reduce the scope of wrong treatment. Though the proposed model is developed for global architecture for a medical system of a country, but it can be implanted for a medical system of any organization within a small domain. Finally, our proposed model gives environment-friendly platform in health sector for any country.

ACKNOWLEDGMENT

The authors gracefully acknowledge the support from Bangladesh Bank and Institute of Information and Communication Technology (IICT) of Bangladesh University of Engineering & Technology (BEUT).

REFERENCES


BIOGRAPHY

Mohammad Tauhidul Alam is currently Maintenance Engineer of Bangladesh Bank (Central Bank of Bangladesh), Dhaka, Bangladesh and ex-lecturer of Computer Sciene & Engineering Department at BGC Trust University, Chittagong, Bangladesh. Mr. Alam earned B.Sc. in Computer Sciene & Engineering from Chittagong University of Engineering and Technology(CUET), Bangladesh and Masters in Information & Communication Technology from Institute of Information & Communication Technology (IICT), Bangladesh University of Engineering & Technology (BUET), Bangladesh. He has published journal and conference papers. Mr. Alam has done research projects with University of Chittagong and IICT(BUET). His research interests include digitalization of health sector using ICT, Telemedicine, Information Security, Data Analysis, optimization, interoperability. He is a member of Institute of Engineers Bangladesh(IEB) and Bangladesh Computer Society(BCS).

Dr. Md. Liakot Ali is currently Professor and Director of Institute of Information & Communication Technology (IICT) at Bangladesh University of Engineering & Technology (BUET), Dhaka,Bangladesh. Mr. Ali received his B.Sc degree in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology (BUET) in 1993, M.Sc. in Electrical, Electronic and Systems Engineering from Universiti Kebangsaan Malaysia (UKM) in 1998 and Ph.D in Electronic Engineering from Universiti Putra Malaysia (UPM) in 2001. He served as a R & D Engineer in few reputed national companies of Malaysia and also as Lecturer in Universiti Putra Malaysia. He has published journal and conference papers. His research interests include advanced electronic system design, IC design & testing and ICT application in health sector. He is fellow of Bangladesh Computer Society(BCS) and member of Institute of Engineers Bangladesh(IEB).