

Hospital Paperless Communication Technologies

Mehmet Unluturk (✉ mehmet_unluturk@yahoo.com)

Yasar University: Yasar Universitesi <https://orcid.org/0000-0003-1274-9361>

Semih UTKU

Dokuz Eylul University: Dokuz Eylul Universitesi

Research Article

Keywords: Electronic Health Records, HL7, RFID, Multiple Document Interface (MDI), NFC, Symmetric Encryption

Posted Date: May 14th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-392306/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Hospital Paperless Communication Technologies

Mehmet S UNLUTURK^{1,*}, Semih UTKU²

¹Yasar University, Department of Software Engineering, Izmir, Turkey

²Dokuz Eylul University, Department of Computer Engineering, Izmir, Turkey

* Corresponding author, e-mail: mehmet.unluturk@yasar.edu.tr

Abstract

Nowadays, patient-related records are kept in cumbersome file cabinets that result in wasted effort, during burdensome searches. As a result, when a patient goes to a different hospital, all those records need to be copied or all those tests have to be repeated for the same patient. In the present research, a secure, paperless operating room architecture (PORA) has been implemented which provides easily accessible patient information that can be safely shared between different hospitals. PORA is composed of three modules. The modules are the patient data input module, operating room server module, and treated patient information output module. In all, the modules allow researchers to edit, review and analyze patient-related data easily; as well as giving patients access to their healthcare information. Near Field Communication (NFC) technology supported with symmetric encryption is employed in PORA to provide the information security of transmitted data. NFC is utilized during the collection of medical records through wireless communication. This solution achieves better communication and accuracy among OR staff members. The PORA has been effectively used to help healthcare personnel and patients receiving treatment across different hospital operating rooms. PORA might be a unique solution for seamless patient information sharing between independent operating rooms.

Keywords: Electronic Health Records; HL7; RFID; Multiple Document Interface (MDI); NFC; Symmetric Encryption.

1. Introduction and Related Work

Information technology provides new opportunities for improving e-health [1] offerings [2]. A sustainable global open innovation ecosystem has been created for the healthcare sector in 2014 by European Union. Future Internet Social and Technological Alignment Research (FI-STAR) project [3] has been supported for the use of cloud computing. Patient treatment and diagnosis data's fast transmission and sharing are today's hot topic, in health management. Especially, the digital data involved in operation rooms (OR) is critical for e-health. For example, the "Software to data" paradigm underlines the importance of centralized databases for digital healthcare applications [4]. Software to data concept supports the provision of fast access to digital records in central databases. On the other hand, "E-Hospitals" integrate all people involved in healthcare into a seamless network, by allowing widespread data sharing [5]. Moreover, modern mobile technologies are increasingly used to reduce medical errors and enhance the quality of health services [6]. For example, Paschou et al. [7] provide a personnel rostering system that incorporates mobile technologies to reduce time overheads and increase staff satisfaction for healthcare units.

Nevertheless, problems still exist in healthcare information systems. For instance, verbal communication problem between patients and doctors is critical in healthcare services. In Canada, each year about 9,000 new brain stroke cases are consulted [8]. There is evidence that difficulty in getting reliable information from patients causes critical health problems. However, if there is fast access to the patient's records at a central database, then the available data can be self-explanatory in supplying the information about the patient.

Unfortunately, the manual processes of today's healthcare services are regarded as another major obstacle to providing fast and efficient healthcare services [9]. Patient history is still handled by pen, paper, and human memory; which is criticized in the work of Omachonu and Einspruch [10]. The work emphasizes the problem of health data integration and recommends paperless systems. Manual methods used today cannot provide appropriate and efficient solutions for the healthcare industry [11]. A solution is needed to increase the reliability of patient reports, which makes the data in paper files available to clinical processes. The solution requires computerized hospital information systems with improved distributed and interoperable information sources for operation rooms. Sulaiman et al provide a computerized hospital information system called Total Hospital Information System (THIS). THIS is aimed at providing a paperless environment [12].

Besides, there are many different applications and solutions for improving OR effectiveness [13]. For example, Strum et al [14] studied the utilization and capacity planning, in surgical services. 58,251 surgical records were studied to determine a model for measuring OR utilization cost. The provided model reports the cost of small delays in OR at a cost of approximately \$10.00 per minute, suggesting an incredibly expensive OR cost. In another study, Garbey et al propose an innovative, cost-effective OR management software system that provides automatically, daily OR scheduling [15]. Some other OR solution systems rely completely on radio frequency identification (RFID) [16]. For instance, RFID solutions have been used to improve the effectiveness of OR by tracking blood samples [17-18]. The related work points at paperless environments in all departments in hospitals.

In the rest of the study, the next section presents our motivation and contributions leading to the implementation of PORA and its modules. Section 3 discusses the security of PORA. Section 4 presents the discussion and finally, section 5 presents the conclusion and future work.

2. The Implemented Paperless Communication Network Architecture

2.1 Motivation and Contributions

Currently, there are no standards across operating room information system (ORIS) vendors. Furthermore, mobility and accessibility are limited within the available systems. Current software solutions usually run on desktops and assessments are usually made at the bedside. The result is limited vertical integration. In other words, the data collected within one section cannot be easily transferred to the next level of the healthcare system. Hence, it is obvious that interfacing of current ORIS with other electronic systems is undesirably limited [19]. The limitation can be identified as a missing online link between today's hospital information systems and the events in the OR [20]. There is a lack of a robust and efficient method of automatic information collection from the OR. In this study, to improve the current operating room information systems, Paperless Operating Room Architecture (PORA) solution has been implemented. This solution achieves better communication and accuracy among OR staff members. Paperless OR solution utilizes many technologies such as NFC, RFID, and location systems to manage the communication within the hospital. The PORA provides the following contributions to healthcare;

- Centralized databases for digital health applications,
- Data's fast transmission with HL7 standard,
- Allowing widespread data sharing,
- Reducing medical errors and enhance the quality of the health information,
- Seamless patient information sharing between independent operating rooms,
- Reducing redundant testing,
- Generating more accurate health data,
- Secure, paperless operating room architecture
- Better tracking of patients.

2.2 Paperless Operating Room Architecture (PORA)

Before explaining the modules of PORA in detail, the PORA actors and roles are depicted in Fig. 1. Doctors use the paperless system to input, view, update or delete patient data; prescribed medicine, treatment notes, and discharge report using a phone, PC, or tablet. The nurse matches the patient with the medicine and administers it using the database records provided by PORA. The patient is another actor carrying a wristband that identifies the correct patient uniquely, in the system. The registry is responsible for printing the patient wristband and linking the patient information into PORA. The login process into the paperless system by the actors is further explained in detail in Section 3 (Security in PORA).

The implemented PORA contains three modules (Fig. 2). The first module is called Patient Data Input Module (PDIM), the second module is called Operating Room Server Module (ORSM) and the third module is called Treated Patient Information Output Module (TPIOM).

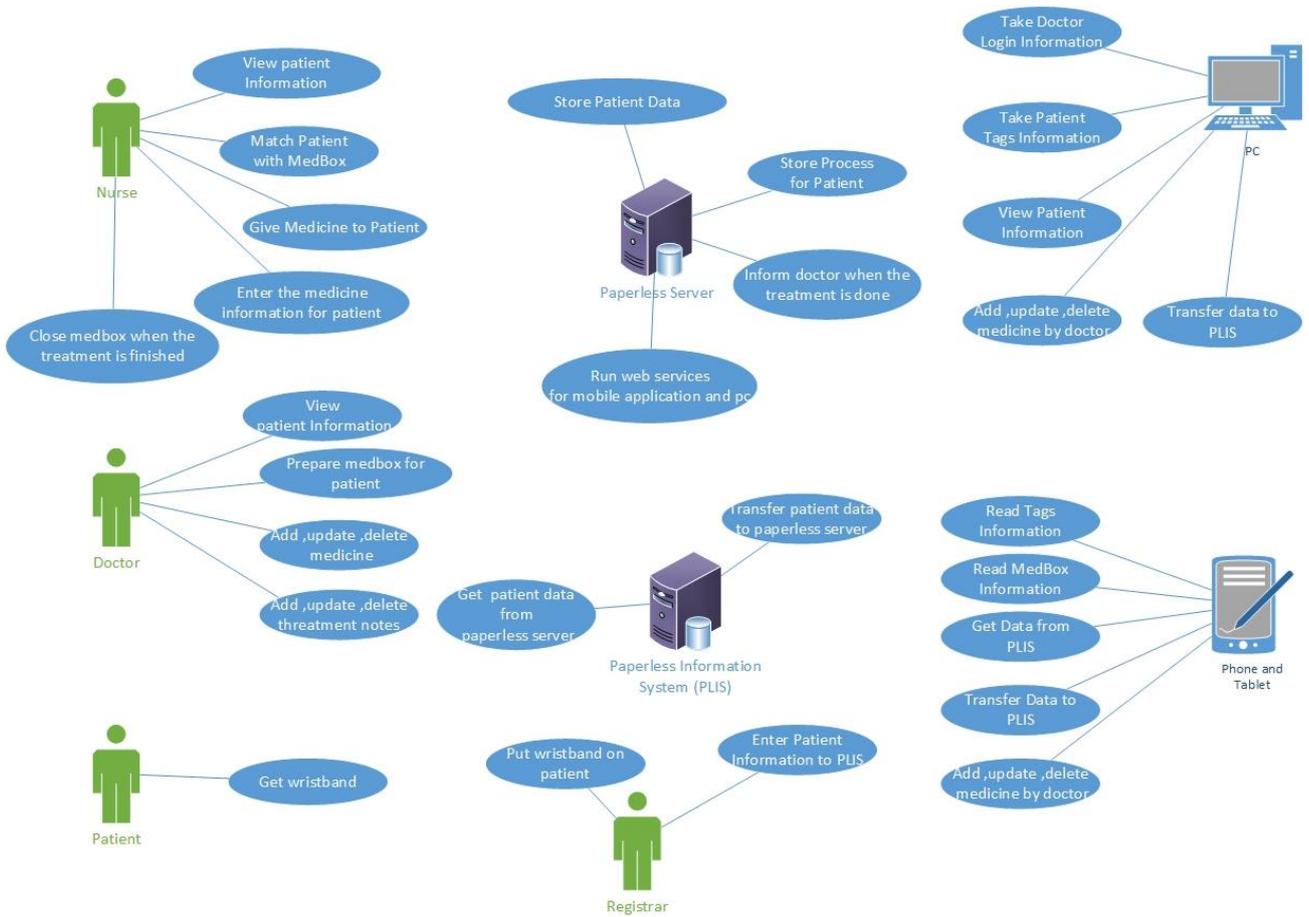


Figure 1: Paperless operating room actors and roles

2.2.1 Patient Data Input Module (PDIM)

PDIM collects patient's information for the PORA system by using its sub-modules. The PDIM of Fig. 2 contains four sub-modules. These are Location Client, Anesthesia Device Client, Operation Room Bed Client, and Hospital Information System (HIS) Client.

The Location Client is part of the PDIM. The Location Client provides location information of the patients with RFID (radio-frequency identification) and is integrated with the ORSM part of the PORA. The Location Client knows how to communicate with RFID tags worn by patients. As the patient moves from one room to another, RFID tags transmit these location messages to the Real-Time Location Server (RTLS) [21]. The operating room control panel client application is the consumer of these messages and the RTLS relays these messages to the control panel.

The Anesthesia device client (ADC) knows how to connect and communicate with the anesthesia device [22-23]. The client application sends the *FC_READ* command to receive anesthesia readings of the patient. These readings are recorded in the transaction tables. From the transaction tables, the control panel reads them and displays them for the hospital staff. UML class diagram is depicted in Fig. 3. Figure 3 shows the interface between the anesthesia device client and the transaction tables. Transaction table connection requires a connection object and a command object that is defined inside *IDatabaseAccess*.

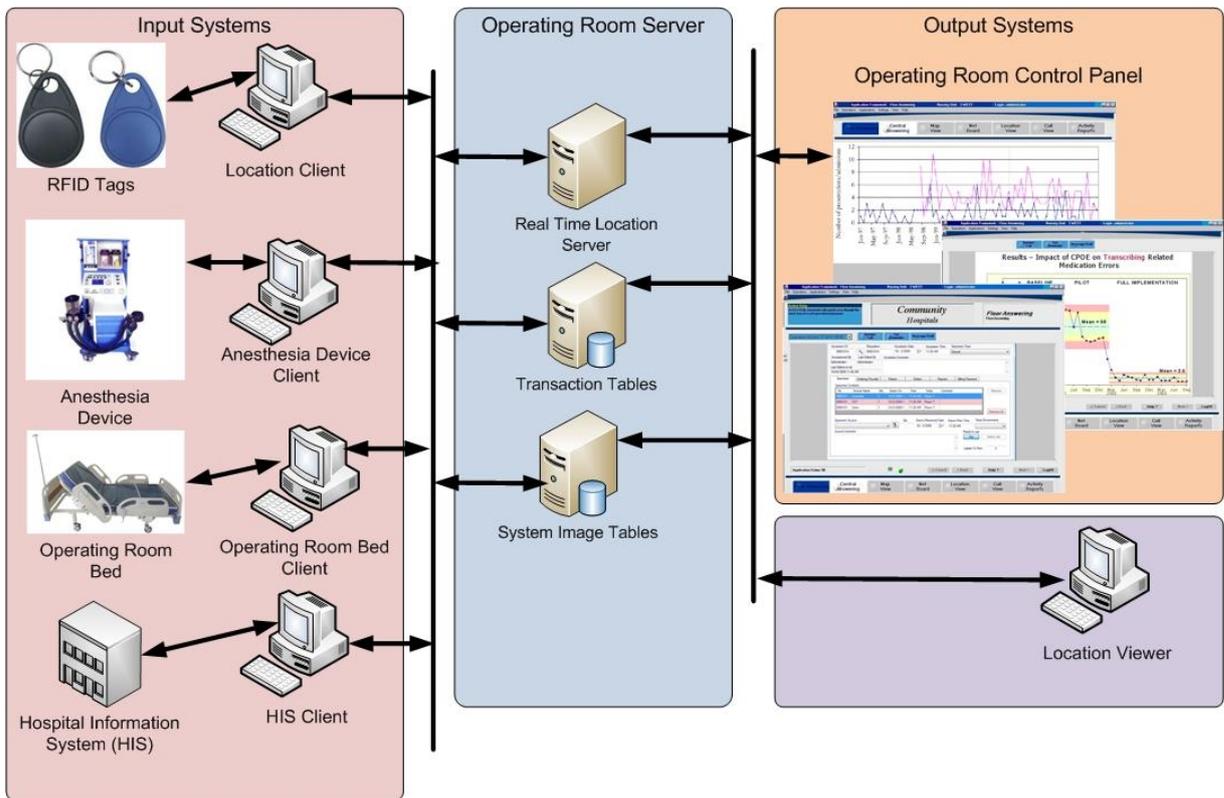


Figure 2: Paperless operating room architecture

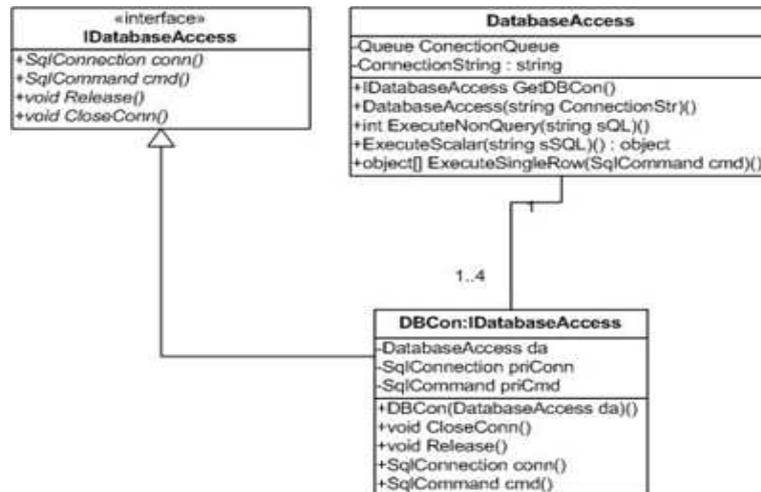


Figure 3: UML class diagram for Transaction tables

Main class *DatabaseAccess* holds a queue of connection objects. *DBCon* has this queue and implements the *IDatabaseAccess*. The client application calls the *DatabaseAccess.ExecuteNonQuery()* method to get a connection object from the *ConnectionQueue* and a command object to place the anesthesia readings into the traction tables.

The operating room bed client (ORBC) communicates with the operating room bed to properly initialize the bed before the patient arrives in the operating room through the operating room control panel (All-In-one). The most important feature of a surgery bed is that it is fully adjustable. It can be adjusted in many ways to make it easier to perform procedures during the surgery. Furthermore, it has precise adjustments to meet the specific needs of a patient. These necessary adjustments can be made through

the control panel's screen by the nurse in the operating room. With an All-In-one control panel, a nurse can see currently where the patient is and the patient's demographic information, make the necessary adjustments to the surgery bed, and the doctor can monitor the patient's anesthesia readings during the surgery.

HIS Client (HISC) provides patient's demographic information. The HISC receives the demographic data of the patient who is in the surgery room using HL7 [24] and shows these data in the room control panel to the staff in the operating room. Using a paperless system like this eliminates the duplication of entering the same data in different places and helps to decrease the data entry errors. The following string is generated according to the HL7 (Health Level 7) protocol [24] as the patients are accepted to the hospital. This string includes the demographic information about the patient as well as the patient-bed information.

```
MSH|^~\&|REGADT|MCM|PCAPP|GATEWAY|198808181320|SECURITY|ADT^A01|MSG00002|P|2.2|<CR>
EVN|18|198808181318||<CR>
PID|||PATID5678^9^M11||SMITH^CARTER^V^JR||19310615|M||C|303 EDWARDS
...DRIVE^FIELDGREEN^NY^29420|AL| (312)949-1131|
(312)949-...0101|M||PATID12345001^2^M10|987654321|143257^NYC|<CR>
NK1|1|JANE^ALICE^U|WIFE|| (312)949-1131<CR>
PV1|1|I|1WES^440^1^A|||004444 ...
```

Patient bed information comes from the Patient Visit 1 (PV1) field of the above HL7 string. This field contains five components: nursing unit; room number; bed ID; facility and bed status. For the above string, Mr. Smith is admitted to bed 4401. And the following XML string is created for RTLS (Fig. 2) after parsing the above HL7 string.

```
<HIS>
  <PatientAdmit>
    <Name>SMITH CARTER V JR</Name>
    <Bed>4401</Bed>
    .....
  </PatientAdmit>
</HIS>
```

The RTLS relays this XML message to the control panel. On the control panel, a nurse can see the bed information and as well as the other demographic information about SMITH on the screen.

2.2.2 Operating Room Server Module (ORSM)

ORSM is the server part of the system which stores sharable PORA data. The ORSM contains three sub-parts. These are real-time location servers (RTLS), transaction tables, and system image tables.

The PORA has a real-time location server (RTLS). The RTLS listens to the location messages that come from the location client. The RTLS is the operating room server and is used for all-time critical information transfer where delays of seconds can affect the usefulness of the control panel and the location viewer. It receives all location changes from the RFID tags and delivers them to the control panel application which has registered to receive location messages. Because of the real-time nature of the information, the RTLS does not hold any data. This system is very scalable due to the RTLS publishes real-time events to only those consumers that have subscribed to them.

The transaction tables hold the patient's clinical data while in surgery and the doctor can review these data after the surgery. Inside the operating room, the nurse can see the location of the patient on the operating room control panel screen. During the

operation, the information that comes from the anesthesia device is received by the anesthesia device client and is saved into the transaction tables. Furthermore, this can allow transmitting these data from one hospital to another and can help researchers to search the health-related data securely. Since the patient data is saved, the patient himself/herself is also able to access his/her health-care information.

The system image tables hold the current status of the patient. When the status of the patient is changed, the old data is replaced with the new current status. The location view uses these tables to show the current status of the patient whether the patient is still in the surgery room or not to the patient’s relatives outside the operating room. Transaction tables and the system image tables are created using SQL Server 2008. The next section explains the operating room control panel in detail.

2.2.3 Treated Patient Information Output Module (TPIOM).

The TPIOM has two parts. These are the Operating Room Control Panel (All-In-one) and location viewer. The operating room control panel is the main part of the TPIOM which is an MDI (multiple document interfaces) form that composes of different user interfaces where each interface shows a different set of data. The first application that is loaded inside the control panel shows the location of the patient, the second application shows the demographic data of the patient, the third application shows the configurable settings for the operating room bed, and the last application shows the data coming from the anesthesia device. Each of these applications implements the following *ICommunicateWithApp* interface. Moreover, any new application that implements the *ICommunicateWithApp* interface (Fig. 4.a); will become part of the panel.

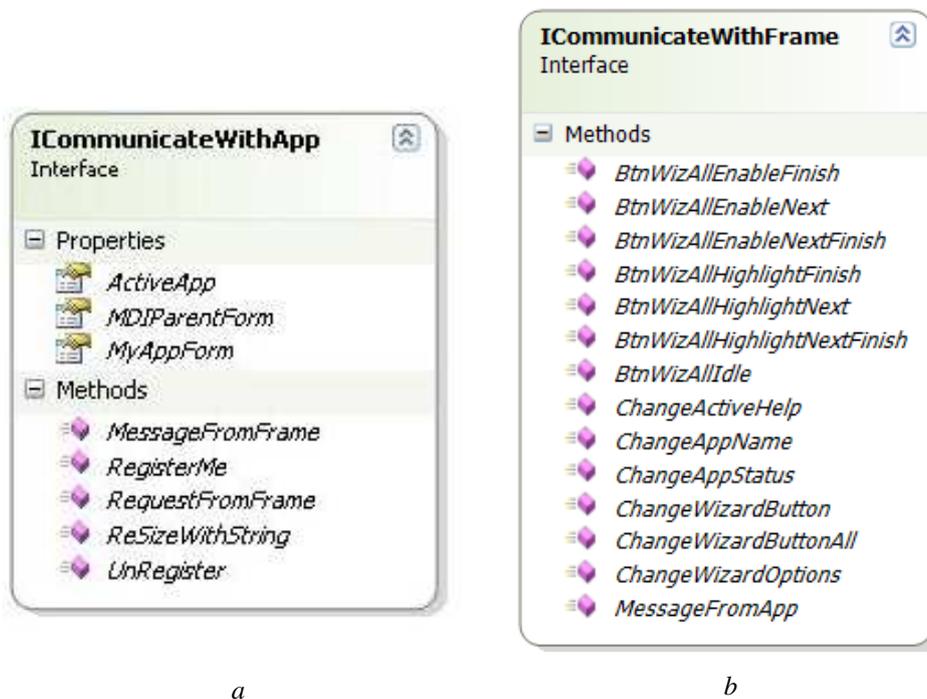


Figure 4: Application Interface (a) *ICommunicateWithApp* Interface, (b) *ICommunicateWithFrame* Interface

When the application is loaded into the MDI form as a background process, the value for *ActiveApp* will be *false*. When it becomes true, the MDI form draws the application’s main form (*MyAppForm*) inside the control panel’s client area. The *ReSizeWithString* command carries the information to resize the *MyAppForm*. The *RegisterMe* command sends the

ICommunicateWithFrame interface (Fig. 4.b) to the application so that the application can send messages such as warning messages to the control panel. When the nurse makes changes on the screen, those messages are sent through the *MessageFromFrame* command. When there is a request from the control panel, and the panel expects a response from the application, then the control panel uses the *RequestFromFrame* command.

Control panel implements *ICommunicateWithFrame* (Fig. 4.b) interface. Each foreground application sends messages using the *MessageFromApp* command. The *BtnWizAll** and the *Change** commands are used by the active application to disable/enable buttons, on the hospital's logo, the text content for help, and the menu items on the control panel's screen. The hospital information system client is presented in the next section.

The location viewer displays the location information about the patient. The RFID tag is worn by a patient [25]. The antenna on this tag picks up the electromagnetic energy beamed at it from a reader device. This energy makes this tag transmit its unique ID to the reader device and allowing the patient to be remotely identified [26-27]. The reader translates the radio wave received from the tag into digital information that is transmitted to the location client (Fig. 2). The location client creates the following XML message and sends it to the RTLS.

```

<LocationChg>
  <MsgID>155</MsgID>
  <BadgeID>2345</BadgeID>
  <LocName>101</LocName>
  <TimeEntered>11/23/2014 4:23:34 PM</TimeEntered>
  <PrevLocName>Hallway</PrevLocName>
  <Patient>
    <BadgeTypeName>Patient</BadgeTypeName>
    <LastName>Doe</LastName>
    <FirstName>John</FirstName>
    <MiddleName>JD</MiddleName>
    <PatientID>99998745</PatientID>
  </Patient>
</LocationChg>

```

Location viewer receives the above XML message from the location client through RTLS. The location viewer parses that message and displays the information about the patient on the location viewer client for the nurse. Location viewer client application screen is depicted in Fig 5.

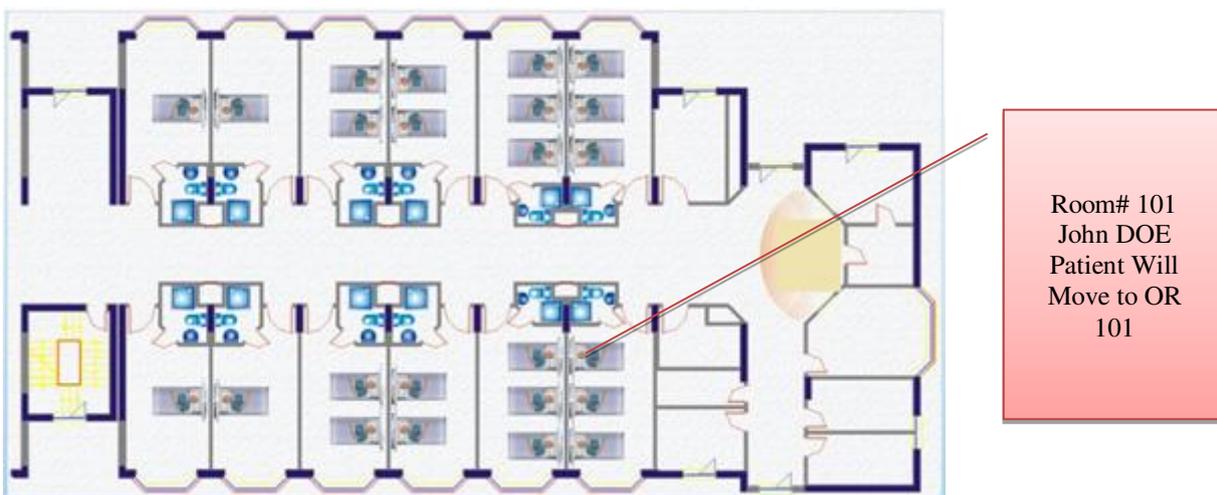


Figure 5: Location viewer client screenshot

3. Security in PORA

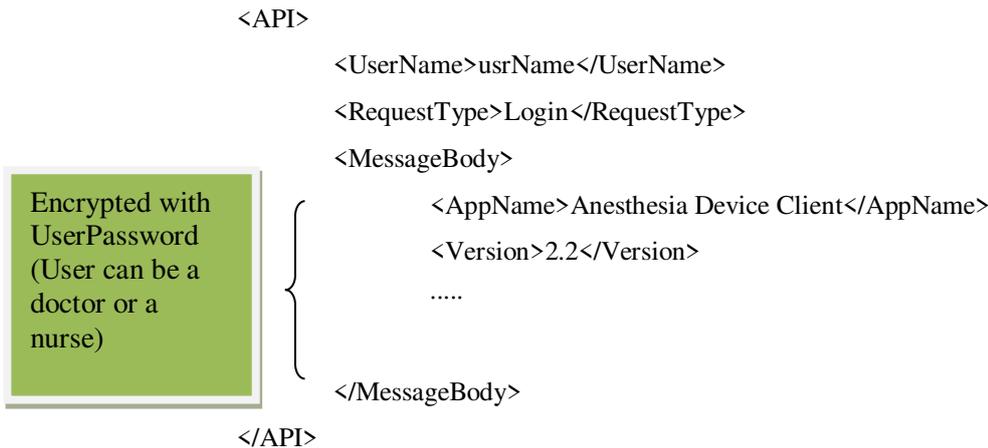
Security of the patient information is very critical. Messages are XML messages and they are clear text. To prevent the attacks, these messages need to be encrypted before they are sent over the hospital network. The doctor, nurse, and patient are the main actors of the PORA solution. Each one has an NFC card or wristband (for a patient) to authenticate themselves with the paperless operating room architecture (Figure 2). The main component of the security solution is to have all the client machines equipped with an NFC reader in the operating room. The security of the system starts with registering the NFC cards of the doctors, nurses, and the NFC wristband of the patient. NFC technology is utilized for the authentication of the main actors. The next section presents the card registration of the main actors [28].

3.1 Actor Registration

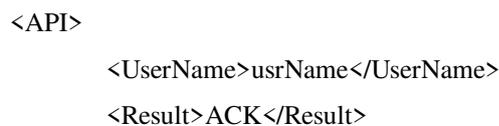
The process of registration starts with getting a card ID and writing that information into the system database. The owner of the card (it could be a doctor or a nurse) also enters the user name and password. So, the credentials of the owner are saved along with the card ID into the database. This information will be used by the system to authenticate the doctor or the nurse.

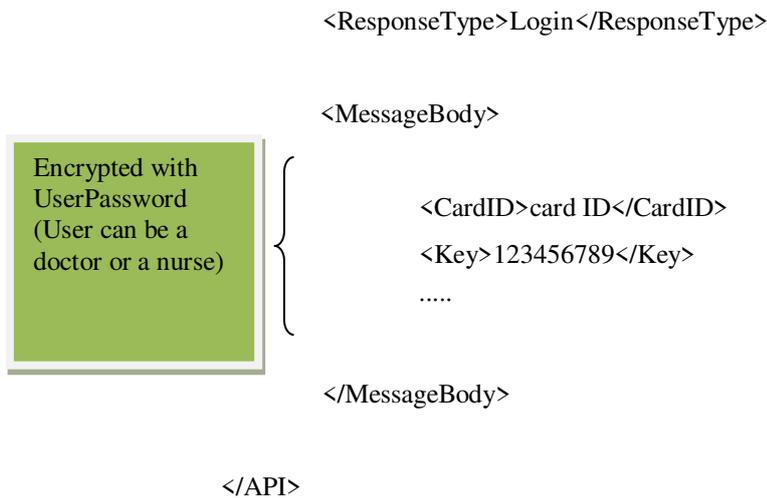
3.2 User Login

Before the client application logs in with the operating room server, the client application asks the doctor or the nurse to enter their user name and password. The client application creates the following Login XML message and encrypts the *MessageBody* only with the user password and sends the XML message to the server.



The encryption method is symmetric encryption at this stage. When the server gets the XML message, it uses the *usrName* to get the *UserPassword* from the database. If the server cannot find the password, then it rejects the connection with the client application. If the server finds the password, it decrypts the *MessageBody* with the *UserPassword*. The server checks the database if the details of the client such as *AppName* and *Version* number do match with the details presented inside the *MessageBody*. If they do, the server gets the *cardID* from the database for *usrName*. The server encrypts the *cardID* and the symmetric key (which will be used to encrypt the future messages) with *UserPassword* and sends it back as a response for the Login request.





When the client application receives the response XML message, it decrypts the *MessageBody* with the *UserPassword*. When it sees the *ACK* inside the *Result* field, it asks the user to have their card read by the NFC reader attached to the client machine. The *cardID* read by the client machine is compared with the *cardID* in the *MessageBody*. If they do match, then the doctor or the nurse is authenticated to use the client application. Otherwise, it will disconnect the connection with the server and will ask the user to enter the user name and password again. The next section presents how to generate the value for the *Key* field (symmetric key, seen in the above XML response message) for the symmetric encryption process by the server.

3.3 Generating Keys

The server uses the memo-HASP4 hardware dongle to generate keys and to control how many client applications can run in the operating room. For example, if the hospital buys two licenses for the operating room bed client, the server will let connect only two-bed clients to the server concurrently, otherwise, the third bed client will wait until one of the two-bed clients drops the connection with the server. The information about the number of licenses is written inside the memo-HASP4 hardware dongle before it is shipped to the hospital.

The server runs the following C#.NET code to get the unique ID from the dongle.

```

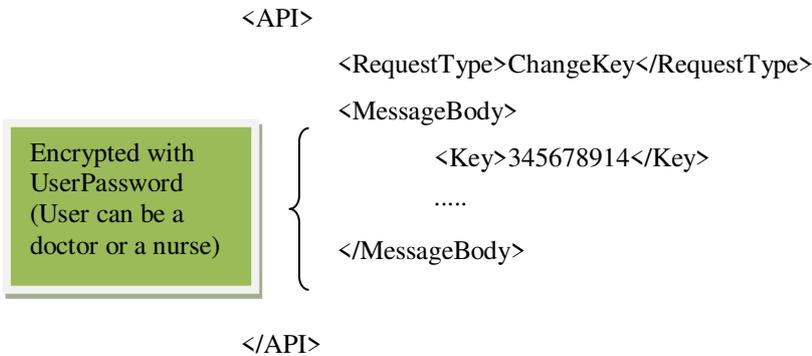
int intRandomNumber = RandNums.Next(10) + 1;
Hasp.hasp(
    (int)HASP_SERVICE.LOCALHASP_HASPCODE,
    (int)m_dblArrayHaspTable[intRandomNumber, 1],
    (int)HASP_CONSTANTS.HASP25,
    m_intPassw1,
    m_intPassw2,
    ref m_lngP1,
    ref m_lngP2,
    ref m_lngP3,
    ref m_lngP4

```

);

where $m_intPassw1$ and $m_intPassw2$ are the unique HASP passwords provided when the dongle is purchased. The $m_dblArrayHaspTable$ is the two-dimensional HASP table that consists of unique numbers and is provided by the HASP dongle. The return four values are kept inside the m_lngPX (where $X= 1, 2, 3, 4$). The server uses one of those four values as the unique key for the symmetric encryption process of the PORA solution.

It repeats this process at certain time intervals. Once the unique id changes, it encrypts the following XML message. The request type is the *change key*. Inside the message body, there is the new *Key* and is encrypted by the client's user password.



The future request-response messages are encrypted/decrypted with this new *Key* from the dongle.

3.4 Patient Registration

When a patient enters the hospital, the personal information is taken by a nurse and is recorded by the hospital information system. The HIS delivers this information through HL7 to other client applications such as HISC (Fig. 2) in the hospital. During the registration, the NFC wristband is assigned to the patient and personal information with the NFC wristband ID is sent to the database by the HIS client (Fig. 2). Before the surgery starts, the patient has to be authenticated using the NFC wristband carried by the patient. All the patient consultation information is displayed in the operating room control panel (Fig. 2). At this stage nurse or doctor can see the patient information, current treatments, or the history of the previous treatments with all the details on the control panel. This security process provides a patient the right treatment.

Furthermore, this PORA solution can track patients within the hospital and utilize the NFC technology coupled with symmetric encryption. After the communication starts, the XML messages used between the disparate devices are all clear text messages and can be easily seen by intruders. To prevent unauthorized access to the PORA system, these messages are encrypted with the key provided by the HASP dongle. The next section presents the discussion.

4. Discussion

Within the PORA, the majority of the network traffic consists of location messages. There are between 10-20 location moves within one minute. Messages are XML messages and carry enough information to identify the location of the nurse, equipment, or the patient remotely. This network traffic can be very significant which delays the process of paperless transactions within the hospital. Several different methods need to be implemented to reduce the traffic within the network.

If a new device such as an Anesthesia device from a different vendor needs to include in the PORA system, there needs to have a client software application created for it. This is the bridge application that connects the device to the PORA network.

Unfortunately, the software is device-dependent. And every time a new device is added, specific device-dependent software needs to be created for the newly added device. The part where the network communication happens is established through the same network component that each client uses (software-reuse). But the communication part with the newly added device is device-dependent. Until standards get developed, the PORA might be an effective way to connect disparate devices within the hospital network. Table 1 summarizes the comparison between analyzed proposals and PORA.

Table 1 Comparison of Proposals and PORA

	E-Hospitals[5]	Personnel Rostering System [7]	THIS[12]	OR Management Software [16]	PORA
Centralized databases	Provide	No	Provide	No	Provide
Allowing widespread data sharing	Provide	No	Provide	No	Provide
Information sharing between OR	General solution	No	General solution	Yes	Yes
Secure Architecture	No	No	No	No	Yes
HL7 standard	No	Yes	Yes	No	Yes
Paperless Solution	Yes	Yes	Yes	Yes	Yes
Mobile Solution	No	Yes	No	Yes	Yes
NFC / RFID	No	No	No	RFID	NFC / RFID

There are many commercial software products available in the market. GE Medical Systems offers a digital operating room environment to improve the efficiency of doctors and nurses. Furthermore, this system enhances patient satisfaction, and this digital environment aims to integrate all the devices to report electronically in real-time. However, there is no secure login process similar to the one presented in this paper for the PORA system.

Doctors, nurses, patients, and equipment are not remotely tracked by using RFID as well. In the PORA system, the location information is transferred automatically into the system where the nurses can easily track the patient's whereabouts before and after the surgery within the hospital. Another example is the Inova Health System. It uses the fingerprint coupled with encryption technology for the login process to its paperless system. This paperless system prevents constant documentation during surgical procedures, and many incompatible devices are integrated within the surgical room to pump medical data into their system as medical records in real-time. These medical records provide accurate billing and correct inventory for the hospitals. However, the electronic data pumped by several incompatible devices are not protected and are all clear text messages. Table 2 summarizes the differences between the PORA system and the other commercial software products available in the market.

Table 2. Comparison of PORA System with the other commercial software products

Consideration	GE Medical Systems	Inova Health System	PORA System
Secure Login	No	Yes	Yes
Secure Communication between Devices	No	No	Yes
Patient Tracking	No	No	Yes

5. Summary and Future Work

The paperless operating room is presented to create an electronic health record system where the nurses or doctors do not enter any information inside the operating room. The patient's location information comes from the location system and is recorded as a database transaction inside the database tables. The bed occupancy and the patient's demographic data come from the Hospital's ADT system and all this information is shown on the control panel's (all-in-one) screen. Before the patient arrives, a nurse can adjust the operating room's bed settings easily on the control panel's screen. During the surgery, the patient's anesthesia readings are recorded as database transactions and can be analyzed by the doctor after the surgery. Within all this system, hospital staff becomes paperless. All this electronic information can also be shared with outside healthcare providers.

Patient information is top secret and must be protected from unauthorized people. There are many different ways to create secure solutions inside the hospital. Better technology is using the NFC technology. It is easy to identify the NFC cards but it is not easy to copy them. Using the symmetric encryption methods and getting the secure encryption keys from the HASP hardware dongle may be an effective methodology for well-secured solutions for the hospitals.

For future work, these services may be offered inside the cloud-based systems. This will help the hospitals to save money since the maintenance of the current hardware will be handled by outside companies.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

6. References

- [1] Chiasson MW, Davidson E (2004) Pushing the contextual envelope: developing and diffusing IS theory for health information systems research. *Inf Organ* 14(3):155–188. doi:10.1016/j.infoandorg.2004.02.001
- [2] Lin IC, Hou YH, Huang HL, Chu TP, Chang RE (2010) Managing nursing assistants with a web-based system: An empirical investigation of the mixed-staff strategy. *J Med Syst* 34:341–348. doi:10.1007/s10916-008-9246-5
- [3] EU Project, “FI-Ware. Future Internet Core Platform,” Future Internet — Public Private Partnership (FI-PPP), Apr. 2011–Mar. 2014, <http://www.fi-ware.eu/>
- [4] Thuemmler C, et al. (2013) Applying the Software-to-Data Paradigm in Next Generation E-Health Hybrid Clouds. *Information Technology: New Generations (ITNG)* 459-463, doi: 10.1109/ITNG.2013.77
- [5] Randeree E, Rao HR (2004) E-health and assurance: Curing hospital websites. *Int J Electron Healthc* 1(1):33–46. doi:10.1504/IJEH.2004.004653
- [6] Waterson P, Glenn Y, Eason K (2012) Preparing the ground for the “paperless hospital”: a case study of medical records management in a UK outpatient services department. *Int J Med Inform* 81(2):114–129. doi:10.1016/j.ijmedinf.2011.10.011
- [7] Mersini P, et al. (2015) Enhanced healthcare personnel rostering solution using mobile technologies. *J Sys Soft* 100:44-53. doi:10.1016/j.jss.2014.10.015
- [8] Long H, et al. (2014) Enabling RFID technology for healthcare: application, architecture, and challenges. *Telecommun Syst* 58(3):259-271. doi:10.1007/s11235-014-9871-x
- [9] Jha AK, Doolan D, Grandt D, Scott T, Bates DW (2008) The use of health information technology in seven nations. *Int J Med Inform* 77(12):848–854. doi:10.1016/j.ijmedinf.2008.06.007
- [10] Omachonu VK, Einspruch NG (2007) Systems engineering in the healthcare service industry. *Int J Healthc Technol Manag* 8(1):161–172. doi: 10.1504/IJHTM.2007.012108
- [11] Costa AL, Oliveira MMB, Oliveira MR (2004) An information system for drug prescription and distribution in a public hospital. *Int J Med Inform* 73(4):371–381. doi:10.1016/j.ijmedinf.2004.02.006
- [12] Ahmadi H, et al. (2015) Exploring Potential Factors in Total Hospital Information System Adoption, *J Dec Sup Sys*. 2(1):52-59
- [13] Hasan AE, et al (2015) Future Internet in Surgical Operating Theatre. *Information Technology* 580-585. doi:10.1109/ITNG.2015.97
- [14] Strum DP, Vargas LG, May JH, Bashein G. (1997) Surgical suite utilization and capacity planning: a minimal cost analysis model. *J Med Syst* 21:309–22. doi:10.1023/A:1022824725691
- [15] Garbey M, et al. (2015) An intelligent hospital operating room to improve patient health care *J Comp Surg* 2:3. doi:10.1186/s40244-015-0016-7
- [16] Liu CC, Chang CH, et al. (2011) RFID-initiated workflow control to facilitate patient safety and utilization efficiency in operation theater. *Comput Methods Prog Biomed*. 104(3):435-42. doi:10.1016/j.cmpb.2010.08.017
- [17] Kumar S, Swanson E, Tran T (2009) RFID in the healthcare supply chain: Usage and application. *Int J Health Care Qual Assur* 22(1):67-81. doi:10.1108/09526860910927961
- [18] Lahtela A, Saranto K (2009) RFID and medication care. *Stud Health Technol Inform*. 146:747-8. doi:10.3233/978-1-60750-024-7-747

- [19] Jesse ME, Mohamed AR (2011) Anesthesia Information Management Systems: A Review Of Functionality And Installation Considerations. *J Clin Monit Comput*. doi: 10.1007/s10877-010-9256-y
- [20] Agarwal S, Joshi A, Finin T, Yesha Y (2007) A pervasive computing system for the operating room of the future. *Mobile Netw Appl* 12:215–228. Doi:10.1007/s11036-007-0010-8
- [21] Kim DS, Kim J, Kim SH, Yoo SK (2008) Design of RFID based the Patient Management and Tracking System in hospital. *Conf Proc IEEE Eng Med Biol Soc*. 1459-61. doi:10.1109/IEMBS.2008.4649442
- [22] Bressan N, et al. (2007) Synchronization Software for Automation in Anesthesia. *Conf Proc IEEE Eng Med Biol Soc*. 5298-301. doi:10.1109/IEMBS.2007.4353537
- [23] Cossu M, Furfori PA, Taddei A, Mangione M, Del Sarto P (2011) Anesthesia Information Management System in cardiac surgery. *Computing in Cardiology*. 577- 580
- [24] Health Level Seven. HL7 message standards. Ann Arbor: Health Level Seven International. <http://www.hl7.org>
- [25] Chowdhury B, Khosla R (2007) RFID-based Hospital Real-time Patient Management System. *Int Conf on Comp and Inf Sci*. 363-368. doi:10.1109/ICIS.2007.159
- [26] O'Halloran M, Glavin M (2006) RFID Patient Tagging and Database System, *International Conference on Networking*.162, doi:10.1109/ICNICONSMCL.2006.187
- [27] Cangialosi A, Monaly JE, Yang SC, Leveraging RFID in hospitals: Patient life cycle and mobility perspectives. *IEEE Communications Magazine*. 45(9): 18-23. doi:10.1109/MCOM.2007.4342874
- [28] Özcanhan M H, Dalkılıç G, Utku S (2014) Cryptographically supported NFC tags in medication for better inpatient safety. *J Med Syst* 38(8):1-15. doi: 10.1007/s10916-014-0061-x