AC 2009-311: PIMS: AN ARCHITECTURE FOR A WEB-ENABLED PATIENT INFORMATION AND MONITORING SYSTEM

Mudasser Wyne, National University, San Diego

Mudasser F. Wyne received his Ph. D. from University of Birmingham, UK. He has also received degrees in B.Sc. in Electrical Engineering and MS in Engineering. He is currently serving as a Professor of Computer Science at National University, San Diego, USA. He has served at different positions in academia for the last 20+ years at various universities in USA and other countries. He is currently serving on the editorial boards of various journals and program committees for many international conferences. He is also the co-chair for ICSTC-2009 conference. His research interests include Database, intelligent systems, information system and health informatics. He is the author of numerous journal and conference publications. He has managed numerous projects for various private companies and government organizations. Dr. Wyne is a member of ASEE and ACM.

Arzu Baloglu, Marmara University, Turkey

Dr. Baloglu, completed her undergraduate at Technical University of Istanbul, her MBA in production management, and her PhD in Information Technology at University of Istanbul. She has experience of 15 years in production and technology management. She worked for various plants including manufacturing, service and consulting companies as middle or top manager (Ernst and Young Consulting Turkey), where she added important values within 5 years. Also she worked in SAP Business for a long time and managed various SAP/ERP projects in Turkey and also abroad. Now she is serving in ERP, CRM and e-business categories as senior consultant and lecturing at various universities. Additional to these she is sometimes giving conference seminars and company trainings in her expertise areas. Dr. Baloglu has about 15 professional and academic papers, published in various technology magazines and books. And she currently works for Marmara University - Dept. of Computer Engineering under title of Asst. Prof and also teaches the some courses in Yeditepe University as part time lecturer.

PIMS: AN ARCHITECTURE FOR A WEB ENABLED PATIENT INFORMATION & MONITORING SYSTEM

Abstract

Health Related information and personalized information retrieval and access is critical to applications in the medical and healthcare domain where the accuracy of the retrieved information and obtaining it in a time-critical situation are extremely important. In this paper we present our ideas regarding a new architecture for a web enabled Patient Information and Monitoring System (PIMS). PIMS is a multi tier web-enabled system, which focuses on medical information storage, management and retrieval, instead of simply financial functions, so characteristic of more traditional Hospital Information Systems (HIS). We observe that many medical information systems suffer from the centralized nature and inflexibility of their design, and fail to satisfy the distributed requirements of a global healthcare system. Our motivation for PIMS derives from the tremendous increase in available electronic medical information and demand for quick information access. We present the conceptual and operational architecture for an information system that integrates advanced web and information technology to retrieve information. In addition, the system provides not only all of the functionality of a traditional HIS, but also incorporates the distributed flexibility and access of the Web.

Keywords: *Web enabled, Information System, Distributed System, Knowledgebase, Database, Software Architecture, Protocols.*

1. Introduction

Healthcare has become one of the most important service industries undergoing rapid structural transformations. In this transformation, a number of factors have contributed towards making access to patient health information, a critical success factor for health organizations including hospitals, clinics and other medical facilities[11]. A patient's health record may be composed of heterogeneous data with varying granularity as well as different display formats. On the other hand this data may directly come from clinical observations or be the result of several processing steps performed on images captured from different sources[10]. Information overload and complexity of data storage format leads to the need of more flexible solutions for information presentation to the users, whether they are patients, staff, physicians or simply general users seeking health information. In general, health professionals have to review large quantities of data to gain access to relevant patient information. Medical information must also be available and shareable among different physicians so that they can exchange their diagnosis or discuss patient history and symptoms. However, this access needs to be without the constraints of semantic and location diversity.

In today's information age where knowledge updates continuously and quickly, people need fast, accurate and efficient means of acquiring and processing information. In many countries, and especially developing countries, a driving force for healthcare has recently been the trend towards better coordination of all health related activities[12]. In this respect, the focus has changed from isolated procedures in a single healthcare institution (e.g. a hospital or a clinic) to the patient-oriented care process spreading beyond institutional boundaries. This approach, as a result, leads to a shift towards better integrated and shared healthcare services. In this new scenario the healthcare providers and healthcare professionals in a region and even worldwide, have to cooperate and exchange data and information in order to secure better treatment for patients[1].

Hospitals and healthcare providers have always been among the first to use information technology (IT) to improve their services. However, applications developed for hospitals in the late 1950s and early 1960s were designed from business computing models and thus were used for accounting, billing, inventory and similar business-related functions. Applications developed after this time were primarily used for storing patient information, such as contact information, date of birth, allergies, treatment and procedures. These applications, named Hospital Information System (HIS), were designed primarily for front desk medical staff use only. Most of these types of traditional HIS would have following deficiencies[9]:

- Limited financial billing and basic health record information. Such systems are finance-centric, thus making it very difficult to manage medical information efficiently.
- Inability to integrate and share the scattered Electronic Medical Records (EMRs) especially when a patient has been hospitalized or treated in different facilities..
- Based on Client/Server architecture, they only provide limited functions and cannot efficiently support new web technology. Some are not even able to support the international standard Health Level-7(HL7).

Modern healthcare environments can exploit immense advances in Information and Communication Technologies (ICT) in order to increase the quality as well as the quantity of healthcare services provided. However, several privacy and security problems become much more intense in shared environments, where healthcare services are offered by multidisciplinary teams of healthcare professionals, to patients and other stakeholders or at least through remote interconnected HIS[4,8].

In the remaining part of the paper we present the motivation for the new system, introduction to PIMS, functions that the system can provide, architecture design, communication channels in the system, survey and finally conclusion and future work.

2. Motivation

Today, it is hard to imagine healthcare without IT. Quality of information processing is an important factor for the success of healthcare institutions. Therefore good information systems must support clinical workflow in various ways and thus, translate into better patient care. At the same time, poorly designed HIS can have negative effects on both efficiency and quality of patient care[15]. In most hospitals, HIS consist of patient care processes such as, patient admission completion and documentation of diagnostics and therapeutic tasks, patient discharge and transfers. In addition to this, many of the existing information systems 1) use very centralized data (Physically located at a single healthcare centre) and 2) focus only on providing a single aspect of the patient healthcare. For example, Chronic Disease Management System[14] only deals with the management of the chronic diseases, Regional Health Information System[12] expands the idea to a regional level but the integration of information is not at the high level of architecture (as will be discussed later for PIMS). Personal Health Information Management System[7] contains patient information but at the same time lacks any information about the laboratory exams, images, clinical reports etc. Similarly ICU (Intensive Care Unit) Information Systems[13] only handles data that is generated and used while the patient is admitted to the intensive care unit. Other approaches have been used to bring diversified information together into a central storage point with predefined data structures[2,5]. Healthcare information networks, such as those providing information in preventive healthcare e.g. the European Citizens Advisory System (ECAS) or Regional Health Information Systems (RHIS), like the WashingtonReginal2 or a domain specific application related to medical and healthcare information systems[6] are examples of attempts to integrate diversified information. The US department of Veterans Affairs (VA) began deploying its VISTA (Veterans Health Information Systems and Technology Architecture) system in all of its medical facilities starting around 1983. The system was originally known as the Decentralized Hospital Computer Program (DHCP) system. The initial "core" system that was deployed consisted of a limited number of clinical and administrative software modules, which included patient registration, inpatient ADT, outpatient clinic scheduling, pharmacy, laboratory, and radiology. Over the years many additional software modules were added, and the DHCP was eventually renamed VISTA. It is built on a client-server architecture, which ties together workstations and personal computers with graphical user interfaces at Veterans Health Administration (VHA) facilities, as well as software developed by local medical facility staff. VISTA also includes the links that allow commercial off-the-shelf software and products to be used with existing and future technologies. The Decision Support System (DSS) and other national databases that might be derived from locally generated data lie outside the scope of VISTA. (www.va.gov/vista_monograph).

Thus we conclude that most of the HIS currently in use suffer from the centralized nature of their design, and fail to meet the distributed requirements of a national healthcare system due to their lack of flexibility. The dynamic medical and healthcare environment, characterized by an ever increasing legislation, new medical standards, reorganizations and changes in medical processes, is causing the medical and healthcare information networks presently in use to become unstable. Users today, more than ever, require an agile, extremely flexible system that can meet all their needs in a time critical manner as well as can be easily adapted with minimum effort to meet their changing needs.

Our motivation for a new system, PIMS, derives from the fact that there is a tremendous increase in available medical information electronically and the demand to have quick access to this information. However, the distributed nature and complexity of data causes an information overload problem for existing system. This can seriously impede information retrieval precision as well as slow down the information retrieval process. Since patients receive medical assistance in multiple clinics and hospitals during their lifetime, this leaves vital information in a dispersed manner. At the same an efficient patient care should take into account all of the related information in order to check for incompatibilities, avoid unnecessary exams, and obtain relevant clinical history. Thus we are committed to the goal of integrating all the related patient information within a given healthcare system for all hospitals and other medical facilities. In addition we also desire to provide the patient related information over the internet to physicians, patients and other general users. In our approach we want to exploit the very fact that internet is easily available to everyone so we can integrate web and HIS and use distributed data to our advantage. Hence, healthcare facilities using PIMS will gain a competitive advantage over their competitors by providing more efficient services and reducing the turn around time. In addition the use of such a system will result in enhanced customer satisfaction, since patients can also have access to needed information services.

3. Access Levels

In this section we will discuss different access levels that are offered by PIMS. The system in general is capable of accommodating users based on the need and use of information. A brief description of user groups and their interaction with PIMS at various levels follows.

General User: For this type of user the system will work like an online medical encyclopedia. General Users can search for any topic related to medicine as well as for diseases, their symptoms, and remedies. In addition, general users may also search for the location of health centers in the neighborhood. First aid tips will also be accessible to help people in emergency situations. In fact, all of these options will also be available to users at other levels.

Patient User: A user can login to the system as a patient and can gain access to many additional options than a general user, as these options are more user-specific. A Patient user can enter their symptoms and the system will search the knowledgebase for diseases which are related to the specified symptoms. The system will then advise the patients about possible different diagnoses with regards to the disease. The system will also suggest some precautions and preventative measure to be taken. In this situation the system may also prompt users with more questions to collect further relevant information and the patient may be directed to visit the clinic. Frequently, the symptoms may not match exactly with a disease included in the knowledgebase, in which case a visit to physician is the recommended option. In addition to providing information, PIMS will also save all the data provided by the user in a database, so that during a visit to the clinic the relevant information can be retrieved.

Physician User: Under this level the user will have access to patient information, medicine usage, clinical treatments and lab results. More importantly physician will have the capability of sharing patient information with other physicians and consultants, their opinion and write prescriptions. Another important option for the physician is to update the knowledgebase with new findings, treatment methods and medicines.

PIMS in general provides additional options for access to old symptom diagnosis files, reviews/updates current symptom diagnosis files, reviews and/or updates patient and personal information and manages passwords. This system will also provide patient users the ability to search for a physician and see their availability for scheduling an appointment.

4. Conceptual Design

In this section we analyze and specify requirements as well as, introduce the conceptual design and different components of the system based on the architectural requirements. We make an attempt to map user requirements with the design requirements in order to design an efficient and more versatile system. Table #1 specifies both user and design requirements. Components of this conceptual design are 1) adaptive user interface; 2) communication manager; 3) security manager; 4) distributed knowledgebase sub-system a) transaction manager, b) data access, c) concurrency control, and d) physical storage; 5) checkpointing; and 6) recovery. These components are shown in figure 1 and discussed in detail in the following sections.

Table 1. Generalized Requirement Table

USER REQUIREMENTS	DESIGN REQUIREMENTS
Members' information and all other related information must be available.	Database
System should keep information related to the medical domain.	Medical Knowledgebase
Member users should update and retrieve data from the system	Standard and Adhoc query processing
At the same time many users may use the system and access the database, information in the database should not be affected by mistakes, i.e. aborted transactions, system failures.	Multiuser access
Users can use the system easily. They can easily understand the system's usage and can perform tasks without confusion.	User friendly GUI.
A physician can talk with other physicians and share information. A patient can consult with a physician and learn about his/her disease management.	Web- based communication mechanism among users.
Users' personal files must be kept in a secure manner.	Secure information and system access
Information kept in the databases can be used only by allowed users. E.g. Patient's data can be seen only by themselves and physicians, other patients or visitors should not be able to access this data.	User authentication at different levels.

4.1 Distributed Knowledgebase

The concept of distributed system refers to a system that consists of two or more data files located at different sites on a computer network. Although the database is distributed, users need to have access to it without any interference. However, since many users may access the system from different locations or nodes simultaneously, concurrency mechanisms become more vital, in order to keep the data consistent. Backup and recovery operations are required for the system to recover from system crashes in case of any unforeseen circumstance. PIMS architecture includes these mechanisms via transaction management. We plan to store the data in a central repository at an institutional level, and also provide access to it over open networks to remote healthcare professionals as well as users at other nodes and levels. However, such a centralized multi-user inter-networked environment is subject to remote exploits and attacks that can put the confidentiality and integrity of medical information in jeopardy. Thus we need some form of security protection for the stored data. PIMS provides such security mechanisms at multiple levels via access control, authorization and authentication, details for which will be provided in later sections.

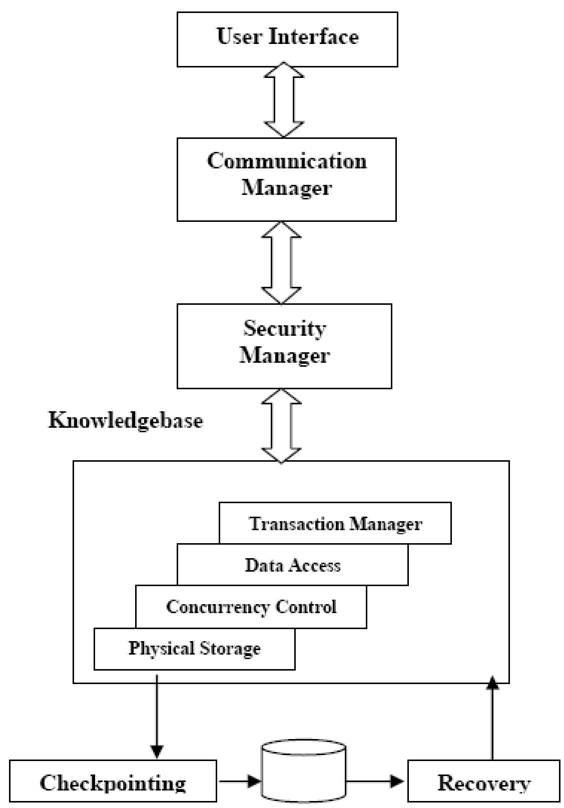

Figure 1: Conceptual Design

Another concern that may arise with regards to distributed systems is whether the data in PIMS is owned by the hosting healthcare unit, related patient, or the healthcare professionals who have created it? We leave this question open at this time however; proof of record of origin can be saved and it can contribute to the protection of the intellectual property of healthcare professionals, who then may feel more comfortable in sharing their data for the common good. A more detailed discussion on this issue is provided in the section on security manager.

4.2 Physical Storage and Access

The question "How the database should be placed in the distributed environment is addressed?" is addressed in this section. There are two basic alternatives to storing data: partitioned and replicated. In partition approach the database is divided into a number of disjoint partitions each of which is placed at a different site. In case of PIMS we opted to use the relational database model to store data that provides persistent storage for data values and associated data structure. The main reason for choosing the relational model of database is that it is less complicated to divide a relational schema into partition as compared to other models (Object Oriented, etc.) and the relational database management system market has matured over years and is now sizeable and finally, most distributed systems in use are also relational[16]. This storage structure used also provides capabilities for efficiently executing 1) read queries for retrieving, and 2) write queries for updating existing information and inserting new information. Since the database is typically stored on disk, special data structures known as auxiliary files are required to speed up data retrieval. However, this arrangement, as is always the case, may not be very efficient for adhoc queries. Further discussion in this respect is beyond the scope of this paper and interested readers are referred to any relevant text on Database Systems.

4.3 Transaction Manager and Concurrency Control

The concept of a transaction describes logical units of database processing that must be completed in their entirety in order to ensure correctness. Transaction Manager (TM) is responsible for managing many concurrent users and executing database transactions. These users require faster access as well as, shorter response time for their transactions. Concurrency control is always required in situations when multiple transactions submitted by various users may have the probability to interfere with one another in a way that may produce incorrect results. TM provides consistency to data objects that are affected by transactions that involve read and/or write operations. This type of concurrency control ensures that data objects are in a consistent state before and after a transaction is executed. The TM ensures that either all the operations in the transaction are completed successfully and their effect recorded permanently in the database, or that the transaction does not affect the database or any other transaction. The TM does not permit a database operation to be executed for a transaction if all required operation are not possible. This may happen if a transaction fails after executing some of its operations but before executing all of them. In this case TM sends an abort message and all data objects affected by this transaction return to their previous states (values). Basically, TM ensures undoing all the operations that are executed on the aborted or failed transaction. In case of a successful transaction, TM sends a commit message to complete the operation and make all the related changes to the data permanently by updating the stored data.

4.4 Checkpointing and Recovery

Recovery from a system failure usually means that the database is restored to the most recent consistent state just before the time of failure. In this case a system log is maintained on the disk that stores information about the changes that were applied to the data items by various transactions. The recovery in case of transaction failure uses the entries in the system log to recover from failure. However, the recovery component of the system must also be equipped to handle more catastrophic failures such as disk crashes. The main technique used to handle such situations is checkpointing (also called database backup), in which the whole database and the log are periodically copied onto a cheap storage medium such as magnetic tape. In case of catastrophic system failure, the latest backup copy can be reloaded from the tape to the disk and the system can be restarted. Recent events like the 9/11 attack and the Katrina hurricane disaster in New Orleans have created a greater awareness of disaster recovery for business critical databases. In PIMS this component provides facilities for recovering from hardware or software failures. For example, if the computer system fails in the middle of a complex update transaction, the recovery component is responsible for ensuring that the database is restored to the state it was in before the transaction began executing. In addition, the recovery component also ensures that the transaction is resumed from the point at which it was interrupted so that its full effect is recorded into the database. Recovery mechanisms also provide atomicity of the transactions by undoing the actions of transactions that did not complete successfully. The component also provides durability by ensuring that actions of transactions survive even with system crashes or media failures.

4.5. Security Manager

We must recognize the great risks that accompany the increased opportunity of information and telecommunication technology. Once a healthcare provider connects its system (PIMS) to a public network, security issues become extremely important. Unauthorized access and data corruption are constant threats. We need to establish proper security measures as preventive measures. Security of data is a broad area that addresses many issues, including the following:

Legal and ethical Issues: These issues deal with the right to access certain information. Some information may be deemed private and cannot be accessed legally by unauthorized persons. In case of medical and personal information this issue becomes extremely relevant.
Policy Issues: At the government, institutional or corporate level there is a clear cut policy as to what kinds of information should not be made publicly available, including personal medical records and related information.
System Issues: The system levels at which various security functions should be enforced. For example, whether a security function should be handled at the lowest level (physical hardware level) or at a higher level (interface level)?
Organization Needs: Organizations like hospitals and healthcare institutions need to identify multiple security levels and classifications the data and users based on these

categories. For example, classifications would include; confidential, unclassified, or shareable (At different levels).

The role of computer controls and security is to protect systems against mishaps, as well as to help organizations ensure that their information system operations address of all the issues stated above. The major goals of information security are:

- To lower the risk that the system and/or healthcare provider ceases operation.
- To maintain information confidentiality.
- To ensure the integrity and reliability of data resources.
- To ensure the availability of data resources.
- To ensure compliance with regards to National Security and Privacy Laws.

There are a variety of controls that are imposed on a user or the system itself and these are used to secure PIMS against the risks listed above. The security manager for PIMS takes a number of measure to address all security related issues and risks. Access control is a measure taken to ensure that only those who are authorized ultimately have access to PIMS. Since the system is web based; keeping it under lock and key will not provide this type of security. Hence, we use a combination of access codes (User ID) and passwords. The person or group responsible for maintaining and running PIMS should encourage users to change their passwords frequently. The security manager is then responsible for an authentication mechanism, validating users, determining which users have access to what information and the level of access. Making the system robust is another option that can resist inappropriate usage, e.g. for incorrect data entry or processing. For example, PIMS is designed to accept information or data in specified formats, and if user enters wrong data (data which the system is not expecting) or the data is entered in an incorrect format; an error message will be generated.

No matter how many steps are taken to prevent system abuse, nonetheless, it may still occur. Consequently, further steps are needed to keep track of transactions, so that if and when abuses are found, they can be traced. Subsequently, this fear of detection will inherently discourage the abuse itself. A popular tool for this is the audit trail: a series of documented facts that help detect who initiated a transaction or operation, at what time, and who was responsible for its approval. In this case whenever a physician orders a lab test or a certain prescription, the security manager for PIMS will prompt the person to provide the specified information (ID, Account number, password, etc.). Since the data authenticity is defined as the preservation of the integrity of the data (i.e. data is not modified during storage or transmission) plus the possibility of origin verification (i.e. the secure identification of the creator or the owner of the data). Both properties can be assured by means of digitally signing and/or time stamping the entire transaction. This information is then attached to the record. Authenticity of an Electronic Health Record (EHR) is crucial for the trustworthiness of information, especially in distributed environments where data is transmitted over insecure channels and stakeholders have usually never physically met[8]. For a more detailed discussion on security and HIPAA (Health Insurance Portability and Accountability Act) compliance we refer readers to[17].

5. PIMS Architecture

This section covers the operational model of the proposed system. PIMS' architecture revolves around three main functionalities, namely, access control, database control and communication control. Figure 2 shows the PIMS architecture based on three blocks, each block representing one of the three functionalities. Access control block, controls the access to the system through the interface, communication and security levels. Database control block, manages the transaction processing, with each access to the database by any level of user being referred to as a transaction. This access can be for retrieving information or modifying existing data or for adding new data to the database. Data manipulation block show the interaction between different levels of users as well as, between users and the data store. These interactions can be at different levels of data manipulation and through various levels of access, namely reading data, modifying data and updating data.

After the authentication and authorization, users should be able to send their requests to the system. Once the request clears, Security Manager then retrieves data from the database. As the Transaction Manager ensures that the database is always in consistent state, the requests that are allowed by the Security Manager also pass through the Transaction Manager. Thus the Security Manager communicates with the Transaction Manager.

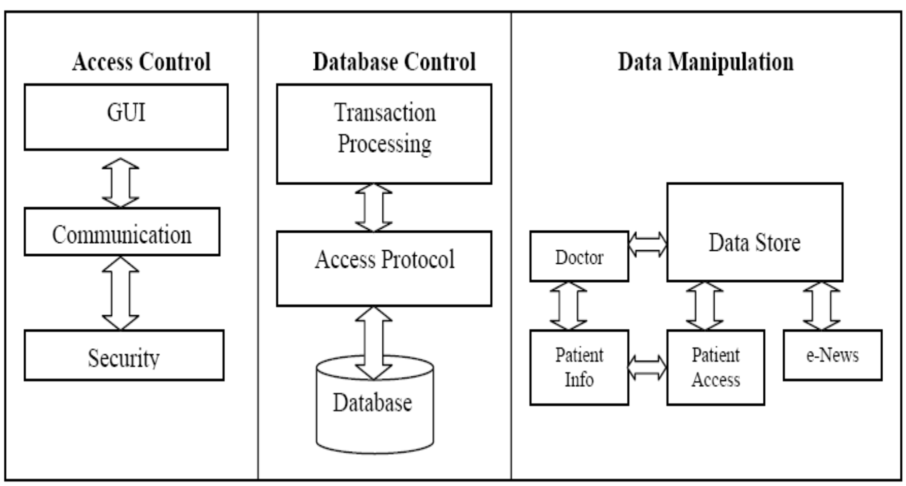

Figure 2. PIMS Architecure

6. Communication Manager and Communication Channel

Communication Manager (Figure 1) is responsible for providing a communication channel (Figure 3) for information gathered from the user as well as information retrieved from the components below communication manager. This component of PIMS will provide access to the login screen, in addition to various other options. It basically represents a user interface management mechanism to control user interface according to the type of user and the user's context to the interface. It analyzes the data that will be viewed for the user interface component. Since many types of users, with varying degree of technical knowledge and authorization, will be accessing the database the system should provide a variety of user interfaces. This ranges from natural language to the graphical interface for casual users, to the menu driven interfaces for physicians and patients. Communication Manager considers the user type and chooses a predefined interface template, and then creates a valid interface for the user. In this way an easy to use interface generation is provided.

The communication channel for PIMS shown in Figure 3 is composed of five main components that are Adaptive UI (User Interface) Manager, Communication Controller, Security Manager, Transaction Manager and Database Manager. The Adaptive UI Manager interacts with the Communication Controller, to provide user communication to retrieve, update or add information to the system, as well as, making sure that that once the user is connected to the system he/she is able to send and receive information from the system. The Communication Controller also interacts with the Security Manager. Since, it is also responsible for executing the entire process in a secure manner. Once the connection is established between the user and system through the Communication Controller, the Security Manager controls any operations that are performed by the user based on the privileges that the user has been granted. This hence keeps the system in a consistent state. It, also, provides excellent security for the system, since security is one of the most important quality-control criteria for systems designed to deal with confidential information. In order to execute the operation requested by users the Security Manager then establishes contact with the Transaction Manager, which in turn sends these requests to the Database Manager, which ultimately manages the process of information retrieval. However, TM does collaborate with the Security Manager to ensure authorization and authenticity as discussed earlier.

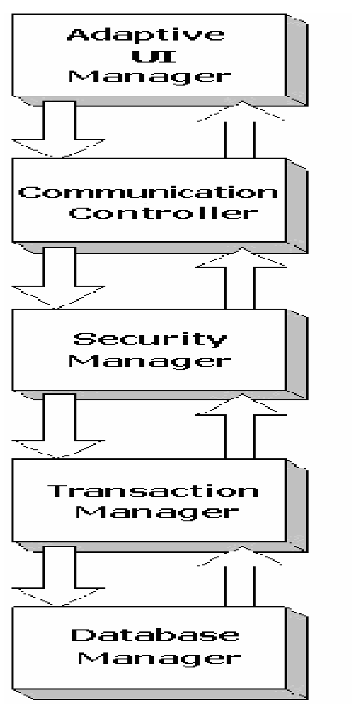

Figure 3: Supply chain

7. Survey and Analysis

The following discussion reviews a survey that was conducted to collect responses from only one category of PIMS users, the physicians. The reason for this is that physicians will be the only critical users of PIMS since they are responsible for updating the database and sharing patient information with colleagues. Other users such as patients and general users were not included in the survey as they are not considered critical users of the system. A questionnaire was designed and given to physicians in various specialties, of different age groups and with varying degrees of work experience. The survey included questions related to online medical systems, and physicians' willingness to use systems like PIMS. The following is analysis of the results from this survey. From these results it can be understood that 75% of physicians accept to use as well as encourage patients to use this system. Further analysis of the gathered data reveals that 83% of physicians who have ten to fourteen years of experience showed willingness to use PIMS. However, 60% of physicians with twenty or more years of experience declined the use of such system. This analysis is presented in Figure 4.

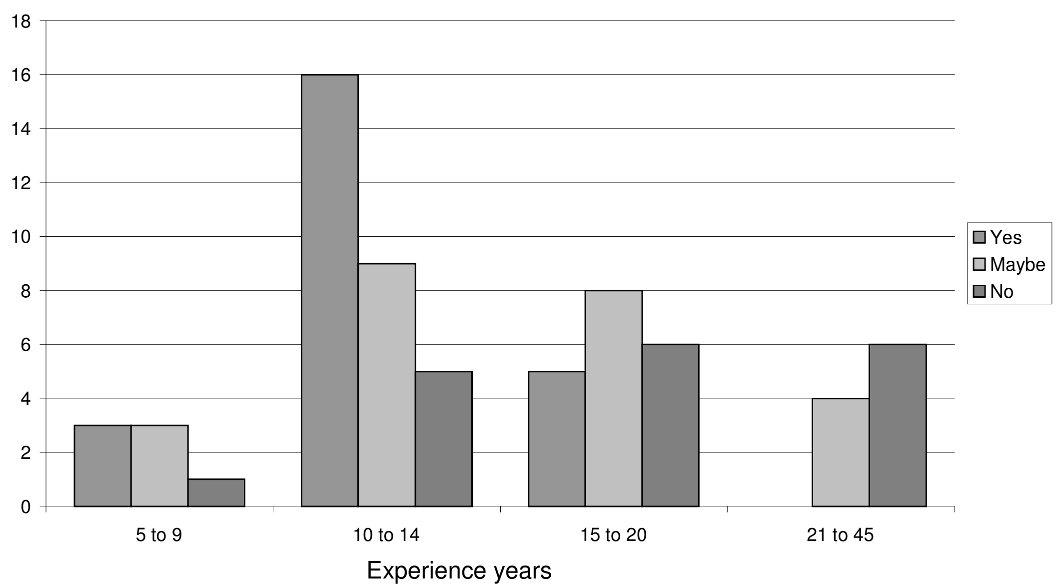

Figure 4: Experience age of respondents

Figure #5 shows the response from physicians based on their specializations. The survey showed that nearly 80% of physicians expressed a willingness to try the system and also agreed to provide feedback and advice about their experience. There are nearly 25% of the respondent who did not approve the use of any web based system including PIMS. However, 36% of the physicians were willing to use PIMS but with some reservations. The survey results show that physicians within the field of Internal Medicine were opposed to an online medical system whereas Psychiatrists showed complete support for such an idea. The basic reason given for such a response was that the Internists believe that they have to diagnose and attend patients while conducting physical examinations whereas psychiatrists can give therapy based on solely verbal patient medical history. We have safely concluded from this survey that physicians can use this system with some reservations about incorrect diagnoses. However, they agree that this system can be a useful tool for assisting them in obtaining a more accurate and efficient diagnosis with lesser turnaround time.

8. Conclusion

In this paper we presented the conceptual and operational architecture for an information system. The proposed system integrates advanced web technology and information systems in a manner that is unique in terms of information that it can retrieve and the level of access that it can provide. Web Enabled Patient Information and Monitoring System (PIMS) is a system that not only provides all the functionalities of a traditional hospital information system, but also possesses additional features. The design presented attends to spatio-temporal reality of the patient. Both geographical location and the temporal aspect of the data gathered by the system is complex. General users can gather information from the medical knowledgebase and learn about aspects related to the medical field. Patients and physicians alike, have a higher level of access than general users. Physicians have access to patients' personal information so as to be able to review and update the medical database and also share the information with colleagues to seek their opinion. For the future we plan to move on to implementing the design and generating a full working PIMS.

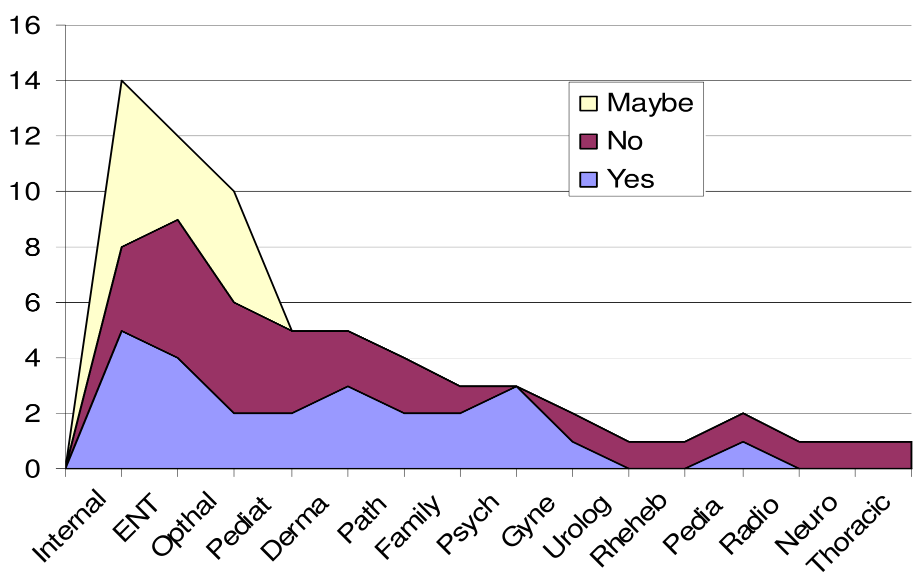

Figure 5: Physicians' opinion based on Specialty

Acknowledgment

The authors are grateful to Dr. Gordon Romeny and anonymous reviewers for their valuable comments and feedback which helped us to improve the quality of this paper.

REFERENCES

1. Berg, M., “Patient Care Information Systems and Health Care Work: A Sociotechnical Approach”, International Journal of Medical Informatics, Elsevier, 55(1), pp. 87-101, 1999.
2. Berman, Oded, Zahedi, Fatemeh and Pemble, Kim, “A Decission Model and Support System for the Optimal Design of Health Information Networks”, IEEE Transaction on Systems, Man, and Cybernetics-Partc-C: Applications and Reviews, 31(2), pp. 146-158, 2001.
3. Bliemel, M., Hassnain, K., ‘E-health: applying business process reengineering principles to healthcare in Canada’, in Int. J. Electronic Business, 2 (6), 2004.
4. Blobel, B., “Authorization and Access Control for Electronics Health Record Systems, International Journal of Medical Informatics, Elsevier, 73(3), pp. 251-257, 2004
5. Chen, Nong and Dahanayake, Ajantha “Rethinking of Medical Information Retrieval and Access”, In the proceedings of the IDEAS Workshop on Medical Information Systems: The Digital Hospital, pp. 59-67, Sept. 1-4, 2004.
6. Horsch Alexander and Balbach, Thomas, “Telemedical Information Systems”, IEEE Transaction on Information Technology in Biomedicine, 3(3), 1999.
7. Kim Eung-Hun, at vl, “Application and Evaluation of Personnal Health Inoformation Management System”, In the proceeding of the 26th Annual International Conference of the IEEE EMBS, pp. 3159-3162, San Francisco, Spet. 1 – 5, 2004.
8. Lekkas Dimitrios, Gritzalis, “Long-Term Verifiability of the Eletronic Healthcare Records’ Authenticity”, International Journal of Medical Informatics, Elsevier, 76(5-6), pp. 442-448, 2007.
9. Li, Hongyan, Xue Ming and Ying Ying, “A Web-Based and Integerated Hospital Information System”, In the proceedings of the IDEAS Workshop on Medical Information Systems: The Digital Hospital, pp. 157-162, Sept. 1-4, 2004.
10. Mrissa, Michael, Benslimane, Djamal, Ghedria, Chirine and Maamer Zakaria, “A Mediation for Web Services in a Distributed Healthcare Information System”, In the proceedings of the IDEAS Workshop on Medical Information Systems: The Digital Hospital, pp. 15-22, Sept. 1-4, 2004.
11. Tuoby, H, “Dynamics of Changing Health Sphere: The United States, Britain and Canada,” Health Affairs, 18(3), pp. 114-134, 1999.
12. Winter Alfred, at val., “Supporting Information Management for Regional Health Information Systems by Models with Communication Path Analysis”, In the proceedings of the IDEAS Workshop on Medical Information Systems: The Digital Hospital, pp. 139-146, Sept. 1-4, 2004.
13. Fan, Y. and Li H., “ICUIS: A Rule-Based Intelligent ICU Information System”, In the proceedings of the IDEAS Workshop on Medical Information Systems: The Digital Hospital, pp. 59-67, Sept. 1-4, 2004.
14. Green, C., Fortin, P. and Maclure M., “Information System Support as a critical success factor for Chronic Disease Management: Necessary but not Sufficient”, International Journal of Medical Informatics, Elsevier, 76, pp. 818-828, 2007.
15. Ammenwerth, E., Ehlers F., Hirsch, B. and Grati, G., “HIS-Monitor: An Approach to Asses the Quality of Information Processing in Hospitals”, International Journal of Medical Informatics, Elsevier, 76, pp. 216-225, 2007.
16. Ozsu. M., “Principles of Distributed Database Systems”, 2nd edition, Prentice Hall, 1999.
17. Wyne, M. and Hyder, S. “HIPAA Compliant HIS in J2EE Environment”, International Journal of Healthcare Information Systems and Informatics (IJHISI), Idea Group Inc., Vol. 2, No. 4, pp. 73-89, 2007.