Threshold Cryptography Based Secure Access Control for Electronic Medical Record in an Intensive Care Unit

Josmy T Jose ,Anju S.S
Department of Computer Science and Engineering
Amal Jyothi College Of Engineering,Kanjirappally

Abstract

The Intensive Care Unit (ICU) is the arena in which many succeed and many others perish in the intense battle between life and death. The advent of Electronic Medical Records (EMR) has not only changed the format of medical records but also increased accessibility of information contained in the repository, especially for research purposes. Privacy concern is arguably the major barrier that hinders the deployment of EMR systems .Stake holders are unwilling to accept the EMR system unless their protected health information containing highly confidential data is guaranteed proper use and disclosure, which cannot be easily achieved without stake-holder control over access to EMR information. The present database security models are not functional enough to meet the requirements for the various types of access control requirements. We are currently implementing a Tablet PC based system for automation of the workflows in an ICU in JMMC, Thrissur. This paper introduces a context-aware access control mechanism that utilizes threshold cryptography and multilayer encryption to provide a dynamic and truly distributed method for access control for different levels of doctors . Context-aware access control will be facilitated by encrypting sensitive data using the secret-sharing mechanism. A prespecified number of entities must collaborate to obtain the secret. The performance of the system is the main barrier that prevents applying security mechanisms. In this paper the performance of the system is analysed and found better results with different key sizes and file sizes.

Keywords:-Threshold Cryptography, Context, Shamir secret sharing scheme, Geolocation

1. Introduction

The Patient Medical Record (PMR) is a systematic documentation of an individual’s medical history. The information contained in the PMR is of great value in planning the patient care optimally. It is also of great value in medical research . Privacy concern is arguably the major barrier that hinders the deployment of electronic medical record (EMR) systems which are considered more efficient, less error-prone, and of higher availability compared to traditional paper record systems. Researchers have begun to study how context and ubiquitous computing can make hospitals and healthcare networks more efficient work environments [8]. One area where context may help is in defining data access policies. Hospitals and healthcare networks are environments, where information security mechanisms are not effective because policies focus on efficiency instead of data protection. Recent headlines report that 15 hospital workers were fired because they reviewed Nadia Suleman’s patient record without permission(http://www.foxnews.com;http://www.healthleadersmedia.com). In a similar privacy breach at a UCLA hospital, information related to Farrah Fawcett’s cancer treatment was given to the National Enquirer. As a result, 165 employees with positions ranging from doctors to orderlies were fired, suspended or warned (http://www.foxnews.com). The lack of privacy and confidentiality of patient records is not a new problem. In 1995, 24 people in Maryland were indicted for selling patient information from the state’s Medicaid database to four HMOs. One of the largest unauthorized disclosures in recent history of medical records and other private information happened in September, when computer tapes were stolen that contained data on almost 5 million people enrolled in TRICARE, the nation's health program for military members, their families and retirees. Some breaches have resulted in personal information being revealed online. The names and diagnosis codes of almost 20,000 emergency room patients at Stanford Hospital in Palo Alto, Calif., were posted on a commercial website for nearly a year before it was discovered in September and taken down. Such breaches can lead to identity theft, credit card fraud or fraud against the Medicaid or Medicare programs. If medical records are altered as a result of an individual posing as someone else to seek health care, the real patient can be put at risk for medical errors. The biggest threat to digital patient records is confidentiality. ‘‘Even before the introduction of the computer, confidentiality deteriorated as care provided by large groups became more common. But computerized records, particularly if embedded in large networks designed to collect comprehensive lifelong data, can rapidly accelerate that trend''. As reported in 1995 (Woodard, 1995) and even today, most hospitals and healthcare networks allow all staff to access digital patient records even when the person does not have direct care responsibility for the patient. The number of breaches of patient records and databases suggests that personal health information is not as private or secure as many consumers might want or expect. While advocates argue that unrestricted access is more efficient, such access limits the effectiveness of security mechanisms like passwords and encryption. As evidenced by previous breaches, healthcare personnel sale information, share passwords and use other means to subvert the system.

Passwords and encryption do not restrict the behavior of authorized users. Therefore, we propose to supplement the use of these mechanisms with contextual information that determine when and under what conditions a patient's record can be accessed by individuals who do not have direct care responsibility for the patient. For example, when a patient's doctor or nurse is not available, any staff doctor or nurse should be allowed to view the patient's record to administer care. Additionally, when a medical emergency occurs, any doctor or nurse should be able to access patient information.

Threshold cryptography based secure access control for electronic medical record in an intensive care unit deals with the security of stored EMR data, transmitting data and the secure access control for different levels of doctors based on their location, duty time, patient status, identity information etc. The patient medical data is stored in the server in an encrypted form using the RSA cryptographic algorithm. Data is encrypted in the application level rather than the storage level to prevent any transmission attacks. The RSA public key is used for encryption and private key for decryption. The decryption key is distributed into different shares based on Shamir Secret Sharing scheme and these shares are stored in the server. Here each share corresponds to different context conditions such as doctors identity, role, location, duty time, patient location, status etc. A threshold value is set based on the required number of context conditions for permitting data access. If a threshold number of context parameters are satisfied then the decryption key is generated from the corresponding key shares and the data is decrypted. We have proposed a network of Tablet PCs interconnected over a separate WiFi network in the ICU to provide the required interface to the clinical staff for the ubiquitous creation of the EMR. The potential advantages of this system were presented to the Senior Management of Jubilee Mission Medical College (JMMC) in Trichur, one of the premier Medical Colleges in Kerala, and they readily agreed for a trial implementation.

2. TABLET PC BASED ICU AUTOMATION SYSTEM

This section describes the Tablet PC based ICU automation system under development in JMMC. Tablet PC was preferred for this application due to its portability. Also, present day android application that runs on these devices has the potential to provide a better feel and performance to the user. The Digital Tablet with its versatile form supports pen navigation and the capability to write directly on the screen and convert to printed text. Fig.2 gives the network architecture of the ICU automation system. It consists of an ICU server connected to the central server using the hospital LAN. Note that the central server is connected with the laboratory and this provides us the capability to get laboratory information directly from the server.

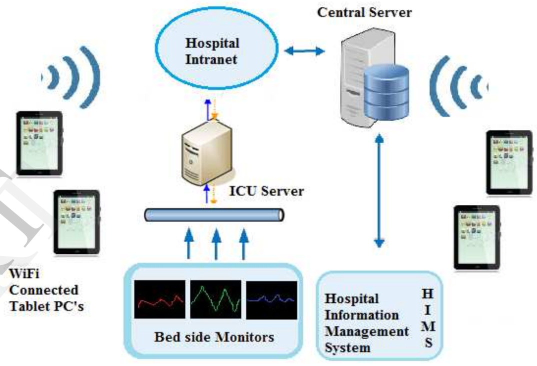


Figure:1 Architectural overview of ICU Automation System

A second network card in the ICU server is used to form a WIFI network to connect to the tablet PCs. These devices act as the primary interface for the nurses, doctors and other staff in the ICU. Our system provides separate authentication for doctors, nurses and other staffs. If login is successful the doctor or nurse can see those patients under their diagnosis. Among the list of patients he can choose one, and can separately view his history of diagnosis, medical records, documents, images, lab results, clinical orders, progress notes etc. Our general workflow supports the ICU automation. The ICU server acquires the tablet data and stores it in its internal database. The data flow happens between the server and the tablet PC through the WiFi network. From the central server the required results are taken and are displayed at the tablet PC near the patient bedside.

There are mainly 3 units for the doctors in neuro department in JMMC. Each unit consists of a unit chief,consulting doctor,and few resident doctors.The consulting doctor can view his patients data any time. The residents are allowed to view the corresponding unit patients details if and only if some of the context parameters are satisfied such as location of patient and doctor, duty time, patient status etc..

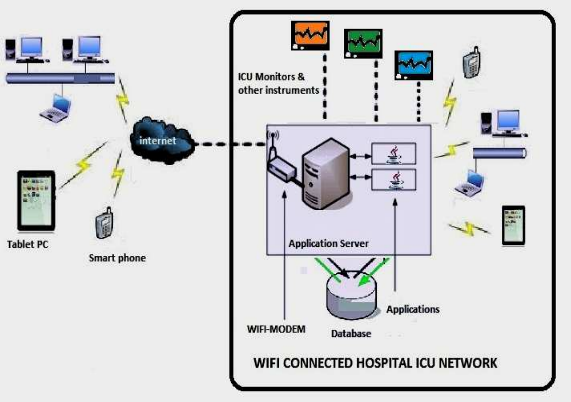


Figure:2 Network architecture of ICU Automation System

3. Approach

In this paper, we use threshold cryptography to enable context-aware access control. Context-aware access control merges data from multiple context sensors and uses this data to determine whether users should be given access to context restricted resources. Our context-aware access control scheme extends the context-based encryption scheme that is presented in [7], encryption is used to restrict access to data resources. The patient medical data is stored in the server in an encrypted form using the RSA cryptographic algorithm. Data is encrypted in the application level rather than the storage level to prevent any transmission attacks. The RSA public key is used for encryption and private key for decryption. The decryption key is distributed into different shares based on Shamir Secret Sharing scheme and these shares are stored in the server. Here each share corresponds to different context conditions such as doctors identity, role, location, duty time, patient location, status etc. A threshold value is set based on the required number of context conditions for permitting data access. If a threshold number of context parameters are satisfied then the decryption key is generated from the corresponding key shares and the data is decrypted. Multilayer encryption idea is used for better security, where threshold cryptography is used for each layer of encryption. Access to resources is limited to users within a specific geographic region. Location data is used to determine whether data should be decrypted or not. The decrypted data is then given to users whose location has been verified. To enable context-aware access control, we introduce the idea of encrypting sensitive data using the secret-sharing mechanism (threshold cryptography,) which is based on the idea of sharing a secret between different entities. A secret is divided into a number of secret shares. In order to derive the secret, a pre-specified number of entities must collaborate to obtain the secret. Threshold schemes are (k-out-of-n), where n is the total number of all entities and k is the pre-specified number of entities which must join forces to derive a secret. Variants of RSA cryptographic algorithms utilized the idea of threshold schemes by sharing the private key as the secret resulting in one public key and n private key shares. There are two models for threshold schemes which are used mostly in RSA cryptographic algorithms. They are either single sharing threshold based on Lagrange's interpolation as proposed by Shamir (1979) or threshold sharing functions like geometric based threshold as in Desmedt and Frankel (1990). In this project, we adopt Shamir secret sharing scheme which is based on polynomial interpolation. Assuming that the secret (d) is a number, to divide d into pieces di we pick a random k -1 degree polynomial f(x) where the first coefficient is the secret d. Given any subset k of these (i, f(i)), the coefficients of f(x) can be found by interpolation and evaluate f(0) which is d. But knowledge of just k -1 is not enough to calculate d. In order to restrict access to data until a higher-level contextual situation is realized, we identify the various low-level sensor data that the higher-level context situation can be derived from. It is possible to add multiple layers of encryption to capture richer access control policies. For example, some sensitive data can only be decrypted when a specific number of authorized users (k-out-of-n) are in the right location or under the right contextual situation. Sometimes it might be necessary to accommodate scenarios where several conditions must be present to grant access to the data, in which case, we can select an n out-of-n secret sharing scheme for the TC layer, assuming the accuracy of all these sensors are sufficient. Alternatively ,it is possible to introduce two layers of encryption, where the first layer consists of the required conditions and uses an n out-of-n scheme, and the other layer consists of these conditions that do not need to be satisfied fully for granting access, and thus, using a k-out-of-n scheme.

4. System Architecture

In this section we give a brief overview on how our mechanism works. Our system consists of a general-purpose distributed middleware, made up from distributed components that are developed using Java RMI. These components provide the common core functionality for enabling smart spaces and their applications. The main components include a policy service, context service, and event service. The policy service manages security policies and encryption keys. The context service processes sensor data to derive high level context. The event service provides secure communication among components within the system. Fig. 3 provides an architectural overview of the system. Component details are provided in the following subsections.

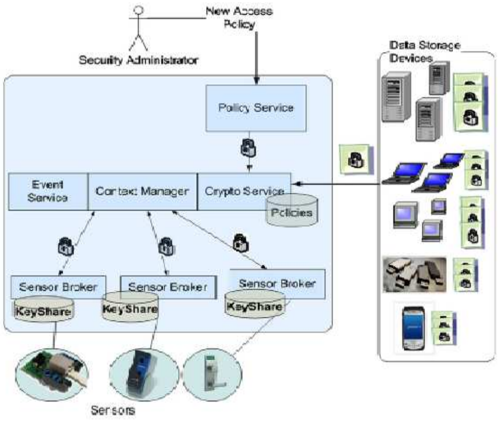


Figure:3 Architectural overview

3.1. Security policy service

The policy service provides primitives for security administrators to create and manage security policies for the smart space environment. Security policies are layered. Each layer of a security policy has at least one corresponding contextual condition. The policy service generates an encryption key for each layer and encrypts the data. The policy service decomposes into n key shares, where n corresponds to the number of contextual conditions that are associated with a layer. The policy service then distributes these key shares to sensor brokers within the smart space environment. Each layer of the security policy is sent to a context manager. Sensor brokers and context managers are components within the context service. Descriptions of these components are provided below.

3.2. Context service

The context service captures and processes contextual information from various sensors. Various contextual information are captured using various sensors, like temperature, lighting levels, sound levels, time and date, schedule, patient vital signs, current location etc. High-level activities (e.g., a closed meeting taking place in a specific room, etc.) can be implied by fusing sensors or gathering raw data from various sensors, and deriving higher level contextual information. For example, if the environment is able to detect the presence of several people, who are sitting at a large table in a room and talking in an orderly fashion, then this could imply that a meeting is taking place. The context service supports deducing high-level activities from low-level sensors. The design of the context service is based on the ideas outlined in [18]. The context service middleware consists of two components, context managers and sensor brokers. The context managers use first order logic to reason about contextual situations and derive higher-level or abstract contexts from sensor data. Sensor brokers mediate access to data produced by sensors and provide primitives for enabling communication with other components and services in a smart space infrastructure. For lightweight sensors, sensor brokers are simply a dedicated PC on which the sensor's component runs. Sensor brokers store the key shares of the corresponding sensors. A context manager is responsible for deriving the higher-level context that corresponds to a layer of encryption. When a context manager receives k decryption shares from the sensor brokers, the manager removes one layer of encryption. The process repeats until all layers are removed. The decrypted data is sent back to the user. If an insufficient number of conditions are met, the data cannot be decrypted and the access operation fails. Fig. 3 illustrates this process.

Doctors current location can be traced in a tablet either using html5 geolocation API or using GPS .In our simulation geolocation API is used for getting users current location, which gives correct values for a limited distance applications like ICU room.HTML5 geolocation API provides support to capture one's

Doctors current location can be traced in a tablet either using html5 geolocation API or using GPS .In our simulation geolocation API is used for getting users current location, which gives correct values for a

limited distance applications like ICU room.HTML5 geolocation API provides support to capture one's location by capturing the latitude and longitude where the user is based. So by using a combination of geolocation API and HERE Maps it is possible to display one's location on a web page. The accuracy of the location depends on the correctness of the latitude and longitude that is captured. Google Gears Geolocation works by sending a set of parameters that could give a hint as to where the user's physical location is to a network location provider server, which is by default the one provided by Google (code.l.google.com). Some of the parameters are lists of sensed mobile cell towers and Wi-Fi networks, all with sensed signal strengths. These parameters are encapsulated into a JavaScript Object Notation (JSON) message and sent to the network location provider via HTTP POST. Based on these parameters, the network location provider can calculate the location. Common uses for this location information include enforcing access controls, localizing and customizing content, analyzing traffic, contextual advertising and preventing identity theft. The Geolocation API is ideally suited to web applications for mobile devices such as personal digital assistants (PDA) and smartphones.

3.3. Event service

Another key component is the event service that allows events to be communicated between distributed objects. With the event service, users can create secure event channels where channel participants are restricted to authorized entities and sensitive events are encrypted, as described in [20]. All relevant sensor components within the smart space infrastructure are connected through a special secure event channel as depicted in Fig. 4. A detailed description of Fig. 4 is provided below.

Step 1: Once the security policy for accessing sensitive data is specified, a security officer can specify the necessary conditions that satisfy the high-level context or the identity and/roles of subject(s) that are authorized to access that data. This will depend on the sensitivity of the information and the sensor availability and setup in the smart space.

Step 2: Once the requirements for access are specified, the secret shares are generated according to Shamir’s secret sharing scheme. Using a secure end-to-end connection over an event channel, the secret shares are distributed to the components of the relevant sensors, as well as meta-data to identify the condition that needs to be met for a given sensor component (or a context synthesizer component) to apply its share to the data. An encryption ‘‘layer’’ can now be added to the data. The encrypted data is stored in the Distributed Storage Service (DSS) – the DSS implements functionality similar to a file system in a traditional OS, with the addition of context-awareness and support for data distribution across various smart devices and the cloud, i.e., encrypted data can be stored at different locations, including PDAs or the cloud, yet the DSS manages to aggregate the data so that it virtually appears to be stored on a single location .

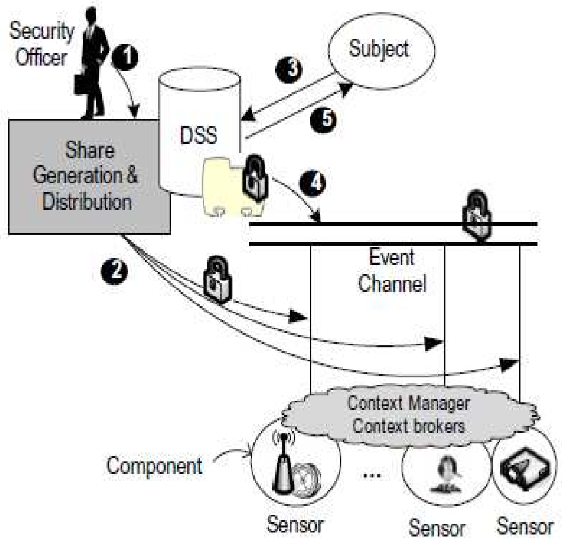


Figure:4 Access control using threshold cryptography

Steps 3 and 4: When a subject requests access to the data, the data is first sent to the event channel of the sensors’ component. Each sensor will apply its share to the encrypted data if the appropriate context is realized. If enough sensors participate, that layer of encryption is removed.

Step 5: If the TC layer is successfully removed, then the remaining data is passed to the subject. It is possible to have multiple layers of encryption here, where each layer needs to be decrypted to access the data. The inner layer can be concerned with validating the identity or the role of the requestor.

5. Implementation

To assess the performance and the practicality of our approach we simulate a smart hospital emergency scenario and apply our approach for dynamic access control. First we assume a three tier policy for data access within our environment. A tier maps to a layer of encryption within our scheme, and the policy that corresponds to the tier defines the context that must be satisfied before the corresponding layer of encryption is removed. We begin my describing the policy at layer 3 which is the outer most layer and conclude with layer1. The consulting doctor only needs to remove the first layer of encryption for viewing patient data. The other levels of doctors ie, don't have direct care responsibility with the patient have to remove the all three levels of encryption to view the patient data.

Layer 3 – The policy at layer three specifies when a patient's records may be viewed: The patient's records may be viewed by a doctor when the patient is being admitted to the hospital, or during the hours that the doctor makes his/her rounds, or if the patient is experiencing a medical emergency.Examples of a medical emergency would be: heart rate is over or under a prespecified threshold, high temperature, high blood pressure or any other vital signs. During our simulation,one of the specified conditions must be met before the outermost encryption layer can be removed.

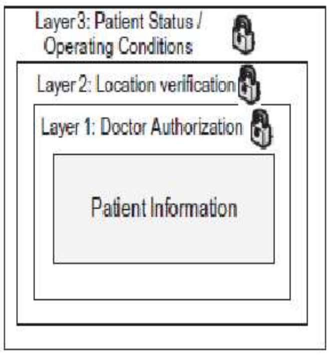

Layer3: Patient Status / Operating Conditions
Layer 2: Location verification
Layer 1: Doctor Authorization
Patient Information

Figure:5 Multilayer Encryption

the patient is experiencing a medical emergency. Examples of a medical emergency would be: heart rate is over or under a prespecified threshold, high temperature, high blood pressure or any other vital signs. Emergency conditions are identified by generating alarms for critical patient conditions ,which are sent to different levels of doctors. During our simulation, one of the specified conditions must be met before the outermost encryption layer can be removed.

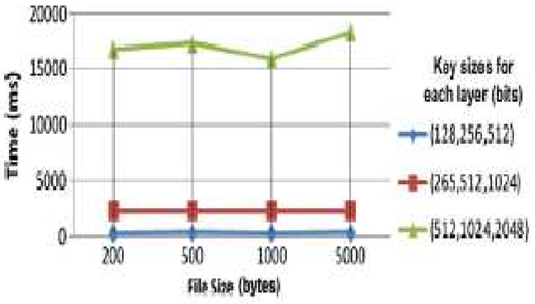
Layer 2 – The policy at layer two concerns the location of patient and doctor: The patient's records may be viewed when both the doctor and patient are located within the hospital and the doctor is within the patient's room or in close proximity to the patient. Also duty time of the doctor should be match with the current time. During our simulation, all conditions must be met before the second layer of encryption can be removed.

Layer 1 – The policy at layer one concerns verifying the doctor's identity and credentials: The doctor may view a patient's records if he is the attending physician, or he is the charge physician, who is filling in for the attending physician, and he is affiliated with the hospital. During our simulation at least two of the conditions must be met before the final layer of encryption is removed.

Fig. 5 illustrates the idea of the multi-layer encryption. Using our mechanism, for the patient's information to be decrypted, each layer should be decrypted (peeled off) only if the right context is realized. This is managed by the policy service which executes the security policy to decrypt the information. Decryption starts with the outermost layer and proceeds if the conditions are met at each successive layer. The patient's records are fully decrypted and made available to the doctor via mobile device if all conditions are met.

6. Results and Discussions

Shoup (1999) proposed a practical RSA threshold signature and decryption scheme that is based on Shamir secret sharing scheme. We adopt this algorithm. We use secure event channels for secure communication between the various objects. For our evaluation purposes we run all components on an Intel Core 2 Duo 2.4 GHz machine and we simulate a variety of contextual information to test the system. We focus on simulating and testing the that was described in the previous section. The scenario performance is evaluated using four file sizes for patient data; 200, 500, 1000 and 5000 bytes. For each configuration, 20 readings are taken and averaged. We evaluated for three different key sizes. The result is shown in the below graph.



7. Related Work

Much recent work on access control systems for ubiquitous and pervasive computing has been based on the Role-based Access Control system (Sandhu et al., 1996) (RBAC). RBAC relies on the principle that access control decisions are based on the roles individuals take on as part of an organization. The key concept in RBAC is a role, which is a placeholder for a set of users. Each role is associated with a set of permissions, which are its rights on objects. These roles may be organized into a hierarchy to reflect the organizational hierarchy among different users in a system. RBAC has been adapted for use in pervasive computing environments (Gill et al., 2001; Viswanatha, 2001; Covington et al., 2000), and the concept of roles is extended to deal with context information.However, RBAC is not sufficiently flexible to handle spontaneous changes in context in an optimized manner. Furthermore, RBAC requires a separate mechanism to enforce the access decisions, in the form of a reference monitor to something similar. The Aware Home project has extended RBAC with object and environment roles (Covington et al., 2000, 2001, 2002) that are used to define context-aware security policies suchas those based on temporal authorizations. However, they do not address permissions under specific high-level contextual situations. Kumar (2001) also consider incorporating context into the RBAC model with contexts and context filters. dRBAC (Freudenthal et al., 0000) is a decentralized trust-management and access control mechanism for systems spanning multiple administrative domains.

8. Conclusion

The introduction of ubiquitous computing technologies in the form of WiFi enablement and Tablet based information entry and the associated automation system is a major milestone in the automation plan of the Intensive Care Unit. It will initiate the shift from manual systems to automated systems and help the staff to concentrate more on their core activity of patient care without wasting their productive time waiting for the arrival of laboratory results. It has been a great opportunity for me to conduct a study on this project at this prestigious Medical College of central Kerala. The above project work presents a novel framework that enables context- aware access control via the use of encryption and threshold cryptography an ensures secure access control for EMR data. The approach is novel in that it combines the use of TC and heterogeneous high-level contexts to make an access control decision. The simulations show that the multilayered access control mechanisms can operate efficiently even for complex scenarios and increasing key sizes. We also envision this mechanism being used in situations to increase the confidence in sensor readings by combining the output of multiple sensors via the use of threshold cryptography.

9. References

[1] As Is document on NICU Automation prepared on behalf of the observation in JMMC Trichur. http://icuautomation.wikispaces.com/DOCUMENTATION.

[2] http://www.jubileemissionmedicalcollege.org/

[3] Integration of ICU data into Electronic Medical Records- Issues and Solutions By Asha Yeldose, Dhanyaja.N , Josmy T Jose and Anju S S-IEEE Proceedings by ICT 2013

[4] William R. Hersh :Electronic Medical Record: Promises and Problems - Biomedical Information Communication Center.Journal Of The American Society For Information Science 46(10):772-776,1995.

[5] Nina Boulus,PhD Candidate,Simon Fraser University Canada :Information about the Electronic Medical Record(EMR)- Publications of Action for Health.

[6] http://securosis.com

[7] Al-Muhtadi, J., Hill, R., Campbell, R., Mickunas, D., 2006. Context and location-aware encryption for pervasive computing environments. In:Third IEEE International Workshop on Pervasive Computing and Communication Security (PerSec).

[8] Bardam, J., 2004. Applications of context aware computing in hospital work Examples of design principles. In: ACM Symposium on Applied Computing.

[9] Covington, M.J., Moyer, M.J., Ahamad, M., 2000. Generalized role based access control for securing future applications. In: 23rd National Information Systems Security Conference.

[10] Covington, M.J., Long, W., Srinivasan, S., Dey, A.K., Ahamad, M.,Abowd, G.D., 2001. Securing context-aware applications using environment roles. In: SACMAT, Virginia, USA.

[11] Covington, M.J., Fogla, P., Zhan, Z., Ahamad, M., 2002. A Contextaware security architecture for emerging applications. In: 18th ACSAC, Las Vegas, NV.

[12] Desmedt, Y., Frankel, Y., 1990. Threshold Cryptosystems, Advances in Cryptology Crypto 89, pp. 307315.

[13] Dey, A.K., 2001. Understanding and using context. Personal and Ubiquitous Computing 5 (1), 47.

[14] Freudenthal, E., Pesin, T., Port, L., Keenan, E., Karamcheti, V., 2002.dRBAC: Distributed role-based

access control for dynamic coalition envi-ronments. In: 22nd International Conference on Distributed Computing Systems.

[15] Gill, B.S., 2001. Dynamic Policy-Driven Role-Based Access Control for Active Spaces. University of Illinois at Urbana Champaign. Hess, C.K., 2002.

[16] A Context File System for Ubiquitous Computing Environments, University of Illinois at Urbana-Champaign, Urbana-Champaign, CS Technical Report UIUCDCS-R-2002- 2285 UILU-ENG-2002-1729.

[17] Holzinger, A, Schwaberger, K., Weitlaner, M, 2005. Ubiquitous computing for hospital applications RFID applications to enable research in real-life environments. In: 29th Annual International Computer Software and Applications Conference.

[18]Ranganathan, A., Campbell, R.H., 2003. An infrastructure for context-awareness based on first order logic. Personal and Ubiquitous Computing 7, 353–364.

[19]Ranganathan, A., Al-Muhtadi, J., Campbell, R.H., 2004. Reasoning about uncertain contexts in pervasive computing environments. In:IEEE Pervasive Computing Magazine.

[20]Lee, A., Boyer, J., Drexelius, C., Naldurg, P., Hill, R., Campbell, R.,2005. Supporting dynamically changing authorizations in pervasive communication systems. In: 2nd International Conference onSecurity in Pervasive Computing.