JHIDC Health Informatics in Developing Countries

www.jhidc.org
Vol.2 • No.2 • 2008

HCRBAC – An Access Control System for Collaborative Context-Aware HealthCare Services in Mauritius

Oveeyen Moonian[a], Sudha Cheerkoot-Jalim[a], Soulakshmee D. Nagowah[a], Kavi Kumar Khedo[a], Razvi Doomun[a], and Zarine Cadersaib[a]

[a]Department of Computer Science & Engineering
Faculty of Engineering
University of Mauritius
Reduit
Mauritius

Abstract

Healthcare is an area dealing with an enormous amount of highly sensitive data being handled by a number of users. As a first step towards an e-health service, Mauritius requires the electronic management of patients' data at its different healthcare institutions. Such data management should allow easy non-obtrusive, but secure, access to data by in house personnel of each healthcare institution, while also providing secure remote access to other institutions within the healthcare service as well as external bodies such as the police and insurance companies.. This paper presents HCRBAC (Healthcare Context-Aware Role-Based Access Control) a data access system for the Mauritian healthcare service, where data access within a healthcare institution is facilitated and controlled through the use of context-awareness, while remote access to data is provided in a secure way. A number of different existing access control mechanisms are first analyzed and a comparative study of these is performed. A combination of the different techniques is then used to provide efficient management of the data access system and allowing any healthcare institution to open up data access to other related institutions, without compromising confidentiality and integrity of data.

Referencing this article

Moonian, O., Cheerkoot-Jalim, S., Nagowah, S. D., Khedo, K. K., Doomun, R., & Cadersaib, Z. (2008). HCRBAC – An Access Control System for Collaborative Context-Aware HealthCare Services in Mauritius [Electronic Version]. *Journal of Health Informatics in Developing Countries, 2(2)*, 10-21, from http://www.jhidc.org/index.php/jhidc/issue/view/7

1. Introduction

Healthcare services provide an area that requires collaborative support from multiple parties and also an area where context-awareness will result in spontaneity of services. Collaborative support is required within a healthcare institution, among different healthcare institutions and from agencies external to the institution. Within a healthcare institution such as a hospital, patient data has to move from record office to doctors' offices, laboratories, x-ray and scanning departments, wards, among others. Collaboration among healthcare institutions is required for patients being transferred from one institution to another, eg. for specialized treatment or when a patient is simply following treatment at two or more different institutions for different diseases. External services such as police department, insurance companies and social security services may also need access to the data. The security provided by the system should be non-obtrusive for data access by regular staff on duty within the institution while it should robustly secure the data from unauthorized accesses, due to the highly sensitive nature of the data. Context Awareness can facilitate access to data by supporting spontaneity, as nurses and other healthcare personnel will not need to specifically log in to a computer to provide a patients treatment. Staff members, when they are next to a patient should be able to automatically obtain the required information of the patient on their PDAs for providing the necessary treatment.

The Mauritian public healthcare service consists of a number of hospitals for generalized treatments and a few hospitals provide specialize treatment. This requires patients' information to move from general hospitals to the specialized ones. We wish to develop a data security system for the Mauritian public healthcare service that secures the current data access facility within healthcare institutions, but goes beyond current provision in healthcare institutions to allow easy data access to on-duty personnel and to also allow secure access from other healthcare institutions and external agents.

This paper studies the different existing access control mechanisms and proposes an access control mechanism that is secure while being flexible, easy to manage and supports distribution. The rest of the paper is structured as follows: Section 2 presents the general features of the Mauritian public healthcare service, section 3 presents overview of existing access control mechanisms, section 4 performs a comparative study of these mechanisms while section 5 interprets the results of the comparative study. Section 6 presents our proposed Access Control Mechanism for the Mauritian Healthcare Service while section 7 concludes the discussion and presents the scope for future works on the project.

2. The Mauritian Public Healthcare Service

The Republic of Mauritius provides free healthcare services to its entire population. It consists of about 134 healthcare locations that include Area Health

Figure 1
State Chart for Medication

Centres, Medi-clinics, a Community Hospital and a number of Community Health Centres which provide medical, nursing, dispensary and support services at local level. In addition, there are five regional hospitals, three district hospitals and several specialist hospitals. The specialist hospitals consist of a mental hospital, an Eye hospital, an Ear, Nose and Throat hospital, a Cardiac Centre and a Chest hospital. The regional hospitals and primary health care centres that include Area Health Centres and Community Health Centres benefit from a wide range of clinical and non-clinical support services. These services include pathology laboratories, X-Ray, CT scan and MRI, pharmacy, blood collection and transfusion, public health and hygiene, medical records and information services, catering, laundry, transport and cleaning. Among these public healthcare institutions, only the Jawaharlal Nehru regional hospital found at Rose Belle and 7 area health centres are partly computerized (ITU 2004). The others operate manually. Figure 1 shows a map of Mauritius with the different healthcare points and population figures. The healthcare services employ over 650 doctors, 2,700 nurses, about 50 dentists and 17 pharmacists (Ministry of Health & Quality of life, 2002).

For the purpose of this project a site visit was carried out at Victoria Hospital situated at Candos. It was found that patient record management including patient registration, room allocation, medicine prescriptions, patient record transfers and various other tasks are being done manually. Each patient has a unique file to record all histories. This file is being used at different levels for respective treatments within the hospital. Only nurses, respective specialists and record management officers will have access to a patient's file. At the end of the day, all patients' data are recorded in a database on a stand-alone computer, mainly for backup purposes. The manual file is still crucial as it represents the formal document which can used in situations like police cases or legal matters. If a patient is transferred from the hospital to another institution, a referral note containing a summary of the patient's history is sent to the new institution. This note is used to create a new file and is the only link between the patient's history and the new institution where he/she will receive treatment.

The services provided by the public healthcare institutions could be improved dramatically by implementing a computerized system at each institution. Patient record management and the other tasks like registration of patients and room allocation could be automated to provide a better service. Moreover, the duplication of data when patients are transferred could be solved by implementing a secure network that links the different health centres throughout the country. The existing manual system poses threats to the privacy of patient medical histories and the misuse of their personal information. Moreover, patient files could be lost during the transfer between the different departments within an institution. Accuracy of information can also be an issue. Strict security measures have to be implemented so that only authorized personnel have access to sensitive information.

This work looks at the security aspect of providing electronic data mangement and proposes a secure, flexible and easily managed access control mechanism for a distributed computerized system to support the mobility of data in the Mauritian public healthcare services. However the proposed access control mechanism goes beyond the support of the simple computerization of the current data mobility requirements. It also provides convenience of use through the support of context awareness.

3. Access Control Mechanisms

In the early days of computer use, access control mechanisms were based on the access matrix model (Lampson, 1971). This model and its implementation as access control lists and capabilities catered for users (subjects) and objects. While such mechanisms were suitable for centralized computer systems where each user would create his/her objects and assign access rights, they do not meet the needs of today's dynamic computing environments where data access crosses computer, organizational and even national boundaries. The type of access allowed may depend on a number of context-based parameters. Another drawback of the access matrix model was that the access control had to be coarse-grained (at levels of files) and the management of access control was tedious. For example when an object was created, the access had to be specified for each user. Although, groups could solve the problem partially, a user could potentially belong to several groups and management of the groups was tedious. The literature contains a number of works on access control mechanisms that attempt to overcome these shortcomings. This section presents an overview of such works while the next section presents a comparative study of their relative merits and drawbacks.

Role-Based Access control (RBAC) (Sandhu et al 1996) allows access permission to information based on responsibilities or roles. Users are made members of appropriate roles. The use of roles facilitates the attribution of access rights as users roles change and this matches the concept of positions and responsibilities in an organization. Promoted or transferred staff members would be assigned new roles and thus automatically inherit new access rights. RBAC stems from the association of access rights to user groups, but it goes beyond the functionalities of groups in that different roles can be established as being mutually exclusive and roles can take on inheritance. Through the support of constraints (eg. permissions or assignment relations) RBAC enables the enforcement of many different access control policies and thus achieves flexibility (Ramaswamy and Sandhu, 1998). Static and dynamic separations of duties are two of the most common types of RBAC constraints (Sandhu et al 1996). One important demand is the enforcement of customized context-based access control policies (Ahn et al. 2000).

Dynamic RBAC (DRBAC) (Zhang and Parashar, 2003) is an extension of RBAC to include context-

aware capability. DRBAC thus assembles the merits of RBAC and simplifies its administration to provide improved flexible and extensible access control. This is achieved by the permissions and context constraints forming a chain of responsibility that can be dynamically defined, monitored and activated. Specifically, role assignments and permission assignments are adjusted based on context information. Every context constraints are evaluated against current context of the access request using state machines for each user, role, permission, environment and session. DRBAC has been experimented in pervasive grid applications and distributed healthcare applications with reasonable effectiveness (Zhang and Parashar, 2003; Zhang and Parashar, 2004).

Context Based Access Control (CBAC) (Covington et al. 2001) is also an extension of RBAC with the notion of environment roles in order to provide for security in context-aware applications (Tolone et al. 2005). Access to different resources is allocated to a subject, based on a set of rules applicable to the context in which he/she is operating (Pigeot et al. 2006). Resources are accordingly bound with contextual information under which to operate (Tripathi et al. 2004). A CBAC system may also contain different filtering levels for allowing resource access (Pigeot et al. 2006).

Proximity-Based Access Control (PBAC) (Ardagna .et al., 2006) is a variation of the more general Location-based Access Control (LBAC), which is itself a specific case of CBAC, where the context is location. In PBAC, access control is based on the proximity of the user to a particular resource to determine access privileges. PBAC schemes consider the following factors: the geometry of the physical workspace to determine proximity zones, the 3-D accuracy of the positioning system (using Active Badge, RFID, etc) used and the access privileges to provide to users within a proximity zone (Gupta .et al, 2006). Each resource is assigned an access control list which is a table consisting of possible roles known as resource-roles and corresponding privileges. These privileges are based on the users' group roles (group roles are assigned based on a specific area or domain a user works) and the system information context (Gupta .et al, 2006).

Task-Based Access Control (TBAC) (Thomas and Sandhu 1993, Thomas and Sandhu 1997) is a dynamic access control technique in which access rights are not granted to subjects but rather to tasks in steps related to the progress of the tasks. This is suitable for automated processes where the activities of tasks cross computer boundaries, departmental boundaries and even organizational boundaries. In general a task may span multiple activities that span multiple network and databases. A task may thus consist of multiple subtasks that need to be individually or collectively authorized. Also, access to a given object may be granted only after a number of previous tasks have been performed. (Kang et al 2001) considers TBAC to be particularly suitable for distributed computing and dynamic information processing activities such as workflow management and agent-based distributed processing. In the TBAC paradigm, permissions are checked-in and checked-out in a just-in-time fashion, based on activities or tasks.

Team Based Access Control (TMAC) (Thomas 1997) is an approach of applying role based access control in collaborative environments where an activity is best accomplished through organized teams. (Altaiby and Chen 2004) describes a team-based access control extension model called TMAC04, built on RBAC. The TMAC04 model efficiently represents teamwork in the real world. It allows certain users to join a team based on their existing roles in an organization within limited contexts and new permissions to perform the required work. By distinguishing permission assignment from context-based, run-time permission activation, TMAC can be considered an active model of access control. As such, it is able to provide just-in-time permissions and support to a higher degree the principle of least privilege in comparison to passive security models (Georgiadis et al. 2001).

4. Comparative Study

This section compares and examines the above access control models with respect to different criteria that have been considered relevant to the Mauritian healthcare system, as listed below.

- **No of Contexts**: High number of contexts allow for finer granularity of access control but also introduce higher complexity. A healthcare system often has to cater for different scenarios/situations and also has a large number of context information. The right balance between complexity and granularity is a determining factor.

- **Dynamicity**: The healthcare environment is constantly changing; therefore dynamicity is an important feature for any access control mechanism to be used in such an environment.

- **Platform and Application Domains**: This criterion is used to determine the appropriateness of each access control mechanism to application domains and environments where it is deployed. Suitability for healthcare services can eventually be deduced.

- **Flexibility and Adaptability**: This criterion is used to evaluate the ability of the access control mechanism to adapt to differing scenarios and environments. A healthcare system typically witnesses a large number of varying scenarios and unforeseen events. Therefore the access control system used should be flexible and adaptable.

- **Centralized/Distributed Management**: The aim of this project is to eventually allow data collections, storage and access in the different healthcare institutions of Mauritius and electronic transfer of such data. Therefore it is essential to have distributed management of access control.

- **Scalability**: A healthcare system crosses the boundary of a single healthcare institution and even that of the healthcare service as a whole. Thus, the number of eventual users of such a system is likely

to be unpredictable. Consequently, scalability of the access control mechanism is a vital factor.

- **Support for user mobility**: Providing for user mobility in the access control will result in an enhanced system that allows high-priority users, such as doctors, to access patient data from different places in a healthcare institution, from different institutions and even from home. Thus such users will not be constrained by locations.

- **Security Services provided**: The security services provided is another important feature of an access control mechanism in healthcare systems where highly sensitive information is stored and hence access control data should not be compromised at any cost.

- **Reliability**: In a distributed computerized system with a large number of components, the failure of one or more components at any time is inevitable. In a healthcare system which needs to be always available, the access control system should be highly reliable in spite of failures of components.

- **Performance**: However robust an access control mechanism may be, user acceptability depends highly on the response time of the system. With the high volume of data in a healthcare system, special care has to be taken to ensure the right tradeoff between the performance and the other features of the access control scheme.

- **Authentication Mechanism Used**: Since the types of users accessing information in a healthcare system is highly varied, a range of authentication mechanisms need to be explored in order to provide the right type of access. Additionally, different authentication mechanisms may be required for different access levels.

The subsections below present the evaluation of the different access control mechanisms with respect to the above criteria.

(i) Number of contexts

RBAC makes use of subject/user information as the only contextual information. DRBAC model additionally uses multiple context information to monitor the context of different subjects/ users. Context constraints are applied before assigning roles to the subject/user. In CBAC access privileges are assigned dynamically when the context (for example, location, time, role, authentication trust level, type of information accessed) changes (DuraiPandian et al., 2006). Like CBAC, the PBAC scheme is highly dependent on the context of the system to track dynamic changes. The context information is grouped into three categories: user context (for example, the location of the user (proximity), and user's capabilities), resource context (for example, capability of the resource, and current load on the resource) and environmental context (for example, number of users in proximity of a resource at a given time) (Gupta .et al, 2006). TMAC also makes use of several contextual information, such as time, shift, and location, can be considered in modeling access control policies. The TBAC considers the time of use, the usage count and the executing tasks in addition to the subjects, objects and access rights in conventional access control mechanism (Thomas, 1997).

(ii) Dynamicity

The RBAC model is mostly static as users are assigned to specific roles and this assignment can only be modified by the system administrator. However, in the highly dynamic and heterogeneous environment, the access privileges of an entity depend on its credential, context and current state, which are dynamic. The DRBAC system fulfills these requirements by adding dynamicity to role assignment. However, the degree of dynamicity in DRBAC is not clearly defined (Zhang and Parashar, 2003), as this depends on context sensing and processing capabilities in the application scenario. The CBAC model is also considered as a dynamic one, since different set of rules are applied when the context changes. It provides dynamic binding to resources, that is, when the user moves from one domain to another, different sets of rules will be executed before granting access to the resource (Tripathi et al. 2004).

PBAC, TMAC and TBAC are also dynamic models. In PBAC, specific permissions will be granted at run time when a user approaches a resource physically in a proximity zone, depending on the load and capability of the resource and the number of users in proximity of that resource at that particular time (Gupta .et al, 2006). TMAC provides fine-grained control over permission activation to individual users and objects. It can be considered as an active model of access control as permissions are activated at run-time, based on the context. (Thomas, 1997). TBAC allows for trustee sets and protection states to be modified dynamically (Chou and Wu, 2004). (Aljareh and Rossiter, 2002) presents the use of TBAC in collaboration networks and argues that a person executing a task can be changed on the fly if required.

(iii) Application Domain

RBAC has been incorporated in the Unix and Linux administration model, the Solaris operating environment (Sun, 2008) and network environments like Novell Netware and Microsoft Windows NT (Microsoft, 2008). Implementation of RBAC has been deployed in a wide range of applications, like J2EE applications including Web services and related applications (Naumovich and Centonze, 2004), Grid environments (Pereira et al, 2006), CommercialDatabase Management Systems (Ramaswamy and Sandhu, 1998) and Distributed Healthcare Applications (Hu and Weaver, 2004). The DRBAC model can also be successfully deployed in organisations where every subject/ user can be assigned a role based on contextual information in the environment. DRBAC has been experimented in pervasive grid applications and distributed healthcare applications (Zhang and Parashar, 2003; Zhang and Parashar, 2003). The CBAC systems can be used for systems which require dynamic binding of resources, authentication and filtering levels as well as access to resource based on contextual information. The work by (DuraiPnadian et al., 2006), proposes such an architecture with its application to an Education system. For example, a student can have access to his grades when he is in the vicinity of the school

but not from a public place. The same concept could be extended to a hospital, a home or an office. The PBAC scheme can be used in hospitals emergency departments where caregivers are automatically logged in to a computer by virtue of their proximity, thus preventing them from being distracted from their natural workflow (Gupta .et al, 2006). It can be used mainly in places where people are busy performing several tasks in parallel and will therefore need easy and fast access to resources (Bardram et al, 2003).

The TMAC model is mainly used in collaborative environments such as those involving workflows (Georgakopoulos et al. 1995). It has mainly been experimented in the health care setting where a variety of teams may be involved in a task. Furthermore, it has been used for solving security issues for clinical workflows associated with patient care (Thomas, 1997). The TBAC has also been used in collaborative systems, such as doctor-patient interactions or client-service providers' interactions (Aljareh and Rossiter, 2002) and in workflow management systems (Thomas, 1997).

(iv) Flexibility and Adaptability

RBAC model shows no flexibility as it makes use of a single contextual information. Compared to RBAC, the DRBAC is flexible as complex context-aware authorization policies can be specified at design time. Context type definition and implementation are independent of the specification of the access rules, and this makes DRBAC flexible and extensible. Like DRBAC, PBAC model couples access control with context information. It defines a set of access control policies that can easily be adapted to different contexts which makes the model flexible. In CBAC, the dynamic binding of resources when new scenarios arise, makes the scheme flexible. CBAC provides a Policy Adaptation mechanism to ensure smooth flow of operations in new scenarios and rules have to adapt to unforeseen events (Toninelli et al., 2006). TMAC is a hybrid access control model. It incorporates the advantages of broad, role-based permission assignment and administration across object types as in RBAC and yet provides the flexibility for fine-grained activation of permissions for individual users on individual object instances.

Finally, TBAC model is flexible in that it can allow a single activity or group of activities to share the same policy (Aljareh and Rossiter, 2002). Furthermore, any member of a trustee set can be granted authorisation.

(v) Centralised v/s Distributed Management

Usually all RBAC components are directly controlled by a single system administrator and the management of roles and their interrelationships, including user assignment and permission assignment, is highly centralized. However in large systems, where the number of users exceeds hundreds or thousands, role management is delegated to a few security administrators. The DRBAC model is easily implemented with a centralized management of the context condition evaluation, but with distributed implementation for context acquisition and processing, since the role assignment is done in real-time. In the DRBAC architecture, a Central Authority (CA) maintains the overall role hierarchy (Zhang and Parashar, 2003). PBAC scheme relies on a central access control module that determines the proximity zone of a resource and users entering the zone (Gupta et al., 2006). The module generates the resource-roles and users within the proximity zone can access the resource based on the privileges associated with the resource-role. CBAC model provides a centralized access control policy (DuraiPandian et al., 2006). However, since dynamic binding to resources is possible, it also provide for Distributed Management. According to (Thomas and Sandhu, 1997), TBAC model is well suited to distributed computing and information processing activities with multiple points of access, control and decision making such as that found in workflow and distributed process and transaction management systems. TMAC can be both centralized and distributed (Thomas 1997) as role based access control is applied in collaborative environments and activities are best accomplished through organized teams.

(vi) Scalability

RBAC is not highly scalable as access permission to information is limited to the number of responsibilities or roles. Besides, according to (Zhang, 08) when the number of roles and permissions go beyond the order of thousands, there is performance degradation and the management of RBAC becomes difficult to handle. The concept of role hierarchy is included in DRBAC model such that new role can be created and extended from existing ones. The DRBAC system has a limitation, since it is role-scalable down the hierarchy. But with very large number of users, having dynamic roles, DRBAC model will be resource greedy in terms of memory and processing.

The PBAC model can be made scalable by using n-tier proximity zones around the resource instead of a single proximity zone (Gupta et al., 2006). Different access privileges will then be given in different zones. Increasing the capabilities of the resources also helps to accommodate more users in the proximity zones. CBAC model can be scalable assuming the infrastructure built is based on modular components which can be fully integrated in a broader pervasive architecture (Tolone et al., 2005). Moreover, (DuraiPandian et al., 2006) proposes an application of an Educational system for its architecture which can be easily extended.

An advantage of TMAC model over other access control models such as RBAC is that it is able to leverage the scalable security administration benefits of role-based permission assignment and yet able to provide fine-grained permission activation and deactivation to individual users and object instances. For example, the system can assign and administer broad permissions for doctors on object types based on some role definitions and yet activate a doctor's permission to a patient's records (object instances) only when he/she is taking care of the patient. The work by (Thomas and Sandhu, 1993) discusses the use of authorization subtasks where a subtask is assigned to a single transient object. This makes TBAC scalable in two ways. The first is

that TBAC can handle increased workload. As the workload increases an authorization step can spawn authorization subtasks taking care of the various requests for authorization. The second way is that TBAC can handle increasing complexity of the authorization steps. In (Thomas and Sandhu, 1997) a family of TBAC models is presented, with a basic model used to build composite ones with additional constraints. In (Aljareh, 2002) a tasks-based security model built on collaboration tasks is presented. One of the characteristics of collaboration tasks is that it can be upgraded to fill in gaps in the original tasks. A new collaboration task can be built from a default task (or task template), which is essentially the idea presented in (Thomas and Sandhu, 1997).

(vii) Support for User Mobility

Since the only context information for RBAC is the user, a change in user location will not cause any change in role assignment. Therefore RBAC has no support for user mobility. In DRBAC model, user mobility is supported since user's role can change with different context conditions. The PBAC scheme supports user mobility only when a user moves in a specific zone. Access privileges are removed as soon as user moves out of the zone (Gupta et al, 2006). In certain circumstances, it can be a benefit especially where people are in a hurry and move out from an ongoing session or forget to logout (Bardram et al, 2003). In CBAC, resources are binded with contextual information under which they should operate. Support for user mobility will be applicable only in boundaries where context rules have been attached to resources. TBAC and TMAC have no support for user mobility as the access control are restricted to the task and team respectively.

(viii) Security Services provided

Since context information is used as a key player while granting access privileges, the security of the context information must be guaranteed. Compromised context information will result in the system making wrong access control decisions. RBAC provides predefined access control, whereas DRBAC provides access control where the active role of the user and the active permission of the role will change dynamically. Such active roles and permission can be stored and transmitted in encrypted format according to the target security level to be enforced. With CBAC, different filtering levels can be provided before granting access to a resource to ensure security of transactions. There is also need for an encryption mechanism that can be costly (Pigeot et al, 2006). With PBAC model, access to a resource is automatically granted when a user enters an established proximity zone around the resource. This scheme has to be combined with RBAC and authentication mechanisms to prevent inadvertent or malicious users from accessing resources. Security framework with self-administering property, such as in TMAC, reduces security administration overhead. In other words, as teams are collaborating and as the workflow progresses, permission assignment and de-assignment, as well as activation and deactivation, are achieved without the manual intervention of a human security administrator. In TMAC, this is achieved by monitoring basic calls issued from host information system to assign and de-assign team members, as well as by recording at run-time when workflow instances are invoked. These are synchronized with the user assignment and activation primitives to automate security administration. TBAC model provides for tight just-in-time need-to-do permissions especially in application environment consisting of transactions and workflows (Rusinkiewicz, 1994; Georgakopoulos, 1995). TBAC approach also leads to access control models that are self-administering (Thomas and Sandhu, 1997), thereby reducing the overhead typically associated with fine-grained subject-object security administration.

(ix) Reliability

In RBAC, access permissions are administratively associated with roles and users are administratively made members of appropriate roles. Thus, management of authorization is quite simple and static, making RBAC reliable. In DRBAC model, the reliability of context security information is a key issue. Corrupted contextual data will lead to wrong evaluation of context conditions, thus incorrect role assignment results in access permissions that affect the security of the system. While the reliability of PBAC scheme is tied to the accuracy of the positioning system used, this accuracy depends on the electromagnetic environment and varies over time. PBAC can make use of error contour maps around the proximity zone to compensate for errors of the positioning system (Gupta et al., 2006). For other models like CBAC, reliability is still an issue. For example, when there is a new scenario where the policy adaptation mechanism will be triggered, there is no guarantee that the new rules applied are most optimal or correct. TBAC dynamically manages permissions as authorizations progress to completion. Authorizations have strict usage, validity and expiration characteristics that may be tracked at runtime, thus making TBAC reliable. TMAC can be used to restrict access to information and functionality in the shared environment to those trusted. It can be used to help coordination by providing only those functions to team members that are currently needed to fulfill their roles. However, managing access permissions assigned to members of dynamic teams and emerging and frequently changing processes raise challenging issues. Therefore, the reliability of TMAC depends on how dynamic the teams and processes are.

(x) Performance

The fact that RBAC uses only one contextual information, makes the scheme perform better than the other schemes. DRBAC scheme, for instance, depends on several factors, such as, number of roles assigned, number of permissions allocated to each role, rate at which transitions occur between roles and frequency of context changes. The overhead of DRBAC is experimentally evaluated in (Zhang and Parashar, 2003) and implementing DRBAC in an application implies higher operational complexity. Similarly, the performance of PBAC scheme varies with the system context, for example, the capability of the resource, the load of the resource or the number of users in the proximity zone. (Gupta et al., 2006) defines a parameter termed Window-of-opportunity that defines the maximum delay that can be allowed to take corrective action. This delay can be used to evaluate the performance of PBAC with

varying context information. For CBAC model, fast response time is one of the basic requirements. With different filtering level and sets of rules which need to be executed, performance issues can arise and different means have to be devised to optimise search. (Pigeot et al., 2006) introduce one way to increase performance through the implementation of a history module which acts as a cache. Currently, only limited performance and complexity evaluations have been carried out on access control models like TMAC and TBAC.

(xi) Authentication Mechanism
RBAC has a very simple authentication mechanism. A user requesting access to a particular resource will be granted access if the role he/she is member of, has the appropriate permissions. Application access control alone cannot provide security. DRBAC model, an enhanced version of RBAC, adds an additional entity, the user's environment, in the authentication procedure. DRBAC must combine with some feasible authentication mechanisms to secure context aware applications in the real world. PBAC method makes use of authentication mechanisms to manage multiple users in a proximity zone and to prevent users from accessing resources for which they are not actually entitled. For example, a nurse standing by computer should not be able to gain access to a doctor's log-in when the doctor is in proximity of the resource (Gupta et al., 2006). In CBAC, use of biometric or non biometric authentication mechanism have been proposed together with contextual information before granting access to any resource (DuraiPandian et al., 2006).

TMAC mechanism creates a general structure of a team with role-based permission assignments to information and functionality in the shared environment. It allows certain users to join a team based on their existing roles in an organization within limited contexts and new permissions to perform the required work. Therefore authentication is performed based on user role and team. TBAC performs authentication based on users and objects, but does not grant access in a static fashion. In addition to verifying the user's access rights to the required object, TBAC also makes use of validity count and authorization steps (Thomas and Sandhu, 1997). Each authorization step makes use of its own protection state, which determines the set of permissions that become valid as a result of the authorization step being turned on.

5. Interpretation of Results

After doing a comparative study in the previous section, this section will now provide an interpretation of the results obtained. Table 1 summarises the access control models examined in this paper against the criteria mentioned. The table makes use of comparative terminology such as Low, Moderate, and High, descriptive terminology such as Centralised, Mixed, and Distributed, and the standard Yes and No terminology for characterization against the criteria. Some of the criteria namely: Platform and Application Domains, Security Services provided and Authentication Mechanism Used, have not been included in the table as these are rather descriptive features which cannot be classified in terms of the comparative terminologies used.

It can be inferred from the results that the RBAC model greatly simplifies security management for administrators, and many complex security policies can be applied more easily. However, it uses a static security mechanism, is not highly flexible and provides no support for user mobility. In DRBAC, roles are adjusted based on context information making it more flexible and dynamic than RBAC. Earlier extensions of RBAC to create CBAC improved access control, but that model is static with poor flexibility and extensibility. New context-aware access control infrastructure is dynamic, distributed and provides enhanced user mobility (Zhang and Parashar, 2004). PBAC is highly dependent upon the resource-role a user is mapped to, for a particular resource. All access control decisions are made after the resource-roles are generated by each resource in a domain. Moreover, in PBAC user mobility is highly supported by using different proximity zones. The TBAC model extends the traditional subject/object-based access control models by including domains that contain task-based contextual information. TBAC, unlike RBAC, also supports type-based instance and usage-based access. In addition, authorizations have a strict runtime usage, validity, and expiration characteristics. Last but not least, TMAC preserves the advantages of scalable security administration that RBAC-style models offer and yet offers the flexibility to activate permissions for individual users and to specific object. Unfortunately, TMAC lacks the self-administration of assignment relations between entities.

Healthcare systems have complex access rules because of the many actors in the system and

Table 1
Evaluation of Access Control Methods

Technique	No. of Context	Dynamicity	Flexibility	Centralized/ Distributed	Scalability	User Mobility	Reliability	Performance
RBAC	Single	Static	Low	Centralised	Low	No	High	High
DRBAC	Multiple	Dynamic	Moderate	Mixed	Moderate	Yes	Moderate	Moderate
CBAC	Multiple	Dynamic	High	Mixed	High	Yes	Moderate	Moderate
PBAC	Multiple	Dynamic	Moderate	Centralised	Moderate	Yes	Low	Low
TBAC	Multiple	Dynamic	High	Distributed	High	No	High	-
TMAC	Multiple	Dynamic	High	Mixed	High	No	High	-

their interlocking access privileges, and most of these rules have to be context-aware. A practical healthcare IT system must support hundreds or thousands of users, roles, objects, and permissions and requires flexible, on-demand authentication, extensible context-aware access control and dynamic authorization enforcement. Security, reliability and performance are also crucial. Moreover, a more integrated system that crosses the various healthcare boundaries (e.g., hospitals, private physicians, insurance companies, pharmacies, police department) is required. Therefore, distributed management is also a required feature in a healthcare environment

The clinical setting is generally characterized by users with a diverse set of qualifications and responsibilities that can naturally be mapped to various roles. Therefore RBAC would be a good start , but the scheme has to be complemented with CBAC, TBAC and TMAC. CBAC would be required as additional context information like location and time have to be considered before granting access to a resource. A Healthcare provider for instance, will have access to information about a patient in a ward if he is located at that ward and only if he tries to access the information within his normal working hours. Moreover, a dynamic and flexible access control mechanism is required for a Healthcare environment to allow for the possibility to adapt to new or unforeseen circumstances. One scenario can be when a doctor is called urgently to the hospital to perform a surgery. Even if it is outside the normal working hours of the doctor, he/she should be allowed access to resources. Similarly the access control mechanism should support user mobility. TBAC could be required when a patient has to undergo a treatment with different surgeries that have to be performed whereby one surgery cannot be performed unless another one has been carried out. Finally, team work is also another important criteria, e.g nurse and doctor who have to collaborate when undergoing a surgery; whereby the need to also implement TMAC in the system.

Having access to resources in a Healthcare environment means having access to very sensitive information. Compromised context information can lead to a wrong access control decision. Fast response time is also an important requirement, meaning that there should also not be too much overhead in performing access control. A suitable scheme should have the right balance between security and performance.

6. The Proposed Access Control Mechanism

We present here **Healthcare Context-aware Role-based Access Control** (HCRBAC) for the Mauritian Healthcare service. The mechanism provided will allow the Mauritian public Healthcare service not only to have a secure computerized system for its current services but will also allow it to provide an augmented service that cross the boundaries of the healthcare institutions. The service provide security that can support patients interacting with their healthcare providers from home and it will also support other institutions such as insurance companies or the police department having access to healthcare data, without compromising the integrity and confidentiality of the data.

The work concentrates on providing an efficiently managed access-control scheme that allows the staff to operate with minimum inconvenience while ensuring that sensitive data is not put to risks. While, data being accessed from a different hospital should ensure rigorous authentication, a patient's record should be easily accessible to nurses on duty in a ward and the identification of such nurses should be automatic. The system also relies on trusted partners for allowing remote accesses from other institutions. The subsections in this section describe how we propose to meet our goals of providing an efficient non-obtrusive access-control mechanism, while also supporting an enhanced service through secure remote accesses.

6.1 Efficient Access-Control Management

As discussed in section 3, RBAC provides efficient assignment of access rights for objects by assigning permissions to roles and is specially suitable for collaborative environments, while DRBAC provides these advantages but also includes context information. In a healthcare system a person should be allowed access to information based on his role but also based on location and time contexts. Efficient access-control management is provided in this work by assigning access rights to roles and assigning roles to users. Roles can also be automatically linked to job positions. Temporal and location-based context are used together with roles to enforce higher level of security than a pure RBAC system. Thus, for most hospital staff, authorized patients information will only be accessible to them when they are on duty and in the location of their duty.

6.2 Non-Obtrusive Secure Authentication for Routine Works

It would be inappropriate to expect hospital staff to log in onto the system each time they require to provide treatment or verify patients' information. We are proposing the use of active badges by hospital staff for authentication purposes. The different wards and rooms in the hospital will contain sensors to identify hospital staff (through the active badges) to allow access of general nature. For access to more sensitive information or modification of information we will make use of biometrics means such as use of fingerprints.

6.3 Secure Remote Accesses for Enhanced Services:

Remote access allows wider use of the healthcare services but also introduces higher levels of threats. Remote access allows medical practitioners from one institution to obtain patients data from other institutions. Remote access also allows patients to view their data from outside the healthcare institutions, schedule appointments or receive results of diagnostic tests from home. It can additionally allow other institutions such as the police and insurance companies to have access to selected patients information. Due to the wide audience having remote access to the data, the system has to ensure the identity of the users accessing the information and also it has to provide

only the allowed kind of access. The additional requirement for remote access is ensuring the identity of the user.

An individual or an organization requiring data from a healthcare institution needs to register with that institution. They will then be provided with user id and passwords. These will be sent encrypted to the healthcare institution. For an individual, the kind of access allowed will be restricted to his own data, thus the above procedure is sufficient. For other organizations restricted kinds of access will be allowed about all patients. These organizations will have to be registered with the healthcare institutions from which they require data. These organizations will be trusted ones and will have to authenticate themselves with the system before data access is allowed. It is assumed that these institutions also authenticate the users on their systems.

For practitioners from other healthcare institutions, the system will rely on the trust between the different healthcare institutions and will thus have two levels of verification. A practitioner **P**, from an institution **X** requesting data access at an institution **Y** will first undergo an authentication at institution **X**. Institution **X** will then authenticate itself with institution **Y** using encrypted messages. Then institution **X** will send the required information about **P** to institution **Y** to allow the data access.

6.4 System Architecture

We propose, an RBAC system, which is context–aware. Users will be allowed access to data, based on their roles and context information, such as time and location. Figure 2, below, shows the architecture of the proposed mechanism. All access to data will only occur through the access-control engine. The latter will first require authentication of users, performed through the authentication system. The authentication system verifies the user name and password. If the authentication information is valid, the authentication system obtains the role of the user from the role manager. The role value is returned to the access-control engine. Access to specific database tables and records will be based on roles as well as specific constraints information based on context. Such context constraints are verified against context information available from external sources or from specific patient records. For example, a nurse may be able to access the data of a patient only if he/she is in the ward and he/she is on duty. A doctor may be able to access data of his patients from anywhere, but may be allowed to access data of other patients only when he is in a ward.

6.4.1 Architectural Components

Authentication System

The Authentication system obtains user information either directly from a sensor (for active badges) or by user explicitly logging in (for remote access to information or to access information of high sensitivity). The authentication system authenticates the user and for valid users verifies their roles through the role manager. It returns, to the user process, the role information. The user process uses the role and user id, together with users work schedule (location and time of duty) to form a capability **(ref)** to be used for data access. For each access of data, the user process presents the capability and operation to the **Access Control Engine**, which is responsible for data accesses.

Access-Control Engine (ACE)

The access control engine is the component that provides access to objects. It obtains the capability from the user process, together with the operation the user wishes to perform. The ACE obtains the type of constraints that applies to this role, from stored information. The ACE also obtains location-based information from the environment and temporal information can be obtained from the system, provided it is kept properly synchronized with a global clock. The ACE verifies the constraints against the information in the patients records and decides whether the required type of access can be provided.

Role Manager

The role manager performs the management of information concerning roles and the targets of the roles. It thus deals with mapping between roles and users. It provides the required API for assigning roles to users and modification of the role assigned to a user.

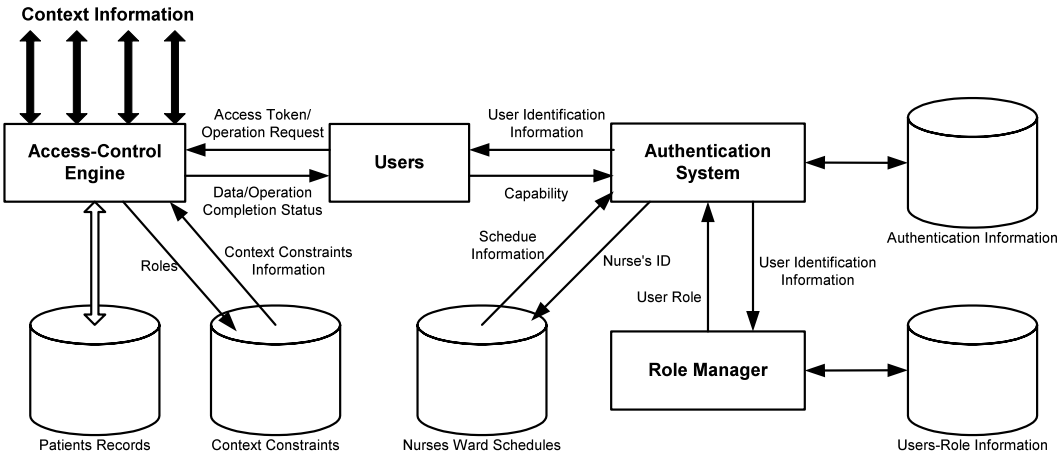

Figure 2
Overall Architecture of Proposed Mechanism

6.5 A Typical Scenario

As a typical scenario, let's consider a nurse requiring access to a patient's data to provide treatment. The system will go through the following steps:

- The RFIC reader will detect the nurse's identification. It sends the identification to the Authentication System.
- The Authentication System checks the identity with the Role Manager to obtain the role belonging to the given identity.
- The role being Nurse, the Authentication System checks with the nurse-schedule file to obtain the ward at which the nurse is posted, the dates and time.
- The Authentication System builds a capability containing the role and the nurse's id as well as information from the work schedules and returns the capability to the user process.
- Each time the user process needs to access data, it produces the capability to the Access Control Engine.
- The Access Control Engine obtains the role and the id from the capability, checks whether the type of access requested is allowed to nurses, verifies the ward, the date and time from external sources and checks against those in the capability. It returns the status of the request, any required error code and any required data.

7. Conclusion and Future Works

The aim of this paper was to develop an efficient, robust and non-obtrusive access control mechanism for the Mauritian public healthcare service. After giving an overview of the Mauritian public healthcare service, the paper has provided discussions on recent developments in data access control schemes. It has discussed the need to replace the early access control matrix scheme with mechanisms that better suit today's dynamic computing environment. It has then presented a number of access control mechanisms and has performed an analysis and comparative study of these mechanisms. It has been inferred from the analysis and comparative study that RBAC provides for efficient access-rights and access control management, but is a static method that does not consider context information as parameters. A public healthcare system needs to have a number of dynamic considerations, thus RBAC has to be augmented by more dynamic schemes. Also to introduce non-obtrusive access we need support from techniques that can make use of context-based information.

Our work thus proposes the use of a combination of RBAC, CBAC and PBAC to provide an access-control system for the Mauritian public healthcare service. The large amount of data and users involved in a public healthcare service requires that the access-control management be efficient. This is expected to be achieved since the scheme is based on RBAC. The scheme also provides for non-obtrusive access control through CBAC and PBAC, but the impact of these on the complexity and efficiency of the system are to be studied. Due to the sensitivity of the data, the access control scheme must also be robust against remote accesses. Robustness is achieved through delegation.

The next stage of the work will consist of mathematical evaluation of the complexity of the proposed scheme, the impact of the non-obtrusive part on the complexity. This will be followed by an implementation of a prototype of the proposed scheme and experimental evaluation of the performance of the prototype.

After an implementation and evaluation of the prototype, we plan to study the effect of including TBAC and TMAC for increased security of operations, the kind of additional benefits these can bring as well as their effects on performance.

References

Aljareh S. and Rossiter N. "A Task-Based Security Model to Facilitate Collaboration in Trusted Mult-Agency Networks". SAC 2002, Madrid, Spain.

Ahn G.J., Sandhu R., Kang M. and Park J. " Injecting RBAC to secure a Web-based workflow system. In Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, 2000.

Alotaiby, F.T. and Chen, J.X. "A Model for Team-based Access Control". (TMAC 2004). Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), Vol. 2, 450.

Alotaiby F.T and Chen J. X. "A Model for Team-based Access Control". (TMAC 2004), Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 2, pp. 450, 2004.

Ardagna C.A, Cremonini M., Damiani E., De Capitani di Vimercati S., Samarati P., 2006, "Supporting Location Based Conditions in Access Control Policies". Proceedings of the ACM Symposium on Information, computer and communications security.

Bardram J.E., Kjær E. R, and Pedersen M. Ø. 2003, "Context-Aware User Authentication—Supporting Proximity-Based Login in Pervasive Computing".

Chou Shih-Chien, Wu Chien-Jung. "An Access Control Model for Workflows Offering Dynamic Features and Interoperability Ability". International Computer symposium, Dec 15-17 2004, Taipei, Taiwan, pp 1314-1319.

Coulouris G., Dollimore J., Marcus R. "Role and task-based access control in the Perdis groupware platform." In Proceedings of the 3rd ACM Workshop on Role-Based Access Control. FairFax VA, 115-121.

DuraiPandian, N., Shanmughaneethi, V., Dr.Chellappan, C., 2006. Information Security Architecture-Context Aware Access Control Model for Educational Applications. JCSNS International Journal of Computer Science and Network Security, VOL.6 No.12, December 2006

Georgakopoulos, D., Hornick, M. and Sheth, A., 1995. "An Overview of Workflow Management: From Process Modeling to Workflow Automation Infrastructure". Distributed, and Parallel Databases. Vol. 3, 119-153.

Georgiadis, C.K., Mavridis, I., Pangalos, G. and Thomas, R.K., 2001. "Flexible team-based access control using contexts". SACMAT 2001, 21-27.

Gupta, S.K.S. Mukheriee, T. Venkatasubramanian, K. Taylor, T.B., 2006, "Proximity Based Access Control in Smart-Emergency Departments". Proceedings of 4th Annual IEEE International Conference

Hu J., Weaver A. C., "A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications". Proceedings of the First Workshop on Pervasive Privacy Security, Privacy, and Trust (pspt2004), August 26, 2004, Boston, MA, USA.

International Telecommunication Union (ITU), The Fifth Pillar: Republic of Mauritius- ICT Case Study, February 2004 available at http://www.itu.int/ITU-D/ict/cs/mauritius/material/CS_MUS.pdf.

Kang M. H., park J.S., and Froscher J.N. "Access Control Mechanisms for Inter-organizational Workflow"- SACMAT'01, May 3-4, 2001, Chantilly, Verginia USA.

Microsoft TechNet, "Role-Based Access Control for Multi-tier Applications Using Authorization Manager", Available at: http://technet2.microsoft.com/windowsserver/en/library/72b55950-86cc-4c7f-8fbf-3063276cd0b61033.mspx?mfr=true Date Accessed: 19 July 2008.

Naumovich G. and Centonze P., "Static Analysis of Role-Based Access Control in J2EE Applications", SIGSOFT Software Engineering Notes, vol. 29, no. 5, pp. 1-10, Sept. 2004.

Pereira A.L., Muppavarapu V. and Chung S.M., "Role-Based Access Control for Grid Database Services Using the Community Authorization Service", IEEE Transactions On Dependable and Secure Computing, Vol.3, No 2., April-June 2006

Pigeot, C.E., Gripay, Y., Pierson, J.M, Scuturici, V.M., 2006. Context-Sensitive Security in a Pervasive Environment, Rapport de recherche RR-LIRIS-2006-017, September 2006.

Ramaswamy, R., Sandhu, R. Role-Based Access Control Features in Commercial Database Management Systems. In Proceedings of 21st NIST-NCSC National Information Systems Security Conference, NISSC'98, 1998

Sandhu R.S., Coyne E.J., Feinstein H.L. and Youman C. E., "Roles-Based Access Control Models" IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

Tolone, W., Ahn, G.J., Pai, T., Hong, S.P., 2005. Access Control in Collaborative Systems. ACM Computing Surveys, Vol. 37, No. 1, March 2005, pp. 29–41.

Sun Microsystems Documentation, "Chapter 17 Role-Based Access Control (Overview)", Available at: http://docs.sun.com/app/docs/doc/806-4078/6jd6cjs4o?a=view Date Accessed: 19 July 2008

Toninelli, A., Montanari, R., Kagal, L., Lassila, O., 2006. A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments. 5th International Semantic Web Conference, Athens, GA, USA, November 2006, LNCS 4273

Thomas R.K., Sandhu R.S., "Towards a task-based paradigm for flexible and adaptable access control in distributed applications" – Proceedings of the 1992-1993 workshop on New Security Paradigms, ACM Press, August 1993.

Thomas R.K., Sandhu R.S., " Task-based authorization control (TBAC): A Family of Models for Active and Enterprise-Oriented Authorization Management". Proceedings of the IFIP WG11.3 Workshop on Database Security, Lake Tahoe, California, August 11-13, 1997.

Thomas, R.K. Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments, ACM Workshop on Role-Based Access Control 1997: 13-19

Tripathi A., Ahmed T., Kulkarni D., Kumar R., and Komal Kashiramka, 2004.Context-Based Secure Resource Access in Pervasive Computing Environments. Second IEEE Annual Conference on Pervasive Computing and Communications Workshops.

Zhang G. and Parashar.M., Dynamic context-aware access control for grid applications. In IEEE Computer Society Press, editor, 4th International Workshop on Grid Computing (Grid 2003), pages 101 – 108, Phoenix, AZ, USA, November 2003.

Zhang, G. and Parashar M. "Context-aware Dynamic Access Control for Pervasive Applications". Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), San Diego, CA, USA, 2004.

Zhang C., Hu Y. and Zhang G. "Task-Role Based Dual System Access Control Model", International Journal of Computer Science and Network Security (IJCSNS) Vol 6 No. 7B, July 2006.

Zhang Z., "Scalable Role & Organization-Based Access Control and its Administration", PhD Thesis submitted to the George Mason University, April 2008.