Um Modelo de Controle de Acesso Baseado em Contexto para Autorizações a Informações Médicas

Gerson Antunes Soares[1,2], Raul Ceretta Nunes[1] e Érico M. H. do Amaral[1]

[1]Federal University of Santa Maria (UFSM), PPGEP/DELC/CT,
Santa Maria, Brazil, 97105-900
<gerson, ceretta, erico>@inf.ufsm.br

[2] Brazilian Lutheran University (ULBRA), SI,
Carazinho, Brazil, 99500-000

Abstract

The advances in computing and communication technologies are allowing an incremental number of access to the Electronic Patient Record (EPR) information. However, to enable clinical information on computer networks claims to be careful about patients privacy and data integrity and confidentiality. The access control mechanisms are a key point to maintain these system requirements. In general, only the patient and his doctor are authorized to access the EPR, except when the access is necessary to provide care on patient behalf. Further, on a hospital environment also the context (time, location, attributes, and so one) could be considered. This paper proposes a context-based access control model (CBAC), that works by considering the context of properties in access time and allows the context relations before setting an authorization. This feature enables the implementation of complex access policies that demand separation of duties and delegation.

Keywords: Access control, context.

Resumo

Os avanços nas tecnologias de comunicação e computação estão possibilitando um número crescente de acessos às informações do Prontuário Eletrônico do Paciente (PEP). Entretanto, a disponibilização de informações clínicas em redes de computadores levanta questionamentos sobre a privacidade dos pacientes e a integridade e confidencialidade dos dados. O controle de acesso é um ponto chave para manter tais requisitos. Em geral, somente o paciente e seu médico são autorizados para acessar o PEP, exceto quando o acesso é necessário para fornecer cuidados de interesse do paciente. Adicionalmente, em hospitais também o contexto (hora, localização, atributo, etc) deveria ser considerado. Este artigo propõe um modelo de controle de acesso baseado em contexto (CBAC), o qual considera o contexto de propriedades no instante do acesso e possibilita a análise de relações contextuais para definir a autorização. Esta característica habilita a implementação de políticas de acesso complexas que demandam separação de responsabilidades e delegação.

Palavras chaves: Controle de acesso, contexto.

1. INTRODUÇÃO

A evolução das tecnologias de comunicação e computação vem incrementando a utilização de sistemas computacionais em diversos domínios, tal como negócios, saúde e educacional. Especialmente na área da saúde, a disponibilização de

informações clínicas em redes de computadores, tal como o prontuário eletrônico do paciente (PEP)[1], necessita manter a privacidade dos pacientes, a confidencialidade dos dados e a integridade da informação [4]. Na prática, tais requisitos podem ser atendidos através do uso de mecanismos de controle de vulnerabilidades, de métodos fortes de autenticação, de restrições de acesso, dentre outros [8]. Sendo o *acesso* um ponto chave para manter a segurança (privacidade, confidencialidade e integridade) da informação, o modelo de *controle de acesso* necessita refletir os requisitos da aplicação.

Existem uma série de modelos de controle de acesso disponíveis, dentre os quais os mais conhecidos são o MAC (*Mandatory Access Control*), o DAC (*Discretionary Access Control*) e o RBAC (*Role-Based Access Control*) [12]. O MAC é direcionado para aplicações militares enquanto o DAC e o RBAC são direcionados para aplicações civis. Diferentemente do MAC e DAC, o RBAC possibilita que o controle de acesso considere as *funções* que um usuário pode realizar dentro de uma organização, tornado-se assim o modelo base mais utilizado atualmente. O RBAC [5] introduz o conceito de *role* (função, papel, perfil ou cargo). Tal conceito permite definir o perfil de cada usuário de forma e especificar regras de acesso baseadas nos diferentes perfis. Por generalidade, o RBAC não especifica como cada perfil deve ser utilizado para atender requisitos distintos, ficando isto a cargo do utilizador.

O acesso a informações médicas presentes no PEP deve ser realizado por um grupo heterogêneo de usuários que, para garantir a integridade do prontuário, devem ter permissões de acesso distintas [10], o que pode ser alcançado com mecanismos de controle de acesso baseados em *perfis de usuários*. Entretanto, em se tratando de acesso ao PEP, além da separação de usuários em múltiplos perfis, o mecanismo de controle de acesso também deve considerar *informações de ambiente*, tais como questões temporais, número de acessos, localidade do recurso ou do usuário, entre outras, bem como as *características dinâmicas da informação* [13], uma vez que seu conteúdo pode ser alterado ao longo do tempo. Observe que o conjunto de informações de ambiente, neste artigo chamado *contexto*, e sua dinamicidade são aspectos importantes para a eficácia do mecanismo de controle de acesso. No ambiente hospitalar a aceitação ou negação do acesso deve no mínimo considerar as freqüentes mudanças de turnos (*aspectos temporais*) e de funções (perfil do usuário), buscando contextualizar o acesso. Além disto, o mecanismo de controle de acesso deve considerar a mudança de contexto ao longo do tempo, o que se reflete na alteração dinâmica das permissões para um dado usuário.

O modelo de controle de acesso baseado em regras temporais, ou TRBAC [2], resolve parcialmente o problema ao incluir regras que controlam a validade temporal. Além disto, por ser um modelo conceitual, assim como o RBAC, o TRBAC não determina como estas regras podem ser utilizadas de uma maneira mais transparente ao usuário, ou mesmo como estas regras podem ser gerenciadas.

Para atender aos requisitos da área médica, o Middleware de Autenticação e Controle de Acesso - MACA [10] baseia-se num modelo de autorização contextual para controle de acesso baseado em perfis[2] de usuários [9]. A idéia chave do modelo é decidir pela autorização positiva ou negativa de acordo com as regras de autorização que relacionam as informações sobre o contexto em que cada autorização está sendo solicitada. Além disto, o modelo trata a *separação de responsabilidades* no âmbito do PEP, conforme exigido pela legislação brasileira [4], e a *hierarquia dos perfis*. Entretanto, associações entre autorizações e perfis ou ativação dinâmica de mais de um perfil são as potenciais causas da ocorrência de conflitos de autorização. O MACA estabelece contribuições significativas para solucionar o controle de acesso ao PEP, mas não resolve apropriadamente a detecção e tratamento de conflitos que possam resultar em possíveis violações da política de separação de responsabilidades, nem trata a delegação de atribuições, que no âmbito hospitalar é uma prática bastante utilizada.

Neste trabalho, propõe-se a especificação de um modelo dinâmico de controle de acesso baseado em contexto, o qual pode ser enquadrado como extensão ao modelo de controle de acesso baseado em perfis (RBAC), chamado CBAC (*Context Based Access Control*). O modelo considera informações sobre os elementos inseridos no ambiente como sendo *propriedades* do contexto e assume o conjunto de idéias, situações, eventos e informações necessárias para o correto entendimento do ambiente, como sendo o contexto. Sendo uma extensão do RBAC/TRBAC, o modelo possibilita o acesso diferenciado para perfis distintos de usuários, ao mesmo tempo em que considera requisitos como temporalidade e hierarquia de privilégios. Sendo o contexto para autorização de acesso definido a partir de propriedades que representam as informações dinâmicas do ambiente, a lógica de controle de acesso pode ser fixada através de *condições de contexto* (regras), mas a concessão de autorização pode variar de acordo com a dinamicidade da propriedade incluída na condição de contexto. Como resultado, tem-se um modelo de autorização que possibilita a

[1] De acordo com o Conselho Federal de Medicina do Brasil [4], um prontuário médico é um "documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo". Quando em sua versão eletrônica é dado o nome de Prontuário Eletrônico do Paciente, ou PEP.

[2] O artigo original referencia controle de acesso baseado em *papéis*, mas para coerência deste texto chamamos controle de acesso baseado em *perfis*, pois ambos derivam de *role-based access control*.

implementação de um controle de acesso que pode ser utilizado na disponibilização das informações do PEP, inserindo novas funcionalidades e contribuindo para que as regras determinadas nos modelos existentes possam ser implementadas de uma maneira mais prática. Desta forma, a delegação de atribuições pode ser tratada de maneira diferenciada, ou seja, através da análise das relações entre as propriedades de uma condição de contexto.

O artigo está estruturado como segue. A seção 2 descreve a terminologia utilizada e apresenta algumas definições para o modelo de controle de acesso proposto. A seção 3 apresenta a arquitetura do CBAC. A seção 4 apresenta a lógica de controle de acesso baseada em contextos. A seção 5 discute a aplicação do termo contexto neste e em outros trabalhos relacionados. Finalmente, a seção 6 tece as considerações finais.

2. CONTROLE DE ACESSO BASEADO EM CONTEXTO

Nesta seção define-se precisamente o que significa *contexto* no âmbito deste trabalho, bem como esclarece seus relacionamentos de forma genérica, ou seja, independente do domínio de aplicação. Inicialmente apresentamos a terminologia a cerca do termo contexto e explicamos de forma textual os conceitos, para então apresentar a especificação formal dos termos utilizados no modelo. Salienta-se que embora a exemplificação utilizada nesta seção seja direcionada para a área da saúde, as proposições podem ser utilizadas em outros domínios.

2.1 Terminologia

A palavra portuguesa contexto (do latin: contextu) significa: ”encadeamento das idéias de um texto” [6]. No âmbito da segurança da informação, e precisamente sobre modelos de controle de acesso, este significado leva a uma definição de contexto como sendo um encadeamento de informações sobre um ambiente, ou o conjunto de idéias, situações, eventos e informações necessárias para o correto entendimento do ambiente. Onde ”informação” pode ser reconhecida como uma ”propriedade de um elemento”. Em síntese, um contexto é um encadeamento de propriedades de um elemento em um ambiente. Observa-se que um ”elemento” pode ser um usuário, um dispositivo ou um recurso, tornando assim o contexto uma definição aplicável a diferentes domínios. Estas informações são modeladas de acordo com a política adotada, e por este motivo as definimos como “propriedade”, pois fornecem os dados necessários a montagem da informação contextual. Cada propriedade distinta pode, por sua vez, ser agrupada diretamente nos contextos a que se referem, isto é, um ”contexto” pode ser definido como um conjunto de informações sobre determinados elementos, como um usuário ou objeto.

A combinação de determinadas informações sobre um dado elemento, por exemplo um dado usuário, quando agrupadas numa classe[3] de informações caracteriza-se como um tipo de contexto. Na área da saúde pode-se determinar tipos de contextos de acordo com a política de acesso utilizada. Por exemplo, médicos plantonistas na emergência devem ser autorizados a acessar dados sobre pacientes em atendimento na emergência, mas não sobre pacientes internados em outras unidades do hospital, a menos que ele seja também o médico de um determinado paciente.

Do ponto de vista do acesso, uma autorização de acesso deve considerar regras ambientais (pacientes internados, local do acesso, etc) associadas a operações (visualização de dados, prescrição de laudos, etc), bem como requisitos temporais (período de plantão, tempo de internação, etc). Observe que a existência destas regras de acesso define uma política de segurança, que determina quais os tipos de contextos são ou não necessários para a elaboração de uma condição de contexto.

Como toda regra de acesso se reporta a informações, neste trabalho modela-se informações como propriedades. Deste modo, um exemplo de contexto para um médico plantonista na emergência pode ser modelado como:

- Tipo de Contexto: Usuário;
- Elemento: Médico;
- Propriedade: Função, com valor de propriedade = plantonista;
- Propriedade: Local, com valor de propriedade = emergência;

Observe que cada propriedade, ou informação, possui comportamento específico. Por exemplo, o valor de uma propriedade denominada “Local” deve ser atualizado no momento de uma requisição de acesso, e pode ter como base os endereços IP’s dos equipamentos e a localização dentro da instituição. Note que a existência de tal propriedade não se restringe a um único elemento, uma vez que esta pode estar relacionada a *n* tipos de contexto.

Em síntese, para conseguir uma separação lógica das propriedades que podem ser utilizadas por diferentes sistemas, utilizamos a noção de contexto e de tipos de contexto. Por exemplo, uma dada aplicação pode conter dois tipos de contextos, um Contexto de Objeto e um Contexto de Sujeito (ou usuário), e manipular as informações de cada contexto

[3] Do paradigma de orientação a objetos, classe é uma descrição genérica de objeto, ou seja, reúne objetos que compartilham propriedades em comum [3].

de maneira a obter políticas de acesso mais complexas. Neste sentido, quando modela-se a política de acesso através de contextos é possível prever a detecção de regras conflitantes, uma vez que uma autorização baseada em uma mesma informação, ou propriedade, não pode assumir valores diferentes.

Outro ponto interessante é que, em um ambiente hospitalar pode ser comum a delegação de atribuições a médicos ou especialistas de outras áreas da saúde para prover assistência a um determinado paciente. Quando tratamos a questão da delegação como sendo uma informação contextual, e geramos regras para que esta delegação seja coerente, como dados temporais, locais, e dados relacionados a esta assistência, podemos assumir que esta prática é perfeitamente plausível e adequada à legislação pertinente.

2.2 Definições

Visando a implementação do modelo, nesta subseção apresentam-se as definições formais que mapeiam o termo contexto de forma determinística. Nestas definições cada informação é apresentada na forma de propriedade.

- (**Propriedade de Contexto**). Uma Propriedade de Contexto é um par (P, V), onde P é o nome da propriedade e V é o valor da propriedade P. Observa-se que como uma propriedade de contexto é aplicável a um dado elemento (usuário, dispositivo ou recurso), pode-se dizer que todo par (P, V) ∈ D, onde D é um domínio;
- (**Contexto**). Um contexto CTX é um conjunto de propriedades de contexto (P,V). Note que um dado contexto CTX pode ser formado por diferentes tipos de contextos. Por exemplo, CTX1 = {(P11,V11), (P12,V12)} e CTX2 = {(P21,V21), (P22,V22)} e CTX3 = (CTX1,CTX2) = {(P11,V11),(P12,V12),(P21,V21),(P22,V22)};
- (**Condição de Contexto**). Uma Condição de Contexto ContextCond é uma fórmula booleana em forma de tupla, tal como (CT, P, ⊕, V), onde CT é o tipo de contexto, P é o nome da propriedade, ⊕ é um operador (por exemplo, <, >,=) e V é o valor que a propriedade assume conforme o operador ⊕;
- (**Autorização**). Uma Autorização é uma tupla (CE, O, AM, CC), onde CE é um conjunto de expressões credenciais do usuário[4], O é o objeto, ou objetos, a ser acessado, AM é o modo de acesso e CC é a condição de contexto. A contribuição deste trabalho caracteriza-se pela inserção da condição de contexto (CC) como regra de autorização, os demais termos são originários da definição de autorização do modelo RBAC.

3. ARQUITETURA DO SISTEMA CBAC

A arquitetura do sistema de controle de acesso está dividida em módulos funcionais, conforme mostra a figura 1, e separa o mecanismo de controle de acesso dos mecanismos de atualização. A dinamicidade do sistema é garantida pela variabilidade dos valores de determinadas propriedades, o que ocorre de acordo com o comportamento pré-determinado para cada uma delas.

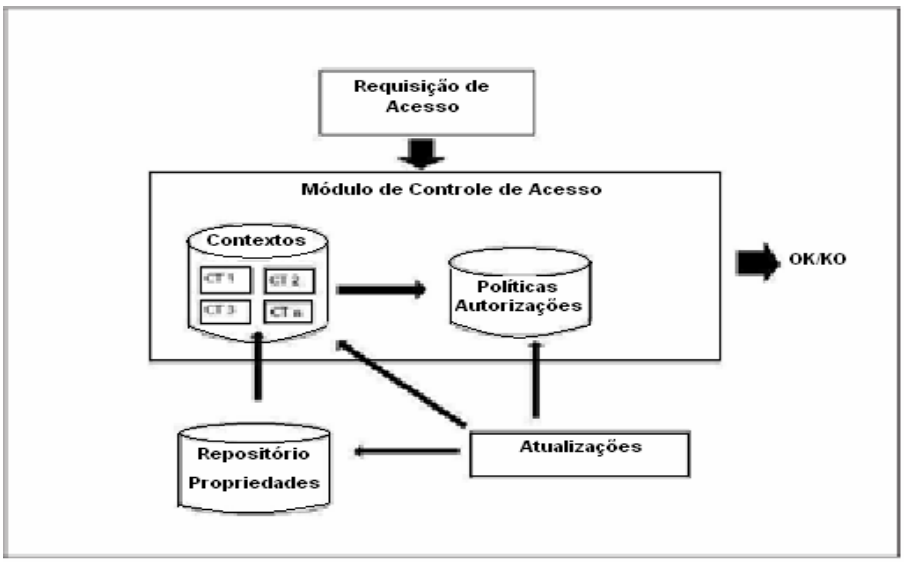

Fig. 1. A Arquitetura do Sistema CBAC

[4] Por definição [5] Expressões Credenciais são os atributos do sujeito necessários para se prover a segurança, como por exemplo, perfil do usuário, a autenticação deste perfil, login, senha, entre outros.

A separação dos mecanismos possibilita uma abordagem genérica ao modelo, não restringindo-o a apenas um tipo de aplicação. Observe que esta separação possibilita determinar claramente as políticas e regras para o controle de acesso de cada sistema, bem como o agrupamento destas informações na forma de Contextos, pois isola a lógica da política de controle de acesso dos mecanismos de imposição da política (regras).

Em cada requisição de acesso são necessárias informações relativas às credenciais do usuário, objeto e modo de acesso. O Módulo de Controle de Acesso verifica as regras necessárias para o acesso e confronta suas informações com os dados de Contexto do sistema, liberando ou não o acesso. As atualizações necessárias ao funcionamento do sistema são reportadas diretamente às *Políticas de Acesso* (Autorizações), *Contexto* (e seus *Tipos de Contexto*) e ao *Repositório de Comportamento de Propriedades*, o que possibilita mapearmos cada informação, ou comportamento de cada propriedade, de acordo com a modelagem previamente determinada para a aplicação.

Na política de acesso é inserida uma Condição de Contexto, conforme definido na seção 2, esta condição nada mais é do que uma regra da política de acesso que determina quais situações podem prover o acesso a determinados recursos. Como tanto a condição contextual como as propriedades nos tipos de contexto se referem as mesmas informações, a manipulação destes dados pode ser tratada da mesma forma, ou seja, uma propriedade (informação) considerada por uma regra de acesso em uma condição de contexto deve ser a mesma indicada no contexto especificado pela política, desta forma se estabelece os valores a que a condição se reporta e no contexto propriamente dito a propriedade assume o valor de acordo com o comportamento da propriedade.

Digamos que uma propriedade com nome *Tempo* é necessária para, em conjunto com outras propriedades, prover acesso a um determinado objeto, esta mesma propriedade é referenciada na *Condição de Contexto*, como regra para a autorização de acesso e no *Contexto* a que ela é relacionada, além de possuir referência no repositório de comportamento de propriedades, o que garante a dinamicidade da mesma, uma vez que se determine como e em que situações o valor da propriedade no contexto sofre alterações. Cabe salientar aqui que os valores na condição de contexto permanecem estáticos, uma vez que a política de acesso é pré-definida. O módulo de atualizações se reporta a alimentação e manutenção do sistema, uma vez que o modelo utiliza propriedades distintas mas que relacionam-se entre os diversos módulos.

Note que a arquitetura proposta possibilita agregar novas funcionalidades ao RBAC, assim como em [9] e [7], pois todos os modelos baseados em regras utilizam um conjunto de políticas de acesso. Por outro lado, a arquitetura proposta possibilita o armazenamento das informações contextuais de forma mais transparente, facilitando a implementação do mecanismo de controle de acesso.

4. LÓGICA PARA O CONTROLE DE ACESSO

Para que as definições formais sejam compreendidas de forma mais clara, optou-se por utilizarmos codificação XML para os respectivos exemplos. O XML provê uma representação estruturada dos dados, e por ser uma arquitetura que não possui elementos nem marcas predefinidas, não especifica como os autores devam utilizar metadados, sendo que existe total liberdade para utilizar qualquer método disponível, desde simples atributos, até a implementação de padrões mais complexos [1], o que possibilita o relacionamento com as definições propostas. Esta seção apresenta a codificação e as descrições XML além da lógica do modelo de controle de acesso baseado em contexto.

4.1 Codificação XML

Em um ambiente hospitalar muitas informações podem ser consideradas como propriedades de um determinado contexto. Tais informações podem ser relacionadas como itens de regras de acesso como, por exemplo, a delegação de atribuições a outros usuários, criando condições de contexto relativas a esta situação. Observe que a modelagem de tais relações torna o controle de acesso a determinados documentos uma tarefa mais prática, uma vez que as informações necessárias à delegação podem ser tratadas como propriedades de um contexto, seja este de um sujeito ou de um objeto, dependendo apenas de como a regra de acesso é modelada.

Para que isso seja possível exemplificamos como uma Política de Acesso pode ser descrita em linguagem XML. De acordo com os modelos de controle de acesso existentes, utilizamos regras para uma política eficiente. Estas regras consideram expressões credenciais dos usuários bem como referências aos objetos. Neste trabalho é acrescentado a estes modelos uma *Condição de Contexto*, a qual pode ser exemplificada da seguinte forma: suponha-se que um determinado arquivo de paciente só pode ser acessado, ou tenha seu acesso liberado, se uma das duas condições seguintes forem satisfeitas; 1) um usuário com função de enfermeira acessa os dados a partir das 10:00; ou 2) o objeto em questão encontre-se no setor de emergência com um contador de acessos com valor inferior a 20 ocorrências. Esta regra hipotética pode ser codificada em XML conforme as definições de *Contexto* e *Condição de Contexto*, apresentados na figura 2.

Observe que um elemento ContextCond é dividido em cláusulas (Clause) que contém as possíveis regras de liberação de acesso. Estas cláusulas contêm os tipos de contextos utilizados (neste caso: Sujeito e Objeto); cada tipo de contexto possui suas propriedades e valores, além de um operador que determina a condição efetivamente da regra.

```
<ContextCond>
.  <Clause>
.    <Context Type="Sujeito">
.      <Property Name="Tempo"/>
.      <Operator OP=">"/>
.      <Value V="10:00"/>
.    </Context>
.    <Context Type="Sujeito">
.      <Property Name="Função"/>
.      <Operator OP="="/>
.      <Value V="Enfermeira"/>
.    </Context>
.  </Clause>
.  <Clause>
.    <Context Type="Objeto">
.      <Property Name="Contador"/>
.      <Operator OP="<"/>
.      <Value V="20"/>
.    </Context>
.    <Context Type="Objeto">
.      <Property Name="Local"/>
.        <Operator OP="="/>
.      <Value V="Emergência"/>
.    </Context>
.  </Clause>
</ContextCond>
```

Fig. 2. Exemplo Elemento XML - ContextCond

Na subseção 3.2, definimos, entre outros, a condição de contexto, no exemplo referenciado como *ContexCond*. Como uma condição de contexto pode possuir várias regras de acesso para uma determinada ação agrupamos estas regras em cláusulas, cada cláusula contém expressões que configuram-se efetivamente nas regras de acesso. Conforme a definição, cada condição de contexto deve possuir um agrupamento de elementos de uma tupla, ou no caso das cláusulas, vários agrupamentos. Cada tupla é traduzida em forma de regra de acesso, com base no exemplo apresentado, podemos traduzir uma tupla (CT, P, ⊕, V) por uma das expressões da primeira cláusula onde: CT é o tipo de contexto (<Context Type = “Sujeito”>), P é o nome da propriedade (<Property Name =“Tempo”>), ⊕ é o operador da regra (<Operator OP=“>”>) e V é o valor da propriedade (<Value V=“10:00”>).

A Condição de Contexto da figura 2 é confrontada com o Contexto do Sistema no momento da requisição de acesso. O Contexto do Sistema, por sua vez, é armazenado e agrupado de acordo com seus tipos de contextos. Cada tipo de contexto pode ser exemplificado como segue: considera-se o Tipo de Contexto Objeto e determina-se as suas propriedades e seus respectivos valores; cada tipo de contexto possui um conjunto de elementos reconhecidos por target, o que é utilizado para se efetuar a separação entre os elementos inseridos em cada tipo; a lógica segue as definições anteriores sobre contexto utilizando propriedades inerentes a cada elemento, como mostra a figura 3. Neste exemplo têm-se o elemento ”Ordem Médica.doc” e as informações (ou propriedades) a ele relacionadas, de acordo com a definição de *Propriedade de Contexto* temos uma tupla (P, V), onde, neste exemplo, as propriedades (P) são: ”Tempo” e ”contador”. O valor de cada propriedade (V) é alterado de acordo com o repositório de comportamento de propriedades, o que faz com que o valor da propriedade “contador” seja incrementado em determinadas situações e que o valor da propriedade “tempo” seja consultado nos momentos em que se determine. Desta forma todas as informações necessárias para o controle de acesso podem ser modeladas como regras na condição de contexto e tratadas de acordo com sua especificação em cada tipo de contexto.

```
<Context Type="Objeto">
.  <Objeto target="Ordem_Médica.doc">
.    <Property Name="Tempo">
.      10:00
.    </Property>
.    <Property Name="contador">
.      12
.    </Property>
.  </Objeto>
</Context>
```

Fig. 3. Exemplo Elemento XML – Context Type

Com a exemplificação dos elementos em XML pode-se verificar que as informações são tratadas da mesma forma (como propriedades), tanto no Contexto, propriamente dito, como na condição de contexto referenciada pela política de acesso. Assim, um contexto pode ser compreendido como um conjunto de elementos Context Type, e uma Condição de Contexto inserida em uma política de acesso pode ser compreendida como um elemento ContextCond.

4.2 Algoritmo de Controle de Acesso

Para a interação entre as condições de contexto e os contextos pré-definidos, utiliza-se o seguinte algoritmo (figura 4):

```
1.  Receber requisição de acesso
2.  Selecionar todas as condições de contexto que satisfaçam a requisição de acesso: CE, O e AM
3.  Selecionar todas as cláusulas nas condições de contexto
4.  Determinar flagc = FALSE                                          // flag de cláusula
5.  Percorrer todas as cláusulas até encontrar uma cláusula verdadeira
6.      Selecionar as expressões em cada cláusula
7.      Determinar flage = TRUE                                       // flag de expressão
8.      Percorrer todas as expressões de cada cláusula até encontrar uma expressão falsa
9.          Para cada expressão comparar Tipo de Contexto, Propriedade e Valor com o Contexto
10.         Se o valor da propriedade não satisfaz o operador da regra determinar flage = FALSE
11.     Se flage == FALSE
12.         Passar para cláusula seguinte
13.     Senão flagc = TRUE                                            // cláusula verdadeira
14. Se flagc == TRUE                                                  // existe um cláusula verdadeira
15.     Permitir Acesso
16. Senão Negar Acesso
```

Fig. 4. Algoritmo de Controle de Acesso

No algoritmo apresentado, uma condição de contexto é uma operação que testa cláusulas, sendo uma cláusula um conjunto de expressões (regras de acesso). A lógica consiste em encontrar uma cláusula verdadeira para autorizar o acesso. Logo, percorre-se as cláusulas com o objetivo de verificar se todas as expressões internas a ela são verdadeiras. Na linha 2 são separadas todas as regras que satisfazem a expressão credencial do usuário (CE), o objeto a ser acessado (O) e o modo de acesso (AM). Em seguida determina-se uma condição para se testar cada cláusula (linha 4) e outra para se testar cada expressão nas cláusulas (linha 7). As linhas 9 e 10 do algoritmo exemplificam a operação de comparação da regra de acesso (expressão) com as informações apresentadas pelo contexto, a fim de verificar se o contexto satisfaz a cláusula e consequentemente todas as regras de acesso relativas a esta. No momento em que isto ocorre, o acesso é concedido (linhas 14 e 15). Se alguma expressão no interior da cláusula é falsa (linha 11 do algoritmo), então toda a cláusula é considerada falsa e é necessário percorrer as demais cláusulas com a finalidade de se determinar o acesso. Quando todas as regras (cláusulas) inerentes à requisição de acesso são percorridas e nenhuma delas é verdadeira o acesso é negado (linha 16).

Considera-se as cláusulas da Condição de Contexto como uma operação ”OR”, determinando que: ou uma ou outra condição é suficiente para liberar o acesso de determinado sujeito a determinado recurso; e um conjunto de expressões em cada cláusula é considerado como uma operação ”AND”, ou seja, a cláusula só é verdadeira se todas as expressões em seu interior forem verdadeiras. Esta consideração permite a manipulação da política de acesso de forma mais rígida ou de forma mais branda, de acordo com a quantidade de cláusulas utilizadas para a concessão de um acesso, isto é, se para um determinado acesso só existe a possibilidade de um única regra de acesso, a regra é mapeada em uma única cláusula, excluindo a possibilidade de um “OR”. Desta forma o acesso só será concedido se, e somente se, esta única regra for satisfeita.

Observe que tal algoritmo possibilita tratar as autorizações de acesso baseando-se em informações contextuais, possibilitando assim uma maior eficiência ao mecanismo de controle de acesso, uma vez que as informações podem sofrer alterações dinamicamente, e teoricamente toda informação pode ser modelada na forma de propriedades.

Com o algoritmo proposto e a modelagem das informações na forma de propriedades de contexto e condições de contexto é possível vislumbrar a utilização do modelo para diversas situações como, por exemplo, o problema da delegação de atribuições a terceiros e a detecção de regras conflitantes, bem como a utilização de hierarquia de privilégios para a concessão coerente de uma delegação, pois a regra de delegação pode ser mapeada obedecendo uma hierarquia, e as exceções à regra podem ter o acesso negado.

5. TRABALHOS RELACIONADOS

Uma das primeiras menções ao termo contexto no âmbito de modelos de controle de acesso à dados médicos foi realizada por Motta e Furuie [9] em 2002, onde o modelo propunha uma implementação do RBAC [5] para controlar o acesso ao PEP. Porém, Motta e Furuie não apresentaram uma definição específica para o termo contexto utilizado e não incluíram o contexto como sendo um componente do sistema, ou seja, apenas utilizaram a noção de contexto para definir regras de autorização estáticas. Deste modo, aprofundam a questão das regras da política de acesso considerando o ambiente hospitalar, mas não incluem no modelo a utilização dos contextos como forma que possibilite a separação das lógicas de políticas.

A dificuldade na distinção ocorre por que o RBAC trata, de forma genérica, apenas autorizações de acesso baseadas em regras. O RBAC deixa livre a utilização das regras, para que os usuários possam especificar o sistema e a aplicação em diferentes domínios, o que de fato leva a pensar em contextos. Na prática, a maior parte dos modelos de controle de acesso propostos após o RBAC fazem uso da idéia básica de regras de acesso e agregam funcionalidades baseando-se neste princípio [2][9].

Assim como Motta e Furuie, Hulsebosch et al. [7] também apresentam um modelo de controle de acesso sensível a contextos, o qual utiliza regras e informações contextuais. Entretanto, também não define precisamente o escopo do termo utilizado, ocasionando uma certa confusão sobre "o que significa o contexto?". O controle de acesso continua sendo modelado através de regras ao invés de usar contextos, como definido na introdução deste trabalho. As regras definidas por Hulsebosch et al. são bem especificadas, porém a utilização do termo "contexto" restringe-se apenas ao contexto no sentido do ambiente a que a política de controle de acesso está inserida. Entretanto, observa-se que se os contextos forem adequadamente modelados (fizerem parte do modelo) as relações contextuais podem ser melhor exploradas. Com o desenvolvimento do CBAC objetivou-se a utilização de informações contextuais no modelo, com intuito de aprimorar a manipulação das regras e a especificação da política de acesso através das relações contextuais.

Em Wilikens et al. [14] é introduzido o conceito de propriedades dinâmicas, o que pode tornar o modelo mais flexível. Os autores utilizam o estado da arte do RBAC para demonstrar a integração do conceito com características de sistemas de saúde, mas a idéia de contexto se dá no sentido de autenticação de usuários, onde parâmetros [14] como localização são utilizados para garantir níveis de autenticidade do usuário.

Uma política de controle de acesso provê a validação de uma requisição de acesso [11]. Esta validação pode depender de vários fatores como, por exemplo, o tempo em que o acesso pode ser liberado. Esta informação depende diretamente do tipo de contexto que o controle de acesso está manipulando. Logo, criar uma representação que associe uma autorização a um contexto que contenha informações dinâmicas (por exemplo , `<Médico, Emergência, local de acesso>`, onde local de acesso possui comportamento variável), possibilita o gerenciamento do controle de acesso de forma dinâmica. Isto contribui para implementações de políticas de segurança especificas, tal como a de acesso ao Prontuário Eletrônico do Paciente, onde a responsabilidade pelo prontuário do paciente é do médico assistente, dos demais profissionais que compartilham do atendimento, da hierarquia médica da instituição nas suas respectivas áreas de atuação, e da hierarquia médica constituída pelas chefias de equipe, chefias de clínica, chefias de setor, hierarquicamente até o diretor da divisão médica e/ou diretor técnico, além do próprio paciente [4]. Baseado nesta legislação, entende-se que o modelo pode atender os requisitos uma vez que possa ser modelado de forma a utilizar hierarquia de privilégios [13] de acordo com a estrutura da Instituição de Saúde.

6. CONSIDERAÇÕES FINAIS

A disponibilização de informações clínicas em rede deve manter a integridade da informação para a segurança dos processos do sistema. Para tal, mecanismos de controle de acesso são necessários. No caso do PEP (Prontuário Eletrônico do Paciente), onde há uma heterogeneidade de usuários e dispositivos interagindo com o sistema, a separação das informações na forma de propriedades distintas possibilita um melhor entendimento e uma facilidade no momento de se gerar as regras de política de acesso. Isto pode ser obtido utilizando-se uma abordagem contextual no controle de acesso, onde considera-se o contexto das propriedades (informações).

Neste trabalho apresentamos um modelo de controle de acesso baseado em contexto, CBAC, o qual fornece autorizações relacionando informações de diferentes contextos. O modelo agrega novas funcionalidades ao RBAC (Role-Based Access Control), que baseia-se principalmente em regras de acesso e perfis de usuários, mas não em informações contextuais. No CBAC o uso de contextos definidos através de propriedades torna o controle dinâmico (a variação de uma propriedade pode tornar positiva ou negativa uma autorização de acesso) e possibilita um melhor mapeamento entre a política de acesso utilizada e a implementação do controle (regras). Possibilita ainda o acesso diferenciado para perfis distintos de usuários, ao mesmo tempo em que considera requisitos como temporalidade e hierarquia de privilégios. Em outras palavras, possibilita que as informações necessárias à elaboração das políticas de acesso possam ser armazenadas de uma forma clara e independente.

Como resultado prático a implementação de uma política de acesso complexa, como a de acesso ao prontuário eletrônico do paciente, pode ser realizada de maneira mais facilitada, pois as relações contextuais podem ser modeladas de maneira mas simples, uma vez que as informações podem ser tratadas como propriedades de um contexto. Correntemente, em conjunto com o CPD (Centro de Processamento de Dados) da UFSM, o modelo está sendo implementado para suportar o controle de acesso ao PEP do Hospital Universitário de Santa Maria.

Referências

[1] ALMEIDA, Maurício Barcellos. (2002). An introduction to XML, its use on the Internet and some complementary concepts. Ci. Inf., mayo/ago. 2002, vol.31, no.2, p.5-13. ISSN 0100-1965.

[2] Bertino, E., Bonatti, P. A., and Ferrari, E. (2001). TRBAC: A Temporal Role-Based Access Control Model. ACM Trans. Inf. Syst. Secur., 4(3):191–233.

[3] Booch, G. (1991). Object-Oriented Design with Applications. Benjamin Cummings, Redwood City, CA. BOO g 94:1 1.Ex.

[4] CFM – Conselho Federal de Medicina, (2002). Resolução 1.639/2002 do Conselho Federal de Medicina do Brasil. Disponível em http://www.arnaut.eti.br/ResoCFM.htm, acesso em Dez/2005.

[5] Ferraiolo, D. F., Sandhu, R. S., Gavrila, S. I., Kuhn, D. R., and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. Information and System Security, 4(3):224–274.

[6] Ferreira, Aurélio Buarque de Holanda (2000). Dicionário Aurélio da Língua Portuguesa. 4. ed. Rio de Janeiro: Nova Fronteira, 2000.

[7] Hulsebosch, R. J., Salden, A. H., Bargh, M. S., Ebben, P. W. G., and Reitsma, J. (2005). Context sensitive access control. In SACMAT '05: Proceedings of the tenth ACM symposium on Access control models and technologies, pages 111–119, New York, NY, USA. ACM Press.

[8] ISO/IEC 15408. (1999). Information Tecnology – Security techniques – Evaluation criteria for IT security. International Organization for Standardization – ISO and International Electrotechnical Commission - IEC.

[9] Motta, G. H. M. B. and Furuie, S. S. (2002). Um modelo de autorização contextual para o controle de acesso baseado em papéis. In II Workshop em Segurança de Sistemas Computacionais (WSeg2002), pages 137–144, Porto Alegre-RS, Brasil. SBC.

[10] Motta, G. H. M. B. and Furuie, S. S. (2003). A contextual role-based access control authorization model for electronic patient record. IEEE Transactions on Information Technology in Biomedicine, 7(3):202–207.

[11] NBR/ISO/IEC 17799. (2002). Tecnologia da informação: Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas ABNT, 55pp.

[12] Samarati, Pierangela and Vimercati, Sabrina De Capitani di. (2001). Access Control: Policies, Models, and Mechanisms. Foundations of Security Analysis and Design, Tutorial Lectures, LNCS, v.2171, p.137-196, 2001.

[13] Soares, Gerson Antunes and Nunes, Raul Ceretta. (2005). Controle de Acesso Baseado em Credenciais Hierárquicas Dinâmicas – DHCBAC. In: II Latin-American Symposium on Dependable Computing - Workshop on Theses and Dissertations, Salvador. Proceedings of the LADC Wokshops. Salvador, 2005. p. 77-82.

[14] Wilikens, M., Feriti, S., Sanna, A., and Masera M. (2002). A Context-Related Authorization and Access Control Method Based on RBAC: A case study from the health care domain. In SACMAT '02: Proceedings of the seventh

ACM symposium on Access control models and technologies, pages 117–124, Monterey, California, USA. ACM Press.