Controle de Acesso Baseado em Papéis em Ambientes Assistidos

Gabriel R. Goulart[1], **Mário A. R. Dantas**[2]

[1]Departamento de Informática e Estatística (INE) - Universidade Federal de Santa Catarina (UFSC)

[2]Instituto de Ciências Exatas (ICE) - Universidade Federal de Juiz de Fora (UFJF)

gabriel.r.goulart94@gmail.com, mario.dantas@ice.ufjf.br

Abstract. *This work presents an access control system based on user and environment roles, using context information to compose the access rules. To validate the functioning of this system, 4 individuals from different age groups performed tests during a two-week period in a home-based environment, where RFID tags were used to identify users in a non-intrusive way. After the tests, it was identified that all access attempts were processed correctly, regardless of the changes of roles or access rules, which shows that the proposed system does indeed work in a ambient assisted living.*

Resumo. *Este trabalho apresenta um sistema de controle de acesso baseado em papéis de usuário e ambiente, utilizando informações de contexto para compor as regras de acessos. Para validar o funcionamento desse sistema, 4 indivíduos de diferentes faixas etárias realizaram testes durante o período de duas semanas em um ambiente assistido domiciliar, onde tags RFID foram utilizadas para identificar os usuários de maneira não intrusiva. Após os testes, identificou-se que todas as tentativas de acesso foram processadas corretamente, independentemente das mudanças dos papéis ou das regras de acesso, o que mostra que o sistema proposto de fato funciona em um ambiente assistido.*

1. Introdução

Segundo uma pesquisa das Nações Unidas, a população idosa dobrará até 2050 [ONU 2017]. Com isso o consumo de serviços voltados para essa população também aumentará, porém se soluções inovadoras não forem encontradas e aplicadas, esses serviços sofrerão com um défice muito grande para suprir as necessidades da sociedade.

Nesse contexto soluções como a de ambientes assistidos são aplicadas com o objetivo de fornecer uma ajuda, e complementar os serviços voltados a saúde e bem estar, não só dos idosos, mas de qualquer indivíduo que precise ser assistido. A utilização dessa solução provê um maior conforto para o indivíduo, pois ele poderá viver no seu ambiente domiciliar e mesmo assim continuar sendo acompanhado pelo o seu médico por exemplo. E se alguma anormalidade acontecer, imediatamente todos os envolvidos no cuidado do indivíduo serão notificados e as ações necessárias serão tomadas.

Com o crescimento e popularização dos ambientes assistidos, não se pode deixar de pensar na segurança desses ambientes, e por este motivo o controle de acesso é de

extrema importância, pois garante acesso ao ambiente, acesso físico, apenas para pessoas aptas a acessá-lo, utilizando diversas abordagens como por exemplo a baseada em papéis.

Seguindo essa linha, este trabalho apresentará um sistema para realizar o controle de acesso baseado em papéis, papéis de usuário e ambiente, juntamente com informações de contexto, ou seja, informações que o ambiente pode prover para o sistema, com o objetivo de realizar um controle de acesso inteligente e sensível ao ambiente.

Este trabalho está dividido da seguinte forma: na seção 2 é apresentado o padrão do controle de acesso baseado em papéis, na seção 3 uma análise dos trabalhos correlatos é realizada, seguindo na seção 4 é apresentado a proposta deste trabalho, já na seção 5 os resultados são discutidos, e por fim a conclusão e trabalhos futuros, apresentados na seção 4.

2. Controle de Acesso Baseado em Papéis

O controle de acesso baseado em papéis, também conhecido como *Role Based Access Control* (RBAC), foi proposto por volta de 1970 quando sistemas multiusuários e multiaplicações começaram a surgir. Sua padronização foi realizada em 2004 pelo *National Institute of Standards and Technology* (NIST). Atualmente o padrão ANSI para o RBAC é o INCITS 359-2012 .

Basicamente essa abordagem associa os usuários aos papéis, e os papéis as permissões. Isso permite que os usuários possam ser associados a outros papéis facilmente, e que as permissões possam ser alteradas ou revogadas de uma maneira simples, ou seja, com a incorporação de novas aplicações no sistema, o impacto para adequar os usuários e papéis é o mínimo possível.

O RBAC é definido por quatro componentes: o RBAC núcleo, RBAC hierárquico, Separação estática de relações de serviço e Separação dinâmica de relações de serviço. O componente mais importante do RBAC é o núcleo, o qual pode ser utilizado sem os outros componentes, pois traz consigo as funções essenciais do controle de acesso baseado em papéis.

2.1. RBAC Núcleo

O núcleo inclui alguns elementos básicos para o controle de acesso. Esses elementos são: usuários (US), papéis (PA), objetos (OBJS), operações (OPS) e permissões (PERMS). Através da Figura 1 se pode observar o conjunto de elementos e suas interações. A relação entre usuários e papéis (AU), e entre papéis e permissões (AP) é de muitos para muitos, o que permite que um usuário possa ser associado a vários papéis. Além disso o núcleo tem um elemento chamado sessão (SE), que por sua vez armazena para cada usuário os papéis ativos relacionados a ele.

Importante destacar que o elemento usuário não precisa ser necessariamente um humano. Esse elemento pode ser representado por um sistema computacional por exemplo. Já o elemento objeto pode ser qualquer recurso do sistema que necessite de controle de acesso, onde se permite ou não realizar as operações OP.

Conforme descrito por [Ferraiolo and Kuhn 2004] segue a especificação do núcleo do RBAC:

- USUÁRIOS, PAPÉIS, OPERAÇÕES e OBJETOS

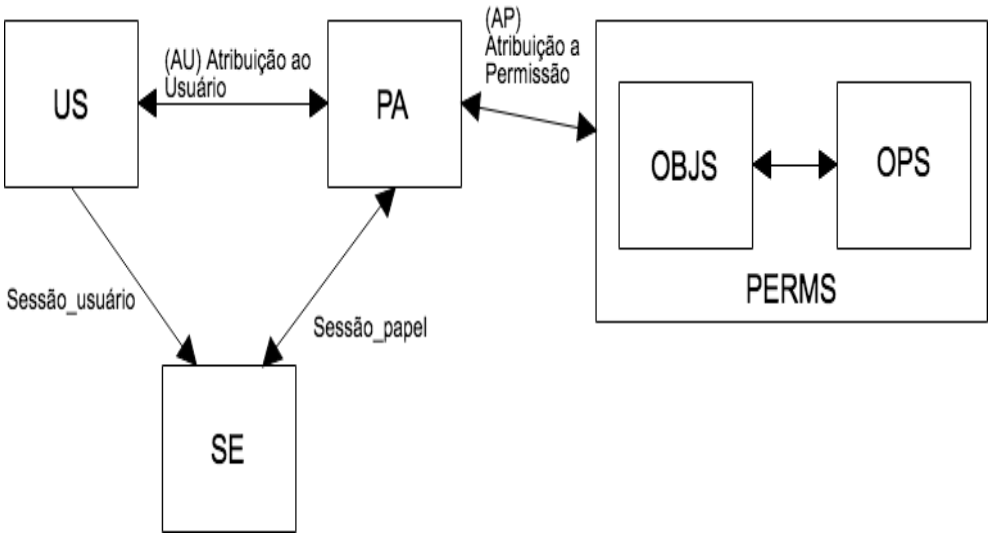

Figura 1. Núcleo do RBAC

- $AU \subseteq$ US X PA, relação de atribuição muitos para muitos entre usuário e papel.
- $usuários\_atribuidos : (p : PA) \rightarrow 2^{US}$, mapeamento do papel p em um conjunto de usuários. $Formalmente : usuários\_atribuidos(p) = u \in US|(u, p) \in AU$
- $PERMS = 2^{(\text{OBJ X OP})}$, conjunto de permissões.
- $AP \subseteq$ PERMS X PA, relação de atribuição muitos para muitos entre permissões e papéis.
- $permissões\_atribuidas(r : PA) \rightarrow 2^{PERMS}$, mapeamento do papel r em um conjunto de permissões. $Formalmente : permissões\_atribuidas(r) = p \in PERMS|(p, r) \in AP$
- $Op(p : PERMS) \rightarrow op \subseteq OPS$, mapeamento da permissão para a operação, o qual dá o conjunto de operações associadas com a permissão p.
- $Ob(p : PERMS) \rightarrow ob \subseteq OBJS$, mapeamento da permissão para o objeto, o qual dá o conjunto de objetos associados com a permissão p.
- $SE =$ conjunto de sessões.
- $sessão\_usuário(s : SE) \rightarrow US$, mapeamento da sessão s em um usuário correspondente.
- $sessão\_papel(s : SE) \rightarrow 2^{PA}$, mapeamento da sessão s em um conjunto de papéis. $Formalmente : sessão\_papel(Si) \subseteq p \in PA|(sessão\_usuário(Si), p) \in AU$
- $sessão\_permissão\_disponível(s : SE) \rightarrow 2^{PERMS}$, permissão disponível para um usuário em uma $sessão = p \in sessão\_papel(s) \cup permissões\_atribuidas(p)$

2.2. RBAC Hierárquico

Esse componente introduz o conceito de hierarquia de papel (HP). A Hierarquia representa naturalmente a estrutura de papéis, refletindo em uma linha de organização das autoridades e responsabilidades.

A hierarquia de papéis define a relação de herança entre papéis, ou seja, se um papel P1 agrega todas as permissões de um papel P2, diz-se que P1 herda P2. Obviamente, como P1 está em um nível de hierarquia maior que P2, ele pode conter mais permissões

que P2. Na Figura 2 se tem um exemplo prático de hierarquia de papéis, onde mostra simplificadamente a estrutura hierárquica dos papéis em um mercado .

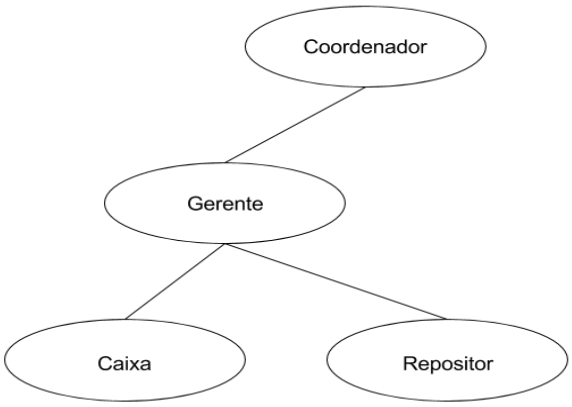

Figura 2. Exemplo de Hierarquia de Papéis

Na Figura 2 o papel Coordenador está no nível mais alto da hierarquia, logo ele possui todas as permissões associadas aos demais papéis. Já o papel Gerente só possui as permissões dos papéis Caixa e Repositor, e no caso, os dois últimos papéis no nível de hierarquia, só possuem as suas permissões.

2.3. Separação estática de relações de serviço

Com o crescimento do sistema, usuários vão sendo associados a novos papéis, e como um usuário pode se associar a mais de um papel, um problema que pode ocorrer é o conflito de interesses, ou seja, o usuário se associa a dois papéis que são conflitantes. Por exemplo, na Figura 2 o usuário se associa ao papel Caixa e ao papel Gerente. Esse tipo de ação deveria ser proibida, pois o papel Caixa é subordinado do papel Gerente, e como que um usuário poderia ser subordinado dele mesmo? Para resolver essa situação, foi agregado ao RBAC a separação estática de relações de serviço, que consiste em restringir associações entre usuário e papéis, ou seja, antes de se associar um usuário a um papel é verificado se essa associação é permitida, caso seja, a associação é feita, caso contrário não.

2.4. Separação dinâmica de relações de serviço

Anteriormente foi discutido sobre separação estática de relações de serviço, porém conflitos podem ocorrer de maneira dinâmica, ou seja, durante a ativação de papéis para um certo usuário. A separação dinâmica de relações de serviço previne que dois papéis conflitantes estejam ativos ao mesmo tempo para um usuário, portanto para um papel P1 que tem conflito com um papel P2 ficar ativo para um usuário U, o papel P2 tem que estar inativo para o usuário U. Importante observar que assim como na separação estática, a solução desse problema se dá pelo uso de restrições, que são verificadas nas ativações dos papéis.

3. Trabalhos Correlatos

Na comunidade acadêmica assuntos relacionados ao controle de acesso já vem sendo discutidos há bastante tempo, principalmente o baseado em papéis. Porém, ainda não se encontram em abundância trabalhos que foquem no uso do controle do acesso em ambientes assistidos, mesmo que nos últimos anos, assuntos relacionados a ambientes assistidos tenham estado em alta.

Nos trabalhos que foram analisados, formas de se aplicar o controle de acesso baseado em papéis foram encontradas, algumas levando em consideração o contexto, outras atribuindo papéis aos ambientes. Entretanto, a maioria dos trabalhos não deixam claro a sua aplicabilidade em ambientes assistidos, de maneira a controlar o acesso em um ambiente real, utilizando todos os recursos que tal ambiente pode oferecer.

3.1. Análise dos trabalhos correlatos

Como citado anteriormente, diversas alternativas para realizar o controle de acesso baseado em papéis são encontradas. [Zhang et al. 2004] utilizam máquinas de estados para fazer o controle de papéis ativos e permissões atribuídas aos papéis. Como a aplicação é consciente de contexto, um agente de contexto coleta as informações e gera eventos que disparam transições nas máquinas de estados.

Outra abordagem consciente de contexto é a de [Covington et al. 2001], que traz o conceito de papel de ambiente, o que não é um elemento do padrão RBAC. Sendo assim, com essa nova atribuição, as permissões são associadas tanto aos papéis de usuários quanto aos papéis de ambiente, provendo uma maior flexibilidade para o sistema como um todo.

[Park et al. 2006] utilizam o conceito de papel de contexto, o que se assemelha ao papel de ambiente apresentado por [Covington et al. 2001]. Entretanto, elementos como datas e tempo são utilizados para formar o papel de contexto, que são associados aos papéis de usuários e assim formam a política de segurança. A seguir um exemplo do controle de acesso utilizando papel de contexto.

- $transação = < papel\_usuário, papel\_contexto, permissão >$
- $bit\_permissão =$ permitir , negar
- $regradapolítica = < transação, bit\_permissão >$, $exemplo << criança, (18h < T < 21h), TV\_Ligar >, permitir >$

[Kayes et al. 2017] utilizam as informações de contexto para ativar o papel do usuário, semelhante aos trabalhos apresentados anteriormente. A utilização do contexto para ativar um papel de usuário é realizada através de expressões contextuais, ou seja, uma composição de contextos, onde se pode utilizar informações como a localização do usuário, dias da semana ou até mesmo as escalas de trabalho por exemplo. O gerenciamento dessas políticas de controle de acesso é realizado utilizando-se ontologias, o que facilita no processo de verificação das condições para ativar um papel, e também na expansão do sistema, como a criação de novas políticas de acesso ou até mesmo de papéis de usuário.

No processo de pesquisa limitou-se a procurar abordagens de controle de acesso baseadas em papéis, as quais fossem sensíveis ao contexto, para que assim houvesse uma

maior proximidade com os objetivos deste trabalho, mesmo que a maioria dos trabalhos foquem em apresentar modelos, que muitas vezes não são aplicados em um ambiente assistido.

4. Proposta

Através da análise dos trabalhos correlatos constatou-se que os modelos de controle de acesso propostos não deixam claro a sua aplicabilidade em ambientes assistidos. Portanto com o objetivo de explorar essa questão, este trabalho propõe um sistema para controlar o acesso físico em ambientes assistidos de maneira não intrusiva, utilizando papéis de usuário e ambiente juntamente com as informações de contexto para construir regras de acesso.

A Figura 3 apresenta um exemplo do funcionamento do sistema. Supondo que um usuário X desempenha o papel de usuário EMPREGADO e está tentando acessar um ambiente Y com papel de ambiente SALA DO CHEFE, e a regra de acesso associada ao papel de usuário e ambiente utilize as seguintes informações de contexto : horário, data e se o chefe se encontra em sua sala. Para que o usuário X consiga acessar a sala do chefe as informações de contexto precisam ser verdadeiras.

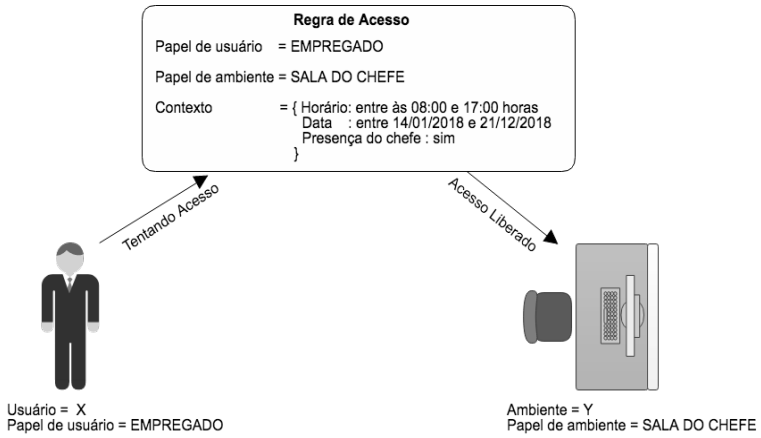

Figura 3. Exemplo do Sistema

A identificação do usuário é realizada de maneira não intrusiva utilizando tags RFID (*Radio Frequency Identification*). As tags são associadas a papéis de usuário, que por sua vez integram a regra de acesso. As informações e associações, como por exemplo entre usuário e papel de usuário, são armazenadas em um banco de dados MySQL. Importante ressaltar que o sistema foi implementado utilizando as linguagens Python e C para Arduino junto com o protocolo de comunicação MQTT (*Message Queuing Telemetry Transport*).

4.1. Controle de Acesso

Neste trabalho o controle de acesso utilizado será o baseado em papéis, o RBAC (*Role Based Access Control*), porém só serão utilizadas as funções básicas, as quais garantem o funcionamento do controle de acesso.

Para que o controle de acesso aproveite todos os recursos que um ambiente assistido pode oferecer, se baseando na expansão do RBAC feita por [Covington et al. 2001],

será adicionado ao modelo o conceito de ambiente e papel do ambiente, o que permitirá uma maior flexibilidade no sistema, pois a regra de acesso não dependerá apenas do papel do usuário, mas também do papel do ambiente. A Figura 4 apresenta a expansão do RBAC que será utilizado neste trabalho.

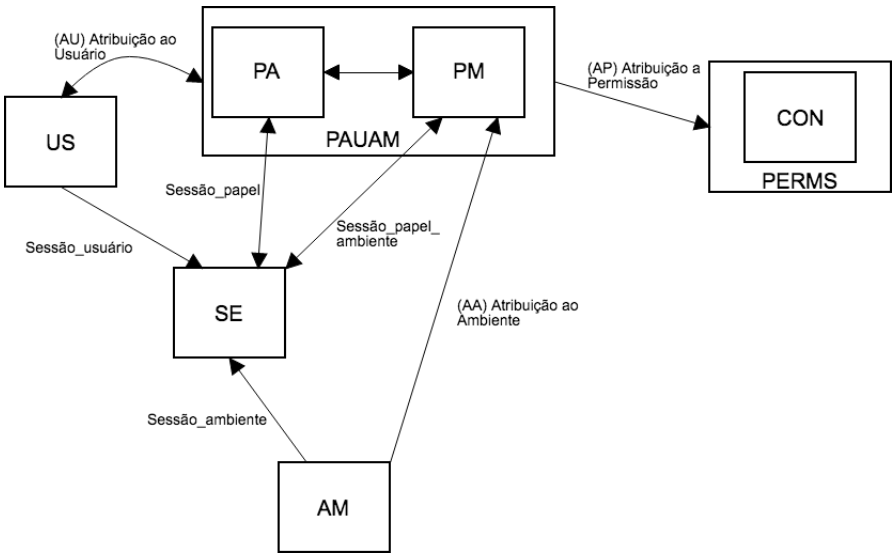

Figura 4. Extensão do RBAC

Especificações para a expansão do RBAC:

- Usuário (US), Papel de Usuário (PA), Ambiente (AM) , Papel de Ambiente (PM), Sessão (SE), Permissão (PERMS), Contexto (CON).
- $PAUAM = 2^{(\text{PA X PM})}$, conjunto de papéis de usuário associados a papéis de ambiente.
- $AU \subseteq$ US X PAUAM, relação de atribuição muitos para muitos entre usuário e papéis de usuário relacionados com papéis de ambiente.
- $AA =$ relação de um para muitos entre ambientes e papéis de ambiente.
- $AP \subseteq$ PERMS X PAUAM, relação de atribuição um para muitos entre papéis de usuário associados a papéis de ambiente e permissões.
- $Sessão\_usuário(s : S) \rightarrow US$, mapeamento da sessão s em um usuário correspondente.
- $Sessão\_ambiente(s : SE) \rightarrow AM$, mapeamento da sessão s em um ambiente correspondente.
- $Sessão\_papel(s : S) \rightarrow 2^{PA}$, mapeamento da sessão s em um conjunto de papéis.
- $Sessão\_papel\_ambiente(s : SE) \rightarrow 2^{PM}$, mapeamento da sessão s em um conjunto de papéis de ambiente.

Outra adaptação importante a ser feita no RBAC, é que a sessão representará que o usuário está registrado em um ambiente, ou seja, representará que o usuário está no ambiente. Caso o usuário não tenha uma sessão ativa para um certo ambiente, significa que o usuário não está no ambiente.

5. Ambiente e Resultados Experimentais

Nesta seção serão apresentados os resultados obtidos através dos experimentos realizados nos ambientes representados pela Figura 5, onde os números na figura, 1 e 2, são os

identificadores únicos de cada ambiente utilizado pelo sistema. A figura também mostra o posicionamento dos módulos do sistema e a localização dos sensores utilizados.

Para mostrar a validade do sistema de controle de acesso baseado em papéis, testes foram realizados durante o período de duas semanas, onde quatro usuários, dois com idades entre 20 e 30 anos, e os outros dois com idades entre 40 e 50 anos, utilizaram o sistema. Importante destacar que o escopo do trabalho foi reduzido, pois este projeto não recebeu nenhum apoio financeiro, portanto foram utilizados uma quantidade minima de ambientes, usuários e sensores.

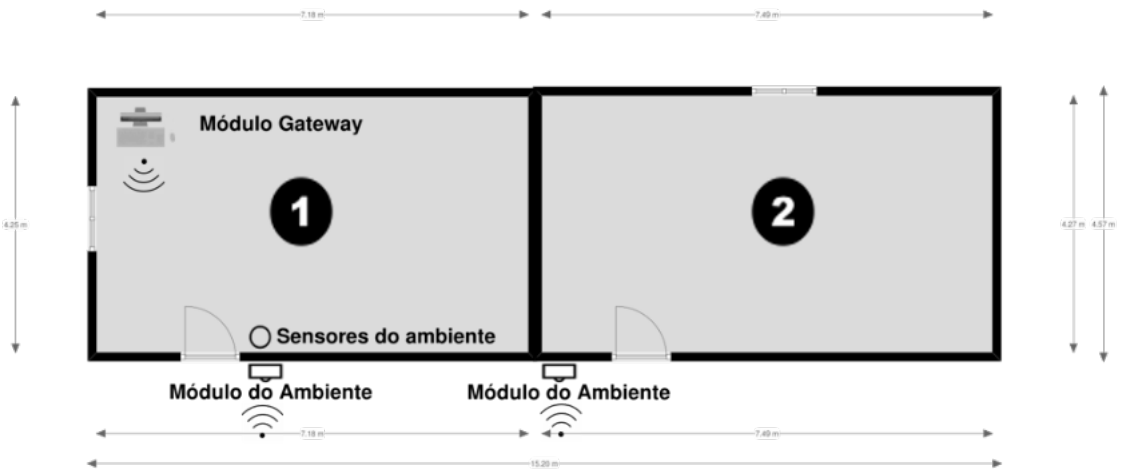

Figura 5. Planta baixa do ambiente de teste

5.1. Resultados

Ao longo de duas semanas de teste, resultados expressivos foram obtidos a fim de mostrar a validade do sistema. Nas 284 tentativas de acesso, o sistema se comportou de acordo com o esperado, lendo a tag do usuário, capturando o contexto do ambiente, processando as regras de acesso e verificando se o usuário poderia ou não acessar o ambiente.

A Figura 6 expõe o gráfico de utilização do sistema através da quantidade de eventos capturados. Esses eventos consistem em tentativas de acesso nos ambientes por parte dos usuários. Durante o período de teste foram registrados 284 eventos, sendo 240 acessos que foram garantidos pelas regras de acesso, e 44 que foram negados.

Já a Figura 7 apresenta os eventos registrados no sistema agrupados por horário. Essa informação é interessante, pois se consegue ter uma noção da utilização do sistema por horário, e assim se obter conclusões. Por exemplo, pode-se observar que por volta das 19 horas o sistema passou por um pico de eventos, o que significa que houveram muitas tentativas de acesso.

Procurando deixar mais explícito o funcionamento e a dinamicidade do sistema de controle de acesso, mudanças no papel de ambiente do ambiente 1 foram realizadas. Em um primeiro momento o ambiente desempenhou o papel de ambiente 1 (Quarto Filho), e após o papel de ambiente 3 (Sala de Estar).

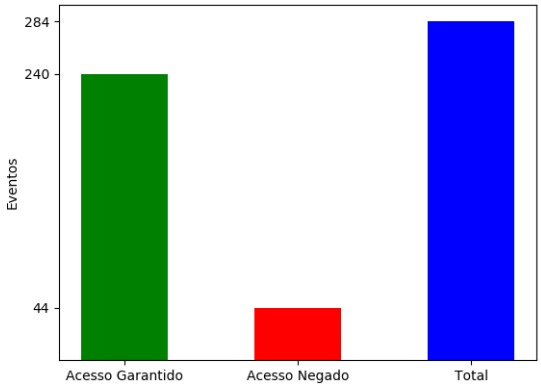

Figura 6. Eventos no sistema

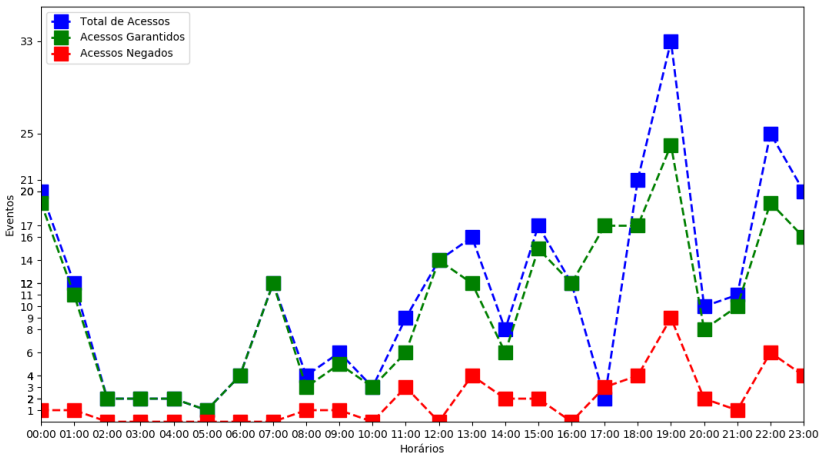

Figura 7. Eventos no sistema por horário

Na Figura 9 se pode observar os acessos no ambiente 1 agrupados por papéis de ambiente e horário, o que comprova que a mudança de papel de ambiente também alterou a forma que o ambiente é utilizado, por exemplo, entre as 2 e 5 da manhã, desempenhando o papel de ambiente 1, houveram por volta de 6 acessos, enquanto que desempenhando o papel de ambiente 3 foram 0 acessos. Esse resultado mostra que o controle de acesso funcionou de maneira correta mesmo com alterações nas configurações. De uma forma mais detalhada a Figura 8 apresenta os mesmo acessos comentados anteriormente só que divididos em acessos totais, negados e garantidos no ambiente 1 desempenhando cada papel.

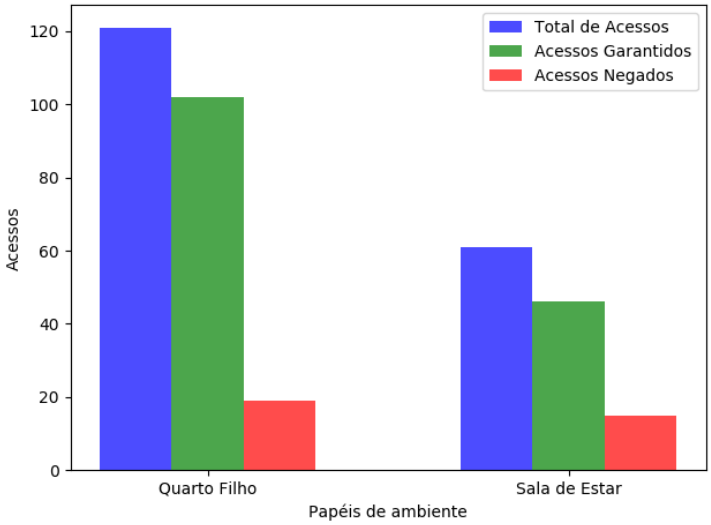

Figura 8. Acessos no ambiente 1 por papel de ambiente

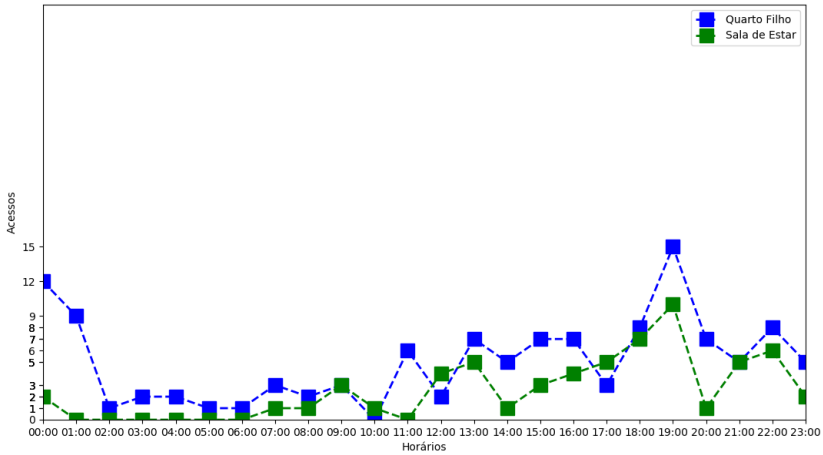

Figura 9. Acessos no ambiente 1 por horário e por papel de ambiente

6. Conclusão e Trabalhos Futuros

Com este trabalho foi possível analisar diversos aspectos relacionados à área de controle de acesso. Sendo assim identificou-se que a abordagem baseada em papéis utilizando informações de contexto, é pouco empregada e explorada em ambientes assistidos. Por este motivo decidiu-se utilizar essa abordagem neste trabalho, implementando um sistema capaz de controlar o acesso, se baseando em papéis de usuário e ambiente em conjunto com informações de contexto.

De acordo com os resultados apresentados na seção 5, este trabalho atingiu o seu objetivo, pois o sistema realizou o controle de acesso, utilizando os papéis e informações que o ambiente pôde prover, funcionando de maneira dinâmica e adaptativa, se adequando as mudanças de configurações e estados dos ambientes controlados. Importante destacar também que de acordo com as configurações das regras de acesso, o controle de acesso proposto neste trabalho pode funcionar tanto com o objetivo de proteger os ambientes de acessos indevidos, quanto proteger os usuários de acessarem ambientes que sejam nocivos a sua saúde.

Para trabalhos futuros é sugerido adicionar ao sistema os demais módulos do padrão de controle de acesso baseado em papéis, conforme apresentado na seção 2. Também é sugerido a implementação de um sistema de gerenciamento, onde se poderá adicionar, editar e excluir papéis, regras de acesso, usuários e ambientes.

Referências

Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M., and Abowd, G. D. (2001). Securing context-aware applications using environment roles. *Proceedings of the sixth ACM symposium on Access control models and technologies*, (January):pp. 10–20.

Da Silva, M. P., Nazário, D. C., Dantas, M. A. R., Gonçalves, A. L., Pinto, A. R., Manerichi, G., and Vanelli, B. (2016). Implementação da IOT para o Monitoramento das Variáveis Meteorológicas num AAL.

Ferraiolo, D. F. and Kuhn, R. D. (2004). Role based access control.

Gershenfeld, N., Krikorian, R., and Cohen, D. (2004). *The Internet of Things*, volume 291.

Jih, W.-r., Cheng, S.-y., Hsu, J. Y.-j., and Tsai, T.-m. (2005). Context-aware Access Control in Pervasive Healthcare. *Context*, (February 2014):2–9.

Junior, V. A. and Santin, A. O. (2015). Modelo de ativação multi-domínios de papéis RBAC usando controle de acesso baseado em atributos. *XV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

Kayes, A. S. M., Han, J., Rahayu, W., Islam, M. S., and Colman, A. (2017). A Policy Model and Framework for Context-Aware Access Control to Information Resources.

Lacerda, F. and Lima-Marques, M. (2015). Da necessidade de princípios de Arquitetura da Informação para a Internet das Coisas.

ONU (2017). World population ageing.

Park, S., Han, Y., and Chung, T. (2006). Context-role based access control for context-aware application. *High Performance Computing and Communications*, pages 572–580.

Priya, P., Charles, I. I. P. J., Britto, I. I. I. S., and Kumar, R. (2014). Context-Aware Architecture for User Access Control. 2(3):201–204.

Saint-Exupery, A. (2009). Internet of Things Strategic Research Roadmap.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1995). Role-Based Access Control Models. *IEEE Computer*, 29(2):38–47.

Sandhu, R. S. and Samarati, P. (1994). Access control - principles and pratice.

Tanikawa, T. C. V. (2016). Reconhecimento e Localização de Indivíduos com Utilização de Sensores no Suporte aos Ambientes Assistidos.

TORĞUL, B., Şağbanşua, L., and Balo, F. B. (2016). Internet of Things: A Survey. *International Journal of Applied Mathematics, Electronics and Computers*, (December 2016):104–104.

Trnka, M. and Cerny, T. (2015). Context-aware Role-based Access Control Using Security Levels. *Proceedings of the 2015 Conference on Research in Adaptive and Convergent Systems*, pages 280–284.

Zhang, G., Zhang, G., Parashar, M., and Parashar, M. (2004). Context-aware dynamic access control for pervasive applications. *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference*, pages 21–30.

Zhou, Z., Wu, L., and Hong, Z. (2013). Context-Aware Access Control Model for Cloud Computing. *International Journal of Grid and Distributed Computing*, 6(6):1–12.