Revista de Sistemas de Informação da FSMA
n. 15 (2015) pp. 2-10

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA ESTUDANTIL

CONTROLE DE ACESSO BASEADO NA INFERÊNCIA EM TRILHAS

Paulo César Albarello, Bruno Guilherme Martini, Jorge Luis Victória Barbosa
Universidade do Vale do Rio dos Sinos (Unisinos)
pcalbarello@uol.com.br, brunogui92@gmail.com, jbarbosa@unisinos.br

Abstract*— Professionals are constantly seeking qualification and consequently increasing their knowledge in their area of expertise. Thus, it is interesting to develop a computer system that knows its users and their work history. Using this information, even in the case of professional role change, the system could allow the renewed authorization for activities, based on previously authorized use. This article proposes a model for user access control that is embedded in a context-aware environment. The model applies the concept of trails to manage access control, recording activities usage in contexts and applying this history as a criterion to grant new accesses. Despite the fact that previous related research works consider contexts, none of them uses the concept of trails. Hence, the main contribution of this work is the use of a new access control criterion, namely, the history of previous accesses (trails). A prototype was implemented and applied in an evaluation based on scenarios. The results demonstrate the feasibility of the proposal, allowing for access control systems to use an alternative way to support access rights.

***Index Terms*— Context awareness. Access Control. Trails.**

***Resumo*— Os profissionais estão constantemente em busca de qualificação e consequentemente tendo um acréscimo de conhecimento na sua área de atuação. Sendo assim, torna-se interessante o desenvolvimento de um sistema computacional que conheça o seu usuário e seu histórico de trabalho e permita que atividades previamente autorizadas para o uso, possam ser permitidas novamente em caso de mudança de função do profissional. Este artigo propõe um modelo para o controle de acesso de usuários que estejam em um ambiente sensível ao contexto. O modelo aplica o conceito de trilhas para o gerenciamento do controle de acessos, registrando o uso de atividades em contextos e aplicando esse histórico como um critério para a concessão de novos acessos. Apesar das pesquisas relacionadas com o modelo proposto considerarem contextos, nenhuma delas usa o conceito de trilhas. Sendo assim, a principal contribuição do modelo consiste no uso de um novo critério para a realização de controle de acesso, ou seja, o histórico de acessos anteriores (trilhas). Um protótipo foi implementado e aplicado em situações baseadas em cenários. Os resultados demonstram a viabilidade da proposta, permitindo que sistemas de controle de acesso possam utilizar uma forma alternativa de concessão de direitos de acesso.**

***Palavras-chave*— Sensibilidade ao contexto, Controle de acesso, Trilhas.**

I. INTRODUÇÃO

Atualmente, devido ao avanço tecnológico nas áreas de telecomunicações e computação, torna-se comum que profissionais realizem suas atividades de forma remota. Por exemplo, um médico poderia consultar o estado de um paciente e receitar remédios através de seu *smartphone* de forma remota, com a mesma disponibilidade de informação como se estivesse presente no quarto do hospital.

Em relação às tecnologias de comunicação móvel, existe uma tendência ao aumento da interconectividade entre os equipamentos e também do crescimento da taxa de transmissão de dados disponibilizada pela internet. Nesse sentido pesquisas indicam que tais mudanças nos sistemas computacionais estimulam a criação de Ambientes Inteligentes [1].

Essa evolução está tornando realidade a visão que Mark Weiser introduziu em 1991 e denominou de Computação Ubíqua [2]. Weiser abordou a possibilidade de tornar a interação pessoa-computador invisível, ou seja, considerou uma realidade onde ocorreria uma natural integração entre os sistemas computacionais e as ações e comportamentos das pessoas.

Nesse sentido, Satyanarayanan [3] classifica a computação móvel como uma evolução da computação distribuída e a computação ubíqua como uma evolução da computação móvel. Cada uma destas tecnologias teve desafios, entre os quais destacam-se os estudos sobre a comunicação remota, a tolerância a falhas, a alta disponibilidade, o acesso a informações remotas, a segurança distribuída, as redes móveis, o acesso a informações móveis, as aplicações adaptativas, os sistemas sensíveis à energia, a sensibilidade à localização e a sensibilidade ao contexto [4]. Essa realidade tecnológica vem gerando novas oportunidades para diversas áreas, tais como Educação [5], Comércio [6] e Saúde [7].

Com a disseminação da Computação Ubíqua, cada vez mais o uso dos recursos poderá ocorrer a qualquer momento e em qualquer lugar, pois o usuário estará utilizando equipamentos computacionais móveis para a execução das atividades. Nesse cenário torna-se ainda mais relevante que os sistemas computacionais possuam meios mais eficientes e eficazes para gerenciar o controle de acesso dos usuários aos recursos, permitindo assim a administração das atividades que poderão ser executadas em um contexto específico [8]. Nesse sentido, a sensibilidade ao contexto [4] vem sendo considerada uma tecnologia estratégica para gerenciamento desse controle.

Esse artigo adota a definição de contexto proposta por Dey, Abowd e Salber [4]: "Contexto é qualquer informação que possa ser usada para caracterizar a situação de entidades que são consideradas relevantes para a interação entre um usuário e uma aplicação, incluindo o próprio usuário e a aplicação. Contextos são tipicamente: a localização, a identidade e o estado de pessoas, grupos e objetos físicos e computacionais".

Estudos mostraram que o acompanhamento de entidades em sistemas de computação móvel com suporte à localização, pode ser usado para o registro do histórico dos contextos visitados durante um período de tempo. Esse registro recebe a denominação de Trilha [1,9]. As trilhas registram atividades de uma entidade nos contextos percorridos, mantendo assim, um histórico de seus deslocamentos e de sua atuação em cada contexto. Um usuário costuma acessar aplicações e serviços que já tenham sido acessados anteriormente, pois seu histórico revela suas necessidades profissionais típicas. Sendo assim, torna-se interessante que os sistemas registrem o uso das atividades em contextos e utilizem este histórico de acessos como um critério para a concessão de novos acessos. Nesse sentido, as técnicas relacionadas ao Gerenciamento de Trilhas [9] podem ser aplicadas.

Este artigo propõe o *EasyConn4All*, um modelo de controle de acesso contextualizado que explora também as trilhas de permissões anteriores concedidas a uma entidade. Quando uma entidade efetua um acesso, as permissões relativas às atividades disponíveis para a entidade são registradas, permitindo que em acessos futuros o sistema de controle de acesso use este histórico para realizar novas concessões.

Os modelos tradicionais realizam o controle de acesso usando diversos critérios, entre eles destaca-se o uso de Papéis [10]. As entidades que possuem o mesmo papel têm permissões semelhantes e o controle de suas atividades é focado na administração do papel. Além disso, conforme discutido na seção II, apesar das pesquisas relacionadas com o modelo proposto [11,12,13,14,15,16] considerarem contextos, nenhuma delas usa o conceito de trilhas para gerenciar o controle de acessos. O *EasyConn4All* usa papéis e contextos, destacando-se como sua principal contribuição a aplicação de um novo critério para a realização de controle de acessos, ou seja, o histórico de acessos anteriores (trilhas).

O artigo está organizado da seguinte forma. A seção II apresenta uma discussão de trabalhos relacionados. A seção III propõe a arquitetura de componentes do *EasyConn4All*. A seção IV discute aspectos de implementação e a seção V aspectos de avaliação. A avalição foi baseada em dois cenários envolvendo testes com o protótipo. Por fim, na seção VI são apresentadas as considerações finais e trabalhos futuros.

II. TRABALHOS RELACIONADOS

Nesse texto foram considerados relacionados os trabalhos de pesquisa que abordam no mínimo a integração de três temas considerados estratégicos nesse estudo, ou seja, o controle de acesso [10], a sensibilidade ao contexto [4] e a mobilidade [3]. Além disso, no processo de busca de trabalhos, priorizou um quarto tema considerado como a contribuição do *EasyConn4All*, ou seja, o uso de histórico de contextos (trilhas [9]). A Tabela I realiza uma comparação usando critérios que foram definidos de acordo com esses quatro temas considerados estratégicos. Os critérios foram escolhidos buscando a discussão da contribuição pretendida para o modelo proposto, ou seja, a aplicação de trilhas no controle de acesso.

O projeto Infraware [11,12] realiza a interpretação semântica do contexto e faz a integração dos dados contextuais para caracterizá-lo. O trabalho utiliza ontologias para especificar modelos e serviços. Além disso, todo pedido feito ao Infraware é recebido por uma camada dedicada ao controle de acesso e privacidade.

O uso que o sistema faz de trilhas diz respeito à manutenção de um histórico de contextos visitados pelo usuário, ou seja, o sistema registra um histórico dos contextos acessados, não armazenando as atividades realizadas em cada contexto e as permissões disponibilizadas para cada atividade. Assim, as trilhas não podem ser usadas para futuros controles de acesso de atividades.

O UbiCOSM [13] usa a sensibilidade ao contexto para a especificação de políticas de trabalho, sendo o controle de acesso ligado ao contexto e não ao usuário. O sistema faz com que permissões sejam associadas a múltiplos contextos e também utiliza a negociação de confiança entre usuários para acesso aos dados. Um usuário portando um dispositivo móvel adquire um conjunto de permissões ao entrar em um contexto específico. Além disso, UbiCOSM utiliza um formato padrão baseado em RDF para expressar as permissões de controle de acesso.

O projeto AWARENESS [14] tem como objetivo a criação de uma infraestrutura de suporte a serviços e aplicações sensíveis ao contexto com controle de acesso. O projeto busca o controle de acesso em ambientes médicos.

O AWARENESS integra serviços que sejam amparados pela computação ubíqua, considerando informações contextuais e a colaboração de aplicações proativas. Destaca-se como sua principal característica o suporte à mobilidade em ambientes sensíveis ao contexto.

O SOCAM [15] fornece uma infraestrutura para a modelagem e criação de serviços sensíveis ao contexto. Os contextos gerenciados pelo modelo podem ser compartilhados e acessados através dos serviços disponibilizados.

O projeto uMED [16] tem o objetivo de possibilitar aos profissionais de saúde que interajam a distância com equipamentos médicos. Este projeto considera que os médicos levam uma vida profissional que envolve bastante mobilidade e possuem uma fragmentação de rotinas de trabalho. Com isto o uMED promove uma otimização no tempo necessário para transição entre atividades. O modelo possui ainda alertas baseados em regras criadas pelos profissionais de saúde. O uMED foi integrado com o *middleware* EXEHDA [17].

Os seguintes critérios foram levados em consideração para a comparação apresentada na Tabela I: (1) Sensível ao Contexto: indica se o trabalho suporta sensibilidade ao contexto; (2) Baseado em Trilhas: indica se o trabalho utiliza informações de trilhas para controlar o acesso; (3) Mobilidade: informa se é possível utilizar serviços em dispositivos móveis; (4) Contextos Dinâmicos: indica se o trabalho suporta mudanças nos contextos ou apenas trata contextos que não

podem ser alterados durante a execução das aplicações (estáticos); (5) Domínio: informa se o trabalho está voltado a um domínio de aplicação específico. Os critérios escolhidos visam possibilitar a análise dos aspectos dos trabalhos relacionados que foram considerados relevantes para comparação com o *EasyConn4All*, principalmente focando na mobilidade e no controle de acesso sensível ao contexto. Existem ainda trabalhos que abordam aplicações sensíveis ao contexto [18,19,20,21], os quais no entanto não focam no controle de acesso conforme proposto pelo *EasyConn4All*.

Os trabalhos relacionados abordados focam em sensibilidade ao contexto, suportando contextos dinâmicos e mobilidade. Além disso, alguns dos trabalhos relacionados normalmente possuem um escopo especificamente voltado para a área médica.

Considerando-se o foco da contribuição do *EasyConn4All*, constata-se que o único trabalho que considera um histórico de acessos é o Infraware, no entanto restringindo-se ao registro dos contextos visitados, sendo assim indicado como "Parcial" no critério (2) na Tabela I.

O *EasyConn4All* usa as trilhas para gerenciamento de acessos das entidades em nível de atividades realizadas nos contextos. Além disso, propõe-se que o *EasyConn4All* possa ser usado em diferentes domínios de aplicação, juntando-se aos trabalhos que possuem essa caraterística.

TABELA I
COMPARAÇÃO ENTRE OS TRABALHOS RELACIONADOS.

Trabalho	(1)	(2)	(3)	(4)	(5)
Infraware	Sim	Parcial	Sim	Sim	Médico
UbiCOSM	Sim	Não	Sim	Sim	Genérico
AWARENESS	Sim	Não	Sim	Sim	Médico
SOCAM	Sim	Não	Sim	Sim	Genérico
uMED	Sim	Não	Sim	Sim	Médico

III. MODELO EASYCONN4ALL

A Figura 1 mostra a organização do *EasyConn4All.* No servidor (*EasyConn4AllServer*) encontram-se cinco componentes (módulos de software) que administram o armazenamento de informações e o controle de acesso. Por sua vez, um cliente (*EasyConn4AllClient*) é o responsável por solicitar as permissões de acesso ao *EasyConn4AllServer*, atuando no suporte a aplicações que queiram implementar um controle de acesso baseado em contextos e trilhas. Uma abordagem mais detalhada sobre a qualificação dos contextos é feita na subseção C.

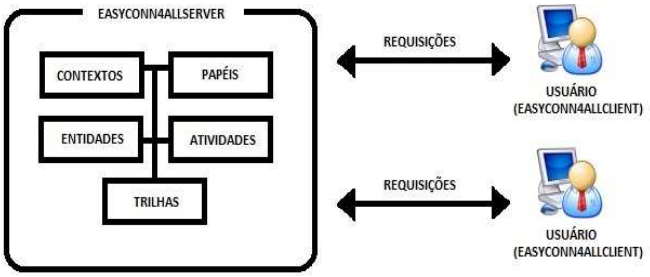

Fig. 1. Arquitetura do *EasyConn4All.*

Visando um melhor entendimento dos conceitos abordados no modelo, será descrito durante a apresentação um cenário para demonstração das funcionalidades. Neste cenário foi utilizado um ambiente escolar. Neste ambiente existe um aluno cursando uma determinada disciplina e utilizando tarefas escolares, como a postagem de materiais e a consulta de dados e materiais escolares.

Considere-se que o aluno está presente em uma aula da disciplina. Através do *EasyConn4AllClient*, ele identifica-se e solicita acesso ao contexto relacionado a aula. O cliente envia estas informações ao *EasyConn4AllServer*.

O servidor recebe a identificação do aluno (entidade) e verifica as informações de contexto relacionadas à aula (por exemplo, data e hora de ocorrência, localização da sala e presença do professor).

Após o processamento do controle de acesso por parte do servidor, é enviada ao *EasyConn4AllClient* uma descrição (lista) das atividades com acesso permitido ou ainda um código de erro informando o motivo da permissão ser negada. Esta mensagem é repassada à entidade pela aplicação que está executando no cliente.

O *EasyConn4AllServer* é o responsável por validar, consistir e remeter a permissão de acesso a atividades registradas. Nele ficam residentes os componentes de controle que são responsáveis pela validação das informações repassadas pelo *EasyConn4AllClient*.

As próximas subseções descrevem os componentes do *EasyConn4AllServer*.

A. Entidades

No *EasyConn4All* uma entidade é qualquer usuário ou aplicativo que venha a interagir com o ambiente, seja por utilizar as atividades disponíveis nos contextos ou por fornecer atividades a outras entidades.

Toda entidade tem seu acesso controlado e toda atividade utilizada por ela ou autorizada a ela por outro meio (como por papéis) possuirá um registro no histórico de usos anteriores para serem verificados novamente quando as trilhas forem avaliadas. Por exemplo, no cenário o aluno e o professor seriam entidades para o sistema.

B. Papéis

O uso de papéis [10] simplifica a tarefa de gerenciar e administrar quais atividades determinados grupos de entidades podem acessar. Se porventura alguma alteração nas permissões for diagnosticada e necessite ser aplicada a um grupo de entidades, uma alteração ou criação de um papel irá satisfazer

esta necessidade, visto que o papel é responsável por agregar atividades distintas ou grupos de atividades vinculadas a um contexto.

No cenário existem os papéis de professores (que terão tarefas relacionadas como registro de notas e frequências) e alunos (que poderão postar materiais e consultar atividades a serem realizadas).

O uso de papéis segue o modelo RBAC [10]. Os papéis são representados por atributos de uma entidade em um banco de dados. Cada entidade possui um papel em um contexto, podendo uma entidade ter diferentes papéis em diferentes contextos.

Caso algum papel tenha que ser desativado, por exemplo, por tornar-se obsoleto, a desativação pode ser feita sem impacto na análise das trilhas de acesso. Se uma entidade teve uma autorização anterior a uma atividade em um contexto, continuará tendo mesmo que o papel que permitiu o acesso inicial tenha sido desativado.

A desativação de um papel faz apenas com que novas entidades, ou ainda entidades já existentes, não venham a utilizar mais este papel. Este recurso permite que as entidades possam ter seu papel alterado no contexto, e assim ter novas atividades associadas.

C. Contextos

No *EasyConn4All* os contextos são tratados como "ambientes" onde encontram-se entidades e atividades. Os contextos são qualificados (equivalente a ativados) seguindo regras condicionais fixas definidas previamente, as quais usam as informações contextuais. Por exemplo, no cenário seria possível estabelecer um contexto como local (sala de aula), horário (data e hora da ocorrência da aula), presença de entidades (alunos e professor) e de atividades relacionadas.

O modelo utiliza a sensibilidade ao contexto como forma de controlar o acesso, considerando cinco tipos de informações compatíveis com a definição de Dey, Abowd e Salber [4]:

- data e hora de ocorrência do contexto;
- localização;
- número mínimo de entidades presentes (especialização do modelo);
- presença obrigatória de entidades (especialização do modelo);
- atividades pertencentes ao contexto (genéricas e podem ser usadas para diversas situações).

O *EasyConn4All* utiliza essas informações para a qualificação do contexto. Sabendo a data e a hora de ocorrência do mesmo, o local onde ele ocorre, os recursos (atividades) que estão disponíveis e quais entidades estão presentes, torna-se possível controlar o acesso das entidades ao contexto, ou seja, o acesso as atividades é condicionado as regras estabelecidas.

A Figura 2 apresenta um diagrama de classes que representa a organização das informações relativas aos contextos. A classe *Contexto* contém as informações de caracterização do contexto. O diagrama mostra que um contexto pode estar relacionado com diversas entidades e atividades, as quais foram representadas por duas classes adicionais.

A data e a hora estabelecem o período de duração do contexto. A localização define o espaço físico de ocorrência do contexto. O *EasyConn4All* utiliza uma representação simbólica para o espaço, ou seja, vincula com um espaço geográfico um nome simbólico, abstraindo como ocorre a localização das entidades.

Além do espaço e do tempo torna-se relevante identificar as entidades que podem qualificar um contexto. Por exemplo, no cenário a presença de um professor em uma sala pode qualificar o início de uma aula. Também se pode usar uma quantidade de entidades para qualificar um contexto, por exemplo, um número mínimo de alunos para início da aula. Atividades também podem ser usadas como instrumento de qualificação de contextos, por exemplo, a aula somente inicia com a disponibilização de um recurso didático na sala.

Uma vez qualificado o contexto, o acesso é permitido às entidades segundo as regras pré-estabelecidas. Além disso, o contexto pode ser desqualificado devido à perda de alguma de suas características. Por exemplo, a saída do professor da sala ou o término do período da aula.

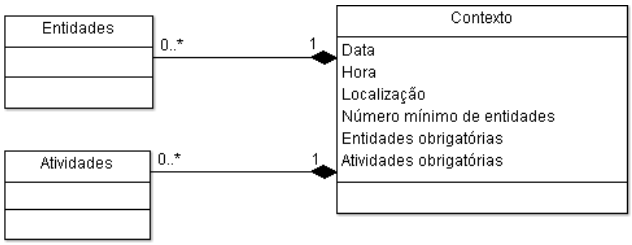

Fig. 2. Contexto e sua relação com Entidades e Atividades.

D. Atividades

Uma atividade é definida como uma ação ou um serviço, disponível em um contexto. No modelo proposto, atividades são os recursos disponíveis em um determinado contexto que têm o objetivo de servir como "utilitários" para alguma entidade que estiver atuando no contexto.

Cada contexto registrado possuirá *n* atividades ligadas a ele e permissíveis de uso por entidades portadoras de um papel específico. Toda atividade poderá ter seu uso dirigido a entidades específicas ou a um grupo de entidades através da atribuição a papéis distintos.

Como exemplo de atividades no cenário seria possível destacar tarefas como registrar frequência de aluno (papel de professor) e consultar material didático (papel aluno).

E. Trilhas

O componente de trilhas do *EasyConn4All* monitora e registra todos os acessos a atividades realizados por uma entidade nos contextos visitados. Assim, torna-se possível uma futura averiguação de atividades executadas previamente. Essa abordagem tem o objetivo de permitir que atividades já utilizadas possam servir de parâmetro para novas concessões.

As entidades possuem associadas a si permissões de uso de atividades que estão vinculadas ao papel que ela possui em um contexto. No momento em que a entidade acessa o *EasyConn4All* é feita uma leitura das atividades permitidas a

ela e estas atividades são catalogadas na trilha de acessos feitos pela entidade.

As trilhas são registradas em um formato sequencial, contendo informações que caracterizem qual atividade foi utilizada previamente, em que situações e por qual entidade ela foi utilizada. No momento em que os componentes verificarem a trilha de uma entidade e comprovarem o acesso anterior, e ainda assim não encontrarem requisitos que bloqueiem ou impeçam a liberação da atividade, ela será novamente liberada para a entidade.

O uso da trilha torna-se um diferencial neste trabalho, visto que um dos critérios para conceder acessos baseia-se em atividades já utilizadas por uma entidade. Um exemplo disto é a possibilidade de mudança do papel da entidade no contexto. O novo papel pode não autorizar um recurso, mas o histórico (trilha) pode mostrar que mesmo com um novo papel, essa entidade pode acessar o recurso, pois já teve acesso antes. Isso é mostrado nos cenários descritos na seção V. O papel também pode ter sido desativado, mas se a entidade acessou no passado, tem autorização para acessar novamente, mesmo se o papel não existe mais no contexto.

O modelo propõe ainda o uso de recursos de configuração de inativação de atividades, tornando possível desativar alguma atividade específica para o uso da entidade, fazendo com que os componentes responsáveis não a liberem para o acesso.

Este controle pode ser entendido, por exemplo, como se um recurso estivesse sendo utilizado por uma entidade e fosse retirado de um contexto. Mesmo que a trilha de acessos registre um uso prévio dele, o sistema não concederá o acesso.

Para exemplificar esta situação, no cenário o aluno poderia ter acesso ao material de sua disciplina (por exemplo, apostilas, vídeos e atividades) durante o período de duração da disciplina. Se por ventura o aluno necessitasse consultar este material futuramente, o sistema permitiria o acesso, pois ele já utilizou o contexto anteriormente e não possui impedimentos ao novo acesso.

O recurso de inativação de atividades registradas se faz necessário no momento em que atividades registradas venham a se tornar inacessíveis para as entidades. Por exemplo, a remoção do recurso do contexto pode tornar o acesso bloqueado para as entidades. Como este recurso bloqueado poderia ter sido utilizado anteriormente (e constaria na trilha de acessos de uma entidade) seu uso seria novamente autorizado, porém esta autorização é indevida. Para manter a integridade dos dados já utilizados, o recurso de inativação das atividades faz com que elas fiquem "escondidas" para acessos futuros. No momento da verificação das atividades disponíveis, o sistema não recupera atividades inativas, deixando o sistema consistente.

IV. PROTÓTIPO EASYCONN4ALL

O diagrama na Figura 3 mostra a estrutura de composição das classes do protótipo *EasyConn4All*. O *EasyConn4AllServer* opera seus módulos de cadastro e configuração através da interface disponibilizada pela classe ***frmPrincipal***, onde estão recursos responsáveis pela ativação e operação dos módulos de controle.

Cada uma das classes é responsável pelo gerenciamento das informações referentes ao assunto que a classe manipula. Serviços como a inclusão, a alteração, a vinculação ou até mesmo a inativação de recursos são atividades inerentes a cada uma das classes responsáveis.

A classe ***ifrmEntidade*** é responsável pelo gerenciamento do controle das entidades. Entidade pode ser uma pessoa ou um objeto (outro aplicativo) relevante para a interação entre um usuário e uma aplicação. Esta classe controla o cadastramento de todas as entidades que poderão utilizar alguma atividade ou ceder serviços para o sistema. Ela possui atributos que são característicos de uma entidade.

A classe ***ifrmPapeis*** controla a administração dos diferentes tipos de papéis gerenciados pelo *EasyConn4All*. Os papéis são os responsáveis por agrupar atividades afins dentro de um contexto. Também é possível neste recurso tornar um papel inativo para evitar futuros usos.

A ***ifrmContexto*** é a classe que administra o cadastramento das regras e das definições de um contexto. Para caracterizar um contexto, o sistema utiliza as informações discutidas na seção III.C. Qualquer das informações que venha a se tornar inválida transformará o contexto em inválido e o sistema irá torná-lo inacessível.

A classe ***ifrmServicos*** gerencia a inclusão de atividades que terão seu acesso controlado pelo servidor. É possível, na classe, tornar uma atividade inativa temporariamente ou definitivamente, através da modificação de atributos. Todas as tarefas referentes à administração dos serviços também estão disponíveis, como a inclusão de novos serviços e a atualização de serviços já cadastrados.

As classes ***ifrmPapelEntidade***, ***ifrmServicoPapel*** e ***ifrmEntidadesContextos*** fazem a ligação entre os objetos instanciados em cada uma das classes abordadas anteriormente. Estas classes criam o vínculo para a posterior comparação e análise por parte dos componentes, na autorização do uso destas atividades.

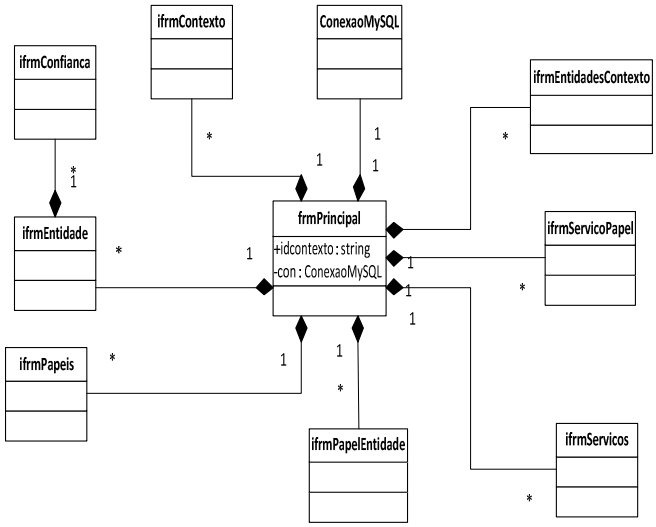

Fig. 3. Diagrama de classes do *EasyConn4All*.

A classe ***ifrmConfianca*** permite o gerenciamento das concessões de permissões entre entidades utilizando o atributo de confiança entre elas. Nesta classe estão disponíveis recursos que podem conceder temporariamente a permissão do uso de uma atividade que a entidade possua a concessão, para outra entidade que esteja necessitando também utilizá-la. O período de concessão poderá variar desde o acesso por um único dia até um período indeterminado.

O sistema *EasyConn4All* foi implementado através de dois protótipos, um deles funcionando em uma estação como servidor de controle de acesso de atividades (também chamado de *EasyConn4AllServer*) e o outro funcionando em clientes (denominado *EasyConn4AllClient*).

Os protótipos foram desenvolvidos com a linguagem Java e foi utilizado o banco de dados MySQL como repositório das informações no servidor. Uma versão para *Android* do *EasyConn4AllClient* foi desenvolvida, permitindo que o usuário se movimente entre contextos.

O *EasyConn4AllServer* tem como uma de suas responsabilidades o suporte ao cadastro de dados básicos. A Figura 4 mostra um conjunto de telas do *EasyConn4AllServer* onde estão exibidas as telas de cadastro de contextos, de entidades e de papéis. Os cadastros devem ser realizados antes que inicie o gerenciamento de controle de acessos pelo sistema.

O *EasyConn4AllServer* tem a incumbência de receber as requisições dos clientes e refiná-las (cruzando informações) para realizar o controle de acesso. As atividades de gerenciamento, como os cadastros dos recursos básicos e suas ligações são mantidas e controladas no servidor.

Os clientes são responsáveis por receber a solicitação do usuário, encapsular a requisição e enviá-la ao *EasyConn4AllServer* que então realiza a leitura da mensagem e providencia o controle de acesso com base nas informações cadastradas. O resultado é enviado ao *EasyConn4AllClient* emissor para a efetivação do controle de acesso.

A Figura 5 mostra o fluxo de informações entre o servidor e o cliente durante o controle de acesso às atividades. O processo de autenticação e validação das atividades que estão disponíveis a uma determinada entidade é baseado nos seguintes passos:

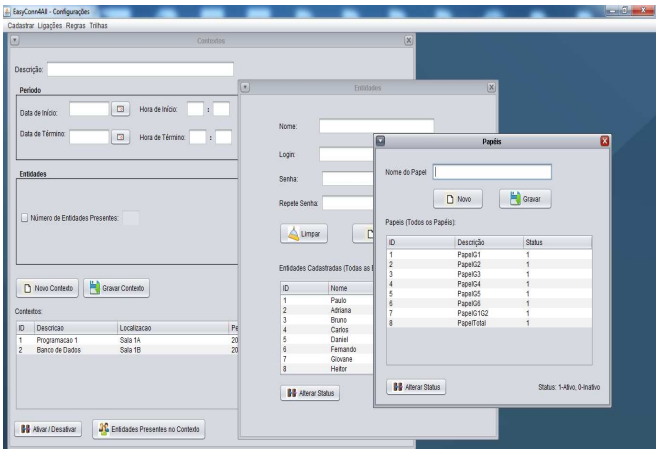

Fig. 4. *EasyConn4AllServer*.

1. a entidade solicita *login* em um determinado contexto já registrado, através de um dispositivo computacional (*notebook*, *smartphone* ou *tablet*) que possua o *EasyConn4AllClient*;
2. o dispositivo envia ao servidor *EasyConn4AllServer* uma descrição da entidade e em qual contexto ela está solicitando inserção;
3. ao receber a solicitação, o servidor inicia o processo de validação da entidade, verificando se ela está registrada no sistema;
4. validado o contexto, o próximo passo é verificar o papel da entidade que está solicitando acesso e buscar as permissões de atividades ligadas a este papel;
5. no passo seguinte, o sistema realiza uma varredura na trilha deixada pela entidade. Todas as atividades que a entidade já tenha acessado e que estejam ativas e válidas serão novamente concedidas à entidade;
6. após a liberação das atividades, o sistema registra o histórico de acessos permitidos que ficará armazenado na base de consulta do *EasyConn4AllServer* para futura liberação de atividades. Assim, forma-se a trilha de acesso da entidade;
7. feita a coleta de informações referentes a quais atividades são permissíveis à entidade, o sistema envia uma mensagem ao *EasyConn4AllClient*, que solicitou o controle de acesso, informando quais atividades serão disponibilizadas para a entidade.

A Figura 6 resume o procedimento de controle. A figura mostra o fluxo das informações durante o controle de acessos baseado em trilhas e papéis.

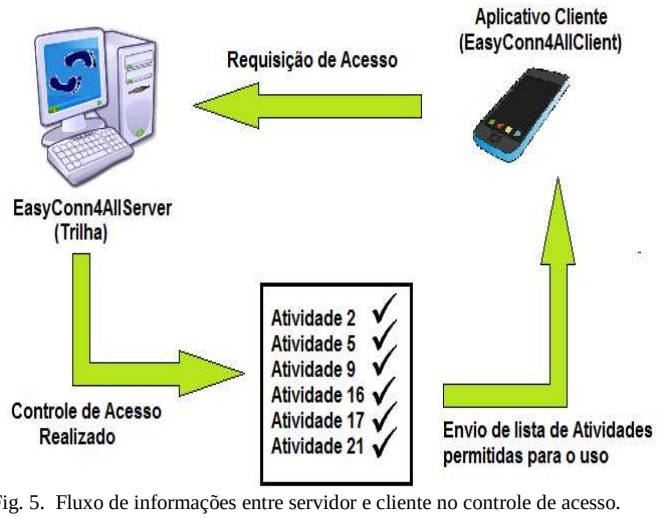

Fig. 5. Fluxo de informações entre servidor e cliente no controle de acesso.

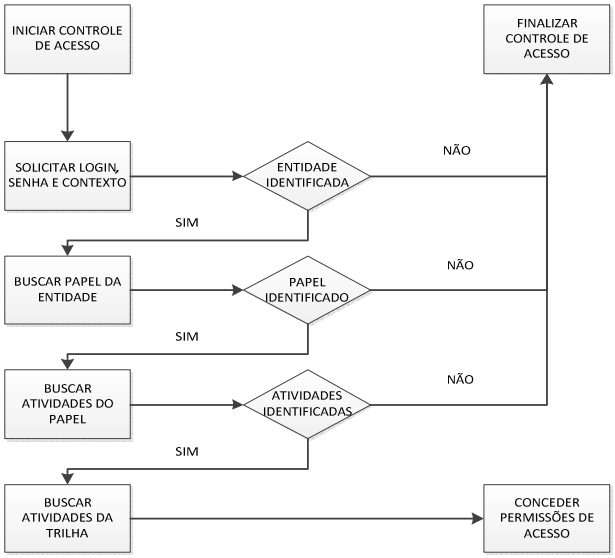

Fig. 6. Fluxograma do controle de acesso baseado em trilhas e papéis.

V. ESTUDO DE CASO

A comunidade científica vem usando cenários para validação de sistemas sensíveis ao contexto (conforme realizado em [4]) e sistemas ubíquos (conforme mostrado em [3], [5], [6] e [7]). Seguindo essa estratégia foram criados dois cenários para avaliação do modelo, que foram executados por um usuário utilizando um *tablet* para acesso a serviços que tiveram a permissão controlada. O cenário 1 mostra o acesso a serviços sendo disponibilizados a um funcionário de um escritório de contabilidade. O cenário 2 mostra um médico utilizando as atividades em um contexto hospitalar.

A. Cenário 1

Neste cenário foram utilizados recursos pertinentes a um escritório de contabilidade onde ocorressem atividades e onde houvesse trabalhadores com incumbências diferentes para cada grupo de atividades.

Para efetivar este cenário, foi criado no componente *Contextos*, um contexto específico para o escritório. Neste contexto, foi definido o tempo para início (data e hora) e o término (data e hora) do trabalho diário. Também foi estabelecida a localização da ocorrência do contexto (identificação da sala de trabalho) e também as entidades (funcionários) que teriam algum tipo de atividade disponível.

O seguinte cenário foi modelado e implementado usando o *EasyConn4All*:

*"Joana (**Entidade**) é uma funcionaria do escritório de contabilidade (**Contexto**). Ao ser contratada, considerando-se a experiência que Joana possuía, foram atribuídas a ela as seguintes tarefas (conforme um **Papel** estabelecido):*

- Planejar os sistemas de registros e operações contábeis atendendo as necessidades administrativas e as exigências legais;

- Realizar serviços de auditoria, emitir pareceres e informações sobre sua área de atuação, quando necessário.

*A Figura 7.a mostra a tela do sistema onde estão listadas as quatro **Atividades** que inicialmente podem ser acessadas por Joana no **Contexto**. As atividades estão relacionadas com as duas tarefas que foram atribuídas a ela.*

*Com o passar do tempo, a empresa percebeu a necessidade de aproveitar os conhecimentos de Joana em outros setores. Após a realização de alguns cursos de formação, Joana foi designada para realizar as seguintes tarefas (novo **Papel**):*

- Elaborar e assinar relatórios, balancetes, balanços e demonstrativos econômicos, patrimoniais e financeiros;

- Coordenar, orientar, desenvolver e executar, quando necessário, as atividades de elaboração do orçamento geral da instituição.

*Considerando sua nova qualificação, quatro **Atividades** tornam-se acessíveis para Joana no **Contexto**. A Figura 7.b mostra a tela do sistema com a listagem de atividades, onde as últimas quatro foram disponibilizadas devido à nova qualificação.*

*Como no cadastro do sistema existe um histórico de atividades já desempenhadas pela funcionária no contexto (histórico do contexto, ou seja, **Trilhas**), o mesmo resgata todas as atividades que já tenham sido disponibilizadas anteriormente e disponibiliza o acesso (veja as quatro primeiras atividades destacadas na Figura 7.b).*

*Mesmo que Joana tenha novas incumbências no escritório, o sistema ainda reconhece que ela possui conhecimento (via **Trilha**) para a realização de atividades já realizadas anteriormente.*

De agora em diante, sempre que Joana entrar no sistema administrativo do escritório de contabilidade, o mesmo buscará na trilha de atividades desempenhadas por Joana e resgatará todas as atividades que Joana tem condições de realizar."

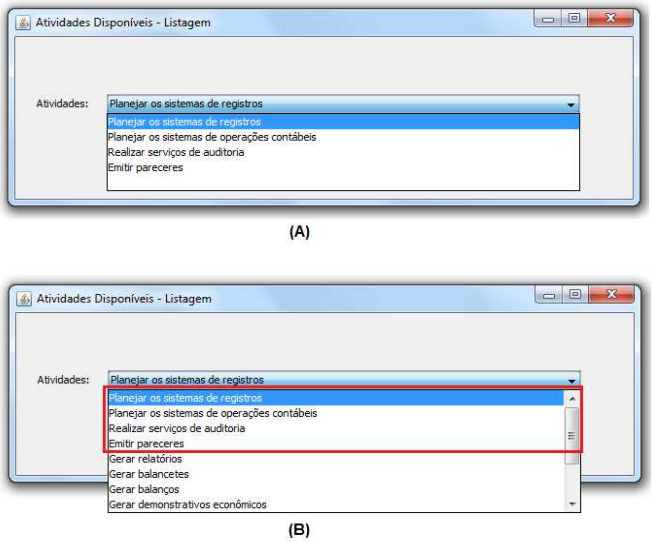

Fig. 7. Controle de acesso no cenário 1. A tela (A) mostra as atividades iniciais e a tela (B) mostra as novas atividades disponibilizadas via Trilha.

Executando esse cenário, os componentes foram capazes de buscar todas as permissões relativas aos papéis que a entidade assumiu e as permissões contidas na trilha de acessos.

As Figuras 7.a e 7.b mostram as telas com os resultados de acessos sendo disponibilizados pelo cliente. Na Figura 7.a estão exibidas as atividades iniciais atribuídas para a entidade nos primeiros acessos. Após a entidade obter (alterar) sua capacitação, o sistema busca as atividades que constam em sua trilha e as disponibiliza também (Figura 7.b).

B. Cenário 2

Neste cenário foi utilizada uma situação de trabalho em um hospital. O cenário envolveu uma entidade que possui o papel de médico cardiologista com uma especialidade inicial, o qual após a realização de cursos passa a ter mais atividades disponibilizadas. O sistema usa a trilha para disponibilizar tanto as permissões para o papel inicial como para o papel atual do médico. A descrição do cenário é a seguinte:

*"Marcos (**Entidade**) é um cardiologista, possuindo especialização (**Papel**) em cardiologia cirúrgica, arritmias cardíacas e coronariopatias. Ele atua no Setor de Cardiologia de um determinado hospital em um período específico (**Contexto**). Quando Marcos esta no setor e utiliza o sistema do hospital, consegue acessar as **Atividades** pertinentes a seu trabalho. A Figura 8.a mostra a tela do sistema disponibilizando quatro atividades que podem ser acessadas pelo médico (por exemplo, "Realizar eletrocardiogramas").*

*Com o passar do tempo, Marcos realizou novas especializações, como por exemplo, atividades relacionadas à valvopatias. Agora Marcos pode tratar também pacientes que tenham valvopatias, hipertensão arterial, insuficiência cardíaca e miocardiopatia. O sistema que controla o acesso dos médicos as atividades de tratamento dos pacientes permite o registro da nova qualificação (**Papel**) de Marcos (**Entidade**), disponibilizando assim novas **Atividades** especializadas. A Figura 8.b mostra o médico acessando o sistema e tendo disponíveis as quatro atividades (últimas na lista) que suportam sua nova qualificação.*

*A partir desse momento, sempre que Marcos se identificar para o tratamento de um determinado paciente, o sistema irá buscar também as atividades relacionadas à sua primeira especialidade (através da **Trilha**) juntamente com as atividades das novas especialidades. A Figura 8.b destaca as atividades anteriores sendo autorizadas através da trilha."*

Caso o médico possua em sua trilha de acessos um registro de alguma atividade que por algum motivo (por exemplo, um caso específico do paciente que passou para outro profissional) não possa ser disponibilizada novamente, o sistema possui recursos que podem tornar a atividade inacessível, mesmo que conste em sua trilha de acesso. Além disso, caso o registro de novas atividades tenha que ser inseridas no sistema para auxiliar de uma maneira mais eficiente o tratamento de um paciente, estas poderão ser incluídas (cadastradas) sem prejuízo às atividades previamente executadas pelo médico.

As Figuras 8.a e 8.b mostram as telas do cliente onde a entidade médico pode acessar as atividades indicadas no cenário. Inicialmente foram disponibilizadas quatros atividades (Figura 8.a), as quais continuam disponíveis mesmo quando o médico obteve novas qualificações. O acesso às atividades anteriores destacadas na Figura 8.b foi mantido através da consulta à trilha.

Assim como no cenário anterior, conclui-se que o sistema, baseado na trilha de acessos, resgatou todas as atividades que a entidade possuía acesso e as disponibilizou novamente.

Os cenários permitiram demonstrar como o sistema pode resgatar as atividades realizadas anteriormente por um usuário e anexá-las juntamente com as atividades atuais, sem qualquer necessidade de solicitação por parte dele. Partindo do princípio que "atividade já realizada é atividade conhecida", o sistema se encarrega de conceder o acesso destas atividades à entidade.

VI. CONCLUSÕES

Este artigo propôs um modelo para controle contextualizado de acessos baseado na inferência em trilhas. O estudo de trabalhos relacionados mostrou que o *EasyConn4All* possui como principal diferencial o uso da trilha de acessos feitos pela entidade em nível de atividade, como um dos critérios para a concessão de novos acessos.

Esta abordagem amplia as possibilidades de controle de acessos em ambientes contextualizados. O modelo mantém um registro sequencial das atividades permitidas em momentos anteriores e utiliza este histórico como um quesito parcial para novas concessões. Isto proporciona maior flexibilidade em relação às formas de controle de acesso existentes. A proposta consiste em uma alternativa ao modelo tradicional de controle de acesso, não sendo um substituto dos modelos já estabelecidos.

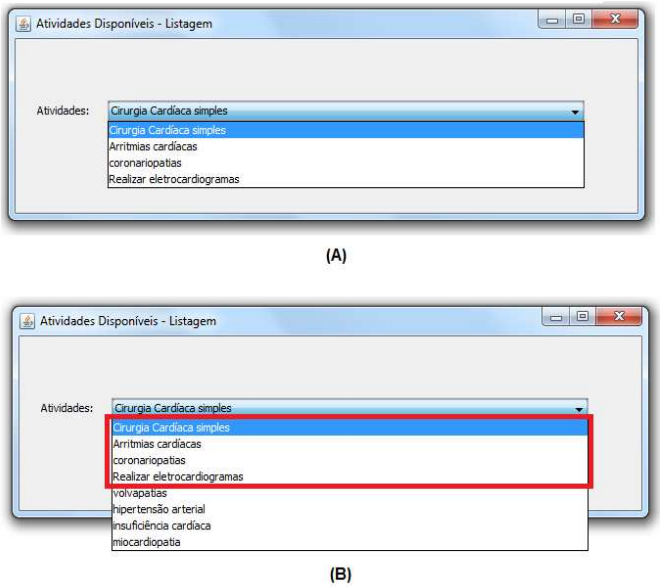

Fig. 8. Controle de acessos no cenário 2. A tela (A) mostra as atividades iniciais e a tela (B) destaca as atividades autorizadas através da Trilha.

O *EasyConn4All* ainda faz uso de papéis para facilitar a administração dos recursos e com isso atingir um número maior de entidades quando alguma alteração nos direitos de acesso for feita.

Os cenários permitiram duas constatações relevantes. Primeiro, foi possível comprovar a viabilidade do uso da análise do histórico de acessos de atividades como instrumento para controle de novos acessos. Segundo, o modelo proposto encontrou aplicação em dois domínios diferentes (setor contábil e hospitalar).

Os trabalhos futuros identificados foram: (1) pretende-se permitir o acesso ao sistema através de navegadores de internet, deixando assim o *EasyConn4All* mais acessível apara outras formas de utilização; (2) devem ser implementados novos cenários envolvendo outros domínios de aplicação, ampliando a avaliação da aplicabilidade do modelo em diferentes campos de atuação; (3) devem ser incluídos recursos que tornem a identificação da entidade uma tarefa segura, reduzindo a possibilidade de fraudes, talvez através da inclusão de certificação digital; (4) finalmente, o EasyConn4All será aplicado em situações reais envolvendo usuários que avaliem sua aceitação como tecnologia [22], focando principalmente na facilidade de uso e utilidade.

REFERÊNCIAS

[1] A. Wagner, J. L. Barbosa, D. N. F. Barbosa, "A Model for Profile Management Applied to Ubiquitous Learning Environments," *Expert Systems with Applications*, vol.41, pp.2023-2034, 2014. Disponível em: 10.1016/j.eswa.2013.08.098.

[2] M. Weiser, "The Computer for the 21st Century," *Scientific America*, vol.l, pp. 94–104, 1991. Disponível em: http://dx.doi.org/10.1145/329124.329126.

[3] M. Satyanarayanan, "Pervasive Computing: vision and challenges," *IEEE Personal Communications*, vol. 8, pp. 10–17, 2001. Disponível em: http://dx.doi.org/10.1109/98.943998.

[4] A. Dey, G. Abowd, D. Salber, "A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications," *Human-Computer Interaction*, vol. 16, n.2, pp.97–166, 2001. Disponível em: http://dx.doi.org/10.1207/S15327051HCI16234_02.

[5] J. L. Barbosa, R. M. Hahn, D. N. F. Barbosa, A. Saccol, "A Ubiquitous Learning Model Focused on Learner Integration," *International Journal of Learning Technology*, vol.6, n.1, pp.62-83, 2011. Disponível em: http://dx.doi.org/10.1504/IJLT.2011.040150.

[6] L. K. Franco, J. H. Rosa, J. L. Barbosa, C. A. Costa, A. C. Yamin, "MUCS : A Model for Ubiquitous Commerce Support," *Eletronic Commerce Research and Applications*, vol.1, pp.1-38, 2010. Disponível em: http://dx.doi.org/10.1016/j.elerap.2010.08.006.

[7] H. D. Vianna, J. L. Barbosa, "A model for ubiquitous care of non-communicable diseases," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, n.5, pp. 1597-1606, 2014. Disponível em: http://dx.doi.org/10.1109/JBHI.2013.2292860.

[8] J. Cao, J. Wang, K. Law, S. Zhang, M. Li. "An Interactive Service Customization Model," *Journal of Information and Software Technology*, vol.48, n.4, pp.280–296 , 2006. Disponível em: http://dx.doi.org/ 10.1016/j.infsof.2005.04.007.

[9] J. M. Silva, J. H. Rosa, J. L. Barbosa, D. N. F. Barbosa, L. A. M. Pallazo, "Content Distribution in Trail-aware Environments," *Journal of the Brazilian Computer Society*, vol. 16, pp. 163-176, 2010. Disponível em: http://dx.doi.org/10.1145/1858477.1858492.

[10] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, "Role-based access control models," *IEEE Computer*, vol.29, n.2, pp.38–47, 1996.

[11] J. G. P. Filho, R. M. Pessoa, C. Z. Calvi, N. Q. Oliveira, "Infraware: um Middleware de Suporte a Aplicações Móveis Sensíveis ao Contexto," in: *SBRC – 24º Simpósio Brasileiro de Redes de Computadores, (SBRC 2006)*. Curitiba-PR, 2006,

[12] R. M. Pessoa, C. Z. Calvi, R. M. Pessoa, R. V. Andreao, "Aplicação de um Middleware Sensível ao Contexto em um Sistema de Telemonitoramento de Pacientes Cardíacos," in: *SEMISH - Seminário Integrado e Software e Hardware*, 2006, Campo Grande/MS. SBC 2006, vol. 1, pp. 32-46.

[13] A. Corradi, R. Montanari, D. Tibaldi, "Context-based access control for ubiquitous service provisioning," in. *IEEE Computer Software and Applications Conference*, Los Alamitos, 2004, vol.1, pp. 444–451. Disponível em: http://dx.doi.org/10.1109/CMPSAC.2004.1342877.

[14] M. Wedgam, "AWARENESS: a project on Context AWARE Networks and Services," in Proc. *14th Mobile & Wireless Communication Summit*, Germany 2005, pp. 19-23.

[15] T. Gu, et. all, "A Middleware for Building Context-Aware Mobile Services," in Proc. IEEE Vehicular Technology Conference, Milan, Italy, 2004, vol.5, pp 2656-2660. Disponível em: http://dx.doi.org/10.1109/VETECS.2004.1391402.

[16] Rodrigues, S. "uMED: Uma arquitetura para o desenvolvimento de software direcionado a medicina ubíqua". Tese de mestrado em ciência da computação . PP-GINF/CPOLI/UCPEL, Pelotas, RS, 2010.

[17] Yamim, Adenauer et al. "EXEHDA: adaptative middleware for building a pervasive grid environment". Frontiers in Artificial Intelligence and Applications: Self Organization and Automatic Informatics (I) . vol. 135, Amsterdam: IOS Press, 2005. P-203-219.

[18] Hong, J. I. "Context Fabric: Infrastructure Suport for Context-Aware Systems". Phd Thesis, The University of California at Berkley. 2001

[19] Arruda Jr, C.R.E. "Context Kernel: Um Web service baseado nas dimensões de informação de contexto". l;85p.:Dissertação (Mestrado em Ciência da Computação e Matemática Computacional) - Universidade de São Paulo. São Carlos. 2003

[20] Yamim, A.C. "Arquitetura para um ambiente de Grade Computacional Direcionado as Aplicações Móveis, Distribuídas e Conscientes do Contexto da Computação Pervasiva". Tese (Doutorado) - Universidade Federal do Rio Grande do Sul. Porto Alegre. 2004

[21] Viterbo Filho J., Sacramento V., da Rocha R.C.A., Endler M.(2006) "MoCA :Uma arquitetura para o Desenvolvimento de Aplicações Sensíveis ao Contexto para dispositivos Móveis". Proc. of the XXIV Brazilian Synposium on Computer Networks (SBRC 2006), Tool Session, Curitiba, 2006.

[22] N. Marangunić and A. Granić, "Technology acceptance model: a literature review from 1986 to 2013" *Universal Access Information Society*, pp. 1–15, 2014. Disponível em: http://dx.doi.org/10.1007/s10209-014-0348-1.