UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA E GESTÃO DO CONHECIMENTO

João Carlos Damasceno Lima

UMA ABORDAGEM DE RECOMENDAÇÃO SENSÍVEL AO CONTEXTO PARA APOIO A AUTENTICAÇÃO IMPLÍCITA EM AMBIENTES MÓVEIS E PERVASIVOS BASEADO EM CONHECIMENTO COMPORTAMENTAL DO USUÁRIO

Tese submetida ao Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina para a obtenção do grau de Doutor em Engenharia e Gestão do Conhecimento.
Orientador: Prof. Dr. Mário Antônio Ribeiro Dantas

Florianópolis

2013

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Damasceno Lima, João Carlos
Uma abordagem de recomendação sensível ao contexto para apoio a autenticação implícita em ambientes móveis e pervasivos baseados em conhecimentos comportamentais do usuário / João Carlos Damasceno Lima ; orientador, Mário Antônio Ribeiro Dantas - Florianópolis, SC, 2013.
161 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento.

Inclui referências

1. Engenharia e Gestão do Conhecimento. 2. Modelagem Comportamental. 3. Autenticação Implícita. 4. Computação Pervasiva. I. Ribeiro Dantas, Mário Antônio. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento. III. Título.

João Carlos Damasceno Lima

UMA ABORDAGEM DE RECOMENDAÇÃO SENSÍVEL AO CONTEXTO PARA APOIO A AUTENTICAÇÃO IMPLÍCITA EM AMBIENTES MÓVEIS E PERVASIVOS BASEADO EM CONHECIMENTO COMPORTAMENTAL DO USUÁRIO

Esta Tese foi julgada adequada para obtenção do Título de Doutor em Engenharia e Gestão do Conhecimento e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina.
Florianópolis, 03/07/2013.

Prof. Gregório Jean Varvakis Rados, Dr.
Coordenador do Curso

Banca Examinadora:

Mário Antônio Ribeiro Dantas, Dr.
Orientador e Presidente

Adenauer Correa Yamin, Dr., UCPel/UFPel

Celso Massaki Hirata, Dr., ITA

Fernando Alvaro Ostuni Gauthier, Dr., UFSC/EGC

Francisco Antônio Pereira Fialho, Dr., UFSC/EGC

João Bosco Mangueira Sobral, Dr., UFSC/INE

Dedico esta tese para minha família: a minha amada Ana Lúcia, a minha querida filha Letícia e aos meus pais, Luiz Carlos (in memoriam) e Vilda Lima.

"se você acha que educação é cara, experimente a ignorância".

Derek Bok, Reitor em Harvard entre 1968 e 1971.

AGRADECIMENTOS

Agradeço aos meus amigos - Cacau, Benhur, Marcelo, Guto, Andrea, Celio e Reimar - pelo suporte incondicional nesta jornada de doutorado. Ao meu amigo Kamil, que trilhou ao lado o meu caminho do doutorado, agradeço pelas valiosas trocas de ideias e pelos serviços de Consulado.

A minha amada Ana Lucia, agradeço pelo carinho, companheirismo, privações e motivação, que tornaram mais leve o longo caminho até o final deste trabalho. A minha filha Letícia, que enfrentou duas mudanças e, sempre alegre, me incentiva nos momentos mais difíceis.

Agradeço a minha mãe, Vilda Lima, por toda ajuda e incentivo para que eu continuasse a estudar e me aperfeiçoar, pessoa simples, mas de grande visão, exemplo de dedicação aos filhos. Especial agradecimento a Norma Pascotto pelos diversos apoios: colaboradora, conselheira, enfermeira e o principal, grande amiga.

Meus sinceros agradecimentos ao meu orientador e grande amigo, Professor Mário Dantas, que me auxiliou e incentivou, em vários momentos difíceis neste período de doutorado. Através de sua visão humanista, conduziu este trabalho com liberdade e compromisso, nunca poupando esforços para que chegássemos ao final desta Tese com resultados e publicações relevantes na área.

À colega professora Iara Augustin, agradeço pelo apoio, discussão, revisão, por ter se interessado na interdisciplinaridade da cognição situada e pela especial cobrança diária para o término desta Tese; às vezes, fugia para não ser cobrado, novamente. Ao final percebo que postergar a entrega do trabalho era mais uma desculpa para não mudar, era uma tentativa de continuar a melhorar indefinidamente e que isto nunca tem fim.

Ao meu amigo Cristiano Rocha, com quem tive grandes momentos de discussão sobre os rumos desta pesquisa e que sempre procurou, de alguma forma, colaborar e incentivar com o desenvolvimento deste trabalho, a ajuda dele foi fundamental para o desenvolvimento deste trabalho.

Aos amigos próximos de Florianópolis – Edson, Kamil (novamente), Matheus, Tiago, Rodolfo, Edmar e Rafael – agradeço pelas contribuições, cada um em sua especialidade, para a realização deste trabalho e as intermináveis sessões de discussão e futebol na academia.

A minha familia de Santa Catarina - Tio Waldyr, Tia Marlene, Consuelo e Santos - pelo apoio que vocês dispensaram a minha família nos diversos momentos que necessitamos e pela confiança, que sempre depositaram em nós.

Agradeço ao CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) do MCT (Ministério da Ciência e Tecnologia), os quais financiaram o desenvolvimento desta Tese.

Por fim, agradeço ao Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento e à Universidade Federal de Santa Catarina pelo acolhimento e suporte, o que possibilitou o presente trabalho.

RESUMO

Muitas empresas começam a adaptar-se às tecnologias e aos dispositivos móveis, incorporando no seu cotidiano, os benefícios proporcionados pela mobilidade e a possibilidade do Trabalho Móvel. Os serviços acessados pelos dispositivos móveis, geralmente, utilizam processos de autenticação baseado em credenciais (por exemplo, senha), que se mostram vulneráveis e inadequados. Logo, abordagens alternativas de autenticação devem considerar as características ambientais (consciência do contexto), restrições dos dispositivos, privacidade das informações armazenadas e informações provenientes dos muitos sensores que estão presentes no espaço pervasivo. Esta pesquisa propõe uma abordagem de recomendação baseado em comportamento do usuário para autenticação implícita no espaço pervasivo em que este se encontra. O comportamento dos usuários é modelado através de um conjunto de características de contexto e de atividades, que os usuários executam. Os usuários possuem atividades diárias, semanais e mensais que formam um conjunto de hábitos executados regularmente. O monitoramento destes hábitos permite indicar se um usuário legítimo está executando as suas atividades ou se outra pessoa está acessando sem autorização os serviços e informações do dispositivo móvel. Portanto, a combinação das características contextuais e as atividades (hábitos) auxiliam o processo de reconhecimento e certificação do usuário. Os processos de filtragem do sistema de recomendação, permitem a adição de novos filtros que calculam a similaridade dos comportamentos dos usuários. Os filtros são classificados em: i) filtros locais, que trabalham com algoritmos de baixa complexidade devido aos recursos computacionais limitados dos dispositivos móveis, e ii) filtros remotos, que trabalham com algoritmos mais complexos e podem executar ferramentas estatísticas nos servidores de autenticação. Os resultados experimentais indicam com sucesso: i) um mecanismo mais dinâmico (adaptável às atividades executadas pelo usuário) e autonômico para autenticação de usuários em um ambiente móvel e pervasivo, e ii) uma eficiência significativa na detecção de anomalias de autenticação através da utilização de modelos de similaridade e permutação espaço-temporal.

Palavras-chave: Modelagem Comportamental; Autenticação Implícita; Computação Pervasiva.

ABSTRACT

Many companies are beginning to adapt to technologies and mobile devices, incorporating in their daily lives, the benefits provided by the mobility and the possibility of Labour Mobile. The services accessed by mobile devices typically use authentication processes based on credentials (e.g., password), that are vulnerable and inadequate. Therefore, alternative approaches to authentication should consider the environmental characteristics (context-awareness), constraints of devices, privacy of information stored and information from many sensors that are present in pervasive space. This research propose a recommendation approach based on user behavior for implicit authentication in pervasive space in which it is located. The user behavior is modeled by a set of characteristics of context and activities that users perform. Users have daily , weekly and monthly activities forming a set of habits, which are performed regularly. The monitoring of these habits is used to indicate if a legitimate user is running their activities or if someone else is accessing without authorization services and information of the mobile device. Therefore, the combination of contextual characteristics and activities (habits) assist the process of recognition and certification of the user. The process of filtering recommendation system , allow the addition of new filters that compute the similarity of users' behaviors. Filters are classified into: i) local filters that work with low-complexity algorithms due to the limited computing resources of mobile devices, and ii) filters remote working with more complex algorithms and statistical tools can perform the authentication servers. The experimental results indicate successfully: i) a mechanism more dynamic (adaptable to the activities performed by the user) and autonomic for authentication users in a mobile and pervasive environment, and ii) an efficiency in the detection of anomalies authentication by using models of similarity and spatio-temporal permutation.

Keywords: Behavioral Model; Implicit Authentication; Pervasive Computing.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AAA	Protocolo de Autenticação, Autorização e Auditoria.
ACL	Access Control Lists - Lista de Controle de Acesso.
AH	Abstraction Hierarchy - Hierarquia de Abstração.
ARM	Activity Recognition Manager - Gerenciador de Reconhecimento de Atividades.
CAFe	Comunidade Acadêmica Federada.
E-SSO	Enterprise Single Sign-on.
EID	Ecological Interface Design - Projeto de interface ecológica.
MCA	Mobile Cognitive Agent - Agente Cognitivo Móvel.
PBC	Vetor de Pesos Acumulativos da Sessão para o Filtro de Conteúdo.
PBH	Vetor de Pesos Acumulativos da Sessão para o Filtro Híbrido.
PIN	Personal Identification Number - Número de Identificação Pessoal.
RNP	Rede Nacional de Pesquisa.
SCA	Static Cognitive Agent - Agente Cognitivo Estático.
SR	Sistema de Recomendação.
SRK	Skills, Rules, Knowledge framework - Framework de habilidades, regras e conhecimentos.
SRM	Sistemas de Recomendação Móvel.
SRSC	Sistemas de Recomendação Sensíveis ao Contexto.
SSO	Single Sign-On.
TAHC	Teoria da Atividade Histórico Cultural.
TBAS	Transaction-Based Authentication Scheme - Esquema de Autenticação Baseado em Transação.
TIC	Tecnologias de Informação e Comunicação.
UbiCOSM	Ubiquitous Context-based Security Middleware - Mediador de Segurança Baseado em Contexto Ubíquo.
UCD	User-Centered Design - Projeto Centrado no Usuário.

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo é apresentada a contextualização, justificativa, delimitação do tema de pesquisa e a aderência desta pesquisa ao programa de pós-graduação. Na seção de pergunta de pesquisa é apresentada a motivação e a hipótese de solução bem como, os principais referenciais teóricos que dirigiram esta Tese. A partir da pergunta de pesquisa e da hipótese foram explicitados os objetivos desta pesquisa.

1.1 CONTEXTUALIZAÇÃO DO TEMA DE PESQUISA

Com a popularização dos dispositivos móveis (*smartphones* e *tablets*), as informações que estavam, normalmente, distribuídas entre diversos servidores e redes de informação, tornam-se disponíveis nas vinte e quatro horas do dia e nos sete dias da semana. Com essa popularização dos dispositivos móveis (*smartphones* e *tablets*), existe uma gradual e incremental inserção dos usuários nos ambientes de computação móvel e pervasiva. Os serviços mais utilizados por estes usuários hoje são: armazenamento e recuperação de dados pessoais, serviços financeiros, redes sociais, mensagens eletrônicas e comércio eletrônico.

A sensação de centralização das informações que os dispositivos móveis proporcionam, permite que os usuários interajam uns com os outros e trabalhem simultaneamente, deslocando-se em um ambiente pervasivo que é suportado pelas Tecnologias de Informação e Comunicação (TIC). O uso intensivo dessas tecnologias tem mudado o modo de viver, em todos os setores (KAKIHARA; SØRENSEN, 2001). Cardoso e Castells (2005) caracterizam a atual revolução tecnológica não como a centralidade de conhecimento e da informação, mas como a aplicação desses conhecimentos e dessa informação na geração de conhecimentos e de dispositivos de processamento e de comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso.

De acordo com a Consultoria IDC foram vendidos 59,5 milhões de celulares e *smartphones* no Brasil em 2012. No ano de 2011 foram vendidos 17 *smartphones*, por minuto. Já em 2012 foram vendidos 30 aparelhos por minuto, totalizando 16 milhões de aparelhos no ano e representando um crescimento de 78 % em relação aos 9 milhões de 2011 (IDC, 2013).

A utilização dos dispositivos móveis expandiu-se para diversas áreas de atividade devido a sua simplicidade, funcionalidade, portabilidade e faci-

lidade de uso (MYERS *et al.*, 2004). A pesquisa TIC Empresas 2011 (CETIC.BR, 2012), organizada pelo Comitê Gestor da Internet no Brasil, entrevistou 5600 empresas, com 10 ou mais funcionários e revelou que 46% destas empresas permitem acesso ao sistema corporativo. Esse estudo informa ainda que 74% destas empresas utilizam *smartphones* corporativos como ferramenta de trabalho nas atividades: i) enviar SMS - 59%; ii) acessar Internet - 47%; iii) enviar e-mail - 44%; iv) enviar MMS - 19%; v) utilizar serviços financeiros - 17%; e vi) interagir com organizações governamentais - 11%.

Nota-se, portanto, que as empresas estão se adaptando aos dispositivos móveis, incorporando no seu cotidiano os benefícios proporcionados pelo aumento de mobilidade dos seus usuários. Dessa forma, os usuários apoiam as atividades empresariais, via telefones e notebooks com acesso à Internet, bem como redes sem fio, possibilitando acesso a dados e informações em qualquer lugar, em qualquer hora, com qualquer dispositivo (características do conceito de pervasividade). As tecnologias móveis aplicadas nas empresas oferecem diversas funcionalidades, tais como o provimento de comunicação móvel, suporte a trabalhadores móveis, serviços baseados em localização, suporte a serviços de emergência nas áreas de saúde, militar e de segurança pública, entre outros (ZHANG; YUAN, 2002).

O uso de dispositivos e tecnologias móveis propicia que os usuários das empresas exerçam o chamado Trabalho Móvel, que é definido como a possibilidade de um indivíduo executar suas tarefas em locomoção, a qualquer hora, em qualquer lugar, em qualquer contexto[1], por meio do uso de tecnologias móveis e sem fio (YUAN; ZHENG, 2009). Ryan *et al.* (2009), em seu estudo "*Worldwide Mobile Worker Population* 2009-2013", relata que o número mundial de trabalhadores móveis ultrapassou a marca de um bilhão no fim do ano de 2010 e, até o final de 2013, o número de pessoas, que trabalharão de tal forma, vai crescer em torno de 200 milhões, atingindo 1,2 bilhão de pessoas, o que equivalerá a mais de um terço de toda força mundial de trabalho.

Por outro lado, essa migração natural de muitas atividades e tarefas de trabalho para o ambiente de computação móvel e pervasivo traz problemas. Dispositivos e tecnologias móveis têm desvantagens em relação à segurança e à privacidade das informações que estão armazenadas localmente (no dispositivo). Torna-se necessário que os novos mecanismos de segurança se preocupem com a perda do dispositivo e o local onde ele é utilizado, pois podem ser

[1]Contexto é o modo em que as ações que são executadas têm significado, e tudo aquilo que emerge diante desta experiência, pode proporcionar novas formas de ação e novos significados (DOURISH, 2004; TAMMINEN *et al.*, 2004).

facilmente perdidos, roubados ou usados por vários indivíduos, permitindo que informações confidenciais possam ser utilizadas de forma indevida.

Um processo chave para a segurança é a autenticação. No contexto deste trabalho, **Autenticação é definida como o ato de estabelecer ou confirmar algo (ou alguém) como autêntico**; isto é, ratifica a autoria ou a veracidade de alguma coisa. A autenticação também remete à confirmação da procedência de um objeto ou pessoa; neste caso, frequentemente, relacionada com a verificação da sua identidade.

As políticas de segurança padrão baseiam-se no uso de senhas alfanuméricas. A autenticação baseada em senha tem a vantagem de ser simples de implementar e de usar poucos recursos (nenhum hardware adicional é geralmente necessário). No entanto, métodos de descoberta de senha comumente utilizados (*phishing*, *keyloggers* e engenharia social) têm sido bem sucedidos. No ambiente da computação móvel, as políticas de segurança permitem a utilização de uma segunda forma complementar de certificação do usuário que pode ser usada para minimizar a desvantagem de perda de informações nos dispositivos móveis. Portanto, a utilização de uma certificação complementar, como parte do processo de autenticação, oferece maior segurança.

Existem serviços que implementam a validação complementar, como google *authenticator*, porém apresentam problemas relativos à usabilidade e ao custo. A opção das empresas tem sido pela utilização de *tokens SecurID*, que são exibidos através de dispositivos auxiliares e que possuem características relacionadas à computação baseada em desktops, onde as informações estão restritas a ambientes seguros (empresas e casas). Essa solução não é adequada à mobilidade e ao ambiente pervasivo porque os dispositivos móveis não possuem os limites de segurança dos ambientes restritos.

Outra dificuldade, oriunda da mobilidade e do uso de dispositivos pequenos (portáteis), é a digitação de senhas seguras, as quais devem conter uma longa cadeia de caracteres entre alfanuméricos, caixa alta e baixa, e caracteres especiais. Digitar sempre essa senha, de tempos em tempos, para realizar o processo de autenticação, torna-se uma tarefa indesejada para o usuário móvel.

Uma solução natural seria adotar a autenticação implícita. De acordo com Shi *et al.* (2011), a autenticação implícita poderá: i) atuar como um segundo fator e complementar as senhas para melhorar o processo de autenticação, aumentar as garantias de identificação do usuário e facilitar a utilização; ii) atuar como o principal método de autenticação para substituir senhas; iii) prever adicional garantia para operações financeiras, tais como compras do cartão de crédito, agindo como um indicador de fraude. Nota-se que, no úl-

timo cenário, é importante que o ato de fazer a transação não exija qualquer ação do usuário no dispositivo.

Porém, é preciso garantir maior segurança a esse processo. Para tal, propõe-se, neste trabalho, utilizar os conceitos de autenticação implícita adicionando informações do comportamento habitual do usuário para realizar a autenticação de forma automática. Em um ambiente pervasivo, deve-se considerar também a mobilidade e as alterações dinâmicas que ocorrem no ambiente. Assim, o sistema pode autenticar o usuário automaticamente mas, considerando determinados limites espaciais e temporais. Assim, propõe-se um sistema de recomendação para tomada de decisão, que indica quando o processo de autenticação deve novamente inquirir o usuário para reconhecê-lo. A inserção dos conceitos de sistemas de recomendação (RICCI *et al.*, 2011) no contexto deste trabalho, é porque estes sistemas permitem a combinação de diversas técnicas computacionais (processos de filtragens) para selecionar itens personalizados com base nos interesses dos usuários e conforme o contexto no qual estão inseridos.

Considera-se a solução de utilizar dados comportamentais, para reconhecer um usuário, uma abordagem viável, por que as pessoas são criaturas de hábitos (ROCHA, 2010); com esta mesma visão Flanagan (2010), defende que "os Seres Humanos são criaturas de hábitos e que a rotina permite uma sensação de controle". Por exemplo, considerando um determinado indivíduo, sua rotina diária incluiria: trabalhar na parte da manhã; talvez fazer uma parada para tomar café; quase sempre usar a mesma rota para se deslocar; no trabalho, permanecer na área de seu prédio de escritórios até a hora do almoço; na parte da tarde, receber ligações de sua casa para pegar o filho na escola; à noite, retornar para casa; durante todo o dia, verificar suas diferentes contas de e-mail; normalmente, usar serviços bancários on-line e às vezes verificar sua conta, com seu *smartphone* quando fora de casa; visitar semanalmente o supermercado; realizar chamadas telefônicas regulares aos membros da família ou pessoas que constam na sua lista de contatos, etc. Esses dados de comportamento (o quê, quando, onde, com o quê, quem) são fontes ricas de informação e podem ser capturadas, reunidas e armazenadas em *smartphones* (SHI *et al.*, 2011).

Os próprios dispositivos móveis podem coletar as informações produzidas pelo usuário no seu uso diário: agenda do usuário, ligações do usuário, mensagens, além de adicionar dados complementares (como tempo e localização) nas informações produzidas. Esse conjunto de dados coletados, em um processo de monitoramento temporal e espacial, explicitam informações que definem um perfil do usuário (formando o conhecimento que o sistema

tem sobre ele), o qual servirá como um critério adicional que tornará mais seguro o processo de autenticação.

1.2 JUSTIFICATIVA E RELEVÂNCIA

A computação móvel e pervasiva está diretamente relacionada à massificação do uso de dispositivos móveis. Estes dispositivos possuem características particulares, como peso, tamanho, dimensões reduzidas da tela e teclados simulados na interface *touch screen*, que limitam a interação com os seus usuários. Devido a essa limitação é normal que os usuários utilizem senhas fracas, tais como, senhas com reduzido número de dígitos, de fácil lembrança e digitação, as quais não são recomendadas devido a facilidade com que podem ser obtidas por terceiros ou quebradas por softwares específicos para esse fim.

Por outro lado, sabe-se que os dispositivos móveis mantém dados sobre o acesso a uma diversidade de serviços, informações e conhecimento de seus usuários e que estes devem ser protegidos do acesso indevido. Nesta proposta de solução, esse mesmo conjunto de conhecimento sobre os usuários, que está armazenado ou acessível ao dispositivo, serve como fonte de informação para um mecanismo de autenticação implícita e mais segura.

Esta proposta de solução foi motivada pela complexidade do processo de autenticação segura em ambientes móveis e pervasivos e pela percepção que os métodos e técnicas da Engenharia do Conhecimento podem contribuir para o desenvolvimento de uma solução inovadora, ao utilizar o conhecimento obtido sobre o comportamento do usuário. Os métodos tradicionais de autenticação reconhecem como verdadeiro o dispositivo que o usuário está utilizando mas não o usuário em si, não garantem que seja o usuário (autenticado) quem efetivamente está utilizando o dispositivo reconhecido. A utilização de uma abordagem de recomendação sensível a contexto que permita reconhecer o usuário através do conhecimento comportamental deste, utilizando as informações e dados obtidos sistemicamente, através de diagnósticos realizados, serve para melhoria do processo de autenticação, ao explicitar um conhecimento latente que, geralmente, permanece encoberto ou que não vem sendo utilizado, mas que está disponível.

A relevância da abordagem proposta está na inovação de utilizar informações de contexto (comportamento do usuário, conhecimento das atividades armazenadas no dispositivo móvel) no processo de autenticação em ambientes pervasivos, usando método de análise de similaridade na execução das

atividades desenvolvidas pelo usuário a ser autenticado e o perfil armazenado deste no sistema. Informações e dados coletados, provenientes de diagnósticos realizados, quando colhidos e tratados adequadamente, podem tornar-se valiosas fontes de conhecimento.

Assim, considera-se que a pesquisa terá as seguintes contribuições: i) como contribuição tecnológica, um novo método de autenticação usando conhecimento comportamental do usuário e ii) como contribuição científica, a representação formal e o cálculo probabilístico deste. Ao integrar diferentes técnicas e teóricas em uma abordagem, inicialmente conceitual, pretende-se cooperar cientificamente no aprimoramento da tarefa de diagnóstico no processo de explicitação de conhecimentos. Esta abordagem proposta permite também aos profissionais da área de segurança adotarem uma perspectiva de inteligência-ambiente ao considerar o contexto na qual a autenticação acontece. Isso evidencia a possibilidade da explicitação de conhecimentos para o avanço metodológico deste processo.

1.3 ADERÊNCIA AO OBJETO DE PESQUISA DO PROGRAMA

Este trabalho está inserido na área de concentração da Engenharia do Conhecimento do Programa de Pós-Graduação de Engenharia e Gestão do Conhecimento (EGC). Este programa tem como missão promover a pesquisa de forma interdisciplinar sobre o conhecimento para agregar valor para a sociedade.

Este trabalho possui uma natureza interdisciplinar porque agrupa disciplinas diversas, de áreas como: Ciência da Computação, Segurança da Informação, Psicologia Cognitiva e Engenharia e Gestão do Conhecimento. O aspecto interdisciplinar contribuiu para o desenvolvimento desta Tese, uma vez que se localiza em um ponto de convergência entre essas áreas do conhecimento humano. As principais contribuições de cada área, acima citadas são:

- **Ciência da Computação:** desta área são utilizados os conceitos e modelos: da computação móvel, computação pervasiva, computação ubíqua e consciência de contexto (*Context-Awareness*);
- **Segurança da Informação:** desta área são utilizados os critérios de classificação biométrico e os conceitos dos processos: de autenticação, de autorização e de auditoria;
- **Psicologia Cognitiva:** desta área são utilizados os conceitos: de con-

textos positivistas, de contextos fenomenológicos, de ação situada, de hábitos, de comportamento e da teoria da atividade;

- **Engenharia e Gestão do Conhecimento:** desta área são utilizados os conceitos e os modelos: de sistemas de recomendação e *Framework* habilidades, regras e conhecimento.

A proposta desta Tese consiste na elaboração de um modelo e de uma arquitetura, que possibilitem a autenticação implícita do usuário por meio do conhecimento de seu perfil comportamental, utilizando métodos, técnicas e ferramentas da Engenharia do Conhecimento e da Cognição Situada.

A aderência desse trabalho ao objeto de pesquisa do programa pode ser reforçada pela natureza interdisciplinar e também pela proposta do trabalho que está coesa com o objetivo principal do Programa, que consiste em investigar, conceber, desenvolver e aplicar modelos, métodos e técnicas relacionados tanto a processos/bens/serviços, como ao seu conteúdo técnico-científico.

1.4 DELIMITAÇÃO

Esta Tese não tem como objetivo o desenvolvimento de um produto de autenticação, mas sim desenvolvimento de protótipos para validação dos conceitos e métodos utilizados na definição deste trabalho e dos seus resultados experimentais.

De acordo com Wazlawick (2010), esta pesquisa tem a natureza original porque busca apresentar conhecimento novo a partir de observações e teorias construídas para explicá-lo. Em relação aos objetivos, ela é classificada como exploratória, porque não consegue provar uma teoria nem apresentar uma diversidade de resultados estatisticamente aceitos. Porém, a utilização da técnica de pesquisa, estudos de caso, a argumentação e o convencimento validam as pesquisas em áreas emergentes e novas, onde só é possível uma metodologia de pesquisa exploratória, resultando na criação de um novo conhecimento.

1.5 PERGUNTA DE PESQUISA

Esta pesquisa tem o propósito de responder à seguinte pergunta: **Como modelar um sistema de autenticação complementar que considere os requisitos de mobilidade, em relação as aplicações, serviços e**

informações, dos usuários em um ambiente pervasivo?

Para responder a essa pergunta é estabelecido um conjunto de metodologias, ferramentas e preceitos teóricos que fundamentam a solução. Esse trabalho busca uma solução ao problema de autenticação em ambiente pervasivo, que requisite a utilização de poucos recursos adicionais de hardware e atue de forma transparente e proativa, isto é, identifique as necessidades dos usuários e atue de forma a facilitar a interação destes com os sistemas, aplicativos e serviços.

A solução proposta nesta pesquisa executa um cálculo probabilístico para verificar se o usuário, que está operando o dispositivo móvel é realmente o seu proprietário e possui acesso às informações e conhecimento armazenados. As atividades rotineiras dos usuários são capturadas e modeladas como um aspecto comportamental do mesmo, sendo que a atividade é produzida na ação do relacionamento do usuário com o ambiente; portanto, usuários diferentes tendem a possuir relacionamentos diferenciados frente ao mesmo ambiente.

Para modelar o comportamento de usuário frente a um plano de ação são utilizados conceitos da Psicologia Cognitiva, em especial a Ação Situada (SUCHMAN, 1987) e a Teoria da Atividade de Vygotski *et al.* (2005), que possui um referencial teórico-metodológico multidisciplinar para pesquisas em Educação, Sociologia do Trabalho e Filosofia. De acordo com Rego (2008), Vygotski afirma que as características humanas não estão presentes desde o nascimento do indivíduo nem são resultados das pressões do meio externo: elas resultam da interação dialética do homem e seu meio socio-cultural[2]. Vygotski concluiu ainda que à medida que o ser humano transforma o seu meio para atender suas necessidades, ele transforma-se a si mesmo.

[2]Neste sentido, Vygotski *et al.* (2005) elaborou o conceito de Zona de Desenvolvimento Proximal (ZDP). Onde considera que todo indivíduo, numa situação de aprendizagem, já possui um certo nível de desenvolvimento, que lhe dá uma capacidade de resolver um problema de forma autônoma, sem o auxílio de outra pessoa. A ZDP representa, então, a área intermediária do processo que liga o nível atual de desenvolvimento com o próximo nível em potencial. Para Vygotski, o estágio do aprendizado, que permite a utilização do conhecimento de forma autônoma, é o desenvolvimento real do estudante. Este estágio é dinâmico e vai se alterando no processo de aprendizagem. O desenvolvimento real produz as possibilidades ainda não consolidadas que potencialmente podem ser construídas; o que gera o desenvolvimento potencial. O desenvolvimento potencial estimulado por meio do processo contínuo de aprendizagem evolui posteriormente para o desenvolvimento real (REGO, 2008).

1.6 OBJETIVOS

Esta seção apresenta os objetivos geral e específicos propostos para esta pesquisa.

1.6.1 Objetivo Geral

O objetivo desta Tese é a elaboração de uma abordagem de recomendação que possibilite a autenticação implícita do usuário através do conhecimento de seu perfil comportamental.

1.6.2 Objetivos Específicos

Do objetivo geral derivam os seguintes objetivos específicos:

- Identificar os modelos teóricos que definem as interações entre os usuários e os ambientes móveis e pervasivos no âmbito das Ciências Sociais;
- Identificar os modelos de autenticação de usuários em ambientes móveis e pervasivos no âmbito da Ciência da Computação;
- Propor uma abordagem de autenticação implícita que incorpore os conhecimentos comportamentais dos usuários;
- Demonstrar a viabilidade da abordagem proposta através de sua aplicação em testes experimentais;
- Publicar e divulgar resultados parciais e finais.

1.7 ORGANIZAÇÃO DO TRABALHO

A Tese é composta por seis capítulos. O *capítulo 1 - Introdução* contextualiza e descreve o problema e a pergunta de pesquisa. Apresenta a justificativa e os objetivos geral e específicos.

O *capítulo 2 - Computação Móvel e Modelos Cognitivos* apresenta uma pesquisa bibliográfica sobre os aspectos relevantes: (i) da computação móvel com seus referenciais teóricos, (ii) das ciências sociais na definição das

relações entre o usuário e o ambiente, com especial interesse na modelagem desses ambientes na forma de contextos ou planos e ações situadas, (iii) da Teoria da Atividade, (iv) *Framework* Habilidade, Regras e Conhecimento e (v) os conceitos relativos ao trabalho móvel.

O *capítulo 3 - Autenticação e Sistema de Recomendação* apresenta os conceitos do processo de autenticação, as principais abordagens de autenticação para sistemas móveis, uma análise comparativa destas abordagens e os modelos computacionais de sistema de recomendação e filtragem de informação que são utilizados nos testes experimentais.

O *capítulo 4 - Modelo e Arquitetura de Autenticação Proposto* descreve o modelo e arquitetura proposta, bem como os seus componentes.

O *capítulo 5 - Processos de Filtragem e Resultados Experimentais* descreve os Processos de Filtragem e apresenta os resultados coletados, que foram publicados em congressos internacionais, como prova de conceito.

O *capítulo 6 - Considerações Finais* apresenta as conclusões sobre a pesquisa realizada, relacionando-as com os objetivos propostos na introdução. São destacadas as contribuições e as sugestões para futuros estudos.

2 COMPUTAÇÃO MÓVEL E MODELOS COGNITIVOS

Neste capítulo são apresentados os referenciais teóricos de computação móvel. Estes referenciais contextualizam a pesquisa e apresentam uma natureza interdisciplinar, uma vez que os conceitos e as teorias apresentados neste capítulo estão presentes em diversas áreas de conhecimento. Esta Tese explora a natureza interdisciplinar para fundamentar o trabalho de pesquisa e apresenta visões alternativas para definir, modelar e explicitar os conhecimentos comportamentais dos indivíduos.

2.1 COMPUTAÇÃO UBÍQUA

Na percepção de Weiser (1991), a integração dos elementos da Ciência da Computação, da Engenharia, das Ciências Sociais e Humanas, definem o fenômeno da Computação Ubíqua. Ele descreve a Computação Ubíqua como a integração contínua de computadores no mundo, no qual os usuários realizam suas atividades diárias. Neste ambiente, Weiser previu que os computadores desapareceriam do nosso olhar, tornando-se comuns e pervasivos em vários aspectos de nossas atividades diárias e passariam a fazer parte de todos os objetos, de forma integrada e onipresente (WEISER, 1991).

A **Computação Ubíqua tem como objetivo tornar a interação homem-máquina transparente, ou seja, integrar a computação com as ações e os comportamentos naturais das pessoas. Se possível, de forma transparente e com a integração de diversos dispositivos computacionais interconectados, atuando de forma onipresente**. Logo, a ideia básica da Computação Ubíqua é que a computação move-se para fora das estações de trabalho e computadores pessoais e torna-se parte ativa (totalmente inserida) na vida cotidiana dos usuários.

Compartilhando da mesma visão, Roussos (2006) define que "o que diferencia a Computação Ubíqua dos paradigmas anteriores é o fato de que a capacidade da computação e das comunicações está incorporada nos objetos, locais e até mesmo nas pessoas", permitindo desta forma a interação entre os dispositivos computacionais. Logo, a Computação Ubíqua é o conceito no qual os pequenos dispositivos computacionais distribuídos e integrados, dispostos em diversos ambientes, fornecem serviços e informações a qualquer momento, em qualquer local. A computação ubíqua está situada no primeiro quadrante da Figura 1, sendo caracterizada por um alto grau de mobilidade (*high mobility*) e alto grau de integração com o ambiente (*high embedded-*

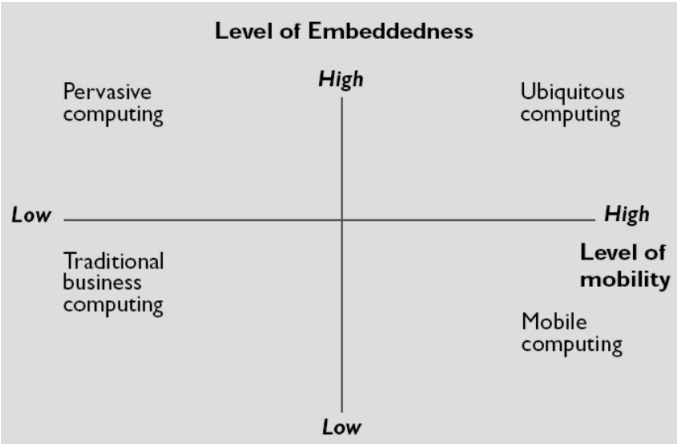


Figura 1: Dimensões da Computação Ubíqua.
Fonte: Lyytinen e Yoo (2002)

ness).

As demais dimensões da Figura 1, representam os demais sistemas computacionais, que são:

- Computação Pervasiva: está situada no segundo quadrante da Figura 1, sendo caracterizada por um baixo grau de mobilidade (*low mobility*) e alto grau de integração com o ambiente (*high embeddedness*). Significa que o computador está embarcado no ambiente de forma invisível para o usuário. Nesta concepção, o computador tem a capacidade de obter informação do ambiente no qual ele está embarcado e utilizá-la para dinamicamente, construir modelos computacionais, ou seja, controlar, configurar e ajustar as aplicações para melhor atender as necessidades dos dispositivos ou do usuário;

- Computação Tradicional: está situada no terceiro quadrante da Figura 1, sendo caracterizada por um baixo grau de mobilidade (*low mobility*) e baixo grau de integração com o ambiente (*low embeddedness*). Normalmente caracterizada por *mainframes*, *workstations* e *desktops*, equipamentos nos quais as pessoas executam tarefas explícitas, como a criação de documentos, troca de mensagens e acesso as redes sociais. Estes equipamentos utilizam uma interface de interação convencional composta de teclado, mouse e monitor;

- Computação Móvel: está situada no quarto quadrante da Figura 1, sendo caracterizada por um Alto grau de mobilidade (*high mobility*) e baixo grau de integração com o ambiente (*low embeddedness*). A computação móvel baseia-se no aumento da nossa capacidade de se deslocar utilizando serviços computacionais, ou seja, o computador torna-se um dispositivo sempre presente, que expande a capacidade de um usuário na utilização de serviços computacionais, independentemente de sua localização.

Embora alguns autores definam a computação ubíqua como a combinação da computação móvel com a computação pervasiva, neste trabalho discordamos desta corrente de pensamento porque os serviços de computação ubíqua previstos por Weiser (1991) são mais complexos, imperceptivelmente integrados aos ambientes, capazes de perceber a presença de seus usuários, ofertando, com transparencia, serviços de informação, controle e conveniência de maneira simples e intuitiva.

Os serviços da Computação Ubíqua, como previu Weiser (1991), tendem a ser incorporados à vida cotidiana de forma que sua presença passe despercebida, invisível, no sentido de ser utilizável sem qualquer esforço, usando linguagens comuns do dia-a-dia, mecanismos alternativos de entrada de dados tais como: toque, fala, pensamento, comportamento e deslocamento, no lugar dos tradicionais dispositivos: teclado e mouse.

De acordo com Weiser (1991), "as tecnologias mais profundas e duradouras são aquelas que desaparecem. Elas dissipam-se nas coisas do dia a dia até tornarem-se indistinguíveis". Nesse sentido, os usuários as utilizam inconscientemente na realização de suas atividades e tarefas. Portanto, como atualmente não existe ambientes computacionais que possam prover este tipo de serviço, optou-se por focar o trabalho em computação móvel e computação pervasiva, ambientes existentes e que possuem as necessidade de serviço de autenticação.

Logo, os serviços e aplicações que utilizam a combinação da computação móvel e computação pervasiva necessitam prover serviços básicos: (i) a identificação automática por meio de tags RFID (Identificação por Rádio Freqüência) que podem ser incorporadas nos objetos ou pessoas; (ii) as redes de sensores que coletam informações do contexto via estímulos biológicos, químicos e mecânicos; e ainda, (iii) o sensoriamento de localização por meio de GPS (Sistema de Posicionamento Global). Estes serviços definem uma das principais áreas de pesquisa dentro da Computação Pervasiva, que é a Computação Sensível ao Contexto (*Context-awareness Computing*) (SILVA *et al.*, 2012).

2.2 COMPUTAÇÃO SENSÍVEL AO CONTEXTO

Na Computação Pervasiva é importante que os módulos de software, que interagem entre si e com os usuários, possam perceber (ser sensível) e responder/reagir ao cenário em que estão sendo explorados e utilizados. Dourish (2004) afirma que "uma preocupação primária da pesquisa em Computação Pervasiva é entender a relação potencial entre a computação e o contexto em que esta está incorporada".

Portanto, os sistemas desenvolvidos sob o paradigma da Computação Ubíqua ou Computação Pervasiva seguem os conceitos de *Context-Awareness* (sensível ao contexto ou consciente de contexto) que em Ciência da Computação refere-se à ideia de que os computadores podem sentir (perceber) e reagir com base em informações do seu ambiente. Os dispositivos podem obter ou possuir informações sobre as circunstâncias em que eles são capazes de operar, com base em regras, ou a estímulos inteligentes, gerando assim uma reação. O termo sensível ao contexto em Computação Ubíqua foi introduzido por Schilit *et al.* (1994).

Os dispositivos sensíveis ao contexto também podem fazer suposições sobre a situação atual do usuário. Dey (2001) define contexto como "qualquer informação que possa ser utilizada para caracterizar a situação das entidades". Como exemplo, pode-se supor que um telefone celular sensível ao contexto pode saber que seu usuário está sentado em uma sala de reunião (contexto de localização). Logo, o sistema no telefone pode concluir que o utilizador se encontra atualmente no âmbito de uma reunião (contexto de ambiente social) e de rejeitar as chamadas que não são urgentes (contexto de tarefa do usuário).

A Consciência do Contexto é um dos conceitos mais estudados e consolidados para o projeto de aplicações pervasivas (MOSTEFAOUI *et al.*, 2004; SILVA *et al.*, 2012). Portanto, no espaço pervasivo, a mobilidade física introduz a possibilidade do movimento dos componentes/entidades durante a execução da aplicação. Enquanto o usuário se movimenta, os recursos acessíveis/disponíveis podem se alterar, não só em função da área de cobertura e heterogeneidade das redes, como em função de sua disponibilidade ser variável no tempo, devido à alta possibilidade de concentração de muitos usuários em um ponto localizado no espaço. Em consequência, a localização corrente do usuário determina o contexto de execução da aplicação (HENRICKSEN *et al.*, 2002).

Dentre as diversas caracterizações sobre contexto que existem atualmente (Schilit *et al.* (1994); Barkhuus (2003); Dey (2001); Hong *et al.* (2009); Mullins *et al.* (2008); Derntl e Hummel (2005) e Baldauf *et al.* (2007)), no es-

copo deste trabalho utilizaremos a definição de Dourish (2004), que classifica o contexto na Computação Ubíqua como: i) Positivista para a visão técnica; e ii) Fenomenologista para a visão social.

2.2.1 Contextos Positivistas

De acordo com Dourish (2004), as teorias positivistas buscam reduzir os fenômenos sociais observados às essências ou modelos simplificados que capturam os padrões subjacentes. Logo, o contexto sob a ótica positivista, é um problema de representação, isto é, questiona como o contexto pode ser codificado e representado pelos sistemas. Para Dey (2001) contexto é "qualquer informação que pode ser usada para caracterizar a situação das entidades". Para Schilit *et al.* (1994) contexto "inclui iluminação, nível de barulho, conectividade de rede, custos de comunicação e a situação social". Para Dourish (2004), contexto diz respeito a tudo aquilo que representa o cenário, o ambiente de uso dos sistemas ubíquos.

As teorias positivistas possuem as seguintes suposições sobre o contexto (DOURISH, 2004):

1. **Contexto é uma forma de informação**. É alguma coisa que pode ser conhecida, logo poderá ser codificada e representada em software;
2. **Contexto é delineável**. Pode-se definir através de um conjunto de aplicações (ou requisitos de aplicação) o que é relevante como contexto das atividades e implementa-las antecipadamente;
3. **Contexto é estável**. Embora os elementos de um contexto possam variar de aplicação para aplicação, elas não variam de instância para instância das atividades ou dos eventos; e
4. **Contexto e atividade são separáveis**. A atividade ocorre dentro de um contexto. O contexto descreve características de um ambiente no qual a atividade ocorre. Logo, uma atividade pode ocorrer em diversos contextos diferentes porque eles (contexto e atividade) não necessitam manter relação para que as atividades aconteçam.

As pesquisas em Computação Ubíqua utilizam a noção de contexto sob alguma das suposições apresentadas anteriormente, demonstrando que o contexto consiste em um conjunto de características do ambiente no qual as atividades são desenvolvidas e que essas características podem ser codificadas e disponibilizadas por sistemas computacionais.

2.2.2 Contextos Fenomenológicos

As teorias fenomenológicas consideram os fatos sociais como propriedades emergentes de interações, que não são previamente dadas, mas sim negociadas e contestadas, e subjacentes aos processos de interpretação e reinterpretação (DOURISH, 2004). Desta forma, o contexto é um problema de interpretação, isto é, demonstra a preocupação com o que realmente é o contexto e como ele pode ser codificado. Dourish (2004) em seu modelo interacional, propõe que, "o contexto não é somente algo que descreve um cenário, é alguma coisa que as pessoas fazem. É uma realização, ao invés de uma observação, um resultado ao invés de uma premissa".

Em conformidade com a teoria fenomenológica, Dourish (2004) apresenta suposições, que discordam da teoria positivista:

1. **Contexto é Relacional:** Contexto é uma propriedade relacional mantida entre objetos e atividades, em que algo pode ou não ser contextualmente relevante;

2. **Contexto é Dinâmico:** O escopo das características contextuais é definido dinamicamente e não delineado e definido antecipadamente;

3. **Contexto é Ocasionado:** Contexto é uma propriedade ocasionada particular para cada cenário, atividade e instância de ação; e

4. **Contexto Emerge da Atividade:** Contexto é ativamente produzido, mantido e desempenhado no curso de uma atividade, logo, contexto e atividade não podem ser separados.

Assim, contexto é caracterizado pela interação. Então, os sistemas baseados em contexto devem utilizar as propriedades de contexto para definir (perceber) o significado de uma atividade que está sendo executada pelo usuário.

Portanto, o contexto emerge nas práticas[1] e nos significados que os usuários dão, na sua interação com os sistemas computacionais. Desta forma, o contexto é o modo em que as ações que são executadas têm significado e tudo aquilo que emerge diante desta experiência, podendo proporcionar novas formas de ação e novos significados (CORSO *et al.*, 2011).

[1] "Prática [...] é um processo em que nós podemos experienciar o mundo e nosso engajamento com ele é significativo" (WENGER, 1999). A prática não é meramente sobre o que as pessoas fazem, mas sobre o que elas experienciam ao fazer. Portanto, o que é crucial para a visão interacional de contexto é ver a prática como um processo dinâmico, que envolve e adapta (DOURISH, 2004)

2.2.3 Contextos: Positivistas ou Fenomenológicos

De acordo com a perspectiva positivista o contexto diz respeito às coisas estáticas, às características do cenário e não depende da ação dos usuários e da interação entre as partes. Na ótica social fenomenológica, contexto diz respeito a agregação das experiências e resultados das práticas incorporadas no uso da tecnologia, permite uma compreensão mais profunda da interação entre usuário e dispositivos que estão imersos em ambientes ubíquos (CORSO *et al.*, 2011). Dessa forma, Dourish (2004) conduz a uma reconsideração do papel do indivíduo e do agente tecnológico no projeto de sistemas ubíquos e interativos e demonstra a preocupação em como a tecnologia é utilizada e incorporada nas práticas.

Com uma ótica fenomenológica, Ciborra e Willcocks (2006) no artigo "*The mind or the heart? It depends on the (definition of) situation*" estabelecem os principais diferenciais entre situacionalidade, ação situada e contexto:

- **Situacionalidade:** refere-se ao indivíduo como um todo, não somente ao "estado mental" do indivíduo e às circunstâncias encontradas, mas também a sua disposição, humor, afetividade e emoção, ou seja, a sua "situação interna". Porém, grande parte dos estudos contemporâneos que utiliza o termo situacionalidade, ainda que com um olhar fenomenológico, acaba por utilizar o mesmo superficialmente, significando na maioria das vezes "contexto" ou "circunstâncias emergentes" de ação e conhecimento (CIBORRA; WILLCOCKS, 2006);

- **Ação Situada:** foi definido por Suchman (1987) como "ações tidas em um contexto particular, circunstâncias concretas [...] as circunstâncias de nossas ações nunca são totalmente antecipadas [...] são essencialmente ad hoc". Logo, as ações não são planos, mas locais de interações com o nosso ambiente, sendo o mundo um inesgotável e rico meio para a ação (SUCHMAN, 1987). De acordo com Ciborra e Willcocks (2006), a definição de ação situada utilizada em diversos estudos permite um olhar de como os sistemas podem lidar com o reconhecimento das circunstâncias locais. Possibilita também perceber e representar as relações sociais, se elas têm um impacto no sistema e produzem respostas apropriadas mesmo para tarefas temporalmente demandadas em ambientes complexos;

- **Contexto:** é definido dinamicamente e vai emergir das atividades executadas pelos indivíduos (Dourish (2004) e Tamminen *et al.* (2004)). O

> Contexto está fortemente relacionado com as interpretações internas e sociais dos usuários (que estão em contínuo estado de transformação e /ou mudanças) quando estes estão executando atividades (TAMMINEN *et al.*, 2004).

Os usuários quando interagem com os aplicativos e serviços de seus dispositivos móveis, envolvem nessa interação os aspectos: racionais, emocionais, estado de espírito, humor e disposição. Todos estes aspectos foram caracterizados por Ciborra e Willcocks (2006) como a situacionalidade. Desta forma, a análise de contexto envolve a situacionalidade do indivíduo (mente e coração) e sua situação no mundo exterior. Portanto, o contexto é gerado pelo significado da interação social entre usuário e os serviços de seu *smartphone*, onde os aspectos socias do indivíduo formam a sua situacionalidade e a interação é a execução de uma atividade através de uma ação situada.

De acordo com Corso *et al.* (2011), a visão fenomenológica possibilita uma melhor compreensão sobre o conceito de contexto, pois permite ver o indivíduo não apenas "onde está", mas sim "como age" e "como sente" durante a interação. Dessa forma, a caracterização da interação, ação situada e situacionalidade formam um arcabouço teórico que define as características e relações dos indivíduos imersos em um contexto.

O modelo de contexto utilizado neste trabalho possui suas bases na Teoria da Atividade, conforme seção 2.3.1. Na próxima seção serão apresentados os conceitos sobre Cognição Situada e as suas relações com os modelos de contexto utilizados na Computação Pervasiva.

2.3 COGNIÇÃO SITUADA

A Cognição Situada (CLANCEY, 1997) é tratada através de outras abordagens, tais como: Ecologia da Mente (BATESON; BATESON, 1972); Enactive View (VARELA *et al.*, 1992); e Biologia do Conhecer (MATURANA; VARELA, 2001). Todas elas tem como ideia central que um indivíduo existe enquanto ser dentro de um ambiente. Isso mostra que a cognição de um ser não se dá de maneira dissociada do meio em que esse ser está inserido. O indivíduo e o meio atuam de maneira inseparável.

Conforme Maturana e Varela (2001) relatam em seu livro "A Árvore do Conhecimento", os seres vivos devem ser tratados como um sistema de informações fechado e determinado estruturalmente. Sendo que o caráter determinado significa, nesse cenário, que nenhum fator externo pode alterar a estrutura do sistema. Caso um agente externo necessite interagir com um

sistema dessa natureza, as mudanças propostas pelo agente só irão afetar o sistema se o próprio sistema assim o desejar. Essa proposição vai de encontro às correntes dominantes da área de Ciências da Cognição, as quais definem o indivíduo como sendo um sistema aberto, que recebe estímulos, trata-os e gera uma saída. Trata-se de uma visão simplista, que desconsidera a situação onde a cognição é gerada.

Pode-se, então, observar que o determinismo estrutural define que o ser vivo e o meio ambiente se relacionam, sendo que o segundo sempre sofre uma ação de mudança estrutural do primeiro. Esse relacionamento, continuará a existir enquanto for harmônico para ambas as partes. Dessa forma, a relação entre o indivíduo e o meio se dá em uma via de mão dupla, onde tanto o ser vivo pode interferir no meio, quanto o meio pode alterar a estrutura do ser.

As mudanças estruturais de um meio ambiente e dos organismos nele inserido, quando comparadas ao longo do tempo, mostram um sincronismo. O passado de organismos e seus sistemas está condicionado às escolhas de quais mudanças estruturais cada um deles se permitiu aceitar.

A Cognição Situada define que todo ato cognitivo é um ato de experiência, e, portanto, situado, resultante do acoplamento estrutural e da interação harmônica do organismo em seu ambiente. A cognição não é, portanto, a representação de um mundo pré-concebido, cujas características podem ser especificadas antes de qualquer atividade cognitiva. Ao contrário, é ação incorporada "... é a atuação de um mundo com base em uma história da diversidade de ações desempenhadas por um ser no mundo" (VARELA *et al.*, 1992).

De acordo com Lave e Wenger (1991) na Cognição Situada, "o conhecimento é inseparável dos contextos e das atividades nos quais se desenvolve". Os contextos (por exemplo: físico e social) nos quais a atividade acontece constituem elementos que integram a atividade. Portanto, a situação (conjunto de contextos) na qual um usuário esta imerso é parte fundamental de como ele constrói um conjunto particular de conhecimentos e habilidades para a execução das suas atividades. Os contextos físicos e sociais são a base para o desenvolvimento de aplicações adaptáveis (sensíveis ao contexto) da Computação Ubíqua, apresentada na seção 2.1.

Para Maturana e Varela (2001), o organismo e o ambiente constituem uma unidade inseparável, não existe um organismo fora de seu nicho ecológico e nem nicho ecológico sem qualquer dos organismo que o compõe. Fialho (2011) observa que "a Cognição Situada rejeita a dicotomia sujeito–objeto. A realidade é vista como algo que depende do seu observador. É o próprio ser humano que constrói o seu mundo. O princípio epistemológico

fundamental é quanto à existência de um organismo–em–seu–ambiente, um ser aí, no mundo, como defendem os adeptos da fenomenologia".

Fialho (2011) em seu livro "Psicologia das Atividades Mentais: introdução às ciências da cognição" faz a conexão entre a Cognição Situada e a Teoria Sociointeracionista de Vygotski *et al.* (2005), onde resume esta teoria como ".. o conhecimento é construído pela interação efetiva com o mundo objetivo onde o social constitui um novo fator às representações mentais". Rego (2008) relata que os estudos de Vygotski sobre aprendizado decorrem da compreensão do homem como um ser que se forma em contato com a sociedade e cita que "na ausência do outro, o homem não se constrói homem"[2]. Com a estrutura formalizada, a Teoria da Atividade demonstrou a ênfase que a teoria sempre deu às interações propositais do sujeito com o mundo e as interações no rico ambiente dos contextos socioculturais.

2.3.1 Teoria da Atividade

Conforme Bessa (2008), a Teoria da Atividade tem como base o trabalho do advogado e psicólogo bielorrusso Lev Semenovitch Vygotski, que pesquisou as influências culturais e históricas no desenvolvimento cognitivo das crianças e nos processos cognitivos em geral. De acordo com Kaptelinin e Nardi (2006), Vygotski chamou estas influências de mediação porque ocorrem com o uso de: i) ferramentas; ii) instrumentos, e iii) artefatos físicos. Ele argumenta que o uso de tais mediadores "muda a estrutura da atividade" porque eles são "internalizados" através de comunicação interpessoal e através de elaborações individuais dos diferentes aspectos que compreendem uma atividade específica.

De acordo com Bannon e Bødker (1989), a Teoria da Atividade é um *Framework* psicológico descritivo que ajuda a entender a consciência e a atividade através de um conjunto de princípios básicos, que incluem:

- **Hierarquia da atividade.** Atividades (a categoria mais alta) são compostas de ações dirigidas a objetivos. Essas ações são realizadas de forma consciente. Ações, por sua vez, consistem em operações não conscientes. A hierarquia da atividade, seus componentes, são apresentados na Figura 2;

- **Orientação a objetivos.** Objetivos são propriedades social ou cultu-

[2]Similar ao provérbio africano: "Uma pessoa só é uma pessoa por causa das outras pessoas" - sugestão do Prof. Luiz Antônio Moro Palazzo na defesa de qualificação deste trabalho.

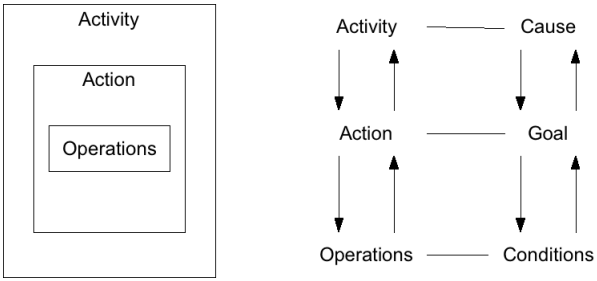


Figura 2: Estrutura Hierárquica da Atividade

ralmente definidas. A forma de fazer o trabalho baseia-se em uma praxis que é compartilhada pelos colegas de trabalho e determinadas pela tradição. A forma como um artefato é usado e a divisão de trabalho influenciam os objetivos;

- **Mediação.** A atividade humana é mediada por artefatos externos (martelo, caneta, computador e outros) e internos (conceitos, linguagem e outros). O uso de artefatos, culturalmente desenvolvidos, modela a forma como as pessoas agem e, através do processo de internalização, influencia a natureza do desenvolvimento mental;

- **Desenvolvimento contínuo.** Os artefatos utilizados e as atividades são reformulados constantemente. Os artefatos refletem conhecimento social acumulado, assim eles transportam a história social de uma atividade para o usuário;

- **Distinção entre as atividades internas e externas.** Os processos mentais são derivados de ações externas através do curso da internalização. Sendo que a internalização é o processo de absorção de informações que ocorre a partir do contato com o ambiente em que o indivíduo está inserido. A externalização é o processo inverso, manifestado através de atos do sujeito.

Portanto, a noção básica da Teoria da Atividade é que o sujeito ao participar de uma atividade, assim o faz porque deseja atingir um determinado objetivo. O interesse está dirigido para o objeto de uma atividade que ele deseja usar e/ou modificar para alcançar um resultado esperado. Sua interação com este objeto é mediada por ferramentas, criando o triângulo básico de "sujeito", "objeto", e mediação por "artefato", que são apresentados na Figura 3.

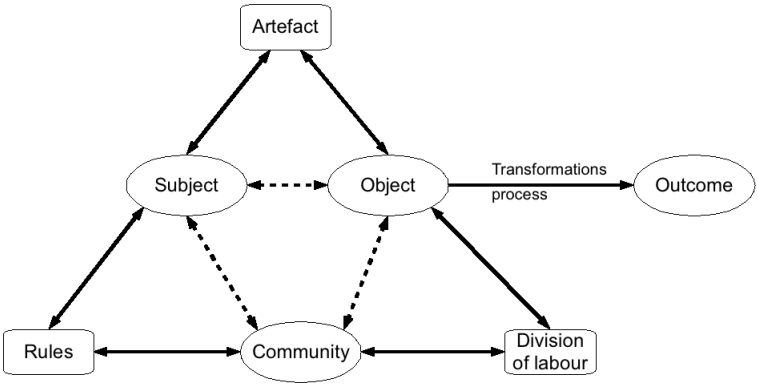


Figura 3: Teoria da Atividade Histórico Cultural (TAHC) expandida.
Fonte: Kuutti (1996)

De acordo com Bessa (2008):

> *A atividade é transformada na unidade básica de análise e o meio mais importante para o desenvolvimento do sujeito e do objeto. Logo, o modelo mais básico da Teoria da Atividade já oferece uma abordagem sólida para a tarefa de compreender a interação do ser humano com o mundo.*
> *Kuutti (1996), argumenta que ao incluir "um contexto significativo mínimo" na análise da atividade de um sujeito, na Teoria da Atividade oferece um modelo capaz de levar em conta o fato de que os indivíduos participam em diversas atividades simultaneamente, e de que cada atividade "contem diversos artefatos (por exemplo, instrumentos, sinais, procedimentos, máquinas, métodos, leis, formas de organização do trabalho e outros.)". Ele também argumenta que cada artefato é ferramenta da negociação e ao mesmo tempo algo limitador, e algo que abre novas possibilidades, e que toda análise sistemática das relações entre um sujeito e seu meio ambiente precisa incluir também a comunidade formada por todos aquelas que compartilham do mesmo objetivo, isto é, as comunidades de prática definidas por Lave e Wenger (1991).*

A abordagem de Kuutti (1996) sobre a Teoria da Atividade se fundamenta em três relacionamentos:

- relacionamentos sujeito-objeto mediados por ferramentas e por artefatos;
- relacionamentos sujeito-comunidade mediados por regras; e
- relacionamentos objeto-comunidade mediados pela divisão de trabalho.

Como o sujeito é parte ativa de uma comunidade e essa possui atividades sociais, as relações entre o sujeito e a comunidade, bem como entre a comunidade e o objeto, são mediados por um conjunto de regras e através da divisão do trabalho, pois o resultado desejado está previsto para ser compartilhado pela comunidade.

De acordo com Kuutti (1996), esse modelo expandido, incluindo um componente de comunidade e de outros mediadores, é comumente referido como Teoria da Atividade Histórico Cultural (TAHC) e é representado no triângulo mostrado na Figura 3.

A inclusão do polo "comunidade" na Teoria da Atividade permitiu o estudo dos contextos socioculturais e das interações entre pessoas e dispositivos computacionais, *smartphones*, telefones celulares e outros artefatos desenvolvidos com os princípios da Computação Pervasiva.

2.3.2 Modelo Sensível a Contexto Baseado na Teoria da Atividade

A Teoria da Atividade é um importante referencial teórico para auxiliar a explicitação dos componentes que formam o conhecimento contextual a ser incorporado aos sistemas pervasivos. De acordo com Kofod-Petersen e Cassens (2006), os componentes da Teoria da Atividade podem ser relacionados com a Taxonomia de conhecimento contextual, conforme o Quadro 1.

Os aspectos da TAHC foram mapeados de forma flexível, permitindo que dois ou mais aspectos participem da mesma categoria de contexto. A visão sobre o conhecimento contextual é embasada na premissa que existem diferentes interpretações, isto é, a informação contextual em uma configuração pode ser considerada como parte do modelo de conhecimento, em outro configuração como o próprio modelo de conhecimento. Esta flexibilidade permite aos projetistas de sistemas pervasivos, se concentrarem nos aspectos do nível de conhecimento, no lugar de modelar detalhes irrelevantes.

A taxonomia de contexto proposta por Kofod-Petersen e Mikalsen (2005), possui uma visão pragmática de artefatos de construção e incorpora

Aspecto TAHC	Categoria
Assunto	Contexto Pessoal
Objeto	Contexto Tarefa
Comunidade	Contexto Espaço-temporal
Mediação de Artefatos	Contexto Ambiental
Mediação de Regras de Mediação	Contexto Tarefa
Mediação de Divisão de Trabalho	Contexto Social

Quadro 1: Aspectos Básicos de uma Atividade e sua Relação com a Taxonomia do conhecimento Contextual.
Fonte: Kofod-Petersen e Cassens (2006)

aos sistemas sensíveis ao contexto, os conceitos gerais encontrados na Teoria da Atividade, conforme Figura 4. Esta taxonomia divide contexto em cinco sub-categorias:

- Contexto Pessoal: descreve as informações físicas e mentais sobre o usuário, tais como: experiência, características físicas (altura, peso, sexo e outras), humor e deficiências (físicas e mentais).
- Contexto Social: descreve os aspectos sociais do usuário, como os diferentes papéis que o usuário pode assumir.
- Contexto Espaço-Temporal: considera as informações relativas à localização, data e a comunidade presente.
- Contexto de Tarefas: descrever o que o usuário está fazendo, quais os objetivos: do usuário, das tarefas e das atividades.
- Contexto Ambiental: captura as situações que cercam o usuário, como serviços, pessoas e informações acessadas pelo usuário.

A especificação dos demais componentes da taxonomia de contexto são apresentados na Figura 13. Esta taxonomia será utilizada pelo sistema autenticação proposto para armazenar as informações contextuais dos usuários, artefatos e atividades que compõem o cenário da autenticação implícita.

2.4 MODELAGEM COGNITIVA

A modelagem do processo cognitivo consiste em se passar de uma descrição dos processos cognitivos feita na linguagem da teoria psicológica,

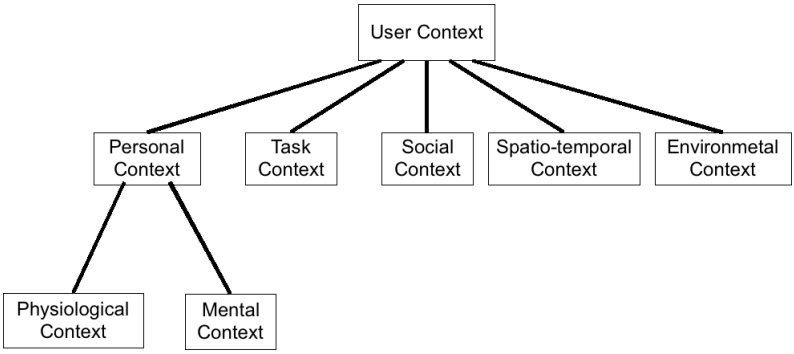


Figura 4: Taxonomia de Contexto.
Fonte: Kofod-Petersen e Mikalsen (2005)

para uma descrição em uma linguagem formal que permita fazer cálculos ou simulações.

Conforme Fialho (2011) a modelagem cognitiva pode apenas se desenvolver sob duas condições:

- precisa dispor de formalismos adequados;
- precisa ter explicitada a descrição dos processos psicológicos em um nível de precisão suficiente para que esta descrição seja completa, sem necessidade de elementos adicionais, para permitir engendrar comportamentos simulados, que se possa comparar aos comportamentos observados.

Dentre os diversos tipos de modelos existentes, os modelos computacionais possuem um formalismo adequado e flexível que conseguem expressar de forma clara os raciocínios formais e não formalizados. A expressão dos conhecimentos sob a forma de esquemas e/ou redes semânticas são exemplos desse formalismo, geralmente realizado por profissionais de computação auxiliados por psicólogos, e tornam-se ferramentas muito mais ricas na modelagem de processo (FIALHO, 2011).

Dentre as diversas arquiteturas cognitivas existentes, nesta Tese será utilizada a arquitetura cognitiva definida no artigo "*Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models*" (RASMUSSEN, 1983), apresentado na seção 2.4.2, e posteriormente completada através do seu Projeto de Interface Ecológico (VICENTE; RASMUSSEN, 1992) que será apresentada na seção 2.4.1.

2.4.1 Arquitetura Cognitiva

Os rápidos avanços em tecnologias, juntamente com demandas econômicas têm levado a um aumento considerável da complexidade de sistemas de engenharia. Como resultado, torna-se difícil para os projetistas anteciparem os eventos que podem ocorrer dentro destes sistemas. Eventos imprevistos, por definição, não podem ser especificados com antecedência e, portanto, não podem ser evitados por meio de treinamento, procedimentos ou automação. Um sistema sociotécnico complexo, concebido com base exclusivamente em cenários conhecidos, freqüentemente perde a flexibilidade para suportar eventos imprevistos (VICENTE, 2001).

A segurança do sistema é, muitas vezes, comprometida pela incapacidade do usuário de se adaptar às situações novas e desconhecidas (VICENTE; RASMUSSEN, 1992). O *Ecological interface design* - Projeto de interface ecológica (EID) tenta fornecer aos usuários as ferramentas e as informações necessárias para torná-los solucionadores de problemas ativos ao invés de monitores passivos, especialmente durante o desenvolvimento de eventos imprevistos.

EID é uma abordagem para o projeto de interface que foi introduzida especificamente para modelar sistemas sociotécnicos complexos, dinâmicos e de tempo real. Tem sido aplicada em uma variedade de domínios, incluindo o controle do processo (por exemplo, usinas nucleares, petroquímicas), aviação e medicina (VICENTE; RASMUSSEN, 1992). Atualmente, esta abordagem esta sendo utilizado no desenvolvimento de jogos eletrônicos e simuladores (LIN *et al.*, 2011) e no tratamento de eventos em sistemas pervasivos (FERRY *et al.*, 2010).

A metodologia de projeto EID tem como foco a análise sobre o domínio do trabalho ou sobre o ambiente. Já outras metodologias como *User-Centered Design* - Projeto Centrado no Usuário (UCD), tem seu foco no usuário final ou em uma tarefa específica.

O objetivo do EID é fazer com que as relações restritivas e de complexidade do ambiente de trabalho sejam evidentes perceptualmente para o usuário, por meio de, por exemplo, sinais visuais e auditivos. Isso permite que mais recursos cognitivos do usuário possam ser dedicados aos processos cognitivos mais elevados e complexos, tais como a resolução de problemas e tomada de decisão. De acordo com Vicente (2001), o EID é baseada em dois conceitos chaves de Engenharia Cognitiva:

- *Abstraction Hierarchy* - Hierarquia de Abstração (AH) - é uma de-

composição funcional de 5 níveis utilizada para modelar o ambiente de trabalho, ou mais comumente referido como o domínio de trabalho. Utilizada para determinar que tipo de informação deve ser exibida na interface do sistema e como as informações devem ser organizadas; e

- *Skills, Rules, Knowledge framework* - *Framework* de Habilidades, Regras e Conhecimento (SRK) - define três tipos de comportamento ou processos psicológicos presentes no processamento de informações do usuário. O SRK foi desenvolvido por Rasmussen (1983) para auxiliar os projetistas na combinação dos aspectos da cognição humana com os requisitos de informação de um sistema.

Neste trabalho, será utilizado o SRK para definição da arquitetura de processamento da autenticação implícita. O modelo de dados e os contextos participantes utilizam os conceitos da Teoria da Atividade, que foram expandidos por Cassens e Kofod-Petersen (2006) para ambientes sensíveis ao contexto.

2.4.2 *Framework* Habilidades, Regras e Conhecimentos

O *framework* das Habilidades, Regras e Conhecimento (ou taxonomia SRK como às vezes é chamado) é um método de medir o desempenho cognitivo humano e determinar em que nível as tarefas cognitivas específicas e atividades estão sendo realizadas. Desenvolvido por Rasmussen (1983), define o comportamento em três níveis distintos: habilidades, regras e baseadas no conhecimento. Ele também fornece informações sobre os tipos de cognição humana envolvidos em cada etapa.

Os componentes que formam a Figura 5 são descritos a seguir de acordo com as especificações e exemplos definidos por Rasmussen (1983).

- **Comportamento Baseado em habilidades** é uma atividade ou tarefa que, para um indivíduo, é um comportamento rotineiro. A tarefa ou atividade é realizada com padrões automatizados e altamente integrado ao comportamento, sem que o usuário coloque uma quantidade significativa de percepção ou consciência para a execução da tarefa ou da atividade, ela pode ser considerada quase como instintiva na natureza. Um exemplo bastante comum de um comportamento baseado em habilidade é andar de bicicleta ou dirigir um carro. Estas são tarefas que os indivíduos experientes podem realizar sem focar muito claramente sobre o que eles estão realmente fazendo. Em vez disso, durante um com-

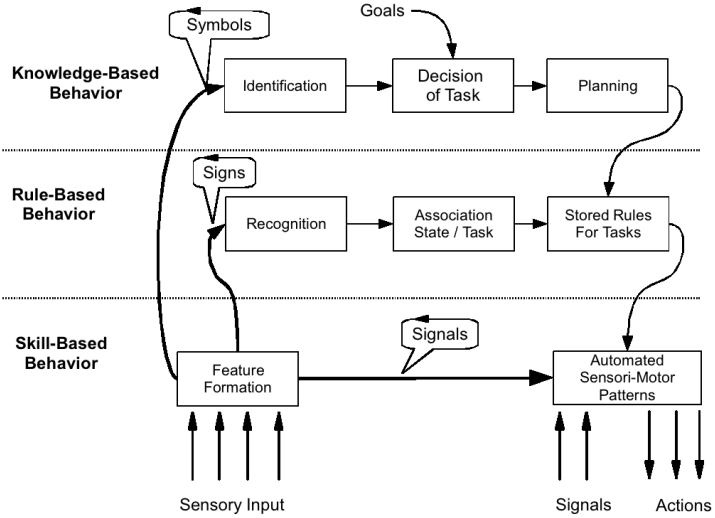


Figura 5: ***Framework*** **Habilidades, Regras e Conhecimentos.**
Fonte: Rasmussen (1983)

portamento baseado em habilidade, os sentidos de um indivíduo estão focados e inconscientemente mantendo-se orientados e informando-os sobre as mudanças no ambiente; assim, processos internos podem detectar obstruções de estradas ao dirigir um veículo ou uma bicicleta.

- **Comportamento Baseado em regras** é semelhante ao baseado em habilidades, no que se refere às ações que estão sendo tomadas para concluir a tarefa, as quais, normalmente, são rotinas para uma pessoa experiente. No entanto, existem controles adicionais e novas rotinas são elaboradas em conjunto, requer mais esforço cognitivo e consciência de que serão utilizadas para completar uma tarefa ou uma ação. O comportamento baseado em regras é guiado por:

  – uma regra de procedimento armazenado;

  – derivação empírica de relatos comunicados por outra pessoa, como por exemplo: instruções, noções transmitidas e lições; ou

  – sucessos anteriores na resolução de problemas e planejamento similares.

Um exemplo do comportamento baseado em regras são as ações complementares à rotina de dirigir um carro por indivíduos experientes. Estas ações complementares podem ser: a troca de pistas em uma estrada, parar em semáforos ou executar uma ultrapassagem. Todas estas ações são abrangidas pelo comportamento Baseado em regras, devido ao esforço adicional cognitivo e à consciência necessária para concluir com êxito as ações e as tarefas.

- **Comportamento Baseado no conhecimento** ocorre principalmente quando a atividade que está sendo envolvida em uma tarefa de um indivíduo nunca ocorreu anteriormente. O sistema cognitivo esgotou todas as suas opções de resolução do problemas através de rotinas baseadas em habilidades ou baseadas em regras. Portanto, terá que usar o processamento lento, sequencial, trabalhoso e de limitados recursos de consciência. Em outras palavras, o indivíduo tem que, mentalmente ou fisicamente, pesquisar e experimentar para encontrar a melhor maneira de completar uma tarefa ou alcançar um objetivo particular. Um exemplo do comportamento baseado em conhecimento é o de um motorista experiente que pode ser capaz de dirigir um carro com pouco esforço através do tráfego e realizar um planejamento consciente, a fim de viajar com sucesso a partir do ponto A para o ponto B. A meta teria de ser estabelecida, com base na análise do ambiente e os objetivos que o indivíduo possui, ele também precisará desenvolver um plano, que pode ser por tentativa e erro ou mais conceitualmente através da compreensão das propriedades funcionais do ambiente, em adição aos resultados previstos do plano formulado.

- **Sinais** são os dados coletados sem tratamento, diretamente do ambiente físico dentro de um domínio espaço-tempo. Os sinais ajudam a garantir que os padrões automáticos de comportamento ocorram no nível baseado em habilidades. Um exemplo de sinais é a percepção de dados ambientais durante um passeio de bicicleta.

- **Signos** são as informações percebidas no nível baseado em regras, e servem para ativar, modificar ou manipular ações predeterminadas. O comportamento baseado em regras é geralmente guiado por procedimentos que tenham ocorrido anteriormente com o indivíduo. No entanto, os signos são limitados à seleção ou modificação do controle das regras. Contudo, eles não participam da resolução de problemas.

- **Símbolos** são informações percebidas no nível baseado no conheci-

mento e são relacionados com construções abstratas e definidos por uma estrutura formal de relações e processos. Os símbolos são utilizados na resolução de problemas e processos de raciocínio mental realizados quando o indivíduo se depara com uma situação estranha, uma situação não familiar.

O *Framework* SRK é utilizado no contexto deste trabalho para caracterizar os dispositivos móveis como artefatos cognitivos de interação e mediação com os usuários. Esta interação se estabelece nos níveis de habilidade e regras com o usuário. Demais informações relativas ao uso do SRK estão na seção 4.5.

2.5 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foram apresentados os referenciais teóricos desta Tese. Porém é importante ressaltar alguns conceitos e definições que serão utilizados durante este trabalho:

- **Computação Móvel**: é um paradigma de computação, no qual se explica a conectividade de dispositivos, que se deslocam em torno de um mundo físico a todo instante. A computação móvel baseia-se no aumento da nossa capacidade de deslocamento utilizando serviços computacionais, ou seja, o computador torna-se um dispositivo sempre presente, que expande a capacidade de um usuário na utilização de serviços computacionais, independentemente de sua localização;
- **Computação Pervasiva**: significa que o computador está embarcado no ambiente de forma invisível para o usuário. Nesta concepção, o computador tem a capacidade de obter informação do ambiente no qual ele está embarcado e utilizá-la para, dinamicamente, construir modelos computacionais, ou seja, controlar, configurar e ajustar as aplicações para melhor atender as necessidades dos dispositivos ou do usuário;
- **Computação Ubíqua**: é o conceito no qual os pequenos dispositivos computacionais distribuídos e integrados, dispostos em diversos ambientes, fornecem serviços e informações a qualquer momento, em qualquer local;
- **Contexto**: é o conceito que emerge nas práticas e nos significados que os usuários dão, na sua interação com os sistemas computacionais ubíquos. Em outras palavras, o contexto é o modo em que as ações que

são executadas têm significado e tudo aquilo que emerge diante desta experiência, pode proporcionar novas formas de ação e novos significados;

- **Cognição Situada**: é um ato de experiência, e, portanto, situado, resultante do acoplamento estrutural e da interação harmônica do organismo em seu ambiente. A cognição não é, portanto, a representação de um mundo pré-concebido, cujas características podem ser especificadas antes de qualquer atividade cognitiva. Ao contrário, é ação incorporada "... é a atuação de um mundo com base em uma história da diversidade de ações desempenhadas por um ser no mundo" (VARELA *et al.*, 1992);

- **Modelos Computacionais**: são os modelos que possuem um formalismo adequado e flexível que conseguem expressar de forma clara os raciocínios formais e não formalizados. A expressão dos conhecimentos sob a forma de esquemas e/ou redes semânticas são exemplos desse formalismo, geralmente realizado por profissionais de computação, auxiliados por psicólogos e tornam-se ferramentas muito mais ricas na modelagem de processo (FIALHO, 2011).

3 AUTENTICAÇÃO E SISTEMA DE RECOMENDAÇÃO

Neste capítulo é realizada uma revisão do processo de autenticação, com um enfoque na autenticação para dispositivos móveis, onde são apresentados os conceitos atualizados de biometria e uma série de trabalhos correlatos que possuem o foco na autenticação por dados biométricos. Como principal contribuição deste capítulo é apresentada uma análise comparativa entre os demais trabalhos que possuem abordagens relacionadas à autenticação sensível ao contexto, orientada ao comportamento do usuário. Ao final são abordadas as características dos sistemas de recomendação, com foco nos sistemas de recomendação sensíveis ao contexto, que são utilizadas nos dispositivos móveis.

3.1 PROCESSO DE AUTENTICAÇÃO

A definição do termo autenticação encontrada nos dicionários, reconhecer e certificar, nos remete a duas ações que são distintas e complementares: só é possível certificar algo (objeto ou pessoa), se este for anteriormente reconhecido. Porém, estes processos de reconhecimento e certificação são influenciados pela área de aplicação. Por exemplo: no direito - o reconhecimento de um fato é realizado através de comprovação documental ou prova testemunhal; na segurança da informação - reconhecer uma pessoa é realizado pela prova de sua identidade ou pela similaridade de suas propriedades (peso, altura, idade, nome da mãe, dados biométricos da mão e outros). Logo, conclui-se que as ações (reconhecer e certificar) são as mesmas, porém os processos utilizados por cada área são diferentes devido à natureza de estudo da área.

No escopo deste trabalho, o processo da autenticação será especificado de acordo com a área de Segurança da Informação. Nessa área, existe o Protocolo de Autenticação, Autorização e Auditoria (AAA) que é uma referência aos protocolos relacionados com os procedimentos de autenticação, autorização e auditoria (ABOBA *et al.*, 2000). A autenticação verifica a identidade digital do usuário de um sistema, a autorização garante que um usuário autenticado somente tenha acesso aos recursos autorizados e, por fim, a auditoria refere-se às informações sobre o uso dos recursos de um sistema pelos seus usuários (ABOBA *et al.*, 2000). Na figura 6 é apresentado os principais processos e mecanismos do AAA, que serão discutidos nas próximas seções.

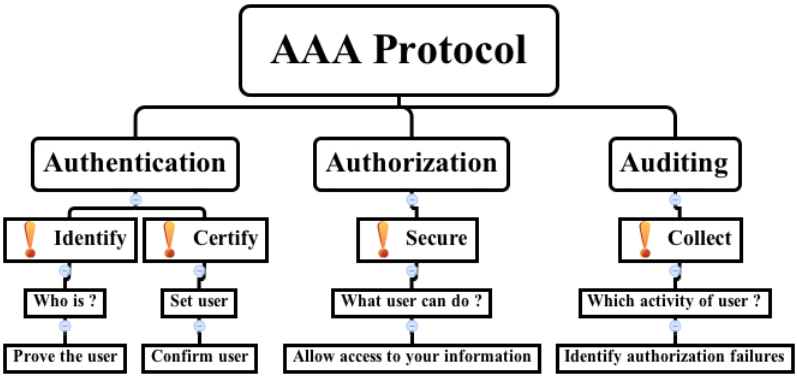


Figura 6: Esquema do Protocolo AAA - Autenticação, Autorização e Auditoria

3.1.1 Autenticação

A autenticação é o meio para obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser. É um serviço essencial de segurança, pois uma autenticação confiável assegura o controle de acesso, determina quem está autorizado a ter acesso à informação, permite trilhas de auditoria e assegura a legitimidade do acesso.

A autenticação é composta pelos processos de reconhecimento e certificação. Durante o reconhecimento, o usuário informa ao sistema quem ele é (geralmente, através de um nome de usuário). A sua identidade é verificada através de um ou mais fatores de autenticação (credenciais).

Em Segurança da Informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema de computação, normalmente, no momento em que ele requisita o acesso (*logon*) a um programa, serviço ou computador. A autenticação normalmente depende de uma ou mais credenciais (geralmente, senha).

3.1.1.1 Fatores de autenticação

Os fatores de autenticação para usuários são normalmente classificados em três casos:

- Identificação biométrica - quem o usuário é, por exemplo: impressão digital, padrão retinal, sequência de DNA, padrão de voz, reconhecimento de assinatura ou qualquer outro meio biométrico;

- Identificação proprietária - o que o usuário possui, por exemplo: cartão de identificação, *token* SecurID, ou telefone celular;

- Identificação positiva - o que o usuário conhece, por exemplo: senha, frase de segurança ou Número de Identificação Pessoal (PIN).

Em redes de computadores privadas e públicas, a autenticação é comumente feita através do uso de identificação (*logon*) e senhas. O conhecimento da senha é assumido para garantir que o usuário é autêntico. Cada usuário se registra inicialmente (ou é registrado por outra pessoa), usando uma senha atribuída ou auto-declarada. Em cada uso subsequente, o usuário deve conhecer e usar a senha previamente declarada. O ponto fraco deste sistema é que as senhas podem ser furtadas ou, acidentalmente, reveladas ou esquecidas. Por esta razão, as empresas, em especial as de Internet, requerem um processo de autenticação mais rigoroso. Exigem que o usuário utilize pelo menos 2 fatores de verificação (credenciais).

3.1.2 Autorização

A autorização é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas Listas de Controle de Acessos (ACL), definindo quais atividades poderão ser realizadas, gerando assim os chamados perfis de acesso.

A autorização define quais direitos e permissões tem o usuário do sistema. Após o usuário ser autenticado, o processo de autorização determina, através das ACL, o que ele pode fazer no sistema.

Definir direitos de acesso, individualmente, para cada usuário e/ou objeto pode ser trabalhoso quando estiverem envolvidas grandes quantidades de usuários e objetos. A forma mais comum de definição de direitos de acesso, nesse caso, é a matriz de controle de acesso. Nessa matriz pode-se fazer duas análises: i) em relação aos usuários; e ii) em relação aos objetos.

Na primeira abordagem, cada usuário recebe uma permissão que define todos os seus direitos de acesso. As permissões de acesso são, então, atributos, associados a um usuário ou objeto, que definem o que ele pode ou não fazer com outros objetos. Essa abordagem, no entanto, é pouco utilizada,

já que, na prática, com grandes quantidades de usuários e objetos, a visualização exata de quem tem acesso a um determinado objeto não é tão clara, comprometendo, assim, a gerência de controle de acesso. Na segunda abordagem, os direitos de acesso são armazenados com o próprio objeto formando a chamada ACL.

Enquanto a permissão de acesso define o que um objeto pode ou não fazer com outros, a lista de controle de acesso define o que os outros objetos ou usuários podem fazer com o objeto a ela associado. As ACLs são bases de dados, associadas a um objeto, que descrevem os relacionamentos entre aquele objeto e outros, constituindo-se em um mecanismo de garantia de confidencialidade e integridade de dados.

De acordo com TCU (2007), a definição das listas de controle de acesso deve ser realizada pelos proprietários dos recursos, os quais determinam o tipo de proteção adequada a cada recurso e quem efetivamente terá acesso a eles.

Em Segurança da Informação, a autorização é o mecanismo responsável por garantir que apenas usuários autorizados acessem os recursos protegidos de um sistema computacional. Os recursos incluem arquivos, programas de computador, dispositivos de hardware e serviços disponibilizados por aplicações instaladas em um sistema.

O processo de autorização inicia, após um usuário ser autenticado. Desta forma, o sistema de autorização verifica se foi concedida permissão para o uso de determinado recurso. As permissões são normalmente definidas por um administrador do sistema na forma de políticas de segurança, normalmente através de ACL. Com base nos privilégios informados na lista, os usuários terão permissão apenas para acessar os recursos necessários para realizar a sua tarefa.

Existem usuários definidos como anônimos ou convidados, que não necessitam passar pelo processo de autenticação. Normalmente, este tipo de usuário possui permissões restritas. Em sistemas de computação distribuído é conveniente liberar acesso a algumas informações ou subsistemas sem a necessidade de fornecimento de uma identidade única.

Os sistemas de computação que trabalham em rede, normalmente, permitem a existência de usuários que são considerados confiáveis, isto é, usuários que foram autenticados por outro sistema de autenticação previamente registrados. Estes usuários têm acesso regulados pela ACL e se diferenciam dos demais usuários, devido à utilização de um mecanismo externo de autenticação.

3.1.3 Auditoria

A auditoria (*accounting*) é o processo de coleta da informação relacionada à utilização, pelos usuários, dos recursos de um sistema. Estas informações podem ser utilizadas para gerenciamento, planejamento, detecção de invasões e outras atividades de monitoramento. As informações que são tipicamente relacionadas com este processo são a identidade do usuário, a natureza do serviço entregue, o momento em que o serviço se inicia e o momento do seu término.

A auditoria em Segurança da Informação tem o papel de assegurar a qualidade da informação e participar do processo de garantia quanto a possíveis e indesejáveis problemas de falha humana. Com dados concentrados em formato digital e procedimentos invisíveis devido à automação, os sistemas de informação são vulneráveis à destruição, abuso, alteração, erro, fraude e à falhas de programas e equipamentos. Os sistemas on-line e os que utilizam a Internet são os mais vulneráveis, pois seus dados e arquivos podem ser acessados através de diversos pontos de rede (TCU, 2007).

As vulnerabilidades dos sistemas para Internet são, normalmente, exploradas pelos: i) *Crackers*[1] que invadem as redes e causam sérios danos ao sistema e às informações armazenadas, ii) Vírus de computador que podem se propagar rapidamente invadindo os sistemas computacionais e iii) Programas de computadores que apresentam problemas.

3.2 AUTENTICAÇÃO EM DISPOSITÍVOS MÓVEIS

Com a popularização dos dispositivos móveis (*smartphones*, *tablets*), há uma migração dos usuários para o ambiente de computação móvel e pervasiva. Os usuários usam esses dispositivos para armazenar e acessar informações importantes (e.g. serviços bancários, redes sociais, mensagens eletrônicas e transações comerciais). Logo, existe um aumento contínuo e rápido de aplicações e serviços *online*, que resulta em um aumento na demanda por novos métodos de autenticação específicos para o ambiente pervasivo.

Esses novos métodos de autenticação, devem prever que os dispositivos móveis, na sua maioria, possuem tamanho reduzido, gerando dificuldades no processo de interação para digitação de senhas alfanuméricas, o que leva os

[1] É o termo usado para designar o indivíduo que pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal.

usuários a escolherem senhas menores e mais fáceis de memorizar, portanto, mais fáceis de serem quebradas por terceiros. Deve-se considerar também que esses dispositivos portáteis podem ser facilmente perdidos, furtados ou utilizados por usuários diferentes possibilitando, assim, que informações de caráter sigiloso fiquem disponíveis e possam ser roubadas ou disseminadas sem autorização.

No ambiente pervasivo, o processo de autenticação torna-se essencial, já que as políticas de segurança permitem que um **segundo fator de validação** de usuário possa ser utilizada de forma complementar à tradicional senha alfanumérica, aumentando a segurança e a sensação de confiança dos usuários. Esta prática já é usual nas empresas e está lentamente entrando no mercado consumidor, mas ainda tem problemas com a usabilidade e custos a serem superados.

De acordo com Furnell *et al.* (2008), uma alternativa seria a utilização de *tokens* SecurID que é um dispositivo para autenticação similar a um *pen drive*, utilizado como um mecanismo de autenticação na computação baseada em *Desktops*. Porém esta alternativa não pode ser considerada no ambiente pervasivo porque:

- os usuários não querem utilizar mais um dispositivo somente para autenticação, isto entra em conflito com a nova tendência mundial de integração dos atuais dispositivos separados (*media players*, *e-readers*, dispositivos de acesso à Internet e telefones celulares);

- os usuários demandam um processo de autenticação mais integrado, tornando assim a autenticação uma experiência mais segura e confiável.

Nesta Tese, os conceitos de autenticação implícita são implementados através da utilização de um segundo fator de cerificação. A autenticação implícita proposta atua integrada a uma abordagem que utiliza as observações do comportamento do usuário como segundo fator para consolidação do processo de autenticação. O estudo do comportamento dos usuários, revela que estes possuem rotinas diárias, semanais e mensais que formam um conjunto de hábitos[2], executados regular e frequentemente.

[2]De acordo com Duhigg (2012) a maioria das escolhas que as pessoas fazem diariamente pode parecer fruto de decisões tomadas com bastante consideração, porém não são. Elas são hábitos e muito embora cada hábito signifique relativamente pouco por si só, ao longo do tempo, as refeições realizadas, as conversas mantidas com os filhos à noite, a forma com as pessoas poupam ou gastam o seu dinheiro, a frequência que realizam exercícios físicos, o modo como organizam os pensamentos e rotinas de trabalho possuem um grande impacto na saúde, segurança, finanças e felicidade.

Conforme Neal *et al.* (2006), as teorias mais recentes caracterizam os hábitos como respostas automáticas, que são estimulados por alguns aspectos no contexto ou pelo próprio ambiente. Os hábitos são aprendidos através de um processo em que a repetição de forma incremental sintoniza os processadores cognitivos na memória procedural (ou seja, o sistema de memória que suporta o controle minimamente consciente das ações qualificadas).

O comportamento repetitivo dos usuários, que pode ser explicitado e utilizado como mecanismos de autenticação, é tratado pela psicologia como hábito. Na psicologia existem trabalhos científicos que relatam que a grande parte das ações cotidianas das pessoas são caracterizadas por repetições. Em estudos, experiência de amostragem diária, que utilizam alunos e amostras da comunidade, cerca de 40% dos comportamentos cotidianos tendem a ser repetidos no mesmo local, quase todos os dias (WOOD *et al.*, 2002). Nesse estudo, as pessoas relataram um conjunto heterogêneo de ações (tais como: ler o jornal, fazer exercícios e comer em restaurantes) que são executadas diariamente e variaram em relação a força do hábito.

Em relação ao hábito podemos afirmar que as pessoas são criaturas de hábito - uma pessoa vai trabalhar na parte da manhã, talvez com uma parada para tomar café, mas quase sempre usando a mesma rota. Uma vez no trabalho, ela permanece na área geral do seu prédio até a hora do almoço. Na parte da tarde, talvez ela receba uma chamada de casa para pegar o filho da escola. À noite, ela vai para casa. Durante o dia, ela verifica seu e-mail, acessa diversas contas. Talvez ela também acesse o *Internet banking* fora de casa através de seu smartphone. Realiza visitas semanais à mercearia, chamadas regulares para os membros da família e outras ações diárias. Todas estas informações podem ser capturadas e armazenadas pelos dispositivos móveis (SHI *et al.*, 2011).

O espaço pervasivo apresentado no parágrafo anterior é rico em informações adicionais (por exemplo: localização, tempo, rota, agenda, aplicativos utilizados, pagamentos efetuados, velocidade de deslocamento, câmeras de segurança e outros) que compõem um contexto computacional, o qual possibilita que estas informações, associadas ao comportamento do usuário, façam parte do processo de autenticação. Além disso, a utilização dos dispositivos móveis se diferencia de pessoa para pessoa (FALAKI *et al.*, 2010). Desta forma, a autenticidade do usuário dependerá da sua interação (relacionamento) com ambiente (contexto, ações, informações). Portanto, pessoas diferentes possuem hábitos, usos e contextos diferentes. Todas estas informações sobre usuário, seus relacionamentos com o ambiente formam uma Assinatura Comportamental.

As informações, contextos e ações relacionadas com o usuário podem ser usadas para criar um perfil ainda mais detalhado (especializado) para cada indivíduo. Este perfil pode ser utilizado para determinar e garantir a identidade e unicidade do usuário. Assim, atualmente, existem três cenários naturais de utilização da autenticação implícita baseada em comportamento:

- sistemas computacionais de apoio aos trabalhadores móveis;
- dispositivos médicos (*smartphone* ou *tablets*), que acessam e manipulam os registros dos pacientes. Estes dispositivos geralmente são compartilhados e por isso devem ser tratados adequadamente em relação à autorização para não violar as exigências de privacidade de informação do paciente;
- sistemas de defesa (acesso a recursos militares, equipamentos e serviços), como os militares possuem hábitos diários mais rotineiros que as demais pessoas, a definição de um perfil específico para cada militar pode garantir a sua identificação e a sua posterior autorização para utilização destes recursos.

3.2.1 A Pesquisa em Autenticação Implícita

Na literatura científica encontram-se diversas pesquisas que possuem o foco na implementação da autenticação implícita. Estas foram classificadas como: i) redução no número de autenticação e ii) biometria.

3.2.1.1 Redução no número de autenticação

Reduzir o número de vezes que o usuário precisa se autenticar; normalmente, é implementado como *Single Sign-On* (SSO) que é um procedimento de autenticação que habilita o usuário a acessar (*Logon*) a diversos sistemas com uma única instância de identificação e se caracteriza por:

- Classificação:
  - *Enterprise Single Sign-on* (E-SSO) - funciona como autenticação primária e intercepta as requisições de *Logon* apresentados por aplicações secundárias, completando-as com o nome de usuário e senha (BELLAMY-MCINTYRE *et al.*, 2011);

  - *Web single sign-on* (SSO na Web) - funciona apenas com aplicativos e recursos acessados através de visualizadores *Web*. Os acessos são interceptados com a ajuda de um servidor *proxy* ou um componente instalado no servidor *Web* de destino. Os usuários não autenticados, que buscam acesso, são redirecionados para um servidor de autenticação e retornam somente após alcançar o sucesso. Os *cookies*(marcadores) são usados para reconhecer os usuários que acessam e informar o estado da autenticação (WANG *et al.*, 2010);
  - Kerberos - é um método popular para externalizar a autenticação do usuário. Usuário se registra no servidor Kerberos e recebe um "bilhete"; quando o usuário utilizar, as aplicações clientes este "bilhete"será reconhecido e certificado (NEUMAN; TS'O, 1994);
  - Identidade Federada - é utilizado também para aplicações *Web*. Ele utiliza protocolos baseados em padrões para permitir que aplicativos possam identificar usuários sem a necessidade de autenticação redundante. O processo de autenticação ocorre em servidor previamente cadastrado no qual o usuário possua acesso. Um exemplo de utilização é a Comunidade Acadêmica Federada (CAFe) utilizado pela Rede Nacional de Pesquisa (RNP) (WANGHAM *et al.*, 2010);
  - OpenID - é um processo SSO distribuído e descentralizado onde a identidade é transformada em uma url permitindo que qualquer aplicação ou o servidor possa certificar (BELLAMY-MCINTYRE *et al.*, 2011). É o mecanismo utilizado pelo Google e Facebook.

- Benefícios:
  - Redução do *phishing*, pois os usuários não necessitam entrar diversas vezes com as suas senhas em todos os aplicativos e serviços;
  - Redução da combinação de identificação e senha, que os usuários devem manter quando acessam os aplicativos e serviços;
  - Aumento da segurança em todos os níveis.

- Críticas:
  - Como SSO oferece acesso a muitos recursos, uma vez que o usuário é autenticado, ele possuirá a “Chave Mestra do Castelo” que

lhe autorizará acesso a todas as informações e serviços. Portanto, SSO requer um foco maior na proteção das credenciais do usuário e isto deve ser combinado com métodos de autenticação fortes, tais como cartões inteligentes e de *token* SecurID;

– SSO torna crítico os sistemas de autenticação, porque se o usuário perder ou tiver seu reconhecimento negado, ele perderá o acesso a todos os sistemas unificados sob o SSO. Logo, o SSO pode ser indesejável para sistemas cujo acesso deve ser garantido a qualquer momento, como por exemplo: sistemas de segurança ou no chão de fábrica.

3.2.1.2 Biometria

Os sistemas biométricos são sistemas automáticos de reconhecimento de identidade baseados em características físiológicas e comportamentais do usuário. Esses sistemas têm como objetivo suprir deficiências de segurança das senhas, que podem ser reveladas ou descobertas e dos *token* SecurID, que podem ser perdidos ou roubados.

Teoricamente, qualquer característica humana pode ser usada como base para a identificação biométrica. Na prática, entretanto, existem algumas limitações. A tecnologia deve ser capaz de medir determinada característica de tal forma que o indivíduo seja realmente único, distinguindo inclusive gêmeos, porém não deve ser invasiva ou ferir os direitos dos indivíduos. (TCU, 2007)

Uma das fragilidades dos sistemas biométricos é a elevada taxa de erro na identificação de unicidade do usuário. Este erro é proporcionado em função da mudança das características dos usuários com o passar dos anos, ou devido a problemas de saúde ou devido a um comportamento anormal. A tolerância a erros deve ser estabelecida com precisão, de forma a não ser grande o suficiente para admitir impostores, nem pequena demais a ponto de negar acesso a usuários legítimos.

A seguir são enumerados algumas características humanas passíveis de verificação por sistemas biométricos para a sua utilização no ambiente pervasivo. A saber:

1. Impressões digitais – são características únicas e consistentes. Nos sistemas biométricos que utilizam essa opção, são armazenados de 40 a 60 pontos para verificar uma identidade. O sistema compara a impressão

lida com impressões digitais de pessoas autorizadas, armazenadas em sua base de dados. Normalmente, utilizam as Interface *touch-screen* para capturar as informações;

2. Voz – os sistemas de reconhecimento de voz são usados para controle de acesso, porém não são tão confiáveis como as impressões digitais, em função dos erros causados por ruídos do ambiente e de problemas de garganta ou nas cordas vocais das pessoas a eles submetidas;

3. Geometria da mão – também é usada em sistemas de controle de acesso, porém essa característica pode ser alterada devido à variação de peso do usuário ou por doenças reumáticas como a artrite;

4. Configuração da íris e da retina – os sistemas que utilizam essas características se propõem a efetuar identificação mais confiável do que os sistemas que verificam impressões digitais. Entretanto, são sistemas invasivos, pois direcionam feixes de luz aos olhos das pessoas que se submetem à sua identificação;

5. Reconhecimento facial através de termogramas - o termograma facial é uma imagem captada por uma câmera infravermelha que mostra os padrões térmicos de uma face. Essa imagem é única e, combinada com algoritmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face, constitui-se em uma técnica não-invasiva, altamente confiável, não sendo afetada por alterações de saúde, idade ou temperatura do corpo. São armazenados ao todo 19.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro. O desenvolvimento dessa tecnologia tem como um de seus objetivos baratear seu custo para que possa ser usada em um número maior de aplicações de identificação e de autenticação.

6. Convergência de múltiplas fontes de dados. De acordo com Bigun *et al.* (2005), os seres humanos são excelentes especialistas em reconhecimento de pessoas e ainda assim eles não realizam bem o processo de reconhecimento com base em uma única modalidade como a imagem facial. O contexto espaço-temporal e a voz, normalmente, são utilizados de forma complementar para identificação de pessoas e/ou objetos. Portanto, a combinação de vários fatores biométricos pode ser utilizada para gerar a decisão de autenticação ou um escore de decisão.

As características humanas enumeradas anteriormente, requerem dispositivos auxiliares e/ou sistemas de processamentos mais elaborados para a

determinação de unicidade dos usuários, isto impossibilita que estas características possam ser processadas em *Smartphones* que possuem recursos computacionais limitados e necessitam preservar um baixo consumo de energia. Com base nestes limitantes e com a extensão do conceito de biométrica, que agora incorpora os aspectos comportamentais dos usuários, começam a surgir pesquisas que avaliam as diversas características de comportamento dos usuários em um espaço pervasivo:

- Controle de acesso baseados em localização (DAMIANI; SILVESTRI, 2008) - tem como objetivo regular o controle de acesso através da consciência de localização (com base em informações de posicionamento) dos usuários e objetos para permitir o acesso a objetos e/ou informações protegidas. Este projeto segue as diretivas de criação de modelos de controle de acesso espacialmente conscientes para aplicações móveis e pervasivas.

  - Benefícios: a modelagem e a arquitetura apresentadas no projeto explicita os vários desafios que precisam ser abordados neste novo modelo de controle de acesso espacialmente consciente, quando aplicado em contextos reais. Entre os desafios destacam-se: i) a necessidade da definição de camadas de segurança sobre o contexto móvel; e ii) definição de um framework de segurança simplificado para o gerenciamento de políticas baseadas em localização e políticas eficientes de execução.
  - Críticas: uma questão importante é a forma de proteger a privacidade de localização, garantindo um acesso seguro. O problema ocorre porque os administradores do sistema estão cientes da posição do usuário e, assim, podem divulgar essas informações a terceiros sem o consentimento do usuário.

- Dinâmica de digitação e padrões de digitação (NISENSON *et al.*, 2003; MONROSE; RUBIN, 1997) - tem como objetivo investigar e desenvolver técnicas automáticas para reconhecimento do usuário com base na dinâmica de digitação. Este método analisa padrão de digitação de um usuário, monitorando as entradas de teclado milhares de vezes por segundo e tem como objetivo identificar usuários com base em padrões habituais em seu ritmo de digitação.

  - Benefícios: a dinâmica de digitação pode ser usada efetivamente como uma salvaguarda, ou segundo fator de autenticação, para o

acesso não autorizado aos recursos computacionais e a informações sensíveis. Este método pode ser portado para um dispositivo móvel, mas com as seguintes restrições: deverá ser adaptado para um teclado específico e trabalhar somente com as informações de seu usuário, já que haverá uma base de dados restrita para as comparações de identificação.

  - Críticas: estes métodos não são facilmente traduzíveis para dispositivos móveis porque possuem teclados significativamente diferentes e muitas vezes fornecem correção automática ou recursos de auto-completar.

- Uso de acelerômetros para identificar o usuário através do reconhecimento da marcha e para detectar se um dispositivo está sendo utilizado pelo proprietário (KALE *et al.*, 2002; GAFUROV *et al.*, 2006) - como a marcha é um fenômeno espaço-temporal, que tipifica as características do movimento de um indivíduo, é possível reconhecer os seres humanos por meio da sua marcha, através de acelerômetros ou por digitalização de imagens em movimento dos usuários.

  - Benefícios: os processos de autenticação biométrica, baseados na marcha de uma pessoa, foram testados em laboratórios, obtiveram baixas taxas de erro entre 5% e 9%, demonstrando um futuro promissor deste método.

  - Críticas: o processo de digitalização de imagens necessita de acesso à câmeras externas, requer processamento de imagens, portanto, necessita de recursos computacionais mais elaborados. Esses requisitos dificultam o processo de identificação. A utilização de acelerômetros externos ao corpo causa diversos inconvenientes aos usuários: estética, peso, redução da agilidade e outros.

3.3 AUTENTICAÇÃO SENSÍVEL AO CONTEXTO ORIENTADA AO COMPORTAMENTO DO USUÁRIO

Esta seção tem como objetivo analisar algumas das abordagens mais relevantes relacionadas à autenticação sensível ao contexto. Por fim, é apresentado um comparativo entre as abordagens analisadas levando em consideração os critérios identificadas na seção 3.3.5.

3.3.1 Autenticação Implícita com Aprendizagem do Comportamento do Usuário

Shi *et al.* (2011) propõem um mecanismo de autenticação implícita através da aprendizagem do comportamento do usuário. O mecanismo concentra-se no uso de dispositivos móveis (PDAs) e apresenta uma técnica para determinar o cálculo de uma pontuação (escore) de autenticação baseado em atividades recentes do usuário, conforme a Figura 7.

Para calcular o escore são identificados os eventos positivos (habituais), a pontuação aumenta quando um evento habitual é observado, como comprar o café sempre na mesma loja, em um período de tempo similar, todos os dias. A pontuação diminui após a detecção de eventos negativos (esporádicos), tais como a chamada de um número desconhecido da agenda do telefone celular, ou mudanças repentinas de locais esperados (evento associado com abuso ou roubo do dispositivo).

A contribuição deste trabalho está no tratamento da passagem do tempo como um evento negativo em que as pontuações degradam pouco a pouco. Quando a pontuação cai abaixo de um limite, o usuário deve explicitamente autenticar-se, inserindo um código. A autenticação com sucesso irá impulsionar o escore. Os limites podem variar para diferentes aplicações, dependendo das necessidades de segurança.

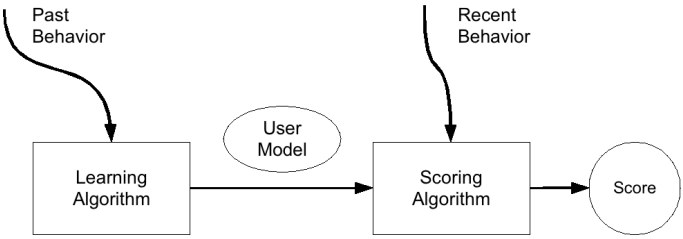


Figura 7: Modelo de Autenticação Implícita.
Fonte: Shi *et al.* (2011)

3.3.2 Autenticação no Nível de Transação

Babu e Venkataram (2009) apresentam um esquema de autenticação para transações móveis, chamado de *Transaction-Based Authentication*

Scheme (TBAS), que visa classificar as transações operadas pelo usuário no nível de aplicação em ambientes de computação móvel. Através dessa classificação, o sistema:

1. pode inferir e analisar o comportamento do usuário através da abordagem de agentes cognitivos (agentes inteligentes). A Figura 8 ilustra o processo de análise comportamental do usuário;
2. pode determinar o nível de segurança necessário, prevendo, então, o custo associado ao atraso do processo de autenticação devido à aplicação de algoritmos de criptografia.

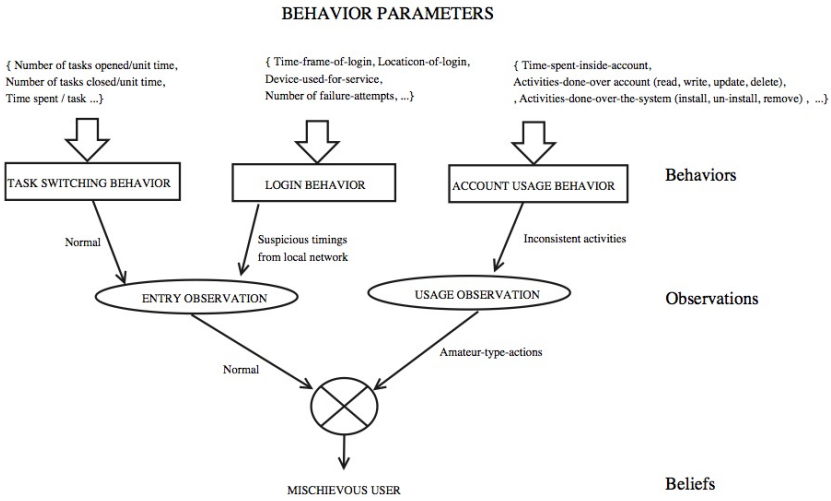


Figura 8: Análise comportamental do usuário.
Fonte: Babu e Venkataram (2009)

O processo de autenticação a nível de transação é realizado enquanto o cliente é autenticado, este processo utiliza dois tipos de agentes cognitivos:

- *Mobile Cognitive Agent* (MCA) - responsável pela autenticação no dispositivo móvel;
- *Static Cognitive Agent* (SCA) - responsável por criar o MCA e enviar este agente cognitivo para o dispositivo móvel.

O processo de autenticação é distribuído em dois componentes lógicos:

- Componente MCA: gera crenças a partir da observação dos diversos comportamentos do usuário, periodicamente.

- Componente SCA: dinamicamente, cria requisitos de autenticação, utilizando a sensibilidade das transações móveis e das mudanças de comportamento do usuário.

Além destes componentes, um **protocolo de desafios** foi integrado ao sistema com a finalidade de neutralizar alguns ataques comumente encontrados neste tipo de ambiente, como: interrupção, modificação e fabricação de transações.

3.3.3 Autenticação baseada no Reconhecimento de Atividades

Hung *et al.* (2008) propõem um mecanismo de segurança baseado em atividades que tem como objetivo auxiliar as atividades dos usuários em ambientes ubíquos. A Figura 9 ilustra a arquitetura proposta. O mecanismo de segurança é composto por:

- sistema de autenticação baseado na identificação humana de imagens (JAMEEL *et al.*, 2006);

- modelo de controle de acesso **orientado a atividades**.

O modelo de controle de acesso suporta diferentes tipos de dispositivos (PDAs, laptops e desktops). O principal componente do mecanismo, o gerenciador de reconhecimento de atividades *Activity Recognition Manager* (ARM) realiza o processo de inferêcia sobre as ações do usuário. Este processo de inferência utiliza as informações da coleta de dados de baixo nível relacionados à atividade e produz informação contextualizada de alto nível.

O gerenciador de autorização utiliza as informações sobre as atividades atuais do usuário a fim de estabelecer as permissões de controle de acesso. Para suportar a execução em qualquer dispositivo, incluido os dispositivos móveis, o gerenciador de autenticação deve ser *lightweight*.

3.3.4 Autenticação baseada no Contexto

Corradi *et al.* (2004) propõem um *middleware* de segurança, chamado de *Ubiquitous Context-based Security Middleware* (UbiCOSM). A Figura 10, apresenta a arquitetura UbiCOSM.

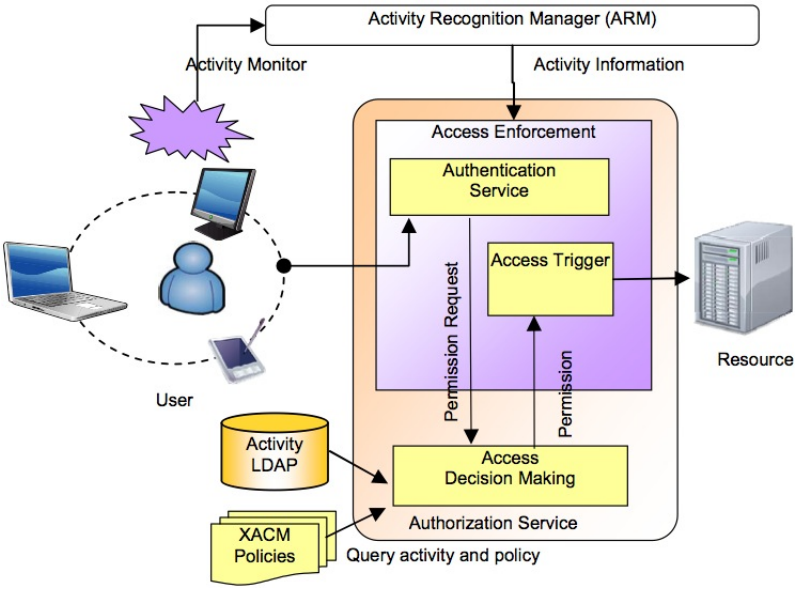


Figura 9: Arquitetura do sistema de segurança baseado em atividades.
Fonte: Hung *et al.* (2008)

Esta abordagem adota o contexto como conceito básico para especificação e execução de políticas de segurança. Portanto, as permissões são associadas diretamente aos contextos, ao invés de o serem com as identidades e papéis dos usuários. As informações sobre os contextos e recursos são providas pelo *middleware* CARMEN (BELLAVISTA *et al.*, 2003).

O gerenciador de controle de acesso do UbiCOSM trabalha com duas classificações de contexto:

- Contextos físicos: identificam espaços físicos delimitados por coordenadas geográficas específicas. Um usuário ou um recurso a ser protegido está vinculado a somente um contexto físico. O gerenciador de controle de acesso realiza a autorização a estes contextos físicos;

- Contextos lógicos: identificam estados lógicos das entidades que compõem um cenário, como por exemplo: usuários e recursos. Uma entidade pode estar vinculada a diferentes contextos lógicos. Os estados lógicos dependem das propriedades lógicas, como por exemplo: condições temporais, estado e disponibilidade de recursos, atividades do

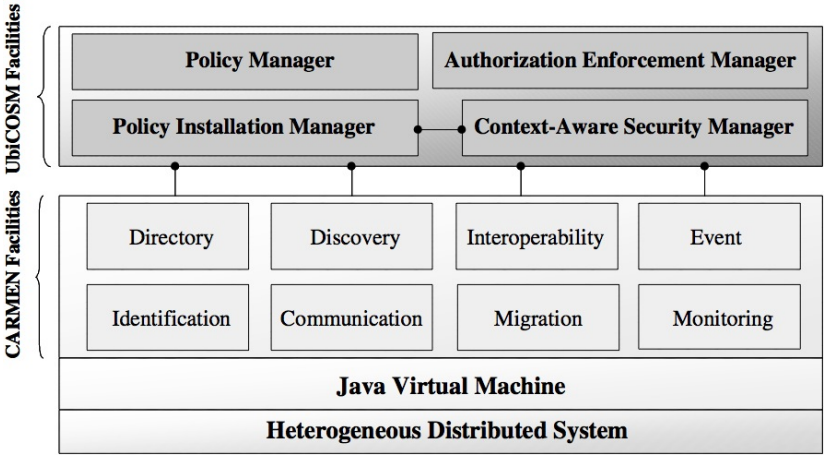


Figura 10: Arquitetura UbiCOSM.
Fonte: Corradi *et al.* (2004)

usuário e características do dispositivo do usuário.

O UbiCOSM possui três diferentes visões. Assim, ele controla a visibilidade dos recursos físicos/lógicos acessíveis diretamente através da localização do usuário (visão de contexto ativo). Portanto, tais visões contêm os recursos que, tanto o usuário deseja acessar (visão desejada), quanto os recursos que foram classificados como acessíveis pelo serviço de controle de acesso, considerando as políticas de controle de acesso dependentes do contexto ativo atual (visão permitida).

As informações necessárias para a definição de tais visões são obtidas através de perfis que provêm descrições explícitas das características dos usuários, dispositivos e recursos. Então, os perfis são decompostos em duas subestruturas: propriedades do usuário e visão desejada, que expressa as preferências do usuário sobre as ações desejadas e visibilidade dos recursos.

A arquitetura UbiCOSM é composta por componetes, conforme a Figura 10, sendo estes componentes responsáveis por:

- *Policy Manager* (PM) - provê ferramentas de edição de políticas de segurança e controle de acesso para os administradores do sistema e usuários finais;
- *Policy Installation Manager* (PIM) - responsável pela manutenção das associações entre contextos e suas permissões. Desta forma, o PIM

instala as políticas de controle de acesso e segurança, armazenando as associações entre os contextos e permissões em tabelas hash;

- *Context-Aware Security Manager* (CASM) - responsável por processar o conjunto de políticas de controle de acesso para os clientes móveis e, então, determina a visão de contexto ativo de qualquer usuário. Portanto, o CASM retorna ao usuário uma visão de contexto ativo baseada na situação do contexto ativo, nas políticas de segurança do sistema e nas políticas impostas pelos outros usuários, que estão participando do domínio;

- *Authorization Enforcement Manager* (AEM) - responsável por proibir ou permitir o acesso dos clientes aos recursos, considerando as interações entre usuários e recursos anteriores.

3.3.5 Critérios para Análise das Abordagens

Johnson (2009) propõe o conceito de contexto relevante à segurança, que consiste em uma derivação entre uma definição amplamente aceita e utilizada de contexto (DEY, 2001) e as definições da segurança da informação apresentadas no seção 3.1.

De acordo com Johnson (2009):

> *Contexto relevante à segurança consiste em qualquer informação que pode ser utilizada para caracterizar a situação de uma entidade que poderia afetar uma tentativa do sistema em proteger informações e sistemas de informações contra acesso, uso, modificação ou destruição sem autorização, a fim de prover confidencialidade, integridade e disponibilidade.*

Consequentemente, um sistema de segurança sensível ao contexto deve basear-se em todas as informações contextuais relevantes que possam determinar ameaças ao uso apropriado do sistema, e, assim, adaptar-se a fim de tratá-las de forma adequada para impedir a intervenção humana de forma explícita. Entretanto, visto que o foco deste trabalho está no processo de autenticação sensível ao contexto, novos requisitos são inseridos a este conjunto de propriedades. Tais requisitos são:

- **Sensibilidade ao contexto:** o sistema de autenticação deve adaptar-se conforme o dinamismo da informação contextual. Tal sistema deve ser

capaz de ajustar suas ações de acordo com as mudanças na situação das entidades relevantes à interação entre o usuário e o sistema de autenticação. Entre tais entidades, pode-se destacar: o usuário, os dispositivos computacionais do usuário, o ambiente e o mecanismo de comunicação entre o usuário e o sistema (JOHNSON, 2009).

- **Autonomicidade e dinamicidade:** o sistema de autenticação deve ser capaz de envolver o mínimo de intervenção humana possível. Além disso, o sistema deve ser capaz de observar, identificar e agregar o conhecimento e habilidades adquiridas pelo usuário durante suas interações com o sistema. Desta forma, tal sistema pode improvisar novas políticas baseadas em novas informações contextuais ou/e no histórico de informações.

- **Flexibilidade:** em um ambiente computacional aberto e amplamente distribuído como um sistema móvel e pervasivo, é desejável a utilização de diferentes meios de autenticação. Isto, deve-se ao fato de que entidades possuem diferentes requisitos de segurança e políticas. Portanto, o sistema deve apresentar a habilidade de prover um nível satisfatório de customização para as diferentes entidades.

- **Preservação da privacidade:** em um ambiente sensível ao contexto, existem diversos sensores monitorando vários tipos de informações importantes sobre os usuários. Tais sensores obtêm informações como: localização, preferências e atividades dos usuários, por exemplo. Portanto, a proteção da privacidade do usuário é um aspecto importante a ser considerado para evitar o uso indevido dessa informação contra a vontade do usuário.

- **Local de Controle de Autenticação:** em um ambiente de computação móvel distribuído, o controle de autenticação deve atuar nos diversos setores onde ocorre a interação com o usuário. Estes setores podem ser definidos como: i) cliente (no dispositivo) - para proteção de informações armazenadas localmente e acesso a suas aplicações; ii) servidor - para proteção ao acesso não autorizado à serviços, informações e aplicações armazenados no servidores.

3.3.6 Análise das abordagens

A seguir, faz-se uma análise das abordagens considerando os requisitos essenciais à autenticação em um ambiente pervasivo. Como pode ser visto no Quadro 2, a maioria das abordagens apresenta uma modelagem contextual fraca, pois considera apenas aspectos sobre as características dos dispositivos utilizados pelo usuário e seu contexto espacial. Sendo assim, tais sistemas possuem uma visão incompleta do cenário, prejudicando o processo de tomada de decisão. A proposta da seção 3.3.1 trabalha com um modelo espaço-temporal limitado, porque o tempo é modelado através de uma simplificação, que não permite inferir atividades semanais ou quinzenais (por exemplo, todo sábado o usuário joga tênis com novos adversários e necessita entrar em contato para marcar o horário).

Uma pequena parte das abordagens analisadas apresenta algum mecanismo de análise e modelagem comportamental do usuário de forma dinâmica. As propostas apresentadas nas seções 3.3.3 e 3.3.4 são estáticas, ou seja, não oferecem mecanismos para que o sistema possa dinamicamente agregar o conhecimento e habilidades adquiridas pelo usuário durante suas interações com o sistema. Na seção 3.3.3, apesar de ser proposto um mecanismo de reconhecimento de atividades, o usuário deve explicitamente informar a atividade que está executando. Na seção 3.3.4, embora seja apresentada uma proposta de utilização de perfis para determinação das permissões dos usuários, o usuário deve explicitamente determinar que atividades pretende desempenhar no sistema.

Como o tempo de vida da bateria é a maior preocupação de usabilidade em dispositivos móveis (RAHMATI; ZHONG, 2009), é desejável que os mecanismos de autenticação levem em consideração aspectos relativos ao consumo de recursos computacionais de forma inteligente, quando estes executam seus procedimentos de segurança. Assim, a validação da proposta da seção 3.3.2 baseia-se na categorização das transações móveis, considerando o nível de segurança necessário para tais operações. Embora exista essa categorização de custos associados ao processo de autenticação, ela é utilizada apenas para determinar o impacto do atraso associado ao algoritmo de criptografia aplicado e definir quais serão os métodos de autenticação (desafios) utilizados. Por outro lado, na seções 3.3.1 e 3.3.3, apesar de os autores citarem que a arquitetura proposta é leve, não são apresentados experimentos ou maiores detalhes sobre como tal arquitetura lida com as restrições energéticas dos dispositivos móveis. As arquiteturas que possuem o local de controle de autenticação no servidor não interferem nas aplicações e no sistema operacional do disposi-

Características	Autenticação Implícita por Comportamento	Autenticação no Nível de Transação	Autenticação por Reconhecimento de Atividades	Autenticação Baseada no Contexto
Bibliográfia e Referência no texto				
Bibliográfia	Shi *et al.* (2011)	Babu e Venkataram (2009)	Hung *et al.* (2008)	Corradi *et al.* (2004)
Referência	Seção 3.3.1	Seção 3.3.2	Seção 3.3.3	Seção 3.3.4
Critérios para Análise das Abordagens				
Modelo Contextual	Espaço Temporal limitado	Espacial	Espacial	Espacial
Modelo Comportamental	Perfil Dinâmico com Filtros através de escores	Agentes Cognitivos	Explícito	Perfil Estático
Atomicidade e Dinamicidade	Sim	Sim	Não	Não
Flexibilidade	Não	Sim	Não	Sim
Privacidade	Sim	Não	Não	Sim
Local de Controle de Autenticação	Cliente	Cliente	Cliente	Servidor

Quadro 2: Quadro das Abordagens de Autenticação Sensível ao Contexto Orientada ao Comportamento do Usuário

tivo móvel, facilitando a sua disseminação e reduzindo o consumo de bateria.

A possibilidade de gerenciamento das políticas de segurança, por parte dos usuários, tem se tornado cada vez mais importante no projeto de soluções de segurança que buscam alinhar a usabilidade à capacidade de manter níveis aceitáveis de integridade, confiabilidade e disponibilidade em aplicações móveis (TONINELLI *et al.*, 2009). Entretanto, segurança e usabilidade têm sido raramente integradas de forma satisfatória no projeto e desenvolvimento de sistemas móveis (HONG *et al.*, 2007).

Desta forma, buscou-se analisar as abordagens propostas quanto à privacidade e flexibilidade de meios e políticas de autenticação. Nas seções 3.3.2 e 3.3.4 é apresentada mais de uma forma de autenticação. Na seção 3.3.2, diferentes desafios são providos ao usuário a fim de comprovar sua identidade, dependendo do nível de segurança necessária para a transação requisitada e do nível de anomalia comportamental do usuário. Por outro lado, na seção 3.3.4, o usuário define suas preferências através de perfis, que são usados, pelo sistema no processo de autenticação e autorização do usuário. Na seção 3.3.1 não é apresentado uma forma de validação ou de geração de desafios, os autores informam que isto poderá ser realizado pelas aplicações, em diferentes níveis. Na seção 3.3.3, a arquitetura proposta provê apenas um único meio de autenticação ao usuário, que é o processo de identificação de imagens proposto, anteriormente, pelos autores em Jameel *et al.* (2006).

3.4 SISTEMAS DE RECOMENDAÇÃO SENSÍVEIS AO CONTEXTO

Na definição do trabalho foi adotada a taxonomia Burke (2007) que fornece uma visão geral dos diferentes tipos de Sistemas de Recomendação (SR), e possui uma forma clássica de distinção entre os sistemas de recomendação e suas referências. Ela distingue seis classes com diferentes abordagens de recomendação:

- filtragem baseada em conteúdo: recomenda itens que são semelhantes aos que o usuário utilizou no passado;
- filtragem colaborativa: recomenda ao usuário ativo os itens que outros usuários com perfis similares utilizaram no passado;
- filtragem demográfica: recomenda itens com base no perfil de localização do usuário. A suposição é que diferentes recomendações devem ser geradas para diferentes nichos demográficos;

- filtragem baseada em conhecimento: recomenda itens com base no conhecimento de domínio específico sobre como os recursos de determinado item atendem as necessidades dos usuários e as suas preferências, em última instância, como o item é útil para o usuário;
- filtragem de base comunitária: recomenda itens com base nas preferências de amigos do usuário. Esta técnica segue o epigrama "Diga-me quem são seus amigos e eu lhe direi quem você é";
- filtragem híbrida: com base na combinação das técnicas acima mencionadas. Um sistema híbrido que combina técnicas A e B tenta usar as vantagens de A para corrigir as desvantagens de B.

Nos ambientes ubíquos muitos recursos podem estar disponíveis e os usuários podem compartilhá-los. No entanto, as situações e as preferências dos usuários são diferentes, mesmo se os usuários estão no mesmo ambiente. Portanto, é desejável um SR apropriado para a partilha dos recursos disponíveis. Estes e outros possíveis modelos para sistemas de recomendação podem ser adequados para usos atuais, mas talvez não para computação ubíqua futura.

Os sistemas de Computação Ubíqua devem possuir conhecimento além da localização. Por exemplo, as ferramentas que uma pessoa está usando poderiam beneficiá-la através da recomendação de outras pessoas que tenham experiência com essas ferramentas. Embora possa ser impossível antecipar as necessidades de cada usuário em qualquer lugar, a qualquer momento, a computação ubíqua permitirá que tais sistemas possam ajudar as pessoas a lidar com esta variedade crescente de opções (MCDONALD, 2003).

Portanto, os SR que provaram ser bem-sucedidos para os usuários de computadores pessoais não podem ser diretamente aplicados para usuários móveis, devido aos obstáculos que estão normalmente presentes em ambientes de computação móvel, tais como: limitação de dispositivos móveis, limitação das redes sem fio, o impacto do ambiente externo e as características comportamentais desses usuários (RICCI *et al.*, 2011).

3.4.1 Sistemas de Recomendação Móvel

Os Sistemas de Recomendação Móvel (SRM) são sistemas que fornecem assistência aos usuários no processo de tomada de decisões *on the go*, ou, em outras palavras, à medida que avançam em novos ambientes desconhecidos. Alguns exemplos: os consumidores que tomam decisões nas compras

nas lojas de varejo, ou estudantes que tenham reuniões para decidir sobre a atribuição de trabalho (HEIJDEN *et al.*, 2005).

Como os dispositivos móveis são populares e estão se tornando uma das principais plataformas de acesso à informação e aplicações de negócio, técnicas de recomendação podem aumentar a usabilidade de aplicações móveis e pervasivas, proporcionando mais informação e conteúdo focado e adaptado às necessidades do usuário. Ricci *et al.* (2011) comenta as principais técnicas que têm sido propostas nos últimos anos e ilustra as funções suportadas pelos SRM.

Como se tem observado, na maioria dos SRM, a recomendação é alvo de conteúdo de Internet, multimídia (vídeos, músicas, filmes, livros), promoções de produtos, experiências turísticas e informações de trânsito. As fontes de dados são usuários e transações Internet. Para aqueles que adicionam sensibilidade ao contexto aos SRM, as informações de contexto mais usuais são as de localização do usuário (aplicações sensíveis à localização).

As aplicações baseadas em contexto atuam pró-ativamente recuperando o conteúdo de interesse com base na tarefa atual do usuário ou no perfil dele. Roberts *et al.* (2008) descreve a implementação de um SRM para atividades de lazer, com o nome Magitti, que foi construído para a implantação comercial sob rigorosos requisitos de escalabilidade. Em Ricci e Nguyen (2007) é apresentado o sistema MobyRek e realizada uma análise crítica de suas recomendações. Esse sistema foi projetado para ser executado em um telefone celular, logo, com uma interface de entrada de dados limitada. A funcionalidade de pesquisa permite que o usuário determine o que deseja e as condições, retornando uma lista de produtos classificados. O resultado de uma avaliação empírica do sistema mostra que ele pode, efetivamente, apoiar os processos de seleção de produtos de uma forma amigável.

Embora os sistemas apresentem necessidades diferentes, eles compartilham um projeto comum: os sistemas coletam diferentes tipos de (contextos) informações, que caracterizam o usuário (como preferências, atividades, localização e dispositivo) e usa-os para filtrar e classificar como relevantes os itens de conteúdo, na tentativa de antecipar as necessidades ou os produtos em que o usuário pode estar interessado, enquanto ele se desloca.

3.4.2 Segurança Pervasiva e Sistemas de Recomendação

Os problemas de segurança em sistemas de recomendação são tratados com dois objetivos: (i) controlar usuários mal-intencionados (RAY; MAHANTI,

2009), e (ii) garantir a privacidade do usuário (ZHAN *et al.*, 2010). Assim, o foco desta Tese é a utilização do sistema de recomendação para identificação do usuário nos ambientes móveis e pervasivos.

O objetivo das pesquisas em Segurança em ambientes móveis e pervasivos é compreender e analisar os novos requisitos de segurança e privacidade decorrentes da alta mobilidade, sensibilidade ao contexto e invisibilidade destes sistemas. Como estes sistemas começam a estar disponíveis é necessário propor soluções para implantar segurança em aplicações, serviços e informações, que podem estar disponíveis em qualquer lugar, em qualquer hora, em qualquer dispositivo e em qualquer rede.

De acordo com Johnson (2009), os ambientes pervasivos necessitam de mecanismos de segurança sensíveis ao contexto, porque as mudanças no contexto permitem adaptações com base na situação atual. Portanto, os mecanismos que usam essa abordagem são capazes de lidar, eficazmente, com as limitações dos sistemas de segurança tradicionais, que são projetados para ambientes estáticos. No entanto, a maioria das pesquisas sobre o desenvolvimento de sistemas sensíveis ao contexto de autenticação é limitada ou vaga (RICCI; NGUYEN, 2007). Normalmente, estes sistemas só consideram aspectos tradicionais, por exemplo, a localização do usuário. Como resultado, eles fornecem uma visão abstrata e fraca de uma determinada situação. Assim, as decisões tomadas dentro destes sistemas são pobres, porque elas são baseadas em um cenário incompleto.

Poucos trabalhos abordam questões sobre a segurança pervasiva e sistemas de recomendação sensíveis ao contexto (SRSC). Kim *et al.* (2009) propõe um novo método de gestão de chaves de autenticação, chamado 3DE_sec, para minimizar a carga do autenticador, mesmo com nós móveis ou a inserção ou exclusão de nós. O sistema proposto gera perfis personalizados (usando inferência de dados capturados a partir de sistemas RFID), contendo as preferências do usuário e os diferentes estilos de vida e uso dos serviços de recomendação, ele atualiza com base na história passada e serviços disponíveis atualmente. A arquitetura do sistema é composto por coletor de perfil, agregador de perfil, coletor de recomendações e gerenciador de serviço. Os resultados da avaliação indicam que o método pode definir uma chave compartilhada de forma rápida e segura, usando múltiplas chaves para cada nó, antes da implantação de um serviço de recomendação seguro e eficiente em RFID.

Romero-Mariona *et al.* (2008) propõe um sistema de recomendação para ajudar os desenvolvedores a escolher entre os diversos requisitos de segurança. Como parte de sua pesquisa, eles identificaram dez características-

chave (suporte elicitação, nível de envolvimento do cliente, nível de ambiguidades, nível de abrangência, nível de clareza, nível de rastreabilidade, nível de segurança geral, dificuldade em atualizar as especificações de segurança, nível de suporte de automação e o nível de escalabilidade), que são usadas para recomendar as perspectivas de segurança e quais as mais adequadas a um projeto específico.

3.5 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foi apresentado uma síntese dos conceitos do processo de autenticação, que envolve os componentes do protocolo AAA - Autenticação, Autorização e Auditoria. Na seção 3.2 são apresentados alguns projetos que envolvem autenticação em dispositivos móveis e os conceitos da autenticação implícita.

Na seção 3.3 foi realizada uma análise comparativa entre os demais trabalhos que apresentam abordagens relacionadas à autenticação sensível ao contexto orientada ao comportamento do usuário. A seção 3.3.6, apresenta o Quadro 2, referente ao quadro resumo desta análise comparativa. De forma sintética fica evidenciado:

- A necessidade de desenvolver sistemas de autenticação complementar, devido as limitações dos dispositivos móveis e que as pesquisas na área, apesar de começarem em 2004, somente recentemente despertaram um maior interesse da comunidade científica;

- Que poucos modelos e abordagens utilizam as características espaço-temporal como mecanismo de inferência de localização e comportamento dos indivíduos;

- Que as abordagens relacionadas não permitem a utilização de mecanismos de autenticação no cliente (dispositívo móvel) e no servidor simultaneamente;

- Que somente uma das abordagens se preocupou em incorporar os conceitos da psicologia cognitiva, porém, de forma limitada e através de agentes cognitivos.

Com relação à segurança em sistemas de recomendação, esta Tese possui uma abordagem diferente das citadas na seção 3.4.2. Esta Tese tem como objetivo determinar o momento adequado para renovar a autenticação

do usuário automaticamente ou, se não for possível, perguntar ao usuário informações cadastradas e, assim, proceder com o processo de autenticação.

4 MODELO E ARQUITETURA DE AUTENTICAÇÃO DA PROPOSTA

Neste capítulo são apresentados o modelo e a arquitetura de autenticação implícita elaborados nesta Tese. O modelo apresenta os seus elementos, as características de funcionamento e comportamento do protótipo desenvolvido. A arquitetura apresenta os seus componentes e as interações entre eles. Neste trabalho, a arquitetura é representada de três formas diferentes para explicitar os componentes e os seus referenciais teóricos.

4.1 MODELO DE AUTENTICAÇÃO PROPOSTO

Modelo é um catálogo de componentes a serem estudados, onde cada um deles apresenta suas funcionalidades. Na formalização do modelo de autenticação são discutidos os componentes e os atores principais que formam a base para definição: dos fluxos de informação e comunicação, da arquitetura e do modelo de comportamento utilizado, conforme apresentado na Figura 11.

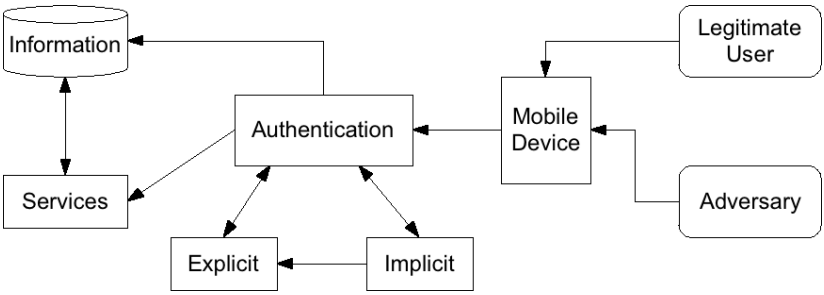


Figura 11: Modelo de Autenticação Proposto

Os usuários que utilizam o dispositivo móvel, de tempo em tempo, são certificados pelo processo de autenticação, pela abordagem desta Tese, a autenticação pode ser:

- **Autenticação explícita** - neste método os usuários são certificados através da sua senha; e
- **Autenticação implícita** - neste método os usuários são certificados pela sua assinatura comportamental, isto é, os comportamentos recen-

tes do usuários são avaliados através de um cálculo de similaridade com os demais comportamentos anteriores, se for constatado um grau de similaridade relevante, será realizada uma autenticação automática ou um questionamento previamente cadastrado pelo usuários legítimo, que possibilitará a autenticação em caso de resposta correta ou a execução da autenticação explicita em caso de erro.

Os atores presentes no modelo, são caracterizados pelos usuários, que podem ser:

- **Usuários legítimos** - são os indivíduos proprietários do dispositivo móvel e / ou autorizados para executar serviços e acessar as informações armazenadas; e

- **Adversários** - são os indivíduos que não possuem autorização de acesso e que utilizam de técnicas de intrusão para acessar os serviços e informações dos dispositivos móveis, que neste trabalho foram caracterizado como:

  - **Usuário atacante** - indivíduo que utiliza de métodos e técnicas computacionais para quebrar a senha e realizar uma autenticação explícita; e

  - **Usuário intruso amigo** - indivíduo que conhece os hábitos e a conduta comportamental do usuário legítimo e simula atividades com o objetivo de realizar uma autenticação implícita.

Como os serviços presentes nos dispositivos móveis podem acessar informações remotas, armazenadas em servidores, o processo de autenticação pode acontecer, também nestes servidores. Desta forma, a autenticação implícita pode ser realizada localmente no dispositivo móvel e remotamente nos servidores de autenticação que disponibilizam serviços remotos ao ambiente móvel e pervasivo.

A determinação do grau de similaridade entre os comportamentos anteriores e recentes dos usuário, são processados por filtros de recomendação. A utilização destes filtros, flexibiliza a implementação da análise de similaridade e permite a escalablidade dos filtros para execução nos dispositivos móveis e nos servidores de autenticação.

Desta forma, os componentes do modelo e seus respectivos elementos, se interrelacionam com o objetivo de classificar os comportamentos dos usuários (formado por: atividades, contextos e eventos), de acordo com os

filtros de recomendação (que podem ser: locais e remotos) e estabelecer critérios para determinar se uma autenticação implícita complementar necessita ser efetivada automaticamente ou realizada através de desafio (solicitação de informações adicionais ao usuário, através de perguntas cadastradas anteriormente), sendo que no pior dos caso é realizada uma autenticação explícita.

4.2 ARQUITETURA DE AUTENTICAÇÃO PROPOSTA

A arquitetura de autenticação está fundamentada no modelo proposto na seção 4.1, com o objetivo de realizar uma transição gradual entre o modelo e os componentes definidos para autenticação. A arquitetura será apresentada através de diferentes visões:

- Arquitetura Proposta - responsável por apresentar os principais componentes explicitados no modelo e os referenciais teóricos que os auxiliaram na sua definição;
- Arquitetura por Componentes e Fluxo de Informações - responsável em apresentar os elementos de cada componente, os fluxos de informações e a formalização dos elementos. Definida na seção 4.4;
- Arquitetura por Níveis de Conhecimento - responsável por apresentar os componentes da proposta através da arquitetura cognitiva de Rasmussen (1983). Definida na seção 4.5.

Os componentes definidos no Modelo de autenticação são apresentados na Figura 12 e são os seguintes:

- **Comportamento:** descreve, através do relacionamento entre os elementos, contexto e atividade, as situações em que o usuário está interagindo com a abordagem de recomendação de autenticação, demonstrando qual é o seu comportamento na execução de determinada atividade. Na definição do comportamento é utilizado o conceito de Teoria da Atividade, apresentado na seção 2.3.1. Os elementos do componente de comportamento são:
  - **Eventos:** um evento descreve o estado de um objeto, entidade ou recurso em um determinado momento. Estes eventos podem ocorrer em grande quantidade devido à natureza do espaço pervasivo, que oferece um elevado número de dados (normalmete

através de sensores) e que podem transmitir informações sobre as mais diversas entidades, como por exemplo informações ambientais, pessoais, interpessoais e outras;

  - **Contexto:** os eventos (conjunto de evento) devem ser classificados (de acordo com o contexto relevante, conforme seção 4.3) e definidos com as propriedades espaço-temporais, que permitem o seu processamento de acordo com as atividades que estão sendo executadas pelo usuário. A classificação dos contextos segue o Modelo de Contexto de Cassens e Kofod-Petersen (2006) e as propriedades espaço-temporais referem-se à localização e ao tempo;
  - **Atividade:** descreve um conjunto de ações que o usuário realiza para executar uma determinada tarefa. Nesta Tese foi adotado a definição que cada ação está relacionada a uma atividade, assim a ação de atender uma ligação telefônica corresponde a uma atividade que será contextualizada, de acordo com as informações dos eventos associados;

- **Recomendação:** os conceitos de sistemas de recomendação são utilizados para implementar os filtros de recomendação (filtragem por conteúdo e filtragem híbrida). A escolha de qual filtro será utilizado é uma decisão do componente de recomendação que utiliza o *Framework* SRK para definir a complexidade e quantidade de processamento que será necessário para processar cada um dos filtros disponíveis frente às informações comportamentais existentes;

- **Autenticação:** o processo de autenticação considera as informações enviadas pelo componente de recomendação para categorizar o usuário em relação ao seu comportamento, às probabilidades condicionais, às distâncias em relação aos agrupamentos de dados e às restrições das aplicações, que estão sendo executadas. Essa categorização permite decidir se a autenticação implícita deve ser executada ou se será necessário lançar um desafio ao usuário (revalidação da autenticação) e esse desafio pode ser categorizado também. Quando o usuário for desafiado e responder positivamente, as informaçoes referentes ao contexto, às atividades e às probabilidades associadas são enviadas ao componente de recomendação para atualizar e aumentar a base de conhecimento das informações para a próxima autenticação implícita.

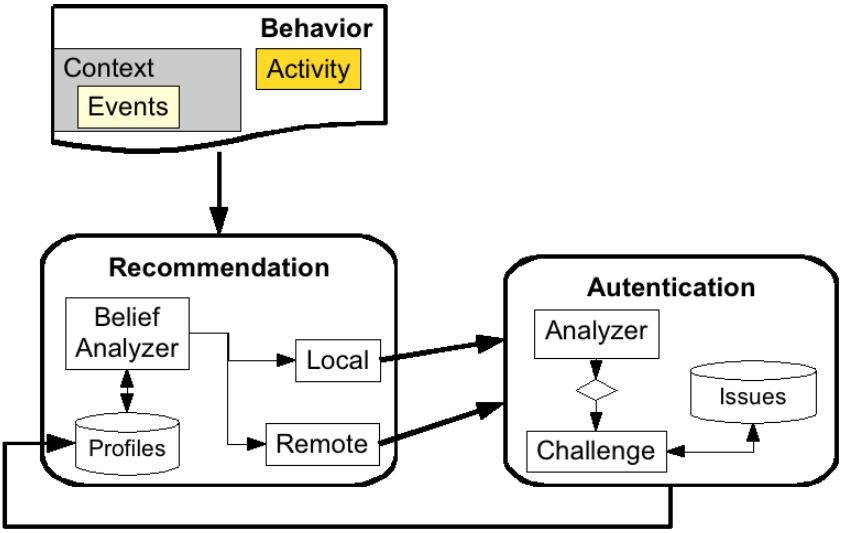


Figura 12: Arquitetura de Autenticação Proposta

4.3 CONTEXTOS RELEVANTES PARA AUTENTICAÇÃO

O espaço pervasivo consiste em um ambiente rico em situações (contextos), que cercam o usuário. Tais contextos são relevantes para o processo adaptativo de serviços e informações oferecidas ao usuário através de aplicações sensíveis ao contexto (DEY, 2001). Portanto, as diversas experiências que podem ser realizadas pelo usuário, em um ambiente pervasivo, são pessoais e, então, dificultam a modelagem e a representação genérica do contexto do usuário e seus parâmetros.

Neste trabalho o modelo de contexto utilizado, Figura 13, é o definido por Cassens e Kofod-Petersen (2006). A importância da utilização deste modelo de contexto e a sua fundamentação foram apresentados na seção 2.3.2. Este modelo de contexto é uma evolução do modelo proposto por Kofod-Petersen e Mikalsen (2005), que possui uma visão pragmática de artefatos de construção e incorpora aos sistemas sensíveis ao contexto, os conceitos gerais encontrados na Teoria da Atividade.

Com a finalidade de identificar os contextos e propriedades relevantes aos usuários e seus comportamentos em ambientes pervasivos, foram analisados os recursos oferecidos pelos dispositivos móveis e concluiu-se que os

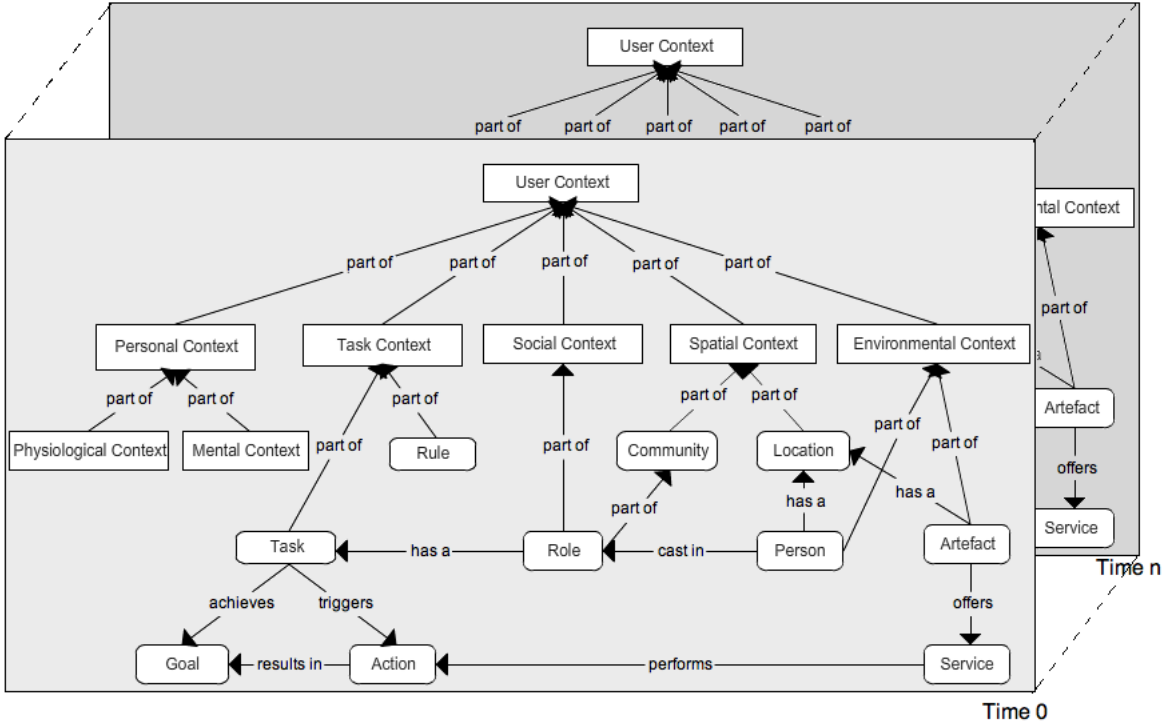


Figura 13: Modelo de Contexto Adaptado.
Fonte: Cassens e Kofod-Petersen (2006)

contextos relevantes à autenticação são:

- **Contexto Operacional:** descreve o que o usuário está fazendo, como os objetivos, as tarefas e as atividades. Este contexto está relacionado com os seguintes Aspectos da TAHC: Assunto, Objetos e Mediação de Regras;

- **Contexto Interpessoal:** descreve os aspectos sociais do usuário, ou seja, as relações e canais de comunicação que este possui com as pessoas da sua comunidade. Este contexto está relacionado com o Aspecto de Mediação de Divisão de Trabalho da TAHC;

- **Contexto Espacial:** considera os atributos relativos à localização do usuário. Este contexto está relacionado com o Aspecto de Comunidade da TAHC;

- **Contexto Ambiental:** captura as situações que cercam o usuário, como serviços, pessoas e informações acessadas. Este contexto está relacionado com os seguintes Aspectos da TAHC: Objeto e Mediação de Artefatos;

A propriedade temporal foi integrada ao modelo de contexto, com a finalidade de melhorar o processo de tomada de decisão. Portanto, todos as informações e conhecimentos armazenadas no modelo de contexto possuem um histórico temporal. Logo, a evolução da capacidade de aprendizagem do usuário, o período de aquisição de habilidades e conhecimento e a evolução de suas atividades e comportamentos são registradas no tempo, no formato de planos temporais.

No modelo de contexto, a propriedade temporal é representada pelos diversos planos temporais de informação e conhecimento armazenados. Os planos temporais são nominados por *Time* 0 até *Time n*, na Figura 13.

Os aspectos da TAHC, definidos na seção 2.3.1, estão relacionados com as categorias propostas por Kofod-Petersen e Cassens (2006), definidos na seção 2.3.2. O Quadro 3 tem o objetivo de explicitar o enquadramento dos contextos emergentes em relação aos aspectos da TAHC e a proposta de Categoria.

Aspecto TAHC (KUTTI, 1996)	**Categoria** (KOFOD-PETERSEN; CASSENS, 2006)	**Contexto Relevantes**
Assunto	Contexto Pessoal	Contexto Operacional
Objeto	Contexto Tarefa	Contexto Operacional
Comunidade	Contexto Espaço-temporal	Contexto Espacial
Mediação de Artefatos	Contexto Ambiental	Contexto Ambiental e Contexto Operacional
Mediação de Regras de Mediação	Contexto Tarefa	Contexto Operacional
Mediação de Divisão de Trabalho	Contexto Social	Contexto Interpessonal

Quadro 3: Aspectos de uma Atividade Relacionado com a Taxonomia do Conhecimento Contextual e com os Contextos Relevantes desta Proposta

4.4 ARQUITETURA POR COMPONENTES E FLUXO DE INFORMAÇÕES

Nesta representação da arquitetura são apresentados os elementos de cada componente, os fluxos de informações e a formalização dos elementos. A formalização servirá de base para a definição do Modelo de Comportamento e estabelecer os critérios de comparação entre os contextos e atividades.

A arquitetura está dividida em componente (Comportamento, Recomendação e Autenticação) e os elementos dos componentes são chamados de módulos que fazem as troca de informações, os quais permitem a definição se o abordagem permitirá a autenticação implícita ou realizará o processo de desafio ao usuário.

4.4.1 Componente de Comportamento

Este componente é responsavel por registrar em B_i o comportamento do usuário através do processo de captura das informações dos sensores contextualizados, ou seja as atividades desenvolvidas pelos usuários. Depois de definido o comportamento B_i, este é enviado para o módulo de análise de crença.

A especificação formal do **Comportamento** é

$$B_i = \langle A_i , C_i \rangle \quad (1)$$

onde B_i representa o comportamento do usuário quando da execução da atividade, A_i representa a atividade definida na seção 4.4.1.3, C_i representa o contexto definido na seção 4.4.1.2 e i as ocorrências de atividades para cada usuário.

4.4.1.1 Elementos do Contexto do Usuário

Para identificar o contexto do usuário, a arquitetura de autenticação sensível ao contexto proposta, ilustrada na Figura 14, utiliza recursos que são comumente encontrados em dispositivos móveis, como *smartphones*, para monitorar o comportamento do usuário em diferentes situações e eventos onde o usuário está imerso no espaço pervasivo. Esses dispositivos são considerados como artefatos especiais, que são comumente usados pelos usuários para executar tarefas e atividades e, consequentemente, para atingir seus objetivos em ambientes móveis (UDEN, 2007). Especificamente, esses dispositivos oferecem acesso a recursos como (LIMA *et al.*, 2010):

- **Chamadas do usuário** - *Users Calls*: provêm as informações das ligações e SMS de entrada e saída, essas informações fazem parte do do contexto interpessoal, que envolve a comunidade onde o usuário está inserido e o contexto ambiental, que diz respeito às pessoas que cercam o usuário;
- **Agenda do usuário** - *Users Schedule*: um dos recursos mais ricos em contexto, pois provê informações da agenda do usuário e lista de atividades que deve executar, essas informações referem-se aos relacionamentos mantidos entre o usuário e os membros de sua comunidade. Pode ajudar a determinar a localização do usuário, as pessoas que o cercam e as atividades que deseja executar em um determinado intervalo de tempo;
- **GPS** - provê informações relativas à localização espacial do usuário;
- **Nível de bateria do dispositivo** - *Battery Level*: provê as informações sobre a taxa de utilização do dispositivo e pode indicar a forma de interação entre o usuário e o ambiente, assim como a intensidade dessa

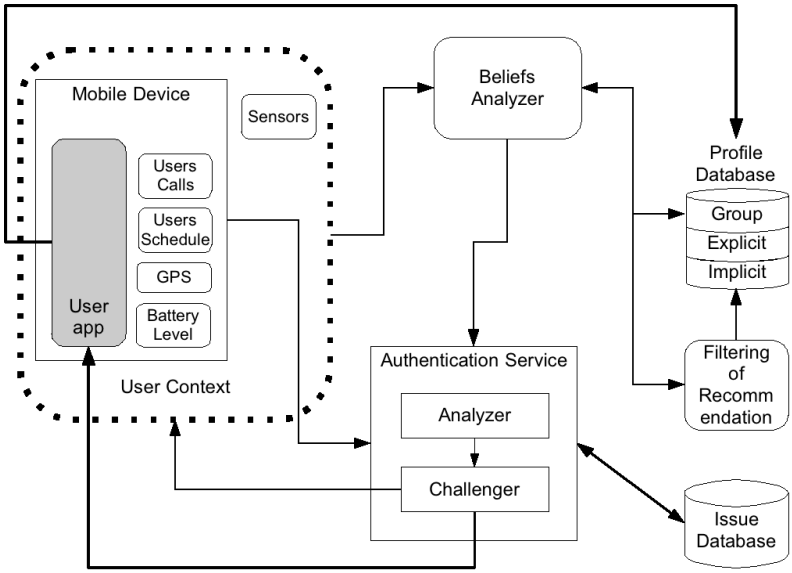


Figura 14: Arquitetura de Componentes Proposta.

interação;

- **Aplicações do usuário** - *User app*: provê informações relacionadas ao contexto operacional e ambiental; em particular, tais aplicações indicam que artefatos o usuário utiliza para alcançar seus objetivos através das atividades desempenhadas;

- **Sensores** - *Sensors*: podem prover informações sobre o ambiente, autenticação visual e outras informações que definem o ambiente no qual o usuário está interagindo com o processo de autenticação.

4.4.1.2 Módulo de Contexto

O módulo de contexto, ou contexto do usuário é responsável por capturar todas as situações que determinam a ocorrência de um novo evento através dos recursos descritos na seção 4.4.1.1.

A especificação formal do **Evento** é

$$E_i = \langle\, id_{entidade} \,,\, situacao_{entidade} \,\rangle \tag{2}$$

O Evento é representado por um identificador $id_{entidade}$ e pelo valor ou situação $situacao_{entidade}$, por exemplo: O primeiro Evento é referente a Temperatura que possui um valor igual a 30 °C. Este evento será representado por $E_1 = \langle\, Temperatura \,,\, 30 \,\rangle$.

O contexto é definido como um conjunto de eventos e as duas propriedades espaço-temporal, com os quais, a localização define onde ocorreu o conjunto de eventos e o tempo define quando ocorreu o conjunto de eventos.

A especificação formal do **Contexto** é

$$C_i = \langle\, tempo \,,\, localizacao \,,\, E_1 \,,\, E_2 \,,\, E_3 \,,\, E_4 \,,\, \ldots \,,\, E_n \,\rangle \tag{3}$$

onde $E_1 \ldots E_n$ representa os eventos definido na equação (2), por exemplo: O primeiro contexto aconteceu no dia 23/02/2013 às 13h23, próximo ao CTC da UFSC (coordenadas: -27.601853 -48.518238), onde a temperatura era 30 °C e a umidade era 75%. este Contexto será representado por:

$$\begin{aligned} C_1 \;=\; & \langle \\ & \langle 2013-02-23 \;\; 13:23:34.234 \rangle \,, \\ & \langle -27.601853 \;\; -48.518238 \rangle \,, \\ & \langle Temperatura \,,\, 30 \rangle \,, \\ & \langle Umidade \,,\, 75 \rangle \\ & \rangle \end{aligned}$$

4.4.1.3 Módulo de Atividade

O módulo de atividade é responsável por relatar quais as ações que o usuário está realizando, bem como compor estas ações na atividade que será processada pelos demais módulos da arquitetura de autenticação.

A especificação formal da **Atividade** é

$$A_i = \langle\, a_1 \,,\, a_2 \,,\, a_3 \,,\, a_4 \,,\, \ldots \,,\, a_n \,\rangle \tag{4}$$

onde $a_1 \ldots a_n$ representa as ações realizadas pelo usuário, por exemplo: $A_1 = \langle\, \langle Call_{in} \rangle \,,\, \langle Call_{out} \rangle \,,\, \langle SMS_{in} = +554899{*}{*}{*}{*}01 \rangle \,,\, \langle SMS_{out} \rangle \,,\, \ldots \,,\, \langle a_n \rangle \,\rangle$.

4.4.2 Componente de Recomendação

Este componente é responsável por calcular as relações entre os comportamentos do usuário, armazenar as informações nas bases de dados de perfis e invocar os filtros de recomendação locais e remotos.

4.4.2.1 Módulos Auxiliares

Este componente de recomendação possui módulos adicionais, que são responsáveis pelo armazenamento dos comportamentos do usuário e demais informações necessárias para o processamento dos filtros de recomendação. Estes módulos são:

- **Perfil de grupo:** um perfil predefinido que considera as características padrões dos agentes (usuários, aplicações, sessão de uso e ambiente) que interagem com o sistema;
- **Perfil explícito:** criado durante a primeira interação do sistema com o usuário através de uma interface interativa; contém os eventos explicitados pelo usuário e extraídos de seus contatos e da agenda pessoal armazenadas no dispositivo móvel. Este perfil pode ser customizado e/ou sincronizado a qualquer momento;
- **Perfil implícito:** criado através do processamento dos eventos do usuário e do seu perfil explícito; contém as informações relevantes sobre os eventos que ocorrem com maior frequência, as ações tomadas pelo usuário e as suas características espaço-temporais.

4.4.2.2 Módulo de Análise de Crenças

O Módulo de Análise de Crenças é responsável pela determinação dos comportamentos, assim como pela classificação dos eventos e pela inferência de comportamentos, através das atividades dos perfis armazenados e eventos que são percebidos e registrados.

Os comportamentos são analisados por similaridade a fim de definir novas ocorrências e determinar a atitude a ser adotada, assim como as ações que serão tomadas em uma nova ocorrência. Este módulo trabalha como um repositório de conhecimento (base de dados de perfis). O funcionamento do

Analisador de Crenças é descrito no Algoritmo 1.

Algoritmo 1 Funcionamento do Analisador de Crenças

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: A_0 {Atividade que o usuário está executando. Definido pela equação (4)}
Parâmetro: C_0 {Contexto onde a atividade está sendo executada. Definido pela equação (3)}

Início
$B_0 \Leftarrow Criar\_Comportamento\ (\ User\ ,\ C_0\ ,\ A_0\ )$
$Nivel \Leftarrow Pesquisar\_Restricao\_Aplicacao\ (\ User\ ,\ B_0\ )$
$Sim\_C \Leftarrow Filtro\_Recomendacao\ (\ User\ ,\ B_0\ ,\ CONTEUDO\ )$
$Sim\_H \Leftarrow Filtro\_Recomendacao\ (\ User\ ,\ B_0\ ,\ HIBRIDO\ )$
$Analisador\_Probabilidade\ (\ User, Sim\_H, Sim\_C, Nivel, B_0\ )$
Fim

4.4.2.3 Filtro de Recomendação

O Filtro de Recomendação tem como objetivo, determinar os novos perfis implícitos, ou seja, a cada combinação de evento com os perfis explícito e implícito é determinado um novo vetor ortogonal. Esse vetor é utilizado para o cálculo da similaridade: se o grau de similaridade for superior a um determinado valor, o perfil é considerado relevante e, então, será armazenado como um novo perfil implícito, com peso igual ao grau de similaridade. O funcionamento dos Filtros de Recomendação é descrito no Algoritmo 2

4.4.3 Componente de Autenticação

Este componente é responsável pela classificação do usuário e determinação do tipo de autenticação que será realizada: explícita, implícita ou desafio ao usuário de acordo com sua classificação.

Algoritmo 2 Funcionamento dos Filtros de Recomendação

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: B_0 {Comportamento do usuário que está sendo analisado. Definido pela equação (1)}
Parâmetro: $Filtros$ {Define quais os tipos de filtros de recomendação serão utilizados, pode conter os valores $[CONTEUDO, HIBRIDO]$ }
Retorno: Sim {Menor indice de similaridade entre os filtros local e remoto}

Início
$Sim \Leftarrow 0$
{ $Verifica\ se\ o\ Filtro\ de\ Conteudo\ foi\ solicitado$ }
if $CONTEUDO \in Filtros$ **then**
  $Sim\_Local \Leftarrow Filtro\_Conteudo\_Local\ (\ User\ ,\ B_0\ )$
  $Sim\_Remoto \Leftarrow Filtro\_Conteudo\_Remoto\ (\ User\ ,\ B_0\ )$
  if $Sim\_Local \leq Sim\_Remoto$ **then**
    $Sim \Leftarrow Sim\_Local$
  else
    $Sim \Leftarrow Sim\_Remoto$
  end if
  { $Verifica\ se\ o\ Filtro\ Hibrido\ foi\ solicitado$ }
else if $HIBRIDO \in Filtros$ **then**
  $Sim \Leftarrow Filtro\_Hibrido\ (\ User\ ,\ B_0\ )$
end if
return Sim
Fim

4.4.3.1 Módulo de Análise de Probabilidades

O elemento que analisa as probabilidades é responsável por categorizar os usuário, baseando-se nas similaridades do seu comportamento, que foi calculada no algoritmo (2). Essa classificação é dividida em três categorias: normal, suspeito e anormal. O funcionamento do Analisador de Probabilidades é mostrado no Algoritmo 3.

Algoritmo 3 Funcionamento do Analisador de Probabilidades

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: *Sim_H* {Graus de similaridade calculado no Algoritmo de recomendação de filtro híbrido}
Parâmetro: *Sim_C* {Graus de similaridade calculado no Algoritmo de recomendação de filtro baseado em conteúdo}
Parâmetro: *Nivel* {Classificação do Nível de Restrição da Aplicação}
Parâmetro: B_0 {Comportamento do usuário que esta sendo analisado. Definido pela equação (1)}

Início
$Natureza \Leftarrow Pesquisar\_Natureza\_Usuario\ (\ User\ ,\ Sim\_H\ ,\ Sim\_C\ )$
if $Natureza \in USER\_NORMAL$ **then**
$Autenticacao\_implicita\ (\ User\ )$
{ *Inicializa o* $Perfil\_de\_Sessao$ *com o Comportamento* B_0 }
$Perfil\_de\_Sessao \Leftarrow B_0$
{ *Adiciona o Comportamento* B_0 *ao* $Perfil\_Implicito$ }
$Perfil\_Implicito \Leftarrow Perfil\_Implicito \cup B_0$
else
$Desafiador\ (\ User\ ,\ Nivel\ ,\ Natureza\ ,\ B_0\ )$
end if
Fim

4.4.3.2 Módulo de Desafio

O módulo de desafio (Desafiador), determina como o usuário será questionado a fim de provar sua identidade no no processo de autenticação, baseando-se na categorização feita pelo Analisador de Probabilidades e no nível de autenticação necessário para a operação desejada. A resposta ao desafio proposto ao usuário é, então, armazenada para consultas futuras. O funcionamento do Desafiador é detalhado no Algoritmo 4.

4.4.3.3 Módulo de Questões

Este módulo armazena os questionamentos e as respostas a serem realiazados ao usuário no momento em que ele é desafiado. O Quadro 4 apresenta alguns exemplos de questionamentos que podem ser utilizados.

Algoritmo 4 Funcionamento do Desafiador

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: $Natureza$ {Classificação da Natureza do Usuário, pode conter os valores $[USER\_NORMAL, USER\_SUSPEITO, USER\_ANORMAL]$ }
Parâmetro: $Nivel$ {Classificação do Nível de Restrição da Aplicação}
Parâmetro: B_0 {Comportamento do usuário que esta sendo analisado. Definido pela equação (1)}

Início
if $Natureza \in USER\_SUSPEITO$ **then**
  $Desafio \leftarrow Pesquisa\_Modulo\_Questoes\ (\ User\ ,\ Nivel\ ,\ SUSPEITO\ )$
else if $Natureza \in USER\_ANORMAL$ **then**
  $Desafio \leftarrow Pesquisa\_Modulo\_Questoes\ (\ User\ ,\ Nivel\ ,\ ANORMAL\ )$
end if
if $Desafiar\_Usuario\ (\ User\ ,\ Desafio\ ,\ Natureza\ )$ **then**
  $Autenticacao\_implcita\ (\ User\ )$
  { *Inicializa o* $Perfil\_de\_Sessao$ *com o Comportamento* B_0 }
  $Perfil\_de\_Sessao \Leftarrow B_0$
  { *Adiciona o Comportamento* B_0 *ao* $Perfil\_Implicito$ }
  $Perfil\_Implicito \Leftarrow Perfil\_Implicito \cup B_0$
else
  $Autenticacao\_Explicita\ (\ User\ )$
end if
Fim

Nível	Natureza Usuário	Desafio
Alto = 3	Suspeito	"Por favor, digite o número do CPF ?"
	Anormal	"Por favor, digite o login e a senha ?"
Médio = 2	Suspeito	"Por favor, digite data de nascimento ?"
	Anormal	"Por favor, digite os 4 últimos números da Carteira de Identidade ?"
Baixo = 1	Suspeito	"Por favor, digite o seu CEP ?"
	Anormal	"Por favor, digite a sua cor favorita ?"

Quadro 4: Desafio para Nível de Autenticação

4.5 ARQUITETURA POR NÍVEIS DE CONHECIMENTO

A arquitetura proposta é baseada na arquitetura cognitiva de Rasmussen (1983), mais especificamente no *Framework* SRK que permite classificar as diversas atividades executadas pelos usuários como habilidades, regras e conhecimentos. Porém, devido às limitações dos dispositivos móveis em relação a capacidade de processamento e armazenamento de informações, a arquitetura de autenticação proposta possibilita a execução dos processos de filtragens tanto nos dispositivos móveis (clientes), quanto nos servidores de autenticação.

Inicialmente, os processos de filtragens foram classificados em relação a capacidade de processamento, conforme Figura 15. Os Filtros de Recomendação que requisitavam recursos computacionais menores foram disponibilizados para execução nos dispositivos móveis, portanto os Filtros Baseados em Conteúdo deveriam ser processados somente nos clientes. Posteriormente, com o aumento do volume de informações e necessidade de certificação de aplicações que possuem informações críticas, estes tipos de filtros foram executados também no servidor de autenticação.

A especificação da arquitetura proposta através do SRK, segue com as diretivas adotadas no projeto, que tem como finalidade caracterizar os dispositivos móveis como artefatos cognitivos de interação com o usuário. Estes artefatos possuem uma modelagem funcional similar à modelagem cognitiva adotada pelos usuários, permitindo uma interação transparente entre artefato e usuário. Esta interação utilizará, basicamente, os níveis de habilidade e regras para comunicação com o usuário.

No processo de aquisição das informações de situacionalidade do usuário, o artefato cognitivo atuará como um monitor que registrará todas as informações relativas ao usuário e os demais contextos relevantes (conforme Figura 13) as atividades que estão sendo executadas. Estas informações armazenadas servirão de base para formação do contexto que poderá ser positivista (conforme a seção 2.2.1) ou Fenomenológico (conforme a seção 2.2.2).

4.6 FORMALIZAÇÃO DO MODELO COMPORTAMENTAL

Como os seres humanos possuem hábitos (WOOD *et al.*, 2002), e de acordo com Flanagan (2010) “os Seres Humanos são criaturas de hábitos e que a rotina permite uma sensação de controle”, podemos concluir que a execução destes hábitos estão relacionadas com o tempo e a localização, logo as

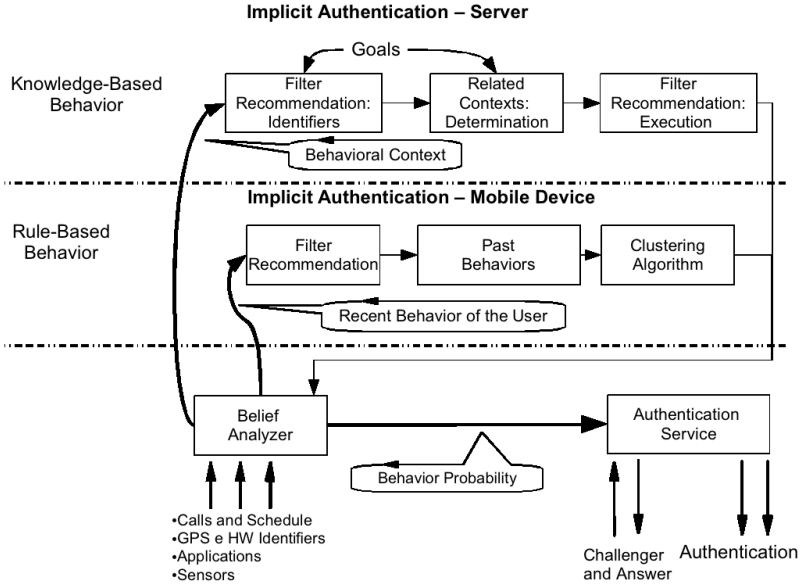


Figura 15: Arquitetura por Níveis de Conhecimento

correlações temporais são importantes para a determinação de eventos sucessivos. Deste modo, a inferência de eventos define as ações e comportamentos que o usuário irá adotar.

Este trabalho utiliza as definições formalizadas de comportamento de acordo com a equação 1, de contexto de acordo com a equação 3 e de atividade de acordo com a equação 4.

No primeiro momento foi utilizado o coseno de vetores para calcular a similaridade entre contextos e atividades. Porém, devido a diversidade de domínios que existem entre os elementos de cada um destes vetores foi necessário a normalização dos seus valores, caso similar foi reportado em (SU; KHOSHGOFTAAR, 2009). Para sanar este problema foi a adotado Correlação de Pearson.

A determinação de similaridade entre dois contextos diferentes é estabelecida através da similaridade de seus eventos e, assim, a possibilidade que atividades desenvolvidas nestes contextos possam ocorrer novamente. A

similaridade entre contexto é definida como

$$Sim\ (\ C_i\ ,\ C_j\ )\ =\ \frac{C_i\ \times\ C_j}{|\ C_i\ |\ \times\ |\ C_j\ |} \tag{5}$$

Aplicando-se a normalização de valores através da *Correlação de Pearson* na equação 5. A nova similaridade entre contextos será:

$$PCCc_{i,j} = \frac{\sum_{u\ \in\ U} (c_{u,i} - \overline{c_i})(c_{u,j} - \overline{c_j})}{\sqrt{\sum_{u\ \in\ U} (c_{u,i} - \overline{c_i})^2} \sqrt{\sum_{u\ \in\ U} (c_{u,j} - \overline{c_j})^2}} \tag{6}$$

A similaridade entre duas atividades pode ser determinada pela reutilização de ações entre as atividades ou pela similaridade entre as ações, definidas a seguir.

$$Sim\ (\ A_i\ ,\ A_j\ )\ =\ \frac{A_i\ \times\ A_j}{|\ A_i\ |\ \times\ |\ A_j\ |} \tag{7}$$

Aplicando-se a normalização de valores através da *Correlação de Pearson* na equação 7. A nova similaridade entre atividades será:

$$PCCa_{i,j} = \frac{\sum_{u\ \in\ U} (a_{u,i} - \overline{a_i})(a_{u,j} - \overline{a_j})}{\sqrt{\sum_{u\ \in\ U} (a_{u,i} - \overline{a_i})^2} \sqrt{\sum_{u\ \in\ U} (a_{u,j} - \overline{a_j})^2}} \tag{8}$$

As definições apresentadas, representam a modelagem do comportamento e a forma de se calcular como os contextos e as atividades podem ser considerados similares, a partir destas definições os processos de filtragem da abordagem de recomendação são caracterizados.

4.7 FILTROS PARA A ABORDAGEM DE RECOMENDAÇÃO

Neste trabalho foram considerados três filtros de recomendação. Nesta seção serão apresentadas as fundamentações e as equações para determinação do grau de similaridade entre os comportamentos dos usuários. A filtragem colaborativa é apresentada, porém, os resultados de sua utilização não serão apresentados devido ao baixo grau de similaridade e a dificuldade de se manter a privacidade dos usuários do grupo.

4.7.1 Filtragem Baseada em Conteúdo

A abordagem de recomendação utiliza as definições de comportamento do usuário para estabelecer as suas diretrizes, assim, se uma determinada atividade, em um contexto temporal passado, foi realizada ($Time_0$ na Figura 13), existe uma probabilidade razoável que esta mesma atividade possa ser executada novamente ($Time_{+1}$ na Figura 13). Este contexto temporal pode ser representado de forma análoga Oku *et al.* (2010):

$$\langle \underbrace{\ldots , (A_{-1} , C_{-1})}_{B_{Passado} = B_{-1}} , \overbrace{(A_0 , C_0)}^{B_{Presente} = B_0} , \underbrace{(A_{+1} , C_{+1}) , \ldots}_{B_{Futuro} = B_{+1}} \rangle \tag{9}$$

A filtragem baseada em conteúdo pode ser calculada no dispositivo móvel (chamado de filtro baseado em conteúdo local) e remotamente (chamado de filtro baseado em conteúdo remoto) em um servidor de autenticação. Logo, o cálculo local da similaridade entre o comportamento recente (passado) e o comportamento presente do usuário é determinado pela equação:

$$\begin{aligned} Sim (B_{-1} , B_0) &= Sim \big((A_{-1} , C_{-1}) , (A_0 , C_0) \big) \\ &= Sim (A_{-1} , A_0) \times Sim (C_{-1} , C_0) \end{aligned} \tag{10}$$

O funcionamento do filtro baseado em conteúdo local é detalhado no Algoritmo 5. Este algoritmo pesquisa as informações mais recentes sobre o contexto do usuário e calcula, através da equação (10), o grau de similaridade entre o comportamento presente (B_0) e o comportamento recente (passado) (B_{-1}).

O cálculo do filtro de conteúdo remoto da similaridade é semelhante ao do Algoritmo 5, porém, executado no servidor de autenticação.

As informações contextuais utilizadas neste processo de filtragem possuem características fenomenológicas, porque consideram o contexto como a interação social (ação situada) entre o usuário (situacionalidade) e o ambiente, no momento da execução da atividade.

Algoritmo 5 Funcionamento do Filtro de Conteúdo Local

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: B_0 {Comportamento presente do usuário que está sendo analisado}

Retorno: {Retorna grau de similaridade do filtro local }

Início
$B\_Anterior \Leftarrow Pesquisar\_Perfil\_Sessao\ (\ User\ )$

{A função Calcular_Filtro_Conteudo_Local implementa a equação (10)}

return $Calcular\_Filtro\_Conteudo\_Local\ (\ B\_Anterior\ ,\ B_0\ )$
Fim

4.7.2 Filtragem Colaborativa

As informações contextuais utilizadas neste processo de filtragem possuem características positivistas, porque consideram o contexto com um cenário que poderá ser utilizado para a determinação das interações comportamentais dos demais usuários com o ambiente.

Este filtro tem como objetivo encontrar outros usuários que possuam um perfil semelhante ao do usuário que está sendo autenticado, com isso é possível determinar se o usuário de comportamento B_0 possui comportamento semelhante àqueles armazenados no banco de dados. A utilização deste filtro necessita que os usuários reduzam a sua privacidade e permitam que seus comportamentos sirvam de base para a determinação da similaridade.

O filtro colaborativo realiza busca em uma matriz tridimensional $\langle\ usuario\ x\ contexto\ x\ atividades\ \rangle$ que, formalmente, é representada por: $R: \langle\ U\ x\ C\ x\ A\ \rangle \rightarrow Sim$, onde *Sim* possui o valor de avaliação no espaço de resultado com domínio estipulado entre [0 , 1.00], sendo que quanto mais próximo de 1 mais similar serão os comportamentos entre os usuários. O *Sim* normaliza os valores e transforma as relações entre os comportamentos, em uma relação linear que pode ser representada em um plano cartesiano, conforme a Figura 16.

Este processo de filtragem utiliza as informações comportamentais dos

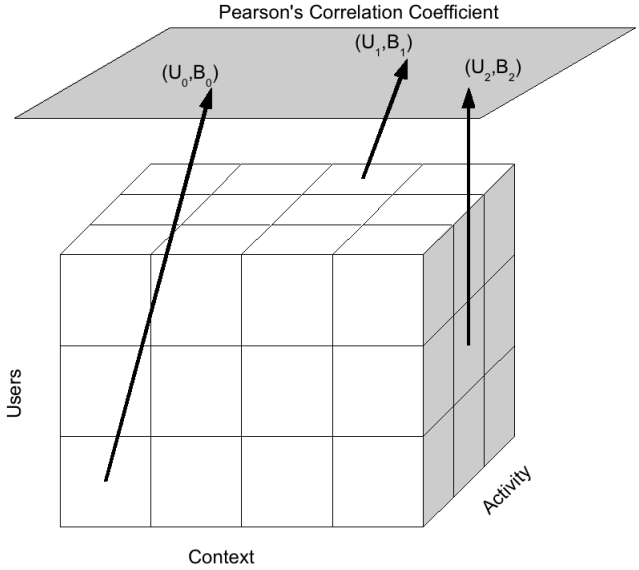


Figura 16: Correlação de Person's aplicado a Filtragem Colaborativa

demais usuários $\Big\langle \underbrace{\big(B_1 = (A_1, C_1)\big)}_{User_1}, \overbrace{\big(B_2\big)}^{User_2}, \underbrace{\big(B_3\big)}_{User_3}, \ldots \Big\rangle$ para prever o comportamento do usuário que está sendo autenticado implícitamente. $\Big\langle \underbrace{\big(B_0 = (A_0, C_0)\big)}_{User_{em\ Autenticacao}} \Big\rangle$. Logo, a similaridade pode agora ser aplicada ao comportamento dos usuários, sendo definida como:

$$\begin{aligned} Sim(B_0, B_1) &= Sim\big((A_0, C_0), (A_1, C_1)\big) \\ &= Sim(A_0, A_1) \times Sim(C_0, C_1) \end{aligned} \tag{11}$$

$$\begin{aligned} Sim(B_0, B_2) &= Sim\big((A_0, C_0), (A_2, C_2)\big) \\ &= Sim(A_0, A_2) \times Sim(C_0, C_2) \end{aligned} \tag{12}$$

4.7.3 Filtragem Híbrida

Na recomendação híbrida é utilizado o modelo de permutação espaço-temporal de Kulldorff (2005), que realiza uma varredura para detecção de conglomerados de dados no espaço e no tempo simultaneamente, considerando casos (contextos) e covariáveis (atividades). A fim de determinar as regiões dos conglomerados, utiliza-se a ferramenta SaTScan, desenvolvida por Kulldorff (2005). A significância estatística é validada utilizando-se o teste de hipótese de Monte Carlo.

A probabilidade condicional $P(E_a)$ da atividade possibilita estimar se a atividade estava ocorrendo no contexto e se ela está ocorrendo atualmente. Assim, existem quatro casos possíveis:

- Mesma atividade no mesmo contexto espaço-temporal – a atividade se repete dentro do mesmo contexto;
- Mesma atividade em contexto espaço-temporal diferente – existem dois contextos onde ocorrem a mesma atividade;
- Atividades diferentes no mesmo contexto espaço-temporal – as atividades formam o mesmo contexto;
- Atividades diferentes em contexto espaço-temporal diferente – existem dois contextos com atividades independentes.

O funcionamento do filtro híbrido é detalhado no Algoritmo 6. Este algoritmo pesquisa as informações na base de dados de perfis (explícito e implícito), formando um vetor de comportamentos, que será enviado em conjunto com o comportamento presente B_0 para uma ferramenta estatística espaço-temporal, que efetuará o cálculo do grau de similaridade.

As informações contextuais utilizadas neste processo de filtragem possuem características positivistas, porque consideram o contexto com um cenário que poderá ser utilizado para a determinação das interações comportamentais dos demais usuários com o ambiente.

4.7.3.1 Análise Estatística Espaço-Temporal

A análise estatística espaço-temporal, apresentada na Figura 17, é definida por uma janela cilíndrica com uma base geográfica circular (ou elíptica,

Algoritmo 6 Funcionamento do Filtro Híbrido

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: B_0 {Comportamento presente do usuário que esta sendo analisado}

Retorno: {Retorna grau de similaridade do filtro local }

Início
$P\_Extendido \Leftarrow Pesquisar\_Perfil\_Explicito\ (\ User\ )$
$P\_Extendido \Leftarrow P\_Extendido \cup Pesquisar\_Perfil\_Implicito\ (\ User\ )$

{A função Calcular_Filtro_Hibrido realiza a chamada da feramenta estatística espaço-temporal, que irá realizar o cálculo da Permutação Espaço-Temporal e sua similaridade, conforme seção 4.7.3.2}

return $Calcular\_Filtro\_Hibrido\ (\ B_0\ ,\ P\_Extendido\ )$
Fim

representado pelos elementos: z_0, z_1, z_2) e com uma altura correspondente ao tempo (representado pelos elementos: t_0, t_1, t_2). A base é definida exatamente como na análise estatística puramente espacial, enquanto a altura reflete o período de tempo de conglomerados potenciais.

A janela cilíndrica é, então, movida no espaço e tempo, de modo que para cada possível localização geográfica e tamanho, a janela também visita cada período de tempo possível. Na realidade, obtém-se um número infinito de cilindros sobrepostos de diferentes tamanhos e formas, ou seja, um conjunto que abrange toda a região de estudo, onde cada cilindro reflete um possível conglomerado.

A análise estatística espaço-temporal pode ser utilizada tanto para a análise retrospectiva, utilizando-se dados históricos, ou para o acompanhamento prospectivo periódico, onde a análise é repetida, por exemplo, diariamente, semanalmente ou mensalmente.

4.7.3.2 Permutação Espaço-Temporal

Os eventos observados na execução das atividades são armazenados em um banco de dados que serão utilizados no processo de detecção de *clusters* (agrupamentos) de informação, que irá explicitar os hábitos dos usuários.

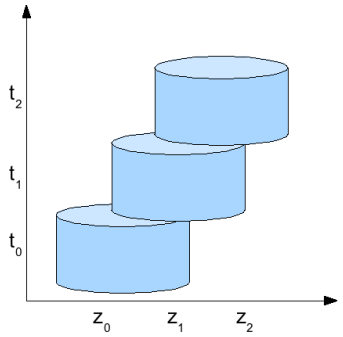


Figura 17: Janelas Cilíndricas da Estatística Espaço-Temporal

Esses agrupamentos podem ser classificados em três grandes categorias:

- agrupamentos puramente espaciais - a ocorrência é maior em algumas regiões do que em outras;
- agrupamentos puramente temporal - apresentam a ocorrência de acontecimentos como sendo maior em um determinado período do que em outros;
- agrupamentos espaço-temporal - ocorrem quando os eventos são temporariamente mais elevados em certas regiões do que em outras, isto permite uma definição no tempo e no espaço.

Os agrupamentos espaço-temporais permitem definir os hábitos dos usuários, porque os hábitos são formados por atividades, que são executadas pelos usuários ao se deslocarem no tempo e no espaço dentro do ambiente pervasivo. Uma das modelagens existentes para prever os eventos num contexto espaço-temporal é a permutação espaço-temporal, que permite a incorporação de informações de covariáveis que são, normalmente, encontradas em outros contextos dentro do espaço pervasivo.

De acordo com Kulldorff (2005), o modelo de permutação espaço-temporal é baseada em três características:

- detecção de *clusters* de dados no espaço e no tempo, simultaneamente;
- trabalha com eventos únicos ou casos; e
- aplicação do modelo probabilístico em uma hipótese nula conclui-se que os eventos seguem uma distribuição hipergeométrica.

Assumindo que a contagem de eventos e, no conjunto de linha de tempo t, localizado em uma região, z, com características circulares de acordo com coordenadas GPS, é definido como e_{zt}. O número total de eventos observados, E, são expressos pela fórmula:

$$E = \sum_{z} \sum_{t} e_{zt} \tag{13}$$

O número total de eventos condicionados, M_{zt}, são expressos pela fórmula:

$$M_{zt} = \frac{1}{E} \left(\sum_{z} E_{zt} \right) \left(\sum_{t} E_{zt} \right) \tag{14}$$

A previsão de um evento compreende a seguinte hipótese: a probabilidade condicional de um evento $P(E_a)$, na região z foi observado no momento t_1 e t_2, define um determinado cilindro a , que se refere a um possível agrupamento, portanto, E_a tem uma média de M_a e segue a distribuição hipergeométrica determinada pela seguinte função:

$$M_a = \sum_{(z,t) \in A} M_{zt} \tag{15}$$

$$P(E_a) = \begin{pmatrix} \sum\limits_{t \in (t_1 \vee t_2)} \sum\limits_{z \in A} E_{zt} \\ E_a \end{pmatrix} \frac{\begin{pmatrix} E - \left(\sum\limits_{t \in (t_1 \vee t_2)} \sum\limits_{z \in A} E_{zt} \right) \\ \left(\sum\limits_{t \in (t_1 \vee t_2)} \sum\limits_{z \in A} E_{zt} \right) - E_a \end{pmatrix}}{\begin{pmatrix} E \\ \sum\limits_{t \in (t_1 \vee t_2)} \sum\limits_{z \in A} E_{zt} \end{pmatrix}} \tag{16}$$

Para determinar as probabilidades condicionais das atividades dos usuários no espaço pervasivo foi utilizado a ferramenta **SaTScan** desenvolvida por Kulldorff (2005), que determina as regiões dos agrupamentos e a sua significância estatística, sendo esta validada através da utilização de um teste de hipótese de Monte Carlo.

A probabilidade condicional das atividades do usuário $P(E_a)$ fornece uma estimativa de atividades passadas e presentes do usuário. Assim, existem quatro casos que podem ocorrer:

- a execução normal - indica que a mesma atividade está sendo executada no mesmo contexto espaço-temporal;

- a execução anormal - indica que diferentes atividades em execução em diferentes contextos espaço-temporal;
- a execução suspeita por contexto - indica que a mesma atividade é realizada em um contexto espaço-temporal diferente, neste caso o contexto de segurança relevante da atividade definirá as políticas de autenticação;
- a execução suspeita por atividade - indicada quando diferentes atividades ocorrem no mesmo contexto espaço-temporal.

4.7.3.3 Ferramenta Estatística SaTScan

Para o desenvolvimento deste trabalho, optou-se por utilizar a ferramenta estatística SaTScan (KULLDORFF, 2005), que é um software livre que visa a análise de dados espaciais, temporais e espaço-temporais. Tal software foi desenvolvido para atender aos seguintes propósitos:

- Realizar o acompanhamento geográfico de doenças, detectar conglomerados (*clusters*) de doenças sobre uma perspectiva espacial ou espaço-temporal e verificar se tais conglomerados são estatisticamente significantes;
- Testar se uma doença é aleatoriamente distribuída sobre o espaço, tempo, ou espaço e tempo, simultaneamente;
- Avaliar a significância estatística de possíveis alarmes de conglomerados de doenças;
- Realizar o acompanhamento periódico de doenças a fim de detectar previamente surtos de doenças;
- Detecção de agrupamentos dos alertas de desmatamento (PINHEIRO *et al.*, 2009); e
- Detecção de conglomerados de homicídios e o tráfico de drogas (FILHO *et al.*, 2001);

Além disso, o software pode ser aplicado em problemas similares em outros campos de pesquisa, como: arqueologia, astronomia, criminologia, ecologia, economia, engenharia, genética, geografia, etc.

O ambiente da ferramenta SaTScan possui sete diferentes modelos de probabilidade para as estatísticas de variáveis discretas. Para dados de contagem, existem os modelos: (1) Distribuição de Poisson, (2) Distribuição Bernoulli e (3) Permutação espaço-tempo. Os modelos (4) Ordinais e (5) Multinomial são projetados para dados categóricos estando estes ordenados ou não. Existem, também, dois modelos para dados contínuos: (6) Distribuição Normal e (7) Distribuição Exponencial. Este último é projetado, principalmente, para os dados de tipo de sobrevivência. Para as estatísticas contínuas existe apenas o modelo de Poisson homogêneo.

A distribuição de Poisson e o modelo de permutação espaço-tempo, permitem um número ilimitado de co-variáveis. Na distribuição de Bernoulli, modelo ordinal, distribuição exponencial e distribuição normal, as co-variáveis podem ser ajustadas para usar diversos conjuntos de dados, o que limita o número de categorias de co-variáveis que podem ser definidas.

Todos os modelos de probabilidade de variáveis discretas podem ser utilizados tanto para localizações individuais, como para agrupamento de dados. O modelo de permutação espaço-tempo se ajusta automaticamente para agrupamentos puramente espaciais e puramente temporal.

4.8 INFLUÊNCIA DAS ABORDAGENS ANALISADAS NESTA PROPOSTO

A abordagem proposta foi influenciada por um conjunto de conceitos e modelos da Ciência da Computação e Engenharia do Conhecimento, porém algumas idéias estavam presentes nos trabalhos relacionados e analisados na seção 3.3. A Figura 18, demonstra graficamente os arcabouços teóricos utilizados e os elementos de cada trabalhalho relacionado que influenciaram esta abordagem.

A abordagem de Corradi *et al.* (2004), apresentada na seção 3.3.4, utiliza os conceitos de "contextos" físicos e lógicos associados ao "perfil do usuário" para determinar o controle de acesso aos dispositivos. Esta abordagem demonstra que desde 2004, já existia a idéia de se utilizar contexto como mecanismo de segurança e que era possível exptender esta visão para utiliza-lo como intrumento de autenticação. Porém era necessário embasar o conceitos de contexto em melhores referencíais teóricos.

Um dos referenciais teórico apresentado neste trabalho enfatiza o conceito de contexto, que pode ser explicado através das correntes de pensamento positivistas e fenomenológicas estudados na Engenharia do Conhecimento,

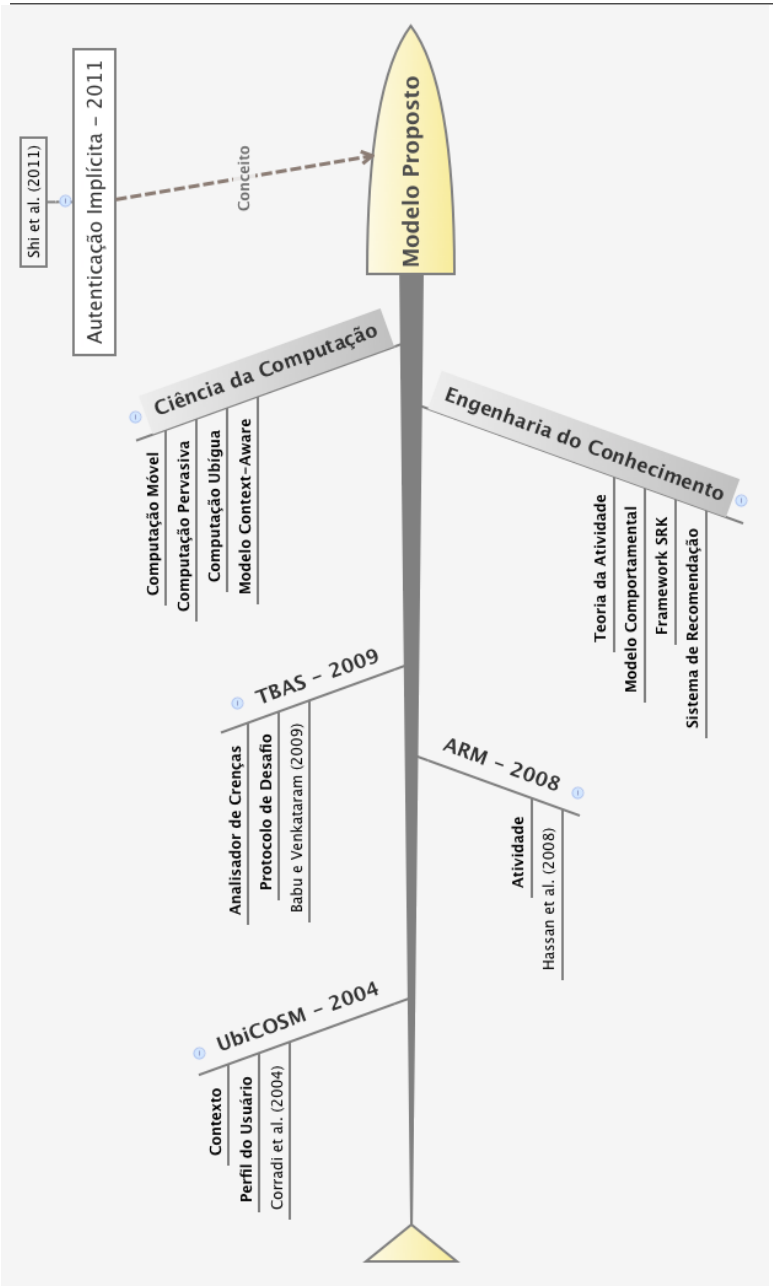


Figura 18: Influência das Abordagens Analisadas nesta Proposta

como tambem, pelos conceitos da computação ubíqua e computação consciente de contexto da ciência da computação. Neste trabalho foi utilizado os conceitos destas 2 áreas para definir e escolher um modelo de contexto que explicitasse o conhecimento comportamental dos usuários.

Na abordagem de Hung *et al.* (2008), apresentada na seção 3.3.3, na qual descreve a utilização das informações das "atividades" dos usuários como fonte para estabelecer as permissões de controle de acesso aos usuários, embora, o processamento de imagens tenha papel mais relevante na autenticação. A utilização das atividades para descrever o usuário e permitir o acesso as informações se revela um ideia interessante. Porém estas atividades devem ser contextualizadas, já que possuem caracteristicas específicas de comportamento e de hábito do usuário.

A teoria da atividade associada ao modelo de consciência de contexto produz um modelo de referência para classificar os contextos existentes e os contextos relevantes a computação pervasiva, esta associação permite validar o modelo e a arquitetura em relação a cognição situada, já que utiliza uma teoria consolidada para formalizar o ambiente onde o usuários está imerso e a relações deste com os objetos, artefatos e ferramentas.

Na abordagem de Babu e Venkataram (2009), apresentada na seção 3.3.2, são descritos: i) a utilização de um "analisador de crenças" para inferir o comportamento do usuário através de agentes inteligentes e ii) um "componente de desafios" que tem a função de evitar ataques através de perguntas e respostas simples. O modelo proposto neste trabalho incorporou os dois conceitos e de forma a homenagear estas idéías manteve as mesmas nomenclaturas.

A abordagem de recomendação adotado no trabalho permite a incorporação de filtros de recomendação. Desta forma, o processo de autenticação torna-se adaptativo porque permite adição de filtros que reconheçam novos comportamento (atividades e contextos) sem a necessidade de alterar o processo de autenticação. A classificação destes filtros e comportamento será realizada por implementação particular do *framework* SRK (RASMUSSEN, 1983).

A abordagem de Shi *et al.* (2011), apresentada na seção 3.3.1, introduz o termo "Autenticação Implícita" para efetuar o processo de autenticação através do comportamento do usuário a partir de escores de utilização de aplicações. Este termo foi incorporado a proposta do trabalho por refletir exatamente o processo de autenticação que será realizado quando da tomada de decisão pela abordagem de recomendação de autenticação. É importante salientar que a arquitetura proposta deste trabalho já estava consolidada e já havia

sido publicada, pelo autor desta Tese, em congresso internacional através do artigo *"An authentication approach based on behavioral profiles"* (LIMA *et al.*, 2010).

4.8.1 Comparativo entre a Abordagem desta Tese e as demais Abordagens de Autenticação Orientada ao Comportamento do Usuário com

O comparativo apresentado nesta seção, relaciona as abordagens apresentadas na seção 3.3 com a abordagem desta Tese (apresentada neste capítulo). Para apresentar o comparativo foi expandido o Quadro 2, para incorporar as características desta Tese, resultando o Quadro 5.

Esta Tese possui diferenciais em relação as demais abordagens porque explora características relevantes ao processo de autenticação para dispositivos móveis. As principais características incorporadas, são:

- Utilização de um modelo estatístico espaço-temporal como mecanismo de inferência de localização no tempo e no espaço dos comportamentos dos usuários;
- Utilização de mecanismos de autenticação tanto no cliente (dispositívo móvel), como no servidores de autenticação;
- Utilização de *frameworks* e conceitos da psicologia cognitiva para modelar o comportamento dos usuários e permitir a autenticação nos dispositivos móveis.

4.9 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foi apresentado o modelo e a arquitetura de autenticação implícita elaborados nesta Tese. A arquitetura proposta, utiliza os conceitos de sistema de recomendação com o objetivo de incorporar, de forma dinâmica, novos filtros e permitir a sua adaptabilidade a novas necessidades dos usuários, que utilizam dispositivos móveis para realização de suas tarefas diárias e trabalho móvel.

A utilização do modelo de contexto proposto por Cassens e Kofod-Petersen (2006) permitiu modelar o comportamento dos usuários através da TAHC (KUUTTI, 1996). Os contextos relevantes a este trabalho são apresenta-

Características	Proposta	Autenticação Implícita por Comportamento	Autenticação no Nível de Transação	Autenticação por Reconhecimento de Atividades	Autenticação Baseada no Contexto
Bibliográfia e Referência no texto					
Bibliográfia		Shi *et al.* (2011)	Babu e Venkataram (2009)	Hung *et al.* (2008)	Corradi *et al.* (2004)
Referência	Capítulo 4	Seção 3.3.1	Seção 3.3.2	Seção 3.3.3	Seção 3.3.4
Critérios para Análise das Abordagens					
Modelo Contextual	Espaço Temporal	Espaço Temporal limitado	Espacial	Espacial	Espacial
Modelo Comportamental	Perfil Dinâmico com Filtros Adaptativos	Perfil Dinâmico com Filtros através de escores	Agentes Cognitivos	Explícito	Perfil Estático
Atomicidade e Dinamicidade	Sim	Sim	Sim	Não	Não
Flexibilidade	Sim	Não	Sim	Não	Sim
Privacidade	Sim	Sim	Não	Não	Sim
Local de Controle de Autenticação	Cliente e Servidor	Cliente	Cliente	Cliente	Servidor

Quadro 5: Quadro das Abordagens de Autenticação Orientada ao Comportamento do Usuário Incorporando a Proposta da Tese

dos no Quadro 3, que descreve o relacionamento entre os aspectos da TAHC e as categorias contextuais.

Os comportamentos dos usuários são modelados como um conjunto de características de contexto e as atividades que os usuários executam. De acordo com Duhigg (2012) os indivíduos possuem rotinas diárias, semanais e mensais que formam um conjunto de hábitos, executados regular e frequentemente. Estes hábitos permitem determinar, de forma implícita, se o mesmo usuário está executando as suas rotinas ou se outra pessoa está tentando ter acesso indevido ao seu dispositivo móvel. Portanto, a combinação das características contextuais e as atividades (hábitos) auxiliam o processo de identificação e autenticação do usuários.

Os filtros de recomendação são classificados como locais e remotos, através da arquitetura cognitiva de Rasmussen (1983), que permite classificar os filtros de acordo com o tipo de comportamento (baseado em conhecimento ou baseado em regras) e da necessidade de processamento. Esta classificação delimita o uso dos recursos computacionais dos dispositivos móveis e permite a utilização dos recursos computacionais dos servidores de autenticação. Os filtros formalizados e implementados foram:

- **Filtro híbrido:** utiliza a permutação espaço-temporal como mecanismo base para o calculo da similaridade entre os comportamentos. A adoção da ferramenta estatística espaço-temporal, conforme seção 4.7.3.2, permitiu a utilização de um modelo estatístico que possibilita a variação na localização e no tempo simultaneamente, requisito básico para os usuários do trabalho móvel;

- **Filtro Baseado em Conteúdo:** possui características fenomenológicas e permite que a autenticação possa ser realizada:

  - Local - implementado no dispositivo móvel através de um algoritmo simplificado que calcula a similaridade entre os comportamentos recentes com o comportamento atual;
  - Remoto - implementado no servidor de autenticação através de um algoritmo que calcula a similaridade entre o comportamento atual e o centroide do agrupamento dos comportamentos recentes.

- **Filtro Colaborativo:** especificado formalmente neste trabalho, porém, devido aos dados coletados para análise serem uma amostra reduzida, os resultados não foram expressivos e a sua utilização não pode ser considerada. Entretanto, em novos trabalhos, devem ser coletadas novas amostras com maior diversidade de usuários e uma relação deve

ser estabelecida sobre a sua utilização e sobre a sua relevância para o processo de autenticação implícita.

Esta Tese foi influenciada pelas abordagens relacionadas e diversos elementos foram incorporados e expandidos, conforme relatado na seção 4.8, porém, a característica interdisciplinar que possui esta Tese foi moldada na época da realização de créditos, em especial na disciplina de Introdução a Cognição. Esta disciplina despertou o interesse e agregou referenciais teóricos que possibilitaram o desenvolvimento da pesquisa.

5 PROCESSOS DE FILTRAGEM COM EXPERIMENTOS

Neste capítulo são apresentados: o cenário dos experimentos, os processos de filtragem, os quais tem como objetivo delinear o que será apresentado como resultado de pesquisa desta Tese.

Os resultados são apresentados através dos processos de filtragens relacionados na seção 4.7. Com a finalidade de facilitar a compreensão, são apresentados esquemas diagramáticos que ilustram o fluxo de informação e conhecimento em cada um de seus níveis.

Ao final do capítulo é apresentada uma análise dos resultados experimentais realizados.

5.1 CENÁRIO DOS EXPERIMENTOS

Os dados foram coletados através de dois dispositivos móveis durante duas semanas, com um total de 280 eventos, que foram contextualizados através das suas características comportamentais. Para formalizar o comportamento dos usuários optou-se pelos seguintes parâmetros: dispositivo móvel utilizado, localização, marca de tempo (*timestamp*) do momento em que o evento ocorre, aplicação executada, restrição da aplicação executada, ligações realizadas ($Call_{out}$) e SMS enviados (SMS_{out}) que estão fora da agenda.

Neste período, três usuários utilizaram os dispositivos móveis para realizar suas tarefas diárias. Estas tarefas, basicamente, estavam relacionadas com o deslocamento diário dos usuários de suas residências até o Campus da Universidade e sua utilização diária.

5.2 FILTRAGEM HÍBRIDA

Os resultados apresentados nesta seção estão relacionadas com a filtragem híbrida e foram parcialmente publicado em Lima *et al.* (2011). A filtragem híbrida utiliza a ferramenta de permutação estatística para determinação dos agrupamentos espaço-temporais, porém, a resposta da permutação espaço-temporal não pode ser utilizada diretamente, devido a mobilidade dos usuários em especial os trabalhadores móveis do conhecimento (jornalistas, agentes do estado e outros), que se deslocam com frequência, em grandes distâncias e para locais ainda não visitados para realizar as suas atividades.

Com o objetivo de explicitar as interações entre os componentes da

arquitetura proposta, será realizado um ciclo de autenticação implícita utilizando a filtragem híbrida. Na interação zero (0) é realizada uma autenticação explícita que definirá os valores para o comportamento anterior B_{-1} e os valores dos elementos do vetor de pesos acumulativos da sessão para o filtro híbrido (PBH). As interações posteriores utilizarão essas informações para determinar a necessidade de autenticação implícita ou de uma nova autenticação explícita. O experimento é apresentado através dos passos das interações, representados por itens numerados, que correspondem aos marcadores da Figura 19, os valores utilizados como exemplo para cada item, corresponde a primeira interação do Quadro 6.

Interações	Permutação Espaço-Temporal (%)	Similaridade (%)	Tempo	Localização	Dispositivo	Aplicação	Restrição	Ligações de Saída	SMS de Saída
1	82,6000	89,1156	0,8260	0,8260	1	1	1	1	1
2	82,6017	87,2426	0,8260	0,8260	1	0	1	1	1
3	82,6022	71,0766	0,8260	0,8260	1	-1	1	1	1
4	82,6044	51,1607	0,8260	0,8260	1	-2	1	1	1
5	82,6049	89,1167	0,8260	0,8260	1	1	1	1	1
6	82,6059	87,2436	0,8261	0,8261	1	1	1	0	1
7	82,6060	71,0776	0,8261	0,8261	1	1	1	-1	1
8	82,6077	89,1173	0,8261	0,8261	1	1	1	1	1
9	82,6091	89,1176	0,8261	0,8261	1	1	1	1	1
10	82,6120	85,8322	0,8261	0,8261	1	1	1	0	0

Quadro 6: Interações de Autenticação para Filtro Híbrido

Para a execução destes experimentos e das interações do usuário, optou-se pelos seguintes parâmetros definidos no cenário, que são: dispositivo móvel utilizado, localização, marca de tempo (*timestamp*) do momento em que o evento ocorre, aplicação executada, restrição da aplicação executada, ligações realizadas e SMS enviados que estão fora da agenda. Estes são os principais passos de uma interação:

1. O dispositivo móvel captura as atividades ($A_1 = \langle a_1 , \ldots , a_n \rangle , \ldots , A_n$) e os contextos ($C_1 = \langle timestamp , location , E_1 , \ldots , E_n \rangle , \ldots , C_n$) que o usuário está executando na realização de suas tarefas e envia para o analisador de crenças;

2. O analisador de crenças cria o comportamento (B_0), através das atividades e dos contextos enviados pela interação anterior e envia à filtragem híbrida. No exemplo da primeira interação, temos $B_0 = \langle\ C_{timestamp} = 126504,\ C_{location} = 27.594,\ C_{device} = 2,\ A_{app} = 10,\ A_{apprestrict} = 2,\ A_{call} = 99990001,\ A_{SMS} = 99990002\ \rangle$;

3. O filtro híbrido localiza os comportamentos anteriores do usuário que

estão armazenados na base de dados de perfil (especificamente os perfis explícitos e implícitos) e envia estes perfis juntamente com o comportamento B_0 para uma Ferramenta estatística espaço-temporal;

4. A Ferramenta estatística calcula a probabilidade condicional $P(E_a)$ determinada pelo modelo de permutação espaço-temporal através da equação (16) e envia este valor para a filtro híbrido. No exemplo: $P(E_a) = 0.8260$;

5. O filtro híbrido calcula a similaridade do comportamento B_0 com os comportamentos anteriores para enviar ao analisador de crenças. O cálculo da similaridade neste filtro possui o seguinte procedimento:

   - De acordo com os elementos do vetor comportamento B_0 são recuperados da base de dados de perfil os pesos definidos anteriormente para cada um destes elementos, montando-se o vetor $P = \langle P.elemento_1 \ , \ \ldots \ , \ P.elemento_n \rangle$. No exemplo: $P = \langle \ P_{timestamp} = 0.2326, \ P_{location} = 0.2326, \ P_{device} = 0.1163, \ P_{app} = 0.0930, \ P_{apprestrict} = 0.1395, \ P_{call} = 0.0930, \ P_{SMS} = 0.0930 \ \rangle$;
   - O vetor $PBH = \langle PBH.elemento_1 \ , \ \ldots \ , \ PBH.elemento_n \rangle$ é recuperado da base de dados de perfil e possuirá os mesmos elementos do vetor P, porém, os valores atribuídos aos elementos resultará da comparação entre o comportamento B_0 e o perfil de sessão (comportamento atual B_{-1}). Os valores atribuídos aos elemento PBH_i são:
     - Se $B_0.i = B_{-1}.i$ então $PBH_i \Leftarrow 1$
     - Se $B_0.i \neq B_{-1}.i$ então $PBH_i \Leftarrow PBH_i - 1$

     No exemplo: $PBH = \langle \ PBH_{timestamp} = 1, \ PBH_{location} = 1, \ PBH_{device} = 1, \ PBH_{app} = 1, \ PBH_{apprestrict} = 1, \ PBH_{call} = 1, \ PBH_{SMS} = 1 \ \rangle$;
   - Para os elementos espaço-temporais (*location* e *timestamp*), o valor a ser atribuído é o valor calculado pela ferramenta estatística no marcador 4, sendo então:

     $$\begin{aligned} PBH_{timestamp} &\Leftarrow P(E_a) \\ PBH_{location} &\Leftarrow P(E_a) \end{aligned}$$

     No exemplo: $PBH = \langle \ PBH_{timestamp} = 0.8260, \ PBH_{location} = 0.8260, \ PBH_{device} = 1, \ PBH_{app} = 1, \ PBH_{apprestrict} = 1, \ PBH_{call} = 1, \ PBH_{SMS} = 1 \ \rangle$;

- O cálculo de similaridade é realizado entre os vetores *PBH* e *P* através da equação $Sim\ (\ PBH\ ,\ P\ ) = \frac{PBH \times P}{|\ PBH\ | \times |\ P\ |}$. No exemplo: $Sim\ (\ PBH\ ,\ P\ ) = 0.891156$

6. O analisador de crenças, ao receber o valor de similaridade *Sim* compara com os dos demais filtros e envia o maior (analisador configurado como otimista) valor para o analisador de probabilidades;

7. O analisador de probabilidades, através da similaridade *Sim*, determina a natureza do usuário, que pode ser: Normal, Suspeito ou Anormal.

   - Se o usurário for considerado Normal a autenticação implícita é realizada e executa-se os passos do marcador (10);
   - Caso contrário, o usuário é considerado Suspeito ou Anormal e as informações de Natureza do usuário e comportamento B_0 são enviados para o desafiador;

8. O desafiador pesquisa na base de dados de questão qual deve ser o questionamento a ser realizado ao usuário, já que o comportamento B_0 possui um grau de similaridade abaixo do esperado pelo sistema de autenticação;

9. A pergunta é enviada ao usuário:

   - Caso o usuário responda corretamente, a autenticação implícita é realizada e executa-se os passos do marcador (10);
   - Caso contrário, é requisitada uma autenticação explícita e se o usuário for autenticado corretamente executa-se os passos do marcador (10);

10. As informações sobre o comportamento B_0 e o grau de similaridade são armazenados na base de dados de perfil. O perfil de sessão é atualizado com valores do comportamento B_0.

    - Se o usuário foi questionado (explicitamente ou implicitamente por ser considerado Suspeito ou Anormal) o vetor *PBH* receberá valor 1 para todos os seus elementos e será armazenado na base de dados de perfil;
    - Caso contrário, o vetor *PBH* será armazenado na base de dados de perfil com os valores alterados pela interação. No exemplo: $PBH = \langle\ PBH_{timestamp} = 0.8260,\ PBH_{location} =$

0.8260, $PBH_{device} = 1$, $PBH_{app} = 1$, $PBH_{apprestrict} = 1$, $PBH_{call} = 1$, $PBH_{SMS} = 1 \rangle$.

A partir do passos de uma interação, apresentados na Figura 19, é possível realizar simulações para demonstrar como o sistema se comporta com outras interações. Com o objetivo de demonstrar a relevância do vetor *PBH*, foram realizadas outras interações, apresentadas no Quadro 6 e representadas graficamente na Figura 20.

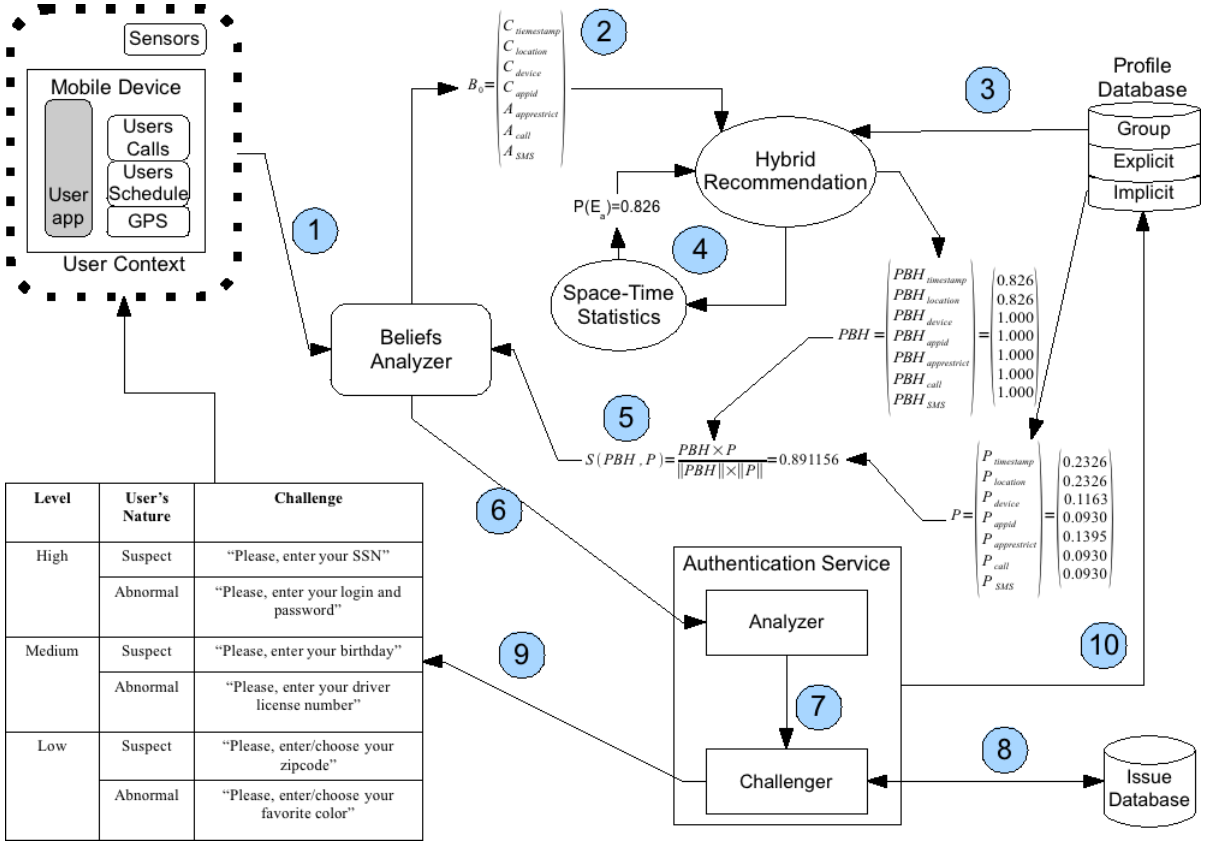
Nas interações (2), (3) e (4), o usuário realizou no mesmo espaço-tempo a execução de uma aplicação diferente das normalmente utilizadas, portanto, o elemento PBH_{appid} sofreu decréscimos sucessivos, que influenciaram na redução do grau de similaridade dos comportamentos esperados para este usuário. Na interação (5), o sistema solicitou uma autenticação explícita, reinicializando os elementos do vetor *PBH* para 1.

Nas interações (6) e (7), no mesmo espaço-tempo o usuário realizou ligações telefônicas para números que não estavam cadastrados na agenda. Nas interações (8) e (9) realizou tarefas definidas como comportamento normal, por exemplo enviar SMS e ligar para pessoas cadastradas na agenda e utilizar aplicações habituais. A interação (10), apresenta a influência da realização de dois eventos diferentes dos habituais e sua repercussão no sistema.

A partir desta representação gráfica, Figura 20, é possível constatar que a filtragem híbrida permite uma variação nas características comportamentais do usuário, caso das interações (2), (6) e (10). Caso a variação exceder os limites de similaridade dos comportamentos uma autenticação implícita é realizada através de questionamento ou, no pior dos casos, uma autenticação explícita é executada.

5.2.1 Determinação dos Parâmetros do Filtro Híbrido

Na implementação dos filtros híbridos foi necessário a parametrização de vetores auxiliares para indicar: o comportamento do usuário, definir quais elementos dentro do vetor comportamento devem ser prioritários e quais os critérios de classificação da natureza do usuário. Estes parâmetros são especificados e discutidos nas próximas seções.



Level	User's Nature	Challenge
High	Suspect	"Please, enter your SSN"
	Abnormal	"Please, enter your login and password"
Medium	Suspect	"Please, enter your birthday"
	Abnormal	"Please, enter your driver license number"
Low	Suspect	"Please, enter/choose your zipcode"
	Abnormal	"Please, enter/choose your favorite color"

Figura 19: Resultados da Filtragem Híbrida

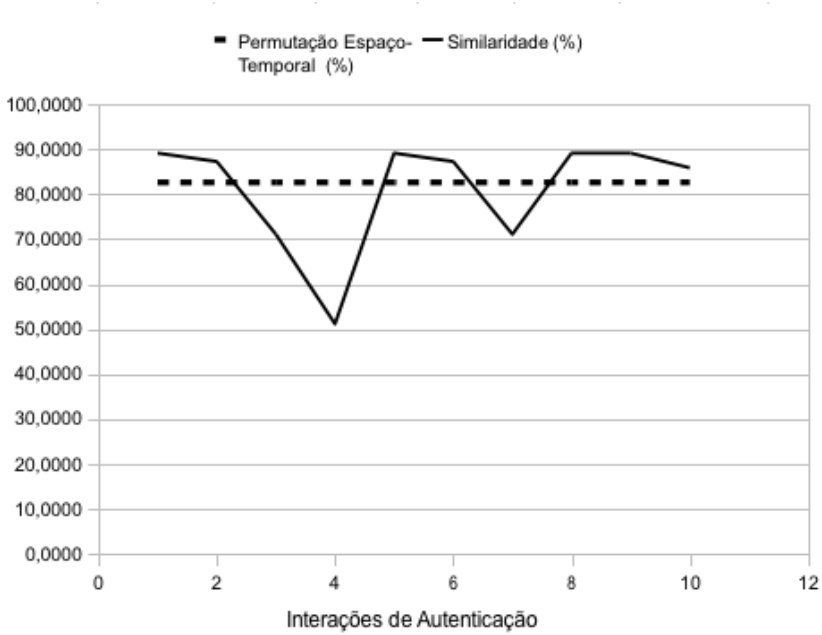


Figura 20: Evolução do Sistema de acordo com o número de interações

5.2.1.1 Probabilidade Condicional da Permutação EspaçoTemporal

A ferramenta estatística permite a utilização de diversos modelos estatísticos, conforme seção 4.7.3.3. No processo de análise de alternativas de modelo foram simulados diversos casos de uso tendo como referencial os dados do Quadro 6.

Devido a natureza dos elementos do vetor comportamental B_0, os modelos avaliados foram: a Permutação Espaço-Temporal e a Distribuição de Poisson. As simulações realizadas para as primeiras interações do Quadro 6, resultou no gráfico da Figura 21.

Os valores dos 3 (três) modelos da Distribuição de Poisson possuem um baixo grau de convergência e as probabilidades condicionais se mantém estáveis a medida em que aumenta o número de interações e de comportamentos adicionados na base de dados de perfis. A Distribuição de Poisson Espaço-Temporal apresentou valores inferiores aos modelos Puramente Espacial e Puramente Temporal, representando uma baixa adaptação ao processo

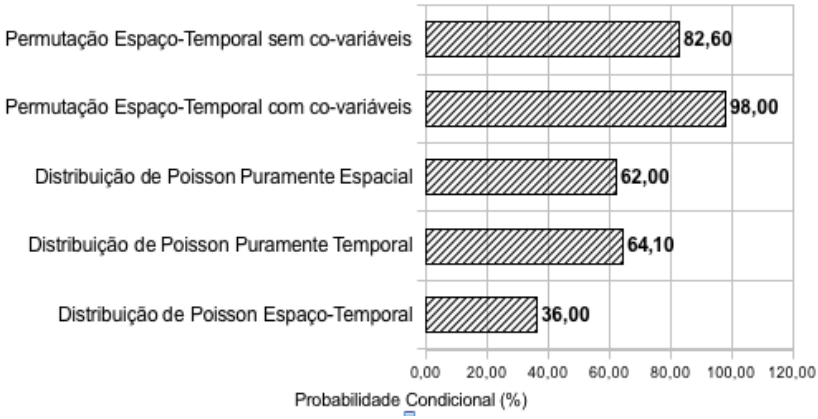


Figura 21: Resultados do Modelo Analítico da Permutação Estatística

de deslocamento no qual um usuário móvel estará submetido.

O Modelo de Permutação Espaço-Temporal pode ser utilizado com co-variáveis e sem co-variáveis, o gráfico da Figura 21 apresenta os valores para cada um dos modelos. A opção de utilização do modelo sem co-variáveis foi devido a dificuldade de se controlar os valores relativos as co-variáveis, já que o modelo trata as co-variáveis como casos e todos os casos possuem um valor estatístico determinado dentro de seu domínio por uma distribuição normal e somente dos dados em análise.

5.2.1.2 Vetor de Pesos dos Elementos Comportamentais (P)

Os elementos do vetor comportamento B_0 são classificados e categorizados, assim é possível estabelecer um peso (grau de relevância) do elemento dentro do vetor de comportamento. Como o comportamento é definido pela equação (1), no primeiro momento optou-se por uma divisão de 50% para os elementos de contexto e 50% para os elementos de atividade. Porém, nos ambientes da computação móvel os aspectos relacionados a localização e tempo são fatores fundamentais para definição do comportamento do usuário.

O vetor de pesos dos elementos comportamentais é definido formalmente como:

$$P = \langle P_1 , \ldots , P_n \rangle$$

Onde os valores do pesos dos elementos P_i devem seguir as equações:

$$\begin{aligned} \sum_{i=1,\ldots,n} P_i &= 1 \\ P_{timestamp} + P_{location} &\leq 0.5 \end{aligned}$$

Os valores iniciais dos pesos são pré-estabelecidos, porém os usuários podem alterá-los. Depois de uma fase de treinamento do filtro híbrido uma outra opção é calcular o peso dos elementos através da frequência de ocorrência dos elementos do comportamento.

$$P_i = \frac{F(B_i)}{\sum_{j=1,\ldots,n} F(B_j)}$$

onde $F(B_i)$ é a frequência de ocorrência do elemento i nos comportamentos dos usuário armazenados na base de dados de perfil.

5.2.1.3 Vetor de Pesos Acumulativos da Sessão para Filtro Híbrido (PBH)

O Vetor de Pesos Acumulativos da Sessão *PBH* tem como objetivo manter na sessão de utilização uma memória dos comportamentos realizados pelo usuário. Portanto, este vetor tem os seus valores recalculado a cada interação de autenticação e representa os estados dos elementos do vetor comportamento.

O domínio dos valores esperados para os elementos do vetor *PBH* são: $[\ 1,\ 0,\ -1,\ \ldots,\ -n\ ]$. Os valores iniciais dos elementos são atribuídos valor 1, esta atribuição é realizada quando o usuário realiza uma autenticação explícita ou responde corretamente as perguntas do módulo de questões.

O Vetor de Pesos Acumulativos da Sessão *PBH* é definido formalmente como:

$$PBH = \langle PBH.elemento_1\ ,\ \ldots\ ,\ PBH.elemento_n \rangle$$

Onde os valores de cada elemento $PBH.elemento_i$ devem seguir as condições:

- Se ($B_0.i\ =\ B_{-1}.i$) então $PBH_i \Leftarrow 1$
- Se ($B_0.i\ \neq\ B_{-1}.i$) então $PBH_i \Leftarrow PBH_i - 1$

5.2.1.4 Critérios de Definição da Natureza do Usuário para o Filtro Híbrido

O critério de definição da natureza do usuário, corresponde a classificação do usuário em relação aos tipos: *Normal*, *Suspeito* e *Anormal*. Esta classificação possui parâmetros variáveis que são calculados todas as vezes que uma autenticação explícita acontecer.

No caso da filtragem híbrida a definição dos parâmetros é pré-estabelecida pelo usuário, que determina quais e quantos elementos de comportamento podem ter os seus valores alterados. Os limites estabelecidos para o gráfico da Figura 20, estão representados por linhas horizontais na Figura 22. Os graus de Similaridade (*Sim*) que forem superior ao *Limite_Normal_Hbrido* serão considerados *Normais*, os que ficarem entre os limites serão considerados *Suspeitos* e os que ficarem abaixo do *Limite_Suspeito_Hibrido* serão considerados *Anormais*.

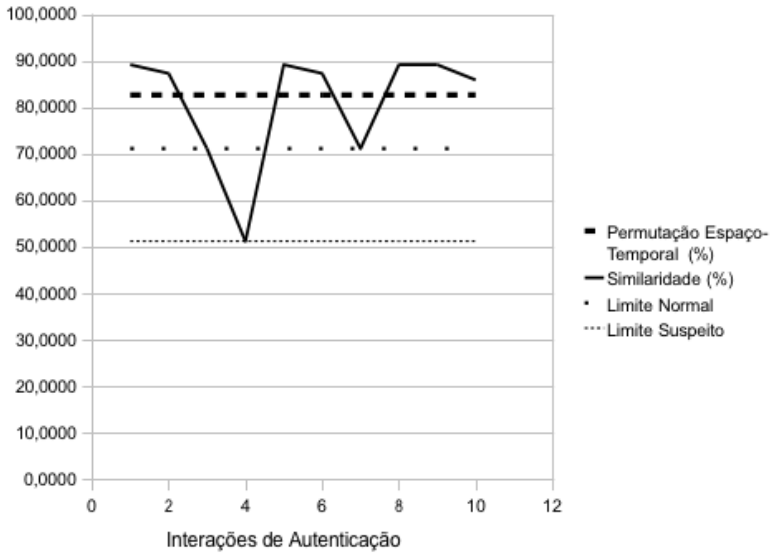


Figura 22: Limites da Natureza do Usuário do Filtro Híbrido

O Algoritmo 7 retorna a natureza do usuário (*Normal*, *Suspeito* e *Anormal*) de acordo com os limites estabelecidos na 22.

A determinação dos limites (*Normal_Hibrido* e *Suspeito_Hibrido*)

Algoritmo 7 Pesquisa da Natureza Usuário para o Filtro Híbrido

Parâmetro: $User$ {Identificador do usuário}
Parâmetro: Sim {Similaridade Calculada para o comportamento B_0}

Retorno: $Natureza$ {Natureza do usuário, pode conter os valores $[USER\_NORMAL, USER\_SUSPEITO, USER\_ANORMAL]$}

Início
if ($Sim > Limite\_Normal\_Hibrido(User)$) **then**
  $Natureza \leftarrow USER\_NORMAL$
else if ($Sim < Limite\_Suspeito\_Hibrido(User)$) **then**
  $Natureza \leftarrow USER\_ANORMAL$
else
  $Natureza \leftarrow USER\_SUSPEITO$
end if
return $Natureza$
Fim

ocorrerá sempre que o usuário realizar uma autenticação explícita. O Procedimento para determinação, será:

1. O usuário determina (configura) em quais elementos e quantas anomalias ele deseja para cada limite. No exemplo, foi definido pelo usuário que ele aceitaria 2 (duas) ligações para números externos (sem cadastro na agenda) como $Limite\_Normal\_Hibrido$ e 3 (três) ligações para números externos como $Limite\_Suspeito\_Hibrido$;

2. Após a autenticação explícita o sistema simula o cálculo de uma nova similaridade de filtro híbrido considerando a primeira anomalia configurada pelo usuário, logo o vetor PBH será definido como: $PBH = \langle\ PBH_{timestamp} = P(E_a),\ PBH_{location} = P(E_a),\ PBH_{device} = 1,\ PBH_{app} = 1,\ PBH_{apprestrict} = 1,\ PBH_{call} = -1,\ PBH_{SMS} = 1\ \rangle$;

3. Aplicando a equação do marcador (5) da Figura 19, é estabelecido o $Limite\_Normal\_Hibrido \leftarrow 0.7109$ a partir das definições do usuário;

4. De forma análoga, $Limite\_Suspeito\_Hibrido \leftarrow 0.5121$ é determinado, porém, com um novo valor para o vetor PBH, que será definido como: $PBH = \langle\ PBH_{timestamp} = P(E_a),\ PBH_{location} = P(E_a),\ PBH_{device} = 1,\ PBH_{app} = 1,\ PBH_{apprestrict} = 1,\ PBH_{call} = -2,\ PBH_{SMS} = 1\ \rangle$.

O critério utilizado para definir a natureza do usuário no filtro híbrido e, portanto, definir quando a autenticação implícita deverá atuar possui as seguintes características:

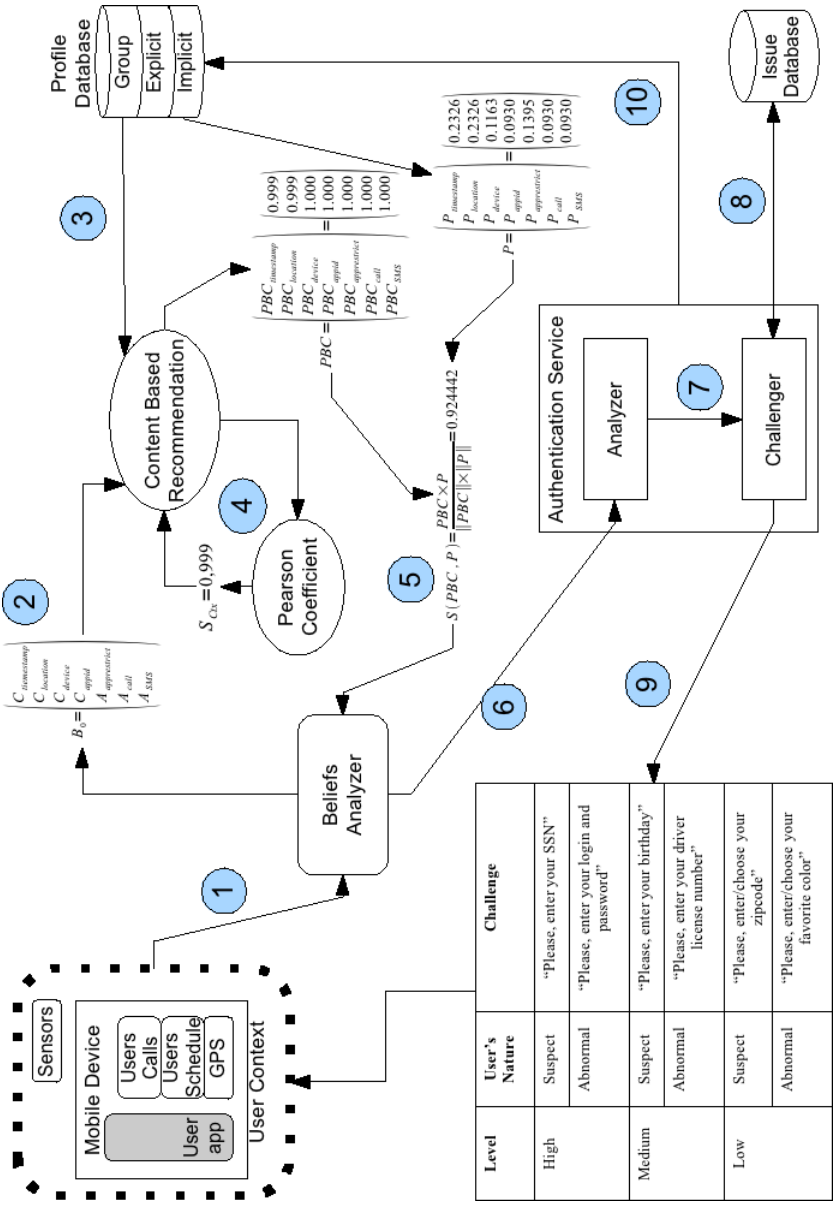
- **Dinâmicas**: já que é recalculado a cada autenticação explícita;
- **Pessoais**: cada usuário pode definir os seu limites através de parâmetros conhecidos;
- **Adaptáveis**: utiliza simulação para se adaptar ao novo espaço-tempo em que o usuário se encontra.

5.3 FILTRAGEM BASEADA EM CONTEÚDO

Os resultados apresentados nesta seção estão relacionados com a filtragem baseada em conteúdo e foram parcialmente publicados em Lima *et al.* (2011). A filtragem baseada em conteúdo utiliza uma equação para cálculo do coeficiente de Pearson, equação (6), para determinar a similaridade de contexto entre o comportamento anterior B_{-1} e o comportamento B_0, comportamento que está sendo avaliado para autenticação implícita. Com o objetivo de explicitar as interações entre os componentes da arquitetura proposta, será realizado um ciclo de autenticação implícita utilizando a filtragem baseada em conteúdo.

Na interação zero (0) é realizada uma autenticação explícita que definirá os valores para o comportamento anterior B_{-1} e os valores dos elementos do vetor de pesos acumulativos da sessão para filtro de conteúdo (PBC). As interações posteriores utilizarão estas informações em conjunto com os comportamentos armazenados na base de dados de perfil para determinar a necessidade de autenticação implícita ou de uma nova autenticação explícita. O estudo de caso é apresentado através dos passos das interações e são representados por itens numerados, que correspondem aos marcadores da Figura 23, os valores utilizados como exemplo para cada ítem corresponde a primeira interação do Quadro 7.

Para formalizar o comportamento dos usuários optou-se pelos seguintes parâmetros definidos no cenário, que são: dispositivo móvel utilizado, localização, marca de tempo (*timestamp*) do momento em que o evento ocorre, aplicação executada, restrição da aplicação executada, ligações realizadas e SMS enviados que estão fora da agenda. Estes são os principais passos de uma interação:



Level	User's Nature	Challenge
High	Suspect	"Please, enter your SSN"
	Abnormal	"Please, enter your login and password"
Medium	Suspect	"Please, enter your birthday"
	Abnormal	"Please, enter your driver license number"
Low	Suspect	"Please, enter/choose your zipcode"
	Abnormal	"Please, enter/choose your favorite color"

Figura 23: Resultados da Filtragem Baseada em Conteúdo

Interações	Similaridade de Contexto (%)	Similaridade (%)	Tempo	Localização	Dispositivo	Aplicação	Restrição	Ligações de Saída	SMS de Saída
1	99,2222	92,4442	0,9922	0,9922	1	1	1	1	1
2	99,7860	90,5404	0,9979	0,9979	1	0	1	1	1
3	99,4868	75,1450	0,9949	0,9949	1	-1	1	1	1
4	99,4262	55,6249	0,9943	0,9943	1	-2	1	1	1
5	98,2228	92,1578	0,9822	0,9822	1	1	1	1	1
6	95,4217	89,7979	0,9542	0,9542	1	1	1	0	1
7	70,8791	86,3045	0,7088	0,7088	1	1	1	-1	1
8	70,8814	67,7330	0,7088	0,7088	1	1	1	1	1
9	70,8831	86,3055	0,7088	0,7088	1	1	1	1	1
10	70,8869	82,9404	0,7089	0,7089	1	1	1	0	0

Quadro 7: Interações de Autenticação para Filtro Baseado em Conteúdo

1. O dispositivo móvel captura as atividades ($A_1 = \langle a_1 , \ldots , a_n \rangle , \ldots , A_n$) e os contextos ($C_1 = \langle timestamp , location , E_1 , \ldots , E_n \rangle , \ldots , C_n$) que o usuário está executando na realização de suas tarefas e envia para o analisador de crenças;

2. O analisador de crenças cria o comportamento (B_0), através das atividades e dos contextos enviados pela interação anterior e envia à filtragem baseada em conteúdo. No exemplo da primeira interação, temos $B_0 = \langle\ C_{timestamp} = 498069,\ C_{location} = 76.982,\ C_{device} = 2,\ A_{app} = 1,\ A_{apprestrict} = 1,\ A_{apprestrict} = 2,\ A_{call} = 82770009,\ A_{SMS} = 82770009\ \rangle$;

3. O filtro baseado em conteúdo localiza o comportamento anterior do usuário B_{-1} e envia as informações para cálculo da similaridade;

4. O cálculo do coeficiente de Pearson, equação (6), utiliza as informações de $B_{Dispositivo}$ para calcular a similaridade entre os elementos espaço-temporal do contexto C_0 e o contexto anterior C_{-1}, conforme definições da seção 5.3. No exemplo: $Sim_{Contexto} = 0.9992$;

5. O filtro baseado em conteúdo calcula a similaridade do comportamento B_0 com o comportamento anterior B_{-1} para enviar ao analisador de crenças. O cálculo da similaridade neste filtro possui o seguinte procedimento:

    - De acordo com os elementos do vetor comportamento B_0 são recuperados da base de dados de perfil os pesos definidos anteriormente para cada um destes elementos, montando-se o vetor $P = \langle P.elemento_1 , \ldots , P.elemento_n \rangle$. No exemplo: $P =$

$\langle P_{timestamp} = 0.2326,\ P_{location} = 0.2326,\ P_{device} = 0.1163,\ P_{app} = 0.0930,\ P_{apprestrict} = 0.1395,\ P_{call} = 0.0930,\ P_{SMS} = 0.0930 \rangle$;

- O vetor $PBC = \langle PBC.elemento_1\ ,\ \ldots\ ,\ PBC.elemento_n \rangle$ é recuperado da base de dados de perfil e possuirá os mesmos elementos do vetor P, porém, os valores atribuídos aos elementos resultará da comparação entre o comportamento B_0 e o perfil de sessão (comportamento atual B_{-1}). Os valores atribuídos aos elemento PBC_i são:
  - Se ($B_0.i = B_{-1}.i$) então $PBC_i \Leftarrow 1$
  - Se ($-B_0.i \neq B_{-1}.i$) então $PBC_i \Leftarrow PBC_i - 1$

  No exemplo: $PBC = \langle\ PBC_{timestamp} = 1,\ PBC_{location} = 1,\ PBC_{device} = 1,\ PBC_{app} = 1,\ PBC_{apprestrict} = 1,\ PBC_{call} = 1,\ PBH_{SMS} = 1 \rangle$;
- Para os elementos espaço-temporais (*location* e *timestamp*), o valor a ser atribuído é o valor calculado pela equação (6) no marcador 4, sendo então:

$$\begin{aligned} PBC_{timestamp} &\Leftarrow Sim_{Contexto} \\ PBC_{location} &\Leftarrow Sim_{Contexto} \end{aligned}$$

  No exemplo: $PBC = \langle\ PBC_{timestamp} = 0.9992,\ PBC_{location} = 0.9992,\ PBC_{device} = 1,\ PBC_{app} = 1,\ PBC_{apprestrict} = 1,\ PBC_{call} = 1,\ PBC_{SMS} = 1 \rangle$;
- O cálculo de similaridade é realizado entre os vetores PBC e P através da equação $Sim\ (\ PBC\ ,\ P\ ) = \frac{PBC \times P}{|\ PBC\ | \times |\ P\ |}$. No exemplo: $Sim\ (\ PBC\ ,\ P\ ) = 0.924442$

6. O analisador de crenças, ao receber o valor de similaridade *Sim* compara com os dos demais filtros e envia o maior (analisador configurado como otimista) valor para o analisador de probabilidades;

7. O analisador de probabilidades, através da similaridade *Sim*, determina a natureza do usuário, que pode ser: Normal, Suspeito ou Anormal.

   - Se o usurário for considerado Normal a autenticação implícita é realizada e executa-se os passos do marcador (10);
   - Caso contrário, o usuário é considerado Suspeito ou Anormal e as informações de Natureza do usuário e comportamento B_0 são enviados para o desafiador;

8. O desafiador pesquisa na base de dados de questão qual deve ser o questionamento a ser realizado ao usuário, já que o comportamento B_0 possui um grau de similaridade abaixo do esperado pelo sistema de autenticação;

9. A pergunta é enviada ao usuário:

   - Caso o usuário responda corretamente, a autenticação implícita é realizada e executa-se os passos do marcador (10);
   - Caso contrário, é requisitada uma autenticação explícita e se o usuário for autenticado corretamente executa-se os passos do marcador (10);

10. As informações sobre o comportamento B_0 e o grau de similaridade são armazenados na base de dados de perfil. O perfil de sessão é atualizado com valores do comportamento B_0.

    - Se o usuário foi questionado (explicitamente ou implicitamente por ser considerado Suspeito ou Anormal) o vetor *PBC* receberá valor 1 para todos os seus elementos e será armazenado na base de dados de perfil;
    - Caso contrário, o vetor *PBC* será armazenado na base de dados de perfil com os valores alterados pela interação. No exemplo: $PBH = \langle\ PBC_{timestamp} = 0.9992,\ PBC_{location} = 0.9992,\ PBC_{device} = 1,\ PBC_{app} = 1,\ PBC_{apprestrict} = 1,\ PBC_{call} = 1,\ PBC_{SMS} = 1\ \rangle$.

A partir do passos de uma interação, apresentados na Figura 23, é possível realizar simulações para demonstrar como o sistema se comporta com outras interações. Com o objetivo de demonstrar a relevância do vetor *PBC*, foram realizadas outras interações, apresentadas no Quadro 7 e representadas graficamente na Figura 24.

Nas interações (2), (3) e (4), o usuário realizou no mesmo espaço-tempo a execução de uma aplicação diferente das normalmente utilizadas, portanto, o elemento PBC_{appid} sofreu decréscimos sucessivos, que influenciaram na redução do grau de similaridade dos comportamentos esperados para este usuário. Na interação (5), o sistema solicitou uma autenticação explícita, reinicializando os elementos do vetor *PBC* para 1.

Nas interações (6) e (7), houve uma variação considerável espaço-tempo e o usuário realizou ligações telefônicas para números que não estavam cadastrados na agenda. Nas interações (8) e (9) realizou tarefas definidas

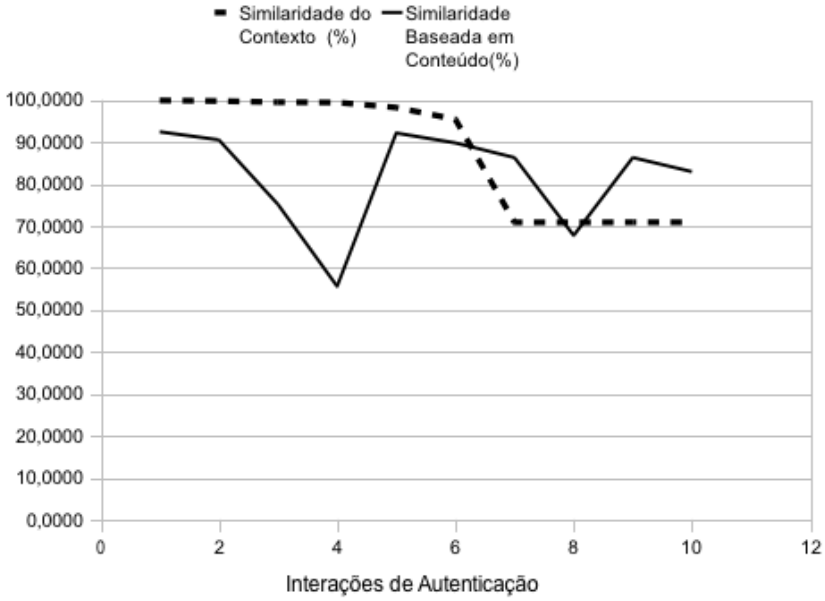


Figura 24: Evolução do Filtro Baseado em Conteúdo de acordo com o número de interações

como comportamento normal, por exemplo enviar SMS e ligar para pessoas cadastradas na agenda e utilizar aplicações habituais. A interação (10), apresenta a influência da realização de dois eventos diferentes dos habituais e sua repercussão no sistema.

A partir desta representação gráfica, Figura 24, é possível constatar que a filtragem baseada em conteúdo permite uma variação nas características comportamentais do usuário, caso das interações (2), (5) e (9). Caso a variação exceder os limites de similaridade dos comportamentos, o sistema realizará um questionamento ao usuário ou, no pior dos casos, uma autenticação explícita é executada.

A definição do Vetor de Pesos dos Elementos Comportamentais (P) seguem as mesmas regras apresentadas no filtro híbrido, na seção 5.2.1.2. Este vetor é compartilhado pelos filtros de recomendação tornando o sistema de autenticação implícita, mais amigável e fácil de configurar.

O Vetor de Pesos Acumulativos da Sessão para Filtro Conteúdo (PBC),

possui definição análoga ao vetor *PBH* definido na seção 5.2.1.3.

5.3.1 Critérios de Definição da Natureza do Usuário para o Filtro Baseado em Conteúdo

O critério de definição da natureza do usuário, corresponde a classificação do usuário em relação aos tipos: *Normal*, *Suspeito* e *Anormal*. Essa classificação possui parâmetros variáveis que são calculados todas as vezes que uma autenticação explícita acontecer. O processo de definição dos limites é similar aos do filtro híbrido definidos na seção 5.2.1.4.

No caso da filtragem baseada em conteúdo a definição dos parâmetros é pré-estabelecida pelo usuário, que determina quais e quantos elementos de comportamento podem ter os seus valores alterados. Os limites estabelecidos para o gráfico da Figura 24, estão representados por linhas horizontais na Figura 25. Os graus de Similaridade (*Sim*) que forem superior ao *Limite_Normal_Conteudo* serão considerados *Normais*, os que ficarem entre os limites serão considerados *Suspeitos* e os que ficarem abaixo do *Limite_Suspeito_Conteudo* serão considerados *Anormais*.

5.4 ANÁLISE DOS RESULTADOS DOS PROCESSOS DE FILTRAGEM

5.4.1 Resultados Coletados

Os resultados coletados nos eventos, do cenário descrito, permitiram a elaboração de gráficos, que demonstram a interação da Autenticação Implícita frente a situações de uso normal pelos usuários e pelo uso indevido de intrusos.

5.4.1.1 Experimento para detecção de uso indevido por intrusão

O gráfico, da Figura 26, apresenta a simulação de uso indevido do dispositivo móvel por outro usuário, que possui comportamento diferente do usuário original. Neste gráfico, o novo usuário utilizou aplicativos diferentes e realizou ligações, que não estavam cadastradas na agenda. Depois de 8 interações os dados de similaridade chegaram ao grau 30, muito inferior aos limites estabelecidos.

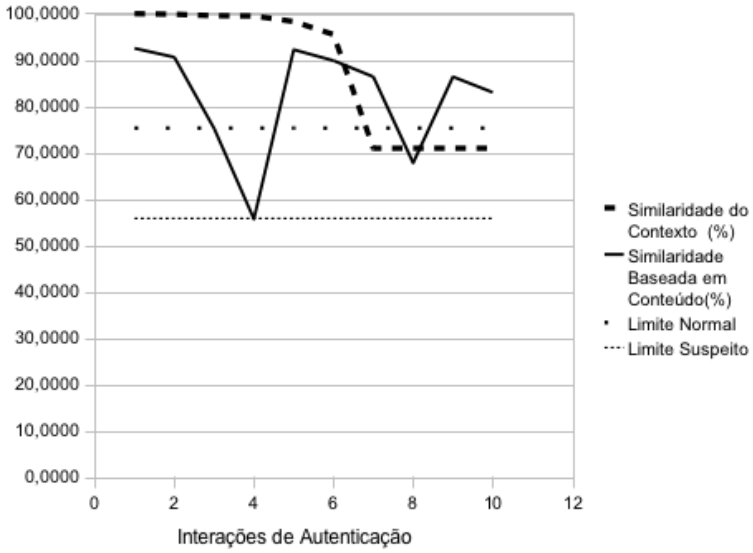


Figura 25: Limites da Natureza do Usuário do Filtro Baseado em Conteúdo

O gráfico, da Figura 27, similar ao anterior, apresenta a simulação de uso indevido do dispositivo móvel por outro usuário. Neste gráfico, o novo usuário realizou duas ligações e enviou um SMS para pessoas que não estavam cadastradas na agenda. Depois de 3 interações a similaridade chegou a um grau próximo a 30, muito inferior aos limites estabelecidos.

Na comparação dos dois gráficos percebe-se, que a anomalia de utilização indevida foi percebida pelos dois filtros, porém, o Filtro Híbrido necessitou de somente três interações para detectar o fato e questionar o usuário.

5.4.1.2 Experimento para detecção de uso autorizado

O gráfico, da Figura 25, apresenta a simulação de uso normal do dispositivo móvel pelo usuário, a partir da quinta interação. Neste gráfico, o usuário utilizou aplicativos diversos e realizou ligações que não estavam cadastradas na agenda. O questionamento realizado na interação 8 é o de usuário suspeito, portanto, o desafiador considera este usuário como sendo o possível proprietário do dispositivo móvel.

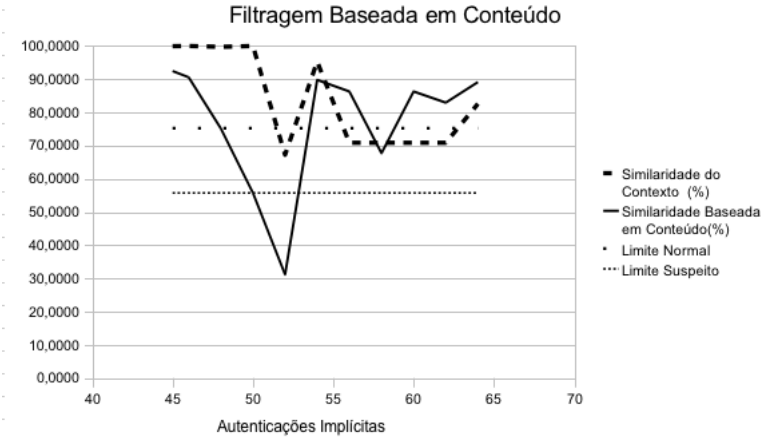


Figura 26: Filtro Baseado em Conteúdo com Simulação de Uso Indevido

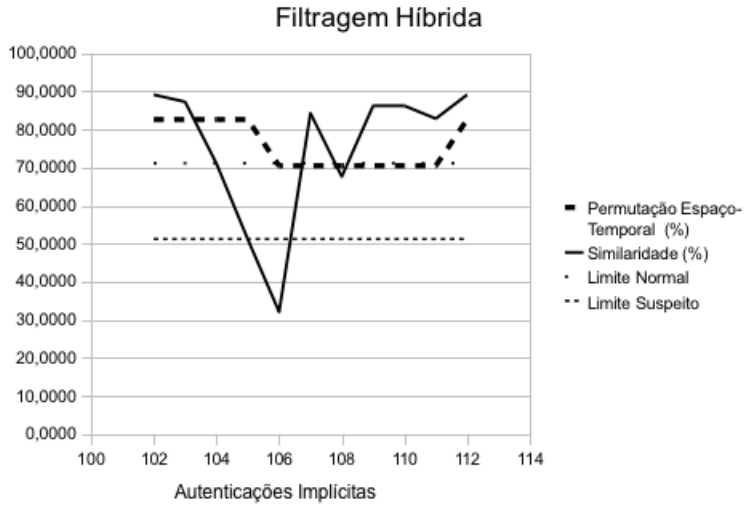


Figura 27: Filtro Híbrido com Simulação de Uso Indevido

O gráfico, da Figura 22, similar ao anterior, apresenta a simulação de uso normal do dispositivo móvel pelo usuário, a partir da quinta interação. Neste gráfico, o usuário utilizou aplicativos diversos e realizou ligações que

não estavam cadastradas na agenda. Depois de 2 interações a similaridade chegou a um grau próximo a 72 e o sistema deve questionar o usuário como suspeito. A Filtragem Híbrida, converge e detecta mais rápido a mudança nos comportamento do usuário e atua através do desafiador.

5.4.2 Considerações Sobre os Resultados

A partir dos resultados apresentados é possível constatar, que esta abordagem de recomendação permite uma flexibilidade na inclusão de novos filtros. Os filtros, que são adicionados, podem ser configurados para trabalhar de forma local ou remota. Os filtros locais necessitam de regras objetivas e com poucos requisitos de processamento, devido as limitações dos dispositivos móveis.

O filtro baseado em conteúdo utiliza o Coeficiente de Pearson para determinar a similaridade entre os comportamentos, portanto, a sua execução pode ser local e / ou remota. Já o filtro híbrido necessita executar a ferramenta SatScan, que demanda recursos computacionais e acesso a base de dados de perfil, este filtro terá sua execução somente de forma remota.

A definição do Vetor de pesos $\vec{P}$ é customizada originalmente pelo usuário, porém, a incorporação de novos métodos para determinação automática dos valores, poderia auxiliar na redução de questionamentos aos usuários e reduzir o número de interações dos intrusos (adversários).

A utilização dos Vetores $P\vec{B}C$ e $P\vec{B}H$ permite que os comportamentos anômalos possam ser registrados e contabilizados. Como os usuários possuem hábitos, os comportamentos anômalos devem ser reduzidos no decorrer da execução de suas tarefas diárias. Portanto, o mecanismo de contabilização de anomalias permite a detecção de comportamentos inesperados, que podem definir um usuário não autorizado caracterizado no modelo como adversário.

O filtro híbrido permite uma detecção mais rápida das anomalias, já que os seus resultados em relação aos elementos de contexto possuem uma maior abrangência, devido a utilização da base de dados de perfil. O filtro baseado em conteúdo utiliza, somente, o comportamento anterior fato este, que provoca um maior número de interações e uma acumulação de erro que irá levar o sistema a questionar o usuário de alguma forma ou solicitar uma autenticação explícita.

A abordagem proposta é capaz de ampliar sua base de conhecimento (perfis) através da agregação dos comportamentos do usuário a cada nova interação (processo de autenticação). Conforme aumenta as interações (maior

número de autenticações implícitas realizadas), aumenta o número de informações na base de conhecimento, resultando em uma melhora na determinação da similaridade entre os comportamentos do usuário. Esse dinamismo, oferecido pela abordagem proposta, provê uma maior autonomicidade da abordagem, ou seja, o sistema de autenticação reduz, a necessidade de entrada de informação de forma explícita ou através de resposta a desafios (autenticação implícita por desafio).

6 CONSIDERAÇÕES FINAIS

No ambiente da computação móvel e pervasiva, a utilização de uma forma complementar de certificação (no processo de autenticação) do usuário pode ser utilizada para minimizar a desvantagem de perda de informações e acessos a serviços não autorizados através dos dispositivos móveis. Portanto, a utilização de uma certificação complementar, oferece maior segurança.

Outra dificuldade, oriunda da mobilidade e do uso de dispositivos pequenos (portáteis), é a digitação de senhas seguras, as quais devem conter uma longa cadeia de caracteres entre alfanuméricos, caixa alta e baixa, e caracteres especiais. Digitar este tipo de senha, de tempos em tempos, para realizar o processo de autenticação, torna-se uma tarefa incomoda para o usuário móvel.

Com a finalidade de solucionar estes problemas em relação as senhas, esta Tese propõe uma abordagem de recomendação sensível ao contexto para apoio a autenticação implícita, baseado nas teorias e conceitos da cognição situada para modelagem dos comportamentos dos usuários (hábitos) e do seu relacionamento com o ambiente (contexto).

Através da pesquisa realizada, com relação à determinação do comportamento de usuários em ambientes de computação móvel, constatou-se a importância de considerar, simultaneamente, dois atributos fundamentais: o contexto e as atividades do usuário. Tais propriedades são importantes pois os seres humanos possuem hábitos (realizam atividades rotineiramente em ambientes específicos - contextos) e porque as correlações de tempo e localização (espaço) são relevantes para determinar eventos sucessivos que definem um perfil comportamental.

Portanto, fez-se necessária a pesquisa de modelos que considerassem a análise desses dois atributos simultaneamente, a fim de obter uma avaliação mais precisa do comportamento do usuário no uso de sistemas computacionais, ou seja, identificando uma conformidade no padrão de comportamento e possíveis anomalias de comportamento, as quais podem ser utilizadas para caracterizar uma falha no processo de autenticação. Para o processo de autenticação, proposta a utilização de uma abordagem de recomendação sensível ao contexto que permite a utilização de três filtros: i) filtragem baseada em conteúdo, ii) filtragem colaborativa e iii) filtragem híbrida. Os resultados, e respectivo modelo analítico, apresentam uma eficiência significativa na detecção e análise de anomalias no processo de autenticação devido à utilização do modelos de filtragens e de permutação espaço-temporal.

Além disso, a abordagem proposta mostrou que atende ao requisito de autonomicidade e dinamicidade, pois através dos perfis comportamentais

definidos pelo modelo, a abordagem é capaz de agregar as habilidades e conhecimentos adquiridos pelo usuário durante a sua interação com o processo de autenticação. Em adição, a proposta provê flexibilidade por permitir diferentes formas de autenticação, conforme os níveis de segurança exigidos pelas aplicações executadas. Portanto, é perceptível que a abordagem proposta neste trabalho de pesquisa foi capaz de contornar com sucesso a falta de alternativas existentes na literatura para atender os requisitos de sensibilidade ao contexto, eficiência computacional, flexibilidade, autonomicidade e dinamicidade simultaneamente.

6.1 PRINCIPAIS RESULTADOS

Ao final desta pesquisa, o objetivo geral - **a elaboração de uma abordagem de recomendação que possibilite a autenticação implícita do usuário através do conhecimento de seu perfil comportamental** - ficou plenamente atendido porque foi desenvolvido uma abordagem de recomendação de autenticação implícita composta por um modelo e uma arquitetura que considera os requisitos para o processo de autenticação sensível ao contexto. Os requisitos foram apresentado na seção 3.3.5 e comparada como as demais abordagens na seção 4.8.1. Com relação ao perfil comportamental do usuário foi realizada uma modelagem que utiliza o relacionamento entre os hábitos (atividades) do usuário e ambiente (contexto) onde estas atividades são realizadas.

No transcorrer da pesquisa foram realizadas etapas diretamente relacionadas aos objetivos específicos, que delinearam de forma sequencial e previamente definida o desenvolvimento desta abordagem de recomendação para autenticação implícita.

O primeiro objetivo específico consiste na identificação de modelos teóricos que definem as interações entre os usuários e os ambientes pervasivos no âmbito das Ciências Sociais. Os resultados foram apresentados no Capitulo 2. Nesse Capítulo são evidenciados: i) os conceitos de computação sensível a contexto e sua visão fenomenológica, que, de forma dinâmica e ocasionada, emerge do relacionamento entre o contexto e a atividade sendo estes considerados indivisíveis; ii) a Teoria da Atividade, que serve de arcabouço teórico para definição das atividades, e os contextos sociais, que relacionam os usuários com o ambiente, os objetos e as comunidades que eles participam; e iii) uma arquitetura cognitiva, baseada no *Framework* SRK, que permite flexibilizar a abordagem de recomendação para executar no disposi-

tivo móvel e nos ambientes computacionais que provem serviços. Estes modelos de interação entre usuários e o ambiente (contexto) caracterizam esta tese como interdisciplinar, uma vez que, preconizam o diálogo permanente entre duas o mais áreas do conhecimento.

No capítulo 3 são apresentados as principais definições sobre o protocolo AAA e sua utilização nos ambientes pervasivos e ubíquos. Existem diversos projetos que utilizam características pessoais dos individuos como critério para autenticação, estes projetos consideram desde os reconhecimento facial ate o deslocamento em marcha dos usuários como característica para identificação e certificação. Contudo, a utilização dos aspectos comportamentais do usuário é relativamente nova. Esta tese explora estas informações, que foram colhidas através de dispositivos móveis como elementos para uma abordagem de recomendação de apoio à autenticação implícita dos usuários que estão em ambientes móveis e pervasivos.

Para o desenvolvimento da proposta foram identificados os principais abordagens correlatas e como estas abordagens trabalhavam o processo de interação dos usuários com os contextos nos quais esses executavam as suas atividades diárias. Esta interação entre o ambiente e o usuário, normalmente, é modelada de forma estática (estável) e não retém as informações do relacionamento cognitivo dos usuários com o ambiente (contexto), gerando um contexto delineável. Diferentemente, a abordagem proposta utiliza os contexto pela visão fenomenológica, o contexto e as atividades executadas pelo usuário, são relacionais e, portanto, este relacionamento é distinto dos demais. Possibilitando, assim, a identificação de características relacionais diferenciadas entre os diversos indivíduos. No capítulo 4 é detalhado o modelo e a arquitetura de recomendação e autenticação desta proposta.

O último objetivo específico *demonstrar a viabilidade da abordagem proposta através de sua aplicação em testes experimentais* - também foi atingido, uma vez que, no Capítulo 5 é apresenta, de forma didática, o processo de recomendação de autenticação utilizando-se experimentos para os dois filtros implementados: filtro híbrido e filtro baseado em conteúdo. Os resultados experimentais demonstram que a abordagem utilizada consegue perceber de forma rápida e eficaz a utilização dos dispositivos por usuários intrusos (atacantes) devido à diferença de comportamento (anomalia) e também à diferença de ambiente (contexto) de utilização. Quando a abordagem proposta constata anomalias de comportamento, de acordo com criterio pré-definidos, o usuário é submetido a questionamentos para provas de sua identidade ou ao processo de autenticação explícita.

Com relação a pergunta de que conduziu esta pesquisa: **Como mode-**

lar um sistema de autenticação complementar que considere os requisitos de mobilidade dos usuários em um ambiente pervasivo? - foi possível chegar a algumas conclusões que são apresentadas a seguir.

As pesquisas sobre mobilidade estão focados na característica corpórea do movimento humano, que fica liberado das restrições geográficas devido às tecnologias de computação móvel, computação pervasiva e serviços de comunicação. Contudo, estas tecnologias oportunizam novas dimensões à interação entre as pessoas, possibilitando a mobilidade espacial, temporal e contextual. Logo, os ambientes pervasivos propiciam que os indivíduos exerçam diferentes papéis sociais, a qualquer hora, em qualquer lugar e utilizando qualquer dispositivo. Ao permitir uma comunicação diferenciada nestes ambientes, a mobilidade muda a forma dos seres humanos interagirem, afetando suas relações sociais, familiares, afetivas e profissionais.

Os conceitos de autenticação (o meio para obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser) devem adaptar-se ao ambientes móveis e pervasivo, uma vez que, as informações e serviços computacionais estão em deslocamento e fora de áreas de acesso restrito. Logo, o processo de autenticação torna-se essencial, as políticas de segurança que permitem a utilização de um segundo fator de validação de usuário, que é utilizado de forma complementar à tradicional senha alfanumérica, aumentando a segurança e a sensação de confiança dos usuários.

Portanto, a necessidade da criação de uma nova abordagem de recomendação para autenticação foi motivada pela complexidade do processo de autenticação segura em ambientes móveis e pervasivos, e pela percepção que os métodos e técnicas da Engenharia do Conhecimento podem contribuir para o desenvolvimento de uma solução inovadora, ao utilizar o conhecimento que pode ser obtido sobre o comportamento do usuário. Os métodos tradicionais de autenticação reconhecem como verdadeiro o dispositivo que o usuário está utilizando mas não o usuário em si, não garantem que seja o usuário (autenticado) quem efetivamente está utilizando o dispositivo reconhecido. A utilização desta abordagem (i) permite reconhecer o usuário através do conhecimento comportamental deste, utilizando as informações e dados obtidos sistemicamente; (ii) através de diagnósticos realizados, serve para melhoria do processo de autenticação, ao explicitar um conhecimento latente que, geralmente, permanece encoberto ou que não vem sendo utilizado, mas que está disponível. Estes conhecimentos comportamentais do usuário compõem uma **Assinatura Comportamental** que define de forma única cada usuário e sua forma de interação com o ambiente e o dispositivo móvel.

6.2 CONTRIBUIÇÕES

A principal contribuição da tese está na inovação de utilizar as informações de contexto (comportamento do usuário, conhecimento das atividades armazenadas nos dispositivo móvel) no processo de autenticação em ambientes pervasivos, usando método de análise de similaridade na execução das atividades desenvolvidas pelo usuário a ser autenticado e o perfil armazenado, e garantindo que a autenticação seja efetuada através de informações não declaradas ou informadas diretamente, mas informações que são coletadas de forma indireta e sistematicamente.

6.2.1 Contribuições na Área de Conhecimento

Ao integrar diferentes abordagens técnicas e teóricas em uma abordagem de recomendação para autenticação implícita, coopera-se cientificamente no aprimoramento da tarefa de explicitação do conhecimento comportamental dos usuários. O desenvolvimento deste modelo e da arquitetura proposta permite também aos profissionais da área de segurança adotar uma perspectiva de ambientes inteligentes ao considerar o contexto na qual a autenticação acontece. Isso evidencia a possibilidade da explicitação de conhecimentos para o avanço metodológico deste processo de autenticação e definição de hábitos dos usuários.

6.2.2 Contribuições na Área Científica

Como contribuição científica deste trabalho tem-se a publicação de seis artigos em congresso internacional e um capítulo de livro internacional, a relação destas publicações está na seção A.

6.2.3 Contribuições na Área Tecnológica

Como contribuição tecnológica deste trabalho tem-se o desenvolvimento de uma abordagem que permite a autenticação implícita complementar (segundo fator) através da utilização das informações comportamentais (contextos e atividades) do usuário para dispositivos móveis.

6.3 TRABALHOS FUTUROS

Como trabalhos futuros, espera-se realizar a análise sobre o impacto do número de usuários sobre o mecanismo de autenticação sensível ao contexto, ou seja, determinar a capacidade desta abordagem em manter uma taxa aceitável de acerto no processo de autenticação, conforme o aumento do número de usuários cadastrados no sistema.

Outro trabalho a ser realizado é implementação de mais experimentos para cada um dos filtros de recomendação, para avaliar o seu desempenho em relação: aquisição de conhecimento, portabilidade para os dispositivos móveis, para autenticar informações e autenticar o próprio dispositivo. Implementar e avaliar a filtragem colaborativa, que foi especificada nesta Tese, porém, não foi implementada

Utilizar as experiências, obtidas na construção desta abordagem, para criar aplicações e sistemas: com modelos sensíveis ao contexto, orientados a atividade, com ações situadas, integradas com os objetos e mediadas com os usuários e as comunidades.

REFERÊNCIAS

ABOBA, B.; CALHOUN, P.; GLASS, S.; HILLER, T.; MCCANN, P.; SHIINO, H.; WALSH, P.; ZORN, G.; DOMMETY, G.; PERKINS, C. *et al.* **RFC 2989-Criteria for Evaluating AAA Protocols for Network Access**. [S.l.], 2000.

BABU, B. S.; VENKATARAM, P. A dynamic authentication scheme for mobile transactions. **International Journal**, Citeseer, v. 8, n. 1, p. 59–74, 2009.

BALDAUF, M.; DUSTDAR, S.; ROSENBERG, F. A survey on context-aware systems. **International Journal of Ad Hoc and Ubiquitous Computing**, Inderscience, v. 2, n. 4, p. 263–277, 2007. Disponível em: <http://inderscience.metapress.com/index/1184787h28163t15.pdf>.

BANNON, L.; BØDKER, S. Beyond the interface: Encountering artifacts in use. **DAIMI PB**, v. 18, n. 288, 1989.

BARKHUUS, L. Context information vs. sensor information: A model for categorizing context in context-aware mobile computing. In: **Symposium on Collaborative Technologies and Systems**. [S.l.: s.n.], 2003. p. 127–133.

BATESON, G.; BATESON, M. **Steps to an Ecology of Mind**. [S.l.]: University of Chicago Press Chicago, 1972.

BELLAMY-MCINTYRE, J.; LUTERROTH, C.; WEBER, G. Openid and the enterprise: A model-based analysis of single sign-on authentication. In: IEEE. **Enterprise Distributed Object Computing Conference (EDOC), 2011 15th IEEE International**. [S.l.], 2011. p. 129–138.

BELLAVISTA, P.; CORRADI, A.; MONTANARI, R.; STEFANELLI, C. Context-aware middleware for resource management in the wireless Internet. **IEEE Transactions on Software Engineering**, Published by the IEEE Computer Society, v. 29, p. 1086–1099, 2003. ISSN 0098-5589. Disponível em: <http://dx.doi.org/10.1109/TSE.2003.1265523>.

BESSA, R. L. de C. Virtualidade ubíqua e a questão do contexto nas interações humano-computador. In: **2o. Encontro Brasileiro de Arquitetura da Informação**. [S.l.: s.n.], 2008.

BIGUN, J.; FIERREZ-AGUILAR, J.; ORTEGA-GARCIA, J.; GONZALEZ-RODRIGUEZ, J. Combining biometric evidence for person authentication. **Advanced Studies in Biometrics**, Springer, p. 103–120, 2005.

BURKE, R. Hybrid web recommender systems. In: BRUSILOVSKY, P.; KOBSA, A.; NEJDL, W. (Ed.). **The adaptive web**. Springer-Verlag, 2007. (Lecture Notes in Computer Science, v. 4321), p. 377–408. Disponível em: <http://portal.acm.org/citation.cfm?id=1768211>.

CARDOSO, G.; CASTELLS, M. **A sociedade em rede em Portugal**. [S.l.]: Campo das Letras, 2005.

CASSENS, J.; KOFOD-PETERSEN, A. Using activity theory to model context awareness: a qualitative case study. In: **Proceedings of the 19th International Florida Artificial Intelligence Research Society Conference, Florida, USA, AAAI Press**. [s.n.], 2006. p. 619–624. Disponível em: <https://www.aaai.org/Papers/FLAIRS/2006/Flairs06-122.pdf>.

CETIC.BR. Tic empresas 2011. Mar 2012. Disponível em: <\urlhttp://www-.cetic.br/empresas/2011/index.ht>.

CIBORRA, C.; WILLCOCKS, L. The mind or the heart? it depends on the (definition of) situation. **Journal of Information Technology**, Nature Publishing Group, v. 21, n. 3, p. 129–139, 2006.

CLANCEY, W. **Situated cognition: On human knowledge and computer representations**. [S.l.]: Cambridge University Press, 1997.

CORRADI, A.; MONTANARI, R.; TIBALDI, D. Context-based access control management in ubiquitous environments. **Network Computing and Applications, IEEE International Symposium on**, Published by the IEEE Computer Society, v. 0, p. 253–260, 2004. Disponível em: <http:/-/dx.doi.org/10.1109/NCA.2004.1347784>.

CORSO, K. B.; FREITAS, H. M. R.; BEHR, A. O contexto no trabalho móvel: uma discussão à luz do paradigma da ubiquidade. In: **8o. Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação - CONTECSI**. [S.l.: s.n.], 2011.

DAMIANI, M.; SILVESTRI, C. Towards movement-aware access control. In: ACM. **Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS**. [S.l.], 2008. p. 39–45.

DERNTL, M.; HUMMEL, K. Modeling Context-Aware e-Learning Scenarios. **Third IEEE International Conference on Pervasive Computing and Communications Workshops**, Ieee, p. 337–342, 2005. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper-.htm?arnumber=1392861>.

DEY, A. Understanding and using context. **Personal and ubiquitous computing**, Springer-Verlag, v. 5, n. 1, p. 4–7, 2001. ISSN 1617-4909. Disponível em: <http://portal.acm.org/citation.cfm?id=593572>.

DOURISH, P. What we talk about when we talk about context. **Personal and ubiquitous computing**, Springer-Verlag, v. 8, n. 1, p. 19–30, 2004.

DUHIGG, C. **O poder do hábito: por que fazemos o que fazemos na vida e nos negócios**. [S.l.]: Objetiva, 2012.

FALAKI, H.; MAHAJAN, R.; KANDULA, S.; LYMBEROPOULOS, D.; GOVINDAN, R.; ESTRIN, D. Diversity in smartphone usage. In: ACM. **Proceedings of the 8th International Conference on Mobile systems, applications, and services**. [S.l.], 2010. p. 179–194.

FERRY, N.; LAVIROTTE, S.; TIGLI, J.; REY, G.; RIVEILL, M. Toward a Behavioral Decomposition for Context-awareness and Continuity of Services. In: SPRINGER. **Ambient intelligence and future trends-International symposium on ambient intelligence (ISAMI 2010)**. [S.l.], 2010. p. 55–62.

FIALHO, F. **Psicologia das Atividades Mentais: introdução às ciências da cognição**. Florianópolis: Insular, 2011.

FILHO, C. B.; ASSUNÇÃO, R.; SILVA, B. da; MARINHO, F.; REIS, I.; ALMEIDA, M. de M. Conglomerados de homicídios e o tráfico de drogas em Belo Horizonte, Minas Gerais, Brasil, de 1995 a 1999. **Cad. Saúde Pública**, SciELO Public Health, v. 17, n. 5, p. 1163–1171, 2001.

FLANAGAN, C. The case for needs in psychotherapy. **Journal of Psychotherapy Integration**, Educational Publishing Foundation, v. 20, n. 1, p. 1, 2010.

FURNELL, S.; CLARKE, N.; KARATZOUNI, S. Beyond the pin: Enhancing user authentication for mobile devices. **Computer Fraud & Security**, Elsevier, v. 2008, n. 8, p. 12–17, 2008.

GAFUROV, D.; HELKALA, K.; NDROL, T. S. Biometric gait authentication using accelerometer sensor. **Journal of Computers**, v. 1, n. 7, p. 51–59, nov. 2006. ISSN 1796-203X.

HEIJDEN, H. van der; KOTSIS, G.; KRONSTEINER, R. Mobile Recommendation Systems for Decision Making. **Mobile Business, International Conference on**, IEEE Computer Society, v. 0, p. 137–143, 2005. Disponível em: <http://dx.doi.org/10.1109/ICMB.2005.68>.

HENRICKSEN, K.; INDULSKA, J.; RAKOTONIRAINY, A. Modeling context information in pervasive computing systems. **Pervasive Computing**, Springer, p. 79–117, 2002.

HONG, J.; SATYANARAYANAN, M.; CYBENKO, G. Guest Editors' Introduction: Security & Privacy. **IEEE Pervasive Computing**, v. 6, n. 4, p. 15–17, 2007. ISSN 1536-1268.

HONG, J.-y.; SUH, E.-h.; KIM, S.-J. Context-aware systems: A literature review and classification. **Expert Systems with Applications**, Elsevier Ltd, v. 36, n. 4, p. 8509–8522, maio 2009. ISSN 09574174. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0957417408007574>.

HUNG, L. X.; HASSAN, J.; RIAZ, A.; RAAZI, S. M. K.; WEIWEI, Y.; CANH, N.; TRUC, P. T. H.; LEE, S.; LEE, H.; SON, Y.; FERNANDES, M.; KIM, M.; ZHUNG, Y. Activity-based security scheme for ubiquitous environments. In: **Performance, Computing and Communications Conference, 2008. IPCCC 2008. IEEE International**. [S.l.: s.n.], 2008. p. 475–481. ISSN 1097-2641.

IDC. Vendas de smartphones crescem 78%. julho 2013. Disponível em: <http://brasileconomico.ig.com.br/epaper/contents/paper136330754375-.pdf>.

JAMEEL, H.; SHAIKH, R.; LEE, H.; LEE, S. Human identification through image evaluation using secret predicates. **Topics in Cryptology–CT-RSA 2007**, Springer, v. 4377, p. 67–84, 2006. Disponível em: <http://www-.springerlink.com/index/EVL6JGT546674294.pdf>.

JOHNSON, G. Towards shrink-wrapped security: A taxonomy of security-relevant context. In: **Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on**. Galveston, TX: IEEE, 2009. p. 1–2. Disponível em: <http://dx.doi.org/10.1109-/PERCOM.2009.4912819>.

KAKIHARA, M.; SØRENSEN, C. Expanding the 'mobility' concept. **ACM SIGGroup bulletin**, ACM, v. 22, n. 3, p. 33–37, 2001.

KALE, A.; RAJAGOPALAN, A.; CUNTOOR, N.; KRUGER, V. Gait-based recognition of humans using continuous hmms. In: IEEE. **Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on**. [S.l.], 2002. p. 336–341.

KAPTELININ, V.; NARDI, B. **Acting with technology**. [S.l.]: Mit Press, 2006.

KIM, J.; SONG, C.; KIM, T.; RIM, K.; LEE, J. Secure and Efficient Recommendation Service of RFID System Using Authenticated Key Management. In: **Ubiquitous Information Technologies & Applications, 2009. ICUT'09. Proceedings of the 4th International Conference on**. IEEE, 2009. p. 1–5. Disponível em: <http://dx.doi.org/10.1109/ICUT-.2009.5405678>.

KOFOD-PETERSEN, A.; CASSENS, J. Using activity theory to model context awareness. **Modeling and Retrieval of Context**, Springer, n. Idi, p. 1–17, 2006. Disponível em: <http://www.springerlink.com/index-/t8718u3937111373.pdf>.

KOFOD-PETERSEN, A.; MIKALSEN, M. An architecture supporting implementation of context-aware services. In: **Workshop on Context Awareness for Proactive Systems (CAPS 2005), Helsinki, Finland, HIIT Publications**. [S.l.: s.n.], 2005. p. 31–42.

KULLDORFF, M. SaTScan: software for the spatial, temporal, and space-time scan statistics, version 5.1 [computer program]. **Inf Manag Serv**, 2005.

KUUTTI, K. Activity theory as a potential framework for human-computer interaction research. **Context and consciousness: Activity theory and human-computer interaction**, p. 17–44, 1996.

LAVE, J.; WENGER, E. **Situated learning: Legitimate peripheral participation**. [S.l.]: Cambridge university press, 1991.

LIMA, J.; ROCHA, C.; AUGUSTIN, I.; DANTAS, M. A Context-Aware Recommendation System to Behavioral Based Authentication in Mobile and

Pervasive Environments. In: IEEE. **Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on**. [S.l.], 2011. p. 312–319.

LIMA, J.; ROCHA, C.; DANTAS, M. An authentication approach based on behavioral profiles. In: **5th Iberian Conference on Information Systems and Technologies (CISTI)**. Santiago de Compostela, Spain: IEEE, 2010. p. 1–4. ISBN 978-1-4244-7227-7. Disponível em: <http://ieeexplore-.ieee.org/xpls/abs_all.jsp?arnumber=5556601>.

LIMA, J.; ROCHA, C.; VIEIRA, M.; AUGUSTIN, I.; DANTAS, M. CARS-AD: a context-aware recommender system to decide about implicit or explicit authentication in ubihealth. In: ACM. **Proceedings of the 9th ACM International Symposium on Mobility management and wireless access**. [S.l.], 2011. p. 83–92.

LIN, C.; LIN, S.; WANG, R.; SUN, T.; CHAO, C.; FENG, W.; TSENG, F. A skill-, rule-, and knowledge-based interaction design framework for web-based virtual reality training systems. **Key Engineering Materials**, Trans Tech Publ, v. 450, p. 564–567, 2011.

LYYTINEN, K.; YOO, Y. Issues and challenges in ubiquitous computing. **Communications of the ACM**, ACM, New York, NY, USA, v. 45, n. 12, p. 62–65, dez. 2002. ISSN 0001-0782. Disponível em: <http://doi.acm-.org/10.1145/585597.585616>.

MATURANA, H.; VARELA, F. **A árvore do conhecimento: as bases biológicas da compreensão humana; The tree of knowledge: the biological basis of human understanding**. [S.l.]: Palas Athena, 2001.

MCDONALD, D. Ubiquitous recommendation systems. **Computer**, Published by the IEEE Computer Society, v. 36, p. 111, 2003. ISSN 0018-9162. Disponível em: <http://dx.doi.org/10.1109/MC.2003.1236478>.

MONROSE, F.; RUBIN, A. Authentication via keystroke dynamics. In: ACM. **Proceedings of the 4th ACM conference on Computer and communications security**. [S.l.], 1997. p. 48–56.

MOSTEFAOUI, G.; PASQUIER-ROCHA, J.; BREZILLON, P. Context-aware computing: a guide for the pervasive computing community. In: IEEE. **Pervasive Services, 2004. ICPS 2004. IEEE/ACS International Conference on**. [S.l.], 2004. p. 39–48.

MULLINS, R.; Carsten Pils, T.; ROUSSAKI, D.; NTUA, D. Context and Knowledge Management. **Mobile Service Platforms Cluster, White paper, June**, p. 1–47, 2008.

MYERS, B.; NICHOLS, J.; WOBBROCK, J.; MILLER, R. Taking handheld devices to the next level. **Computer**, IEEE, v. 37, n. 12, p. 36–43, 2004.

NEAL, D. T.; WOOD, W.; QUINN, J. M. Habits—a repeat performance. **Current Directions in Psychological Science**, SAGE Publications, v. 15, n. 4, p. 198–202, 2006.

NEUMAN, B.; TS'O, T. Kerberos: An authentication service for computer networks. **Communications Magazine, IEEE**, IEEE, v. 32, n. 9, p. 33–38, 1994.

NISENSON, M.; YARIV, I.; EL-YANIV, R.; MEIR, R. Towards behaviometric security systems: Learning to identify a typist. **Knowledge Discovery in Databases: PKDD 2003**, Springer, p. 363–374, 2003.

OKU, K.; NAKAJIMA, S.; MIYAZAKI, J.; UEMURA, S.; KATO, H.; HATTORI, F. A Recommendation System Considering Users' Past/Current/Future Contexts. **ids.csom.umn.edu**, p. 3–7, 2010. Disponível em: <http://ids.csom.umn.edu/faculty/gedas/cars2010/OkuEtAl-CARS-2010.pdf>.

PINHEIRO, J.; VIEIRA, C.; SANTOS, N.; BALIEIRO, A. da S.; AGRIMENSURA, S. de. O uso do sensoriamento remoto e da estatística de varredura (scan) na detecção e quantificação em significância de agrupamentos de desmatamento no sul da amazônia. In: **XIV Simpósio Brasileiro de Sensoreamento Remoto**. Natal, Brasil: [s.n.], 2009. p. 3519–3526.

RAHMATI, A.; ZHONG, L. Human-battery interaction on mobile phones. **Pervasive and Mobile Computing**, Elsevier, v. 5, n. 5, p. 465–477, 2009.

RASMUSSEN, J. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. **Systems, Man and Cybernetics, IEEE Transactions on**, IEEE, n. 3, p. 257–266, 1983.

RAY, S.; MAHANTI, A. Strategies for effective shilling attacks against recommender systems. **Privacy, Security, and Trust in KDD**, Springer, v. 5456, p. 111–125, 2009. Disponível em: <http://www.springerlink-.com/index/d6v15h1276872265.pdf>.

REGO, T. **Vygotsky: uma perspectiva histórico-cultural da educação**. 19. ed. [S.l.]: Vozes, 2008.

RICCI, F.; NGUYEN, Q. Acquiring and revising preferences in a critique-based mobile recommender system. **IEEE Intelligent Systems**, IEEE Computer Society, v. 22, p. 22–29, 2007. ISSN 1541-1672. Disponível em: <http://dx.doi.org/10.1109/MIS.2007.43>.

RICCI, F.; ROKACH, L.; SHAPIRA, B. Introduction to recommender systems handbook. **Recommender Systems Handbook**, Springer, p. 1–35, 2011. Disponível em: <http://www.springerlink.com/index-/X8622U506942LU28.pdf>.

ROBERTS, M.; DUCHENEAUT, N.; BEGOLE, B.; PARTRIDGE, K.; PRICE, B.; BELLOTTI, V.; WALENDOWSKI, A.; RASMUSSEN, P. Scalable architecture for context-aware activity-detecting mobile recommendation systems. In: IEEE. **World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a**. [S.l.], 2008. p. 1–6.

ROCHA, C. C. **A Context-Aware Authentication Approach Based on Behavioral Definitions**. Dissertação (Mestrado) — Federal University of Santa Catarina, Florianopolis, SC, Brazil, 2010.

ROMERO-MARIONA, J.; ZIV, H.; RICHARDSON, D. J. Srrs: a recommendation system for security requirements. In: **Proceedings of the 2008 International Workshop on Recommendation systems for software engineering**. New York, NY, USA: ACM, 2008. (RSSE '08), p. 50–52. ISBN 978-1-60558-228-3. Disponível em: <http://doi.acm.org/10.1145-/1454247.1454266>.

ROUSSOS, G. Ubiquitous computing for electronic business. **Ubiquitous and Pervasive Commerce**, Springer, p. 1–12, 2006.

RYAN, S.; JAFFE, J.; DRAKE, S.; BOGGS, R. Worldwide mobile worker population 2009–2013 forecast. **Framingham, MA: International Data Corporation**, 2009.

SCHILIT, B.; ADAMS, N.; WANT, R. Context-aware computing applications. In: IEEE. **Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on**. [S.l.], 1994. p. 85–90.

SHI, E.; NIU, Y.; JAKOBSSON, M.; CHOW, R. Implicit authentication through learning user behavior. **Information Security**, Springer, p. 99–113, 2011.

SILVA, T. H.; CELES, C.; MOTA, V. F.; LOUREIRO, A. A. Overview of ubicomp research based on scientific publications. **Proceedings of IV Simpósio Brasileiro de Computação Ubíqua e Pervasiva, SBCUP**, 2012.

SU, X.; KHOSHGOFTAAR, T. A survey of collaborative filtering techniques. **Advances in Artificial Intelligence**, Hindawi Publishing Corp., v. 2009, p. 19, 2009.

SUCHMAN, L. **Plans and situated actions: the problem of human-machine communication**. [S.l.]: Cambridge Univ Pr, 1987.

TAMMINEN, S.; OULASVIRTA, A.; TOISKALLIO, K.; KANKAINEN, A. Understanding mobile contexts. **Personal and Ubiquitous Computing**, Springer-Verlag, v. 8, n. 2, p. 135–143, 2004.

TCU, T. **Boas práticas em segurança da informação**. Brasilia, 2007. v. 2. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs-/2059162.PDF>.

TONINELLI, A.; MONTANARI, R.; LASSILA, O.; KHUSHRAJ, D. What's on users' minds? toward a usable smart phone security model. **IEEE Pervasive Computing**, IEEE Computer Society, p. 32–39, 2009.

UDEN, L. Activity theory for designing mobile learning. **International Journal of Mobile Learning and Organisation**, Inderscience, v. 1, n. 1, p. 81–102, 2007. Disponível em: <http://inderscience.metapress.com-/index/EW9VEADD3EUFJHV3.pdf>.

VARELA, F.; THOMPSON, E.; ROSCH, E. **The embodied mind: Cognitive science and human experience**. [S.l.]: MIT press, 1992.

VICENTE, K. Cognitive engineering research at risø from 1962–1979. **Advances in human performance and cognitive engineering research-Performance and cognitive engineering research**, Emerald Group Publishing Limited, v. 1, p. 1–57, 2001.

VICENTE, K.; RASMUSSEN, J. Ecological interface design: Theoretical foundations. **Systems, Man and Cybernetics, IEEE Transactions on**, IEEE, v. 22, n. 4, p. 589–606, 1992.

VYGOTSKI, L.; LURIA, A.; LEONTYEV, A. **Linguagem, desenvolvimento e aprendizagem**. [S.l.]: Ícone, 2005.

WANG, Y.; WEN, Q.; ZHANG, H. A single sign-on scheme for cross domain web applications using identity-based cryptography. In: IEEE. **Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on**. [S.l.], 2010. v. 1, p. 483–485.

WANGHAM, M.; MELLO, E. de; BÖGER, D. da S.; GUERIOS, M.; FRAGA, J. da S. Gerenciamento de identidades federadas. **Minicurso-SBSeg 2010-Fortaleza-CE**, 2010.

WAZLAWICK, R. Uma reflexão sobre a pesquisa em ciência da computação à luz da classificação das ciências e do método científico. **Revista de Sistemas de Informação da FSMA**, n. 6, p. 3–10, 2010.

WEISER, M. The computer for the 21st century. **Scientific American**, New York, v. 265, n. 3, p. 94–104, 1991.

WENGER, E. **Communities of practice: Learning, meaning, and identity**. [S.l.]: Cambridge university press, 1999.

WOOD, W.; QUINN, J. M.; KASHY, D. A. *et al.* Habits in everyday life: Thought, emotion, and action. **Journal of personality and social psychology**, APA AMERICAN PSYCHOLOGICAL ASSOCIATION, v. 83, n. 6, p. 1281–1297, 2002.

YUAN, Y.; ZHENG, W. Mobile task characteristics and the needs for mobile work support: a comparison between mobile knowledge workers and field workers. In: IEEE. **Mobile Business, 2009. ICMB 2009. Eighth International Conference on**. [S.l.], 2009. p. 7–11.

ZHAN, J.; HSIEH, C.; WANG, I.; HSU, T.; LIAU, C.; WANG, D. Privacy-preserving collaborative recommender systems. **Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on**, IEEE, v. 40, n. 4, p. 472–476, 2010. Disponível em: <http://dx.doi.org-/10.1109/TSMCC.2010.2040275>.

ZHANG, M.; YUAN, Y. M-commerce vs. internet-based e-commerce: the key differences. In: **Proceedings of the American Conference on Information Systems**. [S.l.: s.n.], 2002.

ANEXO A – PUBLICAÇÕES

Este apêndice visa ilustrar as publicações realizadas ao longo da pesquisa desse trabalho de tese.

A.1 CAPíTULOS DE LIVROS PUBLICADOS

A.1.1 InTech - Open Access Publisher

- **Título:** CARS-AD Project: Context-aware Recommender System for Authentication Decision in Pervasive and Mobile Environments
- **Livro:** Advances and Applications in Mobile Computing
- **ISBN:** 978-953-51-0432-2
- **Editora:** InTech - Open Access Publisher
- **Data:** Primeiro semestre de 2012
- **Autores:** João Carlos D. Lima, Cristiano C. Rocha, Iara Augustin e Mário A. R. Dantas
- **DOI:** `DOI:10.5772/37125`

A.2 TRABALHOS COMPLETOS PUBLICADOS EM ANAIS DE CONGRESSOS

A.2.1 CISTI 2010 – 5th Iberian Conference on Information Systems and Technologies

- **Título:** Uma Arquitetura de Autenticação Baseada em Perfis Comportamentais
- **Evento:** CISTI 2010 – 5th Iberian Conference on Information Systems and Technologies
- **Local:** Santiago de Compostela, Espanha

- **Data:** Junho de 2010
- **Autores:** João Carlos D. Lima, Cristiano C. Rocha e Mário A. R. Dantas
- **Estrato Qualis/CAPES:** B4

A.2.2 IKE 2010 – The 2010 International Conference on Information and Knowledge Engineering

- **Título:** A Context-Aware Authentication Approach Based on Behavioral Definitions
- **Evento:** IKE 2010 – The 2010 International Conference on Information and Knowledge Engineering
- **Local:** Las Vegas, Nevada, EUA
- **Data:** Julho de 2010
- **Autores:** Cristiano C. Rocha, João Carlos D. Lima, Matheus A. Viera, Miriam Capretz, Michael A. Bauer, Iara Augustin e Mário A. R. Dantas
- **Estrato Qualis/CAPES:** B4

A.2.3 I2TS 2010 – The 9th International Information and Telecommunication Technologies Symposium

- **Título:** Uma Abordagem de Autenticação Sensíel ao Contexto Baseada em Definições Comportamentais
- **Evento:** I2TS 2010 – The 9th International Information and Telecommunication Technologies Symposium
- **Local:** Rio de janeiro, Brasil
- **Data:** Dezembro de 2010

- **Autores:** Cristiano C. Rocha, João Carlos D. Lima, Iara Augustin e Mário A. R. Dantas
- **Estrato Qualis/CAPES:** B4

A.2.4 ISCC 2011 – The 16th IEEE Symposium on Computers and Communications

- **Título:** A2BeST: An Adaptive Authentication Service Based on Mobile User's Behavior and Spatio-Temporal Context.
- **Evento:** ISCC 2011 – The 16th IEEE Symposium on Computers and Communications
- **Local:** Corfu, Grécia
- **Data:** Junho de 2011
- **Autores:** Cristiano C. Rocha, João Carlos D. Lima, Iara Augustin e Mário A. R. Dantas
- **DOI:** `http://dx.doi.org/10.1109/ISCC.2011.5983933`
- **Estrato Qualis/CAPES:** A2

A.2.5 MobiWac 2011 - The 9th ACM International Symposium on Mobility Management and Wireless Access

- **Título:** CARS-AD: A Context-Aware Recommender System to Decide about Implicit or Explicit Authentication in UbiHealth.
- **Evento:** MobiWac 2011 - The 9th ACM International Symposium on Mobility Management and Wireless Access
- **Local:** Miami, Flórida, USA
- **Data:** Outubro de 2011

- **Autores:** João Carlos D. Lima, Cristiano C. Rocha, Iara Augustin e Mário A. R. Dantas
- **DOI:** `http://doi.acm.org/10.1145/2069131.2069146`
- **Estrato Qualis/CAPES:** B3

A.2.6 EUC-2011 - The 9th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing

- **Título:** A Context-Aware Recommendation System to Behavioral Based Authentication in Mobile and Pervasive Environments.
- **Evento:** EUC-2011 - The 9th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.
- **Local:** Melbourne, Austrália
- **Data:** Novembro de 2011
- **Autores:** João Carlos D. Lima, Cristiano C. Rocha, Iara Augustin e Mário A. R. Dantas
- **DOI:** `http://doi.ieeecomputersociety.org/10.1109/EUC.2011.2`
- **Estrato Qualis/CAPES:** B2

A.3 RESUMO DAS PUBLICAÇÕES

Evento	Ano	Local	Estrato Qualis CAPES
CISTI 2010 – 5th Iberian Conference on Information Systems and Technologies	2010	Santiago de Compostela, Espanha	B4
IKE 2010 – The 2010 International Conference on Information and Knowledge Engineering	2010	Las Vegas, EUA	B4
I2TS 2010 – The 9th International Information and Telecommunication Technologies Symposium	2010	Rio de Janeiro, Brasil	B4
ISCC 2011 – The 16th IEEE Symposium on Computers and Communications	2011	Corfu, Grécia	A2
MobiWac 2011 – The 9th ACM International Symposium on Mobility Management and Wireless Access	2011	Miami, USA	B3
EUC-2011 – The 9th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing	2011	Melbourne, Austrália	B2
Capítulo no Livro: Advances and Applications in Mobile Computing - ISBN 978-953-51-0432-2	2012		

Quadro 8: Resumo das Publicações