Um Estudo sobre Consciência de Situação

Ricardo Borges Almeida [1]
Roger da Silva Machado [1]
Orientador: Ana Marilza Pernas [1]
Orientador: Adenauer Corrêa Yamin [1]

Resumo: O tema Consciência de Situação vem sendo explorado por diversas áreas ligadas à Ciência da Computação, sendo, em geral, tratado como um estudo decorrente da área de Consciência de Contexto, agregando conhecimento e raciocínio a esta. Dentre essas áreas, este artigo tem foco nos Sistemas Computacionais Ubíquos, na qual a Consciência de Contexto consiste de um requisito funcional. Com o intuito de fornecer uma fonte para pesquisa e acesso a conteúdo especializado no tema, o presente artigo explora o tema Consciêcia de Situação, apresentando sua conceituação e origem, suas principais áreas de aplicação e vantagens decorrentes, assim como as principais técnicas e abordagens para consciência de situação. Para facilitar o entendimento, exemplos voltados a área de segurança e análise de logs são apresentados no decorrer do trabalho. Ao final um estudo de caso explora a utilização de Consciência de Situação na área de Segurança da Informação, visando apresentar a aplicação prática do tema em uma aplicação real.

1 Introdução

Na Computação Ubíqua (UbiComp) as aplicações precisam ter consciência do seu contexto de interesse e, quando for o caso, se adaptarem ao mesmo. Essa classe de sistemas computacionais, conscientes de contexto, abre perspectivas para o desenvolvimento de aplicações mais ricas, elaboradas e complexas, que exploram a natureza dinâmica das modernas infra-estruturas computacionais. O desenvolvimento de aplicações que possam se adaptar continuamente, permanecendo operacionais continua sendo um importante desafio de pesquisa [1].

Dentre os inúmeros desafios inerentes a estas aplicações, destacam-se a aquisição de informações contextuais relevantes ao contexto de interesse da aplicação a partir de um conjunto de fontes heterogêneas, seu processamento e armazenamento de forma a obter-se um histórico para realização de inferências e, assim, a tomada de decisões que interfiram no estado do ambiente ubíquo.

[1]Centro de Desenvolvimento Tecnológico, UFPel, Caixa Postal 354
{rbalmeida,rdsmachado,marilza,adenauer@inf.ufpel.edu.br}

Estes diferentes contextos de interesse produzem dados que podem ser relevantes ou não para a aplicação. Os elementos contextuais instanciados (dados), quando considerados relevantes para a aplicação são denominados eventos. Estes eventos quando relacionados com outros eventos, que podem ter sido produzidos em diferentes contextos, produzem situações. Sendo assim, dentro do escopo de estudo dos sistemas conscientes de contexto, a consciência de situação tem surgido como foco de pesquisa.

Apesar das pesquisas em análise e consciência de situação terem ganho ênfase recentemente devido às aplicações no âmbito de sistemas ubíquos, os conceitos de situação e consciência de situação têm sido estudados há longo tempo, sendo bem definidos nas áreas de filosofia e ciências cognitivas [2].

Consciência de situação possui muitas aplicações, pois é fundamental para que indivíduos e equipes trabalhem efetivamente em seu ambiente, constatando-se assim que a aplicação deste tema vai além do campo da aviação, podendo ser utilizado em uma grande variedade de domínios. Atualmente, as pesquisas em consciência de situação tem-se disseminado para diversas áreas, como sistemas educacionais web, controle de tráfego aéreo, operação de usinas de energia nuclear, direção de automóveis, anestesiologia, entre outras [2], [3], [4], [5], [6], [7].

Sendo assim, existem muitas definições para situação e consciência de situação de acordo com a área de aplicação, logo elas serão discutidas na seção específica sobre consciência de situação. Antes disso, é necessário apresentar algumas motivações para uso de consciência de situação e seus benefícios, os quais serão apresentados na próxima subseção.

1.1 Motivações e Benefícios

Tanto as motivações quanto os benefícios para utilização de consciência de situação estão ligados diretamente ao domínio de aplicação. Por exemplo, um dos problemas na indústria de transporte aéreo está relacionado aos constrangimentos relativos ao trabalho de equipes nas cabines de comando executado por comandantes e copilotos, no qual deficiências de coordenação entre os agentes emergem através das falhas de consciência situacional coletiva, precedidas por julgamento e decisões incorretos, ocorrência de erros e aumento da carga mental dos operadores [8].

De forma independente da área de aplicação, é possível destacar os seguintes benefícios:

- Auxílio no processo de transformação dos dados em informação;

- Compreensão amplificada do ambiente real;
- Gerenciamento adequado dos erros e das ameaças;
- Efetividade na tomada de decisões.

Para esclarecer a diferença que há nas motivações e benefícios de acordo com a aplicação, observa-se que o exemplo inicialmente apresentado é uma visão da perspectiva humana, no entanto, em sistemas computacionais também pode ser necessário identificar se uma atividade esta ocorrendo baseado em um conhecimento prévio e interconectar diversos eventos, como no caso de sistemas ubíquos e sistemas de detecção de introdução (*Intrusion Detection System* - IDS), fornecendo tanto os benefícios acima como inúmeros outros de acordo com suas necessidades.

A fim de evidenciar a relevância que a consciência de situação pode ocasionar a computação, será apresentado na sequência, motivações e consequentemente os benefícios da utilização de consciência situacional aplicada a segurança da informação através de um exemplo prático.

Graças aos avanços tecnológicos e, particularmente, aqueles propiciados pelas pesquisas em computação ubíqua, novas tecnologias estão cada vez mais integradas ao cotidiano das pessoas, nas comunicações, no setor financeiro e até no entretenimento. Esta situação provê um dinamismo nunca visto na troca de dados, a informação hoje é armazenada e transmitida na forma digital, trafegando pela Internet em velocidades cada vez maiores. As facilidades da Internet, de uso largamente disseminado, como o e-mail e a World Wide Web, estão entre os principais serviços responsáveis por esta disseminação [9].

Infelizmente, todas estas facilidades e potencialidades oferecidas também acabam sendo objeto de interesse de pessoas mal intencionadas, que usam destes recursos para cometer fraudes ou realizar ataques diversos contra sistemas de informação e/ou seus usuários. Logo, segurança e privacidade são desafios presentes na computação de forma geral. Na UbiComp, em particular, a segurança e a privacidade são desafios que ficam potencializados devido à natureza volátil, espontânea, heterogênea e invisível de como ocorre comunicação nos sistemas ubíquos [10].

Para se obter a consciência de situação é possível realizar a correlação de eventos que é considerada uma forma eficaz na detecção de falhas de sistema e de segurança. Visto que os logs armazenam eventos detectados pelo sistema operacional e pelas aplicações, e que eventos são responsáveis por armazenar e tratar todas as mudanças ocorridas em qualquer situação que esteja acontecendo no momento, percebe-se uma grande oportunidade de utilização de consciência de situação. Sendo assim, através da consciência de situação aplicada aos eventos registrados nos logs, é possível obter

uma visão geral da infra-estrutura computacional que forma um ambiente ubíquo com enfoque na perspectiva de segurança da informação, permitindo a tomada de decisões de acordo com as situações detectadas, contribuindo para que se tenha um ambiente pró-ativo, seguro e em pleno funcionamento.

Para demonstrar a aplicação prática de consciência de situação, exemplos ligados à aplicação citada serão apresentados neste trabalho. Na próxima subseção serão apresentados os objetivos gerais e particulares deste capítulo.

2 Base Conceitual

Nesta seção serão apresentados os conceitos considerados relevantes para a compreensão de consciência de situação, assim como os conceitos relacionados ao estudo de caso a ser apresentado ao final do trabalho.

2.1 Evento

O conceito de evento é muito importante quando se trata de consciência de situação, pois eventos são responsáveis por armazenar e tratar todas as mudanças sucedidas em qualquer situação que esteja ocorrendo no momento [11].

Em [12], evento é definido como uma ocorrência dentro de um determinado sistema ou domínio, algo que já aconteceu, ou está previsto para acontecer. Nele, também é citado que o termo evento é utilizado como significado de uma entidade de programação que representa uma instância em um sistema computacional.

A CEE™ (*Common Event Expression*) é uma iniciativa que está sendo desenvolvida por uma comunidade que representa os fornecedores, pesquisadores e usuários finais coordenada pela MITRE (empresa privada sem fins lucrativos dedicada a prestação de serviços ao governo dos Estados Unidos). O principal objetivo do esforço é padronizar a representação e troca de logs de sistemas eletrônicos. Para alcançar este objetivo, eles contaram com a participação de diversas pessoas, entidades do governo e setor privado para criar a CEE *Architecture*, uma arquitetura que define a estrutura e os componentes que formam o padrão de log CEE, documentada em [13]. Dentre os diversos termos definidos para se obter um documento conciso sobre a arquitetura, está o evento, que foi conceituado conforme a seguir, e será adotado neste capítulo:

> **Evento** é uma ocorrência única dentro de um ambiente, geralmente envolvendo uma tentativa de mudança de situação. Inclui normalmente a noção de tempo, a ocorrência, e os detalhes que pertencem explicitamente

ao evento ou ambiente que podem ajudar a explicar ou compreender as causas ou efeitos do evento.

Um evento pode ser dividido em campos que descrevem uma característica do evento. Exemplos de campos de um evento registrado por um acesso a uma página web incluem data, hora, endereço IP (*Internet Protocol*) de origem, identificação do usuário (caso autenticação seja necessária), o objeto requisitado, entre outras informações.

Um registro de evento é uma coleção de campos de um evento que juntos descrevem um único evento. Termos sinônimos a registro de eventos incluem "registro de auditoria" e "entrada de log".

Algumas vezes, eventos são utilizados para representar mudanças em situações, e esta abordagem é utilizada em algumas soluções de monitoramento [12]. O sistema monitorado é representado por um grupo de sensores onde cada um está associado a uma situação inicial. Normalmente é possível verificar os valores de cada sensor através de uma consulta, ou o próprio sensor emite um valor agindo como um produtor de eventos. Desta forma, é possível verificar quando a situação de um sensor foi modificada avaliando o valor identificado. Um exemplo simples a ser considerado é um sensor de temperatura ambiente que inicialmente produz um evento informando que a temperatura se encontra em 28°C (vinte e oito graus Celsius). Dependendo do ambiente esta temperatura pode ser considerada adequada. Posteriormente o mesmo sensor emite a temperatura de 40°C (quarenta graus Celsius), que pode representar um superaquecimento.

Percebe-se então que muitos dos eventos que acontecem ao redor de um indivíduo ou até mesmo em um sistema não são eventos de interesse, ou seja, não representam algo relevante naquele determinado contexto, em contrapartida, outros são relevantes e podem causar uma mudança na situação atual. Um outro exemplo para esclarecer esta observação, considerando três estudantes em um escritório, caso comece a chover, isto pode representar um evento de interesse se algum dos estudantes tiver colocado roupas para secar ao sol, e que agora devam ser recolhidas para que não molhem, do contrário, pode ser considerado como um evento irrelevante, não alterando a situação em que eles se encontram.

Estes foram exemplos simples da identificação de situações através de um único evento, no entanto, é possível considerar que vários eventos de interesse relacionados logicamente em um intervalo de tempo específico podem formar situações onde há a necessidade de reação.

2.2 Contexto

> **Contexto** é qualquer informação que pode ser usada para caracterizar a situação de uma entidade (pessoa, local ou objeto) que é considerada relevante para a interação entre o usuário e a aplicação, incluindo o próprio usuário e a aplicação [14].

Contexto pode ser considerado também como uma descrição complexa de conhecimento compartilhado sobre circunstâncias físicas, sociais, históricas e outras, onde ações ou eventos ocorrem. É o que restringe a interpretação de uma ação ou evento, sem, no entanto, ser parte dessa ação/evento. Contexto é uma coleção de condições relevantes e influências que tornam uma situação única e compreensível [15].

Conforme dito anteriormente, existem seis questões básicas que podem ser realizadas para facilitar a compreensão do contexto, elas são conhecidas como 5W+1H. No entanto, para determinadas aplicações algumas são mais importantes que outras. A seguir as seis questões são apresentadas:

- **Quem (*Who*)**: Informação de presença e disponibilidade dos indivíduos no grupo, e de identificação dos participantes envolvidos num evento ou numa ação.
- **O quê (*What*)**: Informação sobre a ocorrência de um evento de interesse ao grupo.
- **Quando (*When*)**: Informação temporal sobre o evento, o momento em que o evento ocorreu.
- **Onde (*Where*)**: Informação espacial, de localização, o local onde o evento ocorreu.
- **Por que (*Why*)**:Informação subjetiva sobre as intenções e motivações que levaram à ocorrência do evento.
- **Como (*How*)**: Informação sobre a maneira como o evento ocorreu

O contexto é relativo a algo, a um foco. O foco é uma tarefa ou um passo na resolução de um problema ou em uma tomada de decisão [16]. Por exemplo, o contexto de um repórter de TV está em passar a notícia. A figura 1 mostra um exemplo de foco do contexto de um médico. Portanto, o contexto é sempre o foco de atenção atual do usuário. O foco ainda determina onde está o contexto e o que pode ser considerado como importante, pois nem tudo que é contexto de uma situação é relevante para tal.

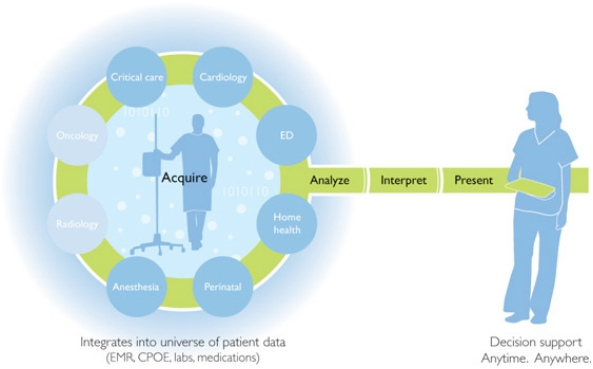

Figura 1. Contexto relativo ao foco

2.3 Consciência de Contexto

> **Consciência de contexto** é a capacidade de um sistema em usar o contexto para prover serviços e/ou informações relevantes para o usuário [14].

Ao se construir e executar aplicações ubíquas sensíveis ao contexto há uma série de funcionalidades que devem ser providas, envolvendo desde a aquisição de informações contextuais, a partir do conjunto de fontes heterogêneas e distribuídas, até a representação dessas informações, seu processamento, armazenamento, e a realização de inferências para seu uso em tomadas de decisão [17].

Os sistemas conscientes de contexto devem ser flexíveis, adaptativos, e capazes de atuar automaticamente para ajudar o usuário na realização de suas atividades.

As áreas da Computação Ubíqua e Inteligência Artificial foram as pioneiras nos estudos e utilização do conceito de contexto e, com isso, foram as que demonstraram o potencial da aplicação desse conceito nos sistemas computacionais. Pesquisas recentes vêm utilizando o conceito de contexto para beneficiar sistemas ligados a outras áreas como, por exemplo:

- **Sistemas Colaborativos**: Utilização de contexto para melhorar a interação e produtividade do grupo, aplicado por exemplo, na área médica.
- **Hipermídia Adaptativa**: Possibilidade de personalização e adaptação do conteúdo de sites web a partir de contextos.

- **Integração de Dados**: Facilitando a resolução de conflitos semânticos com a utilização de contextos.
- **Interface Humano-Computador**: O contexto é utilizado para adaptar as interfaces dos sistemas tornando mais intuitiva a sua interação com os usuários.

Algumas motivações para aplicação de consciência de contexto nos sistemas:

- Auxiliar na compreensão da realidade
- Facilitar na adaptação de sistemas
- Auxiliar no processo de transformação dos dados em informação
- Apoiar a compreensão de eventos
- Ajudar a compreender situações

2.3.1 Exemplos de Sistemas Conscientes de Contexto Atualmente existem algumas aplicações que usam a técnica de ciência do contexto, embora seja uma área ainda em expansão, isso já é consequência do aumento do interesse do estudo dessa técnica. A seguir serão descritas três ferramentas que utilizam a consciência ao contexto.

- **Gmail**: O sistema de gerenciamento de e-mails da Google, utiliza recomendação de links e propaganda adaptada ao conteúdo do e-mail sendo lido pelo usuário. Para isso, ele extrai e utiliza informações contextuais, sob a forma de palavras-chave, contidas no e-mail em leitura e, também no histórico de e-mails. Além disso, o Gmail utiliza uma abordagem contextual para manter as mensagens, usando o conceito de discussão, ou seja, ele agrupa uma mensagem e as respostas a ela associadas como se fossem uma única mensagem, simulando, assim, uma conversa.
- **Guias Turísticos Móveis**: Os serviços móveis no guia de turismo têm como propósito satisfazer as necessidades de informação dos turistas, proporcionando-lhes uma variedade de informações turísticas relacionadas com a viagem, como acomodações, emergências, gastronomia, compras e lazer são exibidos para o turista.
- **CO2DE**: Collaborate to Design (CO2DE) é um editor síncrono/assíncrono de diagramas UML, originalmente projetado para permitir que participantes compartilhem o mesmo espaço de edição e controlem versões dos documentos sendo

construídos [18]. Como ferramenta colaborativa, ele provê funcionalidades para ajudar membros individuais a estar cientes das informações contextuais relacionadas à tarefa corrente. Por exemplo: informação sobre a composição do grupo, o papel de cada membro do grupo, cada novo documento sendo simultaneamente discutido, entre outras.

2.4 Situação

Na área de Computação Ubíqua, Anagnostopoulos (2006) define situação como uma particularização da consciência de contexto, onde situações são vistas como contextos logicamente ligados. No entanto, para este texto, o seguinte conceito será adotado:

> Uma **situação** consiste de um conjunto de elementos contextuais de interesse instanciados relacionados de forma a prover alguma informação válida em um intervalo de tempo específico.

Elemento contextual instanciado e evento serão utilizados como sinônimos neste capítulo. Assim como na avaliação de contexto, as mesmas questões 5W+1H (quem, o quê, quando, onde, por que e como) devem ser levadas em consideração para identificação da situação, porém, em determinadas aplicações algumas destas perguntas são mais importante que outras.

Da perspectiva humana, de modo geral, uma situação é a identificação das instâncias dos contextos válidos em um determinado intervalo de tempo que relacionadas representam um estado específico de um indivíduo. Por exemplo, uma situação pode ser três indivíduos (quem) no escritório de uma casa (onde), cada um estudando para suas respectivas provas (o quê) das 15h às 16h (quando). Os estudantes irão permanecer nesta mesma situação até que um evento ocorra, por exemplo, a campainha da casa tocar, o que faz com que os três percam a concentração e comecem a conversar sobre assuntos diversos.

É possível observar que no exemplo anterior não havia como identificar as questões "por que" e nem a "como" pois estas informações não foram explicitadas. Tornando ele mais completo, considerando que os estudantes estavam estudando para suas provas (por que) através da leitura dos livros indicados por seus professores (como) tem-se todas as questões informadas e identificadas. Logo, fica claro que a utilização dos 5W+1H dependerá da aplicação e das informações possíveis de serem coletadas.

Já, em um sistema operacional, é possível realizar a identificação de situações através da avaliação dos registros de log do sistema. Um exemplo simples seria o registro em um arquivo de log de três falhas na tentativa de autenticação remota em um sistema operacional em um intervalo curto de tempo a partir da mesma origem de acesso. O que leva a detecção de uma possível situação, a de um ataque de força bruta que consiste na tentativa de autenticação utilizando senhas diferentes até que o atacante consiga se autenticar. Para se obter sucesso nesse ataque, é necessário que um sistema de computador realize este processo de tentativa de autenticação várias vezes em um intervalo curto de tempo com senhas diferentes, logo estas tentativas são registradas no arquivo de log que será analisado.

Em um exemplo mais complexo, supondo um servidor de uma aplicação ubíqua com três diferentes serviços rodando. Um dos serviços instalados é um servidor web, o qual registra todos os eventos referentes aos acessos as aplicações web configuradas neste servidor em seu arquivo de log. O segundo serviço é um servidor FTP, utilizado para envio dos arquivos das aplicações web que possui seu arquivo de log para registrar todos os eventos de acesso, envio e recebimento de arquivos, entre outras funções. E por último um firewall, responsável por bloquear a tentativa de acesso a diferentes serviços que não devem estar disponíveis a determinadas origens de acesso, e que também registra os acessos negados à diferentes portas em um outro arquivo de log separadamente.

Neste exemplo apresentado, uma possível situação seria a identificação de um provável ataque ao servidor da aplicação ubíqua, através da correlação dos eventos registrados nos registros de log destes diferentes serviços, onde estes serviços são considerado como diferentes contextos, ou seja, após a identificação dos diferentes contextos válidos para uma situação, e posteriormente a correlação dos elementos contextuais instanciados que foram representados pelos eventos registrados, foi possível identificar uma situação de interesse.

Dessa forma, é possível identificar uma pirâmide, conforme na figura 2, onde os dados devem ser inicialmente coletados por sensores, para posteriormente serem contextualizados, em seguida serem repassados para a identificação da situação, fornecendo assim um conhecimento sobre o que está acontecendo.

2.5 Consciência de Situação

Dentre as diversas definições existentes na literatura devida a diversidade de áreas em que esta teoria pode ser aplicada, neste capítulo optou-se por utilizar a definição apresentada a seguir:

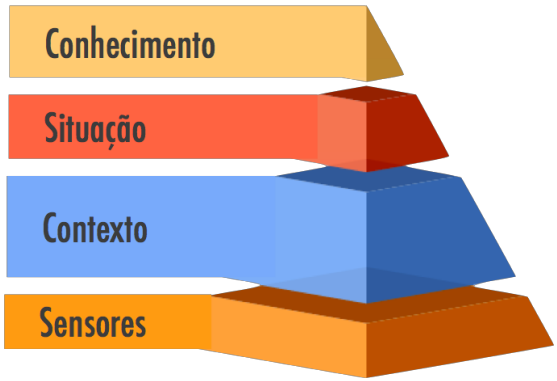

Figura 2. Consciência de Situação: Pirâmide

> **Consciência de situação** consiste da percepção e compreensão de uma ou mais situações e a projeção de seus efeitos em um futuro próximo [19].

O modelo de Endsley destaca três níveis na obtenção de consciência de situação: percepção, compreensão e projeção. Estes níveis serão detalhados a seguir com uma breve descrição da sua função junto a um exemplo de sua utilização visando a proposta de projeto.

2.5.1 Percepção - Nível 1 O primeiro passo para alcançar a consciência de situação é a percepção clara dos elementos relevantes ao seu redor. Dessa forma, este nível mais básico envolve os processos de monitoramento, detecção e reconhecimento, que levam a uma consciência de múltiplos elementos situacionais (objetos, eventos, pessoas, sistemas, fatores ambientais) e seus estados atuais (locais, condições, formas, ações).

Como exemplo, no caso de um sistema para gerenciamento de log, pode-se considerar que a percepção está ligada a capacidade de identificar os diferentes registros de log no sistema, e o processo de monitoramento contínuo destes registros. A figura 3 destaca a percepção de forma hipotética de diferentes registros gerados por diferentes aplicações (SSH, WEB, SQL, WAF), adicionado ao monitoramento do uso da Unidade Central de Processamento (*Central Processing Unit* - CPU).

É importante frisar que os nomes utilizados na figura são apenas representações realizadas a fim de facilitar a compreensão, no entanto, para dar um sentido mais real ao exemplo, é possível realizar o mapeamento das aplicações hipotéticas da figura

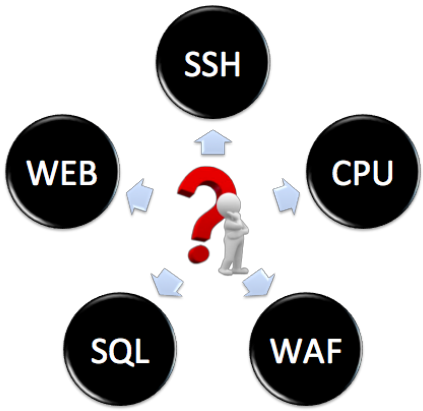

Figura 3. Consciência de Situação: Percepção

para aplicações normalmente utilizadas em um ambiente ubíquo conforme a seguir:

- **SSH**: é o software que permite a conexão com outro computador através da rede, de forma a permitir a execução de comandos de uma unidade remota, neste caso, pode ser utilizado caso o administrador do sistema deseje realizar alguma manutenção manual, instalar novos programas, desativar ou ativar serviços, ...

- **SQL**: *Structured Query Language*, ou Linguagem de Consulta Estruturada, é a linguagem de pesquisa declarativa padrão para banco de dados relacional, no entanto, neste caso será realizado o mapeamento para um Sistema de Gerenciamento de Banco de Dados (SGBD) que realizará o gerenciamento de um banco de dados onde as informações são armazenadas e coletadas quando necessário.

- **WEB**: é o software da aplicação web, responsável por disponibilizar o website para acesso externo.

- **WAF**: ou *Web Application Firewall*, considerando a existência de uma aplicação web, uma WAF desempenha a função de tentar barrar os acessos inválidos ou suspeitos.

- **CPU**: este item seria útil para verificar o consumo da Unidade Central de Processamento, pois é possível que em uma tentativa de ataque ao sistema o consumo aumente consideravelmente.

Percebe-se então, através deste exemplo, a quantidade de informações a serem analisadas devido aos diferentes contextos que a percepção deve levar em consideração, para que seja possível obter um sistema com uma percepção adequada do ambiente.

2.5.2 Compreensão - Nível 2 A percepção só não basta, é necessário ter um entendimento do significado de todos os elementos e eventos. Dessa forma, o próximo passo da formação de consciência situacional envolve uma síntese dos elementos desconexos identificados no primeiro nível através dos processos de reconhecimento de padrões, interpretação e avaliação. Este nível requer a integração dessas informações para entender como isso vai impactar as metas e objetivos do indivíduo. Isto inclui o desenvolvimento de uma visão global do ambiente, ou da parte do ambiente que é de interesse do indivíduo.

Para exemplificar, utilizando o mesmo exemplo, é possível através da correlação de eventos criar uma visão mais aprimorada do ambiente, identificando assim, possíveis situações em que o sistema se encontra. A figura 4 demonstra que utilizando a correlação entre as aplicações WEB, SQL e WAF seria possível realizar a identificação de uma situação, por exemplo, uma tentativa de ataque do tipo *SQL Injection* (Injeção de SQL), que é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL.

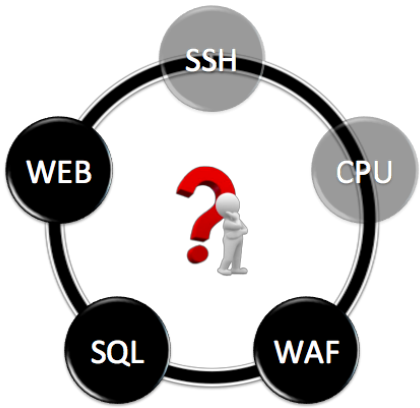

Figura 4. Consciência de Situação: Compreensão

Logo, é possível perceber que a correlação de eventos desempenha um papel fundamental nesta etapa, auxiliando a compreensão do ambiente.

2.5.3 Projeção - Nível 3 O último nível é responsável pela capacidade de antecipação de ocorrências futuras, a partir da compreensão dos elementos no ambiente atual. Ele é alcançado através do conhecimento da situação e da dinâmica dos elementos, e da compreensão da situação (níveis 1 e 2), para depois projetar esta informação à diante no tempo e assim determinar se elas afetarão os futuros estados do ambiente operacional.

Por fim, ainda com base no mesmo exemplo, de forma a demonstrar a importância que cada etapa possui, considera-se que na fase de compreensão foi detectada uma possível tentativa de injeção de SQL, é fundamental que o sistema identifique que futuramente este ataque continuará acontecendo, sendo assim, para este caso, pode ser aconselhado o bloqueio do endereço de origem do acesso ao sistema.

A seguir, na figura 5, é possível identificar a importância da contextualização dos dados e da correlação no processo identificação de uma possível situação. Nela, é demonstrado dois registros de log referentes a serviços diferentes, um registro gerado por uma aplicação de acesso remoto e o outro por um serviço de FTP, onde primeiramente é identificado o tipo de dado de ambos os registros, posteriormente os dados são contextualizados, neste processo de contextualização fica identificado o horário e o endereço IP da tentativa de acesso aos dois serviços, para na sequência serem correlacionados. Neste processo de correlação dos diferentes contextos, representados por diferentes aplicações, é identificado duas tentativas inválidas de acesso a serviços distintos em um intervalo pequeno de tempo, o que caracteriza uma tentativa de ataque neste exemplo hipotético.

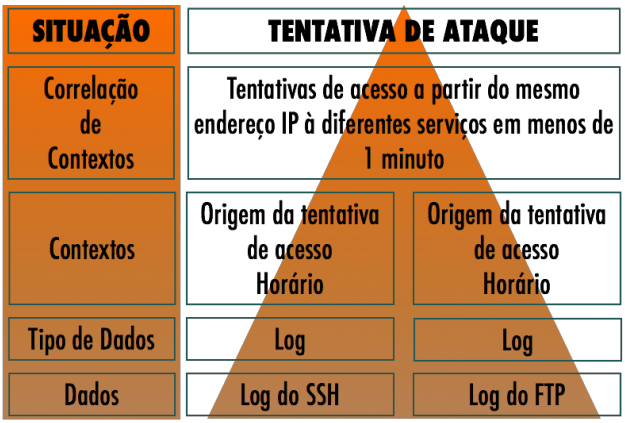

Figura 5. Consciência de Situação: Tentativa de Ataque

Logo, é possível perceber através das subseções apresentadas e dos exemplos, que a consciência de situação é um processo realizado em etapas, e que uma etapa depende da outra, ou seja, não é possível ter um sistema consciente de situação se ele não tiver percepção do que esta ao seu redor, se ele não conseguir compreender o que percebe, ou se ele não tiver a capacidade de antecipar o futuro, por mais próximo que este futuro seja.

No modelo de Endsley, figura 6, ele já previa diversas variáveis que podem influenciar o desenvolvimento e a manutenção da consciência de situação, incluindo indivíduos, tarefas, e fatores ambientais. Por exemplo, os indivíduos variam em sua capacidade de adquirir consciência situacional, assim, simplesmente fornecer o mesmo sistema e treinamento não irá garantir consciência situacional semelhante em indivíduos diferentes. O modelo de Endsley também mostra como a consciência de situação "oferece a base primária para posterior tomada de decisão e aumento de desempenho na operação de sistemas complexos e dinâmicos" [19]. Embora não possa garantir a tomada de decisão bem sucedida, a consciência de situação suporta os processos de entrada necessários (por exemplo, reconhecimento, avaliação da situação, e a previsão) em que boas decisões se baseiam [20].

Dessa forma, após a introdução aos conceitos referentes a consciência de situação, e a apresentação de alguns exemplos, vale apresentar as diferentes áreas em que a consciência de situação tem sido utilizada através dos exemplos a seguir.

2.6 Exemplos de Sistemas Conscientes de Situação

Em sistemas dinâmicos e que necessitam de tomadas de decisões rápidas a consciência de situação pode se tornar chave para atingir o sucesso [21]. Atualmente uma diversidade de áreas vem utilizando conceitos relacionados a consciência de situação (*Situational Awareness*),dentre pode-se citar controle de tráfego aéreo, operação da usina de energia nuclear, direção de automóveis, anestesiologia, computação ubíqua, sistemas educacionais. A seguir será apresentado alguns trabalhos relacionados a consciência de situação.

- ***Enhanced Situational Awareness: Application of DDDAS Concepts to Emergency and Disaster Management*** [22]: Descreve um protótipo de um sistema de informações de emergência e desastres que utiliza conceitos da consciência de situação. O sistema é projetado para usar em tempo real o celular para buscar dados da região geográfica, incluindo a atividade da chamada, duração da chamada, os serviços em uso, e informações de localização do telefone. Com esses recursos utilizados se torna possível o fornecimento da consciência situacional aprimorada para os gestores de centros de operações de emergência.

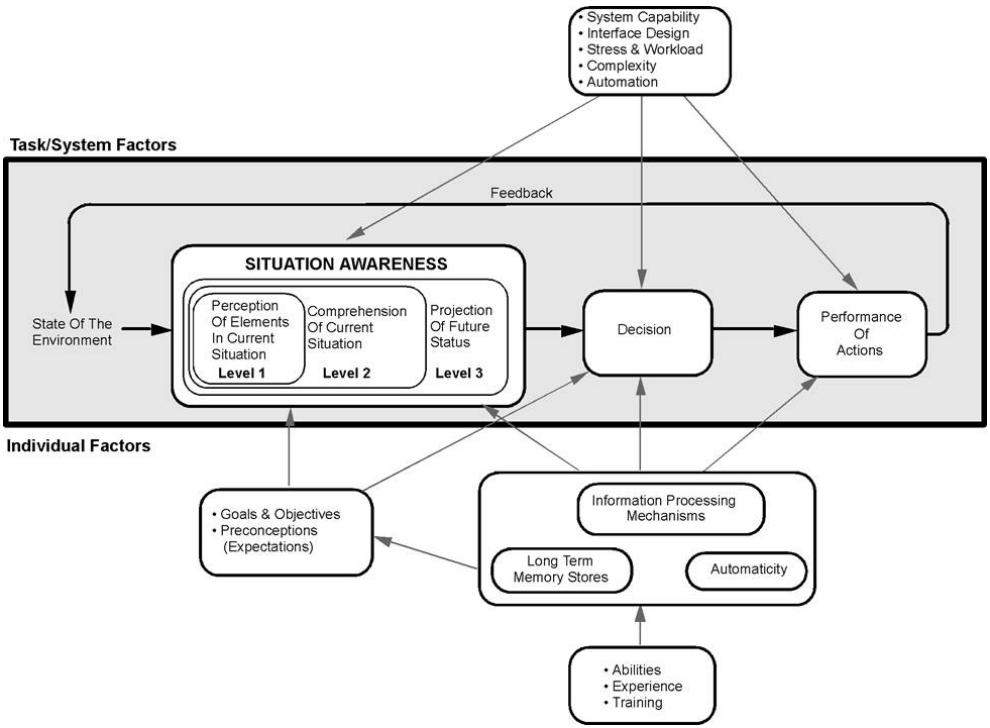

Figura 6. Modelo de Endsley

- ***A Situation-Aware Cross-Platform Architecture for Ubiquitous Game*** [23]: Apresenta um jogo multi-plataforma que deverá fornecer um serviço consistente a qualquer hora e em qualquer lugar, usando quaisquer dispositivos e redes disponíveis, devido a estas caraterísticas pode ser considerado um jogo ubíquo. Na concepção de um jogo ubíquo, é importante notar que vários dispositivos podem entrar em conflito na utilização de um único serviço, sendo assim este serviço deve ser operado de forma inteligente. A fim de resolver o conflito entre vários dispositivos, e de oferecer o melhor ambiente para o jogador do jogo, o trabalho propõe uma arquitetura para jogos on-line *multi-player* utilizando um middleware de consciência de situação para detectar a mudança de localização de um jogador provendo a mobilidade entre plataformas heterogêneas.

- **Sensibilidade à Situação em Sistemas Educacionais na Web** [2]: Apresenta uma solução para o problema da adaptação de ações sensíveis às situações

vivenciadas por alunos em um sistema de educação adaptativo baseado na Web. Para este fim, foi desenvolvida uma solução capaz de auxiliar o funcionamento de sistemas de educação adaptativos, de forma a apresentarem caráter reativo à situação vivenciada pelo aluno. A solução desenvolvida consiste de um módulo de sensibilidade à situação, construído com o objetivo de analisar as diversas particularidades existentes no cotidiano atual do aluno, se mantendo útil a ele independentemente do seu local atual, do dispositivo computacional utilizado e da tarefa em curso, respeitando as características individuais do aluno. De acordo com a situação detectada, ações de adaptação são fornecidas à mídia adaptativa, com intuito de prover uma experiência educacional voltada às necessidades reais do aluno

3 Estudo de Caso - Consciência de Situação aplicada à Segurança de Sistemas de Informação

Neste capítulo será apresentada um estudo de caso voltado à utilização de Consciência de Situação na área de Segurança da Informação, mais precisamente na tarefa de análise de log. A intenção desta análise é identificar possíveis situações que ocorrem no sistema ubíquo e que podem ser identificadas nos arquivos de log sem precisar da intervenção de um humano e assim facilitando esta tarefa. Através destas situações identificadas, é possível a tomada de ações como envio de e-mail para o responsável pela rede ou até bloquear um determinado IP que está atacando um respectivo servidor.

A identificação das situações é realizada através do processamento de eventos, onde os eventos registrados nos diferentes arquivos de log dos sistemas computacionais são correlacionados a fim de se identificar alguma situação de interesse, como por exemplo, uma falha em algum dispositivo, ou um possível ataque à rede. Também pretende-se correlacionar eventos provenientes de diferentes dispositivos, fornecendo uma visão mais aprimorada do ambiente.

Para implementar esta funcionalidade de Consciência de Situação na análise de log é necessário implementar um sistema de gerenciamento de log. Um sistema de gerenciamento de log precisa possuir algumas atividades básicas como as tarefas de análise léxica, análise sobre eventos de log, transmissão, visualização. Para realizar estas atividades serão implementadas duas arquiteturas sendo uma o servidor central, que armazenará os registros de log de vários servidores e dispositivos, e a outra o servidor cliente que estará presente em todos os servidores. Os dispositivos computacionais que possuírem restrições em relação a instalação do servidor cliente, poderão enviar os registros de log para um servidor que esteja com a arquitetura do servidor

cliente em funcionamento.

Visto que o estudo de caso da solução proposta será um ambiente ubíquo, através da figura 7 é demonstrada a arquitetura deste ambiente, onde é possível identificar os Servidores de Contexto (SC), e os Servidores de Borda (SB). Como pode-se perceber, há uma grande heterogeneidade, e uma infraestrutura de rede complexa para comunicação, o que aumenta os desafios da segurança da informação, justificando assim o porque de se utilizar este ambiente como estudo de caso para a solução.

A seguir, serão detalhados as diferentes arquiteturas com seus respectivos módulos.

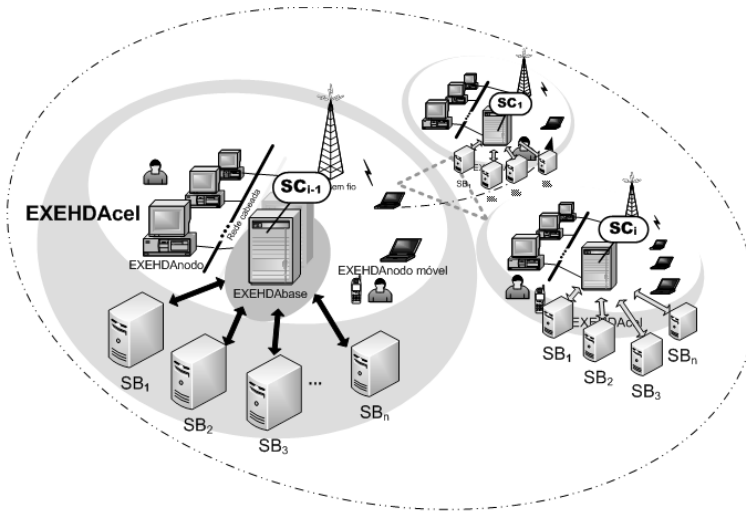

Figura 7. Ambiente Ubíquo

3.1 Servidor Central

A figura 8 apresenta a arquitetura do servidor central, mostrando seus respectivos módulos. A seguir será explicado cada um destes módulos.

3.1.1 Comunicação com o Cliente Módulo responsável pela comunicação com o servidor cliente recebendo os registros de log coletados por cada cliente, e enviando as informações necessárias para execução do cliente.

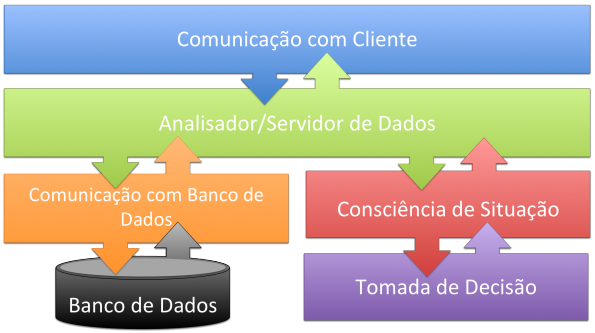

Figura 8. Arquitetura servidor central

3.1.2 Analisador/Servidor de Dados Módulo responsável por analisar os dados recebidos verificando se eles estão no formato correto, por exemplo, analisando a sintaxe SQL. Se os dados estiverem corretos eles são repassados para o módulo de Consciência de Situação, se por acaso eles conterem algum erro eles são repassados para o módulo de Comunicação com o Cliente enviando o erro que foi encontrado.

3.1.3 Consciência de Situação Módulo responsável por identificar possíveis situações em que se encontram o servidor, para realizar esta tarefa se utilizará das técnicas de correlação de eventos. Dentre as possíveis abordagens, foi selecionada a correlação baseada em regras aplicada ao fluxo de dados presente na memória, onde o conhecimento geral sobre determinada área é mapeado para um conjunto de regras.

As ferramentas baseadas em regras devem possuir um mecanismo de comparação que confronta os eventos presentes com o conjuntos de regras criados, sendo assim, ele deve possuir uma estratégia de controle que determina em que ordem as regras serão aplicadas. Dessa forma, caso um conjunto de eventos esteja representado por uma regra, o mecanismo deverá perceber está situação e realizar uma ação, seja a transformação deste evento (conforme discutido nos tipos de correlação) ou até mesmo uma ação efetiva no sistema, em alguns sistemas está ação pode ser explicitada na regra.

Conforme discutido no capítulo de revisão conceitual, destaca-se como vantagens a sua simplicidade, modularidade e fácil manutenção quando comparado aos programas tradicionais que possuem em seu código tanto o conhecimento especializado quanto as informações de controle. No entanto, como desvantagens encontradas na literatura estão: o conhecimento baseado em entrevistas com especialistas humanos; não aproveitamento de experiências passadas; sujeitos a repetição de erros; não

lida com situações não presentes nas regras.

Este módulo irá correlacionar eventos de diferentes servidores afim de tentar encontrar situações que estejam acontecendo em mais de um servidor do mesmo ambiente, por exemplo, um determinado IP que está atacando vários servidores do ambiente em questão.

3.1.4 Tomada de Decisões Este módulo será responsável pela tomada de decisões a partir das situações identificadas pelo módulo de Consciência de Situação, essas decisões poderão ser enviar um e-mail ou um SMS para o administrador da rede informando a situação que se encontra e identificando que ação pode ser tomada para resolução do problema, ou ainda dependendo da situação identificada este módulo pode tomar uma ação para resolução do problema e avisar o administrador da rede que teve que tomar a respectiva ação por causa da determinada situação. Este módulo poderá determinar decisões em qualquer outro servidor que esteja lhe enviando os registros de log, já que ele vai conseguir ter uma visão mais global do que está acontecendo no ambiente e assim poderá tomar uma decisão de forma a solucionar a situação que foi identificada.

3.1.5 Comunicação com o Banco de Dados Módulo responsável pela comunicação com o banco de dados onde serão armazenados os registros de log coletados, e este módulo também será responsável por buscar os itens que devem ser monitorados pelo protótipo.

3.2 Servidor Cliente

A figura 9 apresenta a arquitetura dos servidores clientes, mostrando seus respectivos módulos. A seguir será explicado cada um destes módulos.

3.2.1 Coletor de Logs O protótipo possui dois módulos de coleta de log, o interno que monitora os arquivos de log esperando registros de log serem escritos no arquivo, e o externo que funciona como um servidor e fica esperando os registros de log serem enviados para ele pela rede através do protocolo syslog, mecanismo padrão para logging em sistemas de computadores definido na RFC5424 (RFC - *Request for Comments* é um documento que descreve os padrões de cada protocolo da Internetinformações). Maiores informações a respeito do syslog podem ser encontradas em [24].

3.2.2 Coletor de Status Realiza a coleta de dados referente ao status do servidor como por exemplo a percentagem de uso de memória, de disco, que são úteis para verificar o comportamento do servidor, e também coletará dados como de rede, o

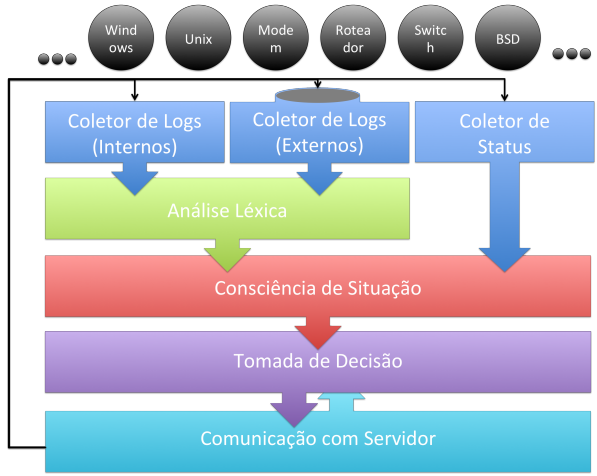

Figura 9. Arquitetura cliente

checksum que pode ser muito útil para a segurança já que com ele podemos verificar se um arquivo foi alterado ou corrompido, por exemplo, poderia detectar a adição de um usuário em sistemas Linux, pois esta adição realiza uma modificação no arquivo /etc/passwd, e pode ser interessante para o administrador da rede ter este controle, por que um invasor possivelmente irá querer criar um usuário por diversas razões, e com este controle essa adição de usuário poderá ser identificada.

3.2.3 Análise léxica Responsável pela tarefa de pré-processamento dos registros de log separando-os em campos, formatando os dados num formato pré-definido, adicionando informações contextualizadas a respeito dos dados, e eliminando campos que não são interessantes para serem analisados neste projeto. Para realizar essa tarefa foi desenvolvido uma gramática para cada tipo de formato de log, onde se define os formatos que são esperados e através desse recurso foi implementado a separação dos registros de log em campos pré-definidos.

3.2.4 Consciência de Situação Utilizará as mesmas técnicas utilizadas pelo módulo de Consciência de Situação do servidor central, só que neste módulo a correlação vai ser entre arquivos diferentes de log e ainda dentre os registros de log de um mesmo arquivo, pois muitas vezes a partir de uma análise separada de um registro não se consegue identificar o problema que está ocorrendo e realizando esta correlação esta tarefa se tornará mais fácil.

3.2.5 Tomada de Decisões Este módulo será bem parecido com o módulo de Tomada de Decisões do servidor central, mas ele somente tomará decisões referentes ao próprio servidor, será uma decisão local.

3.2.6 Comunicação com o Servidor Módulo responsável pela comunicação com o servidor central onde serão armazenados os registros de log coletados em um banco de dados, e este módulo também será responsável por buscar os itens que devem ser monitorados pelo protótipo no banco de dados armazenado no servidor.

4 Considerações Finais

O presente trabalho teve como objetivo apresentar um estudo a respeito dos principais conceitos relevantes à Consciência de Situação, tendo como foco sua aplicação aos Sistemas Computacionais Ubiquos. Uma das principais vantagens obtida pelo uso de sistemas conscientes à situação é o auxílio na compreensão da realidade, sendo possível uma visão aprimorada do ambiente em análise e a adaptação de sistemas computacionais. Através dos exemplos de aplicações já desenvolvidas foi possível perceber a sua utilidade à diversas áreas, incluindo a ciência da computação, utilizando-se dos exemplos aplicados no estudo de caso desenvolvido, demonstrando assim que a consciência situacional pode ser uma grande aliada da segurança da informação.

Como desafios da área destaca-se a coleta de dados de diferentes fontes assim como os desafios inerentes ao ambiente de aplicação, a contextualização dos dados, assim como o processo de geração de conhecimento. Alguns fatores críticos a se observar estão o segurança da informação durante todo o processo de coleta dos dados até a identificação de uma situação, e o desempenho e tempo de resposta principalmente nos que tange a correlação de eventos, sendo esta uma forma de inferência de situações.

Referências

[1] C. A. Costa, A. C. Yamin, and C. F. R. Geyer. Toward a general software infrastructure for ubiquitous computing. *IEEE Pervasive Computing*, 7:64?73, 2008.

[2] A. M. F. Pernas. *Sensibilidade à Situação em Sistemas Educacionais na Web*. Tese de doutorado em ciência da computação, Instituto de Informática-UFRGS, Porto Alegre-RS, 2012.

[3] M. R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37:32?64, 1995.

[4] D.M. Gaba, S.K. Howard, and S.D. Small. Situation awareness in anesthesiology. *Human Factors*, 37:20–31, 1995.

[5] S.G. Collier and K. Follesf. Sacri: A measure of situation awareness for nuclear power plant control rooms. In *International Conference: Experimental Analysis and Measurement of Situation Awareness, Daytona Beach, FL.*, page 115?122, 1995.

[6] C.A. Bolstad. Age-related factors affecting the perception of essential information during risky driving situations. In *Human Performance Situation Awareness and Automation: User-Centered Design for the New Millennium Conference, Savannah, GA.*, 2000.

[7] R.L. Sollenberger and E.S. Stein. A simulation study of air traffic controllers' situation awareness. In *International Conference: Experimental Analysis and Measurement of Situation Awareness, Daytona Beach, FL.*, page 211?217, 1995.

[8] E. et al. Henriqson. Consciência situacional, tomada de decisão e modos de controle cognitivo em ambientes complexos. *Universidade Federal do Rio Grande do Sul*, 19:433–444, 2009.

[9] L. M. Donato. Uma metodologia de forense computacional apoiada por profiling psicológico. Monografia de graduação em ciência da computação, Instituto de Física e Matemática/UFPel, Pelotas-RS, 2004.

[10] M. Langheinrich. *Privacy in Ubiquitous Computing*, pages 95–160. J. Krumm, ed., CRC Press, 2010.

[11] A. Bouzeghoub, K. N. Do, and C. Lecocq. A situation-based delivery of learning resources in pervasive learning. In *Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg*, 2007.

[12] Opher Etzion and Peter Niblett. *Event Processing in Action*. Manning Publications Co., Greenwich, CT, USA, 1st edition, 2010.

[13] MITRE Coporation. Common event expression: Architecture overview.

[14] A. K. Dey. Understanding and using context. *Personal and Ubiquitous Computing*, 5:4–7, 2001.

[15] P. Brézillon. Context in problem solving: a survey. *Knowl. Eng. Rev.*, 14(1):47–80, May 1999.

[16] P. Brézillon and R. M. Araujo. Reinforcing shared context to improve collaboration. *Revue d Intelligence Artificielle*, 19(3):537–556, 2005.

[17] P. Bellavista, A. Corradi, M. Fanelli, and L. Foschini. A survey of context data distribution for mobile ubiquitous systems. *ACM Comput. Surv.*, 44(4):24:1–24:45, September 2012.

[18] M. R. S. Borges, P. Brezillon, J. A. Pino, and J. C. Pomerol. Bringing context to cscw. In *Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference on*, volume 2, pages 161 – 166 Vol.2, may 2004.

[19] M. R. Endsley. Measurement of situation awareness in dynamic systems. *Human Factors*, 37:65?84, 1995.

[20] H. Artman. Team situation assessment and information distribution. *Ergonomics*, 43:1111?1128, 2000.

[21] Ann Blandford and B. L. William Wong. Situation awareness in emergency medical dispatch. *Int. J. Hum.-Comput. Stud.*, 61(4):421–452, October 2004.

[22] GregoryR. Madey, Albert-László Barabási, NiteshV. Chawla, Marta Gonzalez, David Hachen, Brett Lantz, Alec Pawling, Timothy Schoenharl, Gábor Szabó, Pu Wang, and Ping Yan. Enhanced situational awareness: Application of dddas concepts to emergency and disaster management. In Yong Shi, GeertDick Albada, Jack Dongarra, and PeterM.A. Sloot, editors, *Computational Science ICCS 2007*, volume 4487 of *Lecture Notes in Computer Science*, pages 1090–1097. Springer Berlin Heidelberg, 2007.

[23] J. H. Han, D. H. Lee, H. Kim, H. P. In, H. S. Chae, and Y. I. Eom. A situation-aware cross-platform architecture for ubiquitous game. *Computers and Artificial Intelligence*, 28(5):619–633, 2009.

[24] Syslog. http://www.syslog.org. Março 01, 2013.