ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO

Departamento de Engenharia da Computação e Sistemas Digitais

MARIA INES LOPES BROSSO

Autenticação Contínua de Usuários em Redes de Computadores

São Paulo

2006

MARIA INES LOPES BROSSO

Autenticação Contínua de Usuários em Redes de Computadores

Tese apresentada à Escola
Politécnica da Universidade de
São Paulo para obtenção do
Título de Doutor em Engenharia

Área de Concentração:
Sistemas Digitais
Orientador:
Profa. Dra. Graça Bressan

São Paulo

2006

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 05 de Junho de 2006.

_____
Maria Ines Lopes Brosso
Autora

_____
Profa. Dra. Graça Bressan
Orientadora

FICHA CATALOGRÁFICA

Brosso, Maria Inês Lopes
Autenticação contínua de usuários em redes de computadores / M.I.L. Brosso. -- São Paulo, 2006.
156 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1.Redes de computadores (Segurança) I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II.t.

FOLHA DE APROVAÇÃO

Maria Ines Lopes Brosso
Autenticação Contínua de Usuários em Redes de Computadores

Tese apresentada à Escola
Politécnica da Universidade de
São Paulo para obtenção do
Título de Doutor em Engenharia.

Área de Concentração:
Sistemas Digitais

Aprovado em: 05 de Maio de 2006.

Banca Examinadora

_____

Profa. Dra. Graça Bressan
Instituição: Escola Politécnica da Universidade de São Paulo

_____

Prof. Dr. Demi Getschko
Instituição: Pontifícia Universidade Católica de São Paulo

_____

Prof. Dr. Antonio Carlos Ruggiero
Instituição: Instituto de Física e Informática da Universidade de São Paulo/São Carlos

_____

Prof. Dr. Wilson Vicente Ruggiero
Instituição: Escola Politécnica da Universidade de São Paulo

_____

Profa. Dra. Tereza Cristina de Melo Brito Carvalho
Instituição: Escola Politécnica da Universidade de São Paulo

À
minha família.

AGRADECIMENTOS

Ao concluir este trabalho tenho muito a agradecer a todas as pessoas que o compartilharam comigo neste período tão importante da minha vida:

À minha orientadora, Profa. Dra. Graça Bressan, agradeço pelos ensinamentos, pela amizade, pela dedicação em me orientar, pela disponibilidade de horários para me atender, pelas críticas e por me inserir em suas pesquisas.

Aos meus professores e todos os amigos do Laboratório de Arquitetura e Redes de Computadores da Universidade de São Paulo, agradeço pelo apoio; faço um agradecimento especial ao Prof. Dr.Wilson Vicente Ruggiero pelos ensinamentos e sugestões e à Ana Maria Coracini C. P. Novaes pela ajuda.

À Profa. Dra. Geraldina Porto Witter da Faculdade de Psicologia da Universidade de São Paulo, agradeço pelos esclarecimentos sobre a psicologia comportamental.

Aos meus alunos Humberto Sandmann, Wanderlei Rosa, Cláudio Silva, Daniel Sonego, Francis Koji Yonemura, Jonas Alves Neiva e Silva, Renato Lucena, Luis Campos de Carvalho, Aaron Rodrigues, Claudia Juscelino e Amanda Catarina do Curso de Ciência da Computação do Centro Universitário da FEI, agradeço por terem utilizado as minhas pesquisas em seus Trabalhos de Conclusão de Curso.

Agradeço o incentivo dos meus amigos do Centro Universitário da FEI, especialmente do Prof. Dr. Flávio Tonidandel, Prof. Dr. Alessandro La Neve, Profa. Dra. Sonia Schuetze e Profa.Msc.Marli Pirozelli.

Aos meus amigos do Banco Bradesco S.A agradeço pela confiança.

Agradeço o incentivo, desde o mestrado, do meu primeiro orientador Prof. Dr. Marcio Rillo; dele lembro-me dos ensinamentos do passado e que foram úteis neste projeto, dentre eles a preocupação de se dar condições para fazer pesquisa, arrumar tempo para uma atividade longa e criteriosa, escrever, publicar, participar em eventos e ensinar.

Agradeço à minha família pelo carinho.

E, sobretudo, agradeço a Deus, por me permitir iniciar e levar a termo este trabalho, e pelas pessoas que Ele colocou em minha vida para que isto fosse possível.

RESUMO

A Computação Ciente de Contexto permite a obtenção e utilização de informações de contexto adquiridas de dispositivos computacionais no ambiente, com o objetivo de prover serviços; esta dinâmica aliada à evolução das redes de computadores vem provocando profundas modificações nos aspectos sociais e comportamentais das pessoas, uma vez que gradativamente têm necessidade de viverem imersas na tecnologia e integradas ao ambiente, com transparência e mobilidade, e de tal forma que as aplicações de *software* se adaptam ao comportamento das pessoas e nas informações de contexto capturadas do ambiente. Um dos desafios desta interação ser humano – ambiente – tecnologia – ubiqüidade é garantir a segurança. Como principal inovação e contribuição, esta tese propõe um mecanismo de autenticação contínua de usuários que faz uso de informações de contexto do ambiente, da análise do comportamento do usuário, da biometria facial, das teorias comportamentais de Skinner e da Confiança Matemática da Teoria das Evidências de Dempster-Shafer, para compor uma política de segurança adaptativa e um Sistema de Autenticação Contínua de Usuários Conhecidos - KUCAS (*Known User Continuous Authentication System*), que estabelece níveis de confiança para autenticar o usuário através da análise do comportamento dele em um ambiente ou domínio específico nas redes de computadores, num determinado período de tempo. A dinâmica de gerenciamento incluso nesse sistema compara o comportamento atual com o histórico de comportamentos anteriores do usuário e com as restrições de atribuição de confiança; caso haja indícios de mudanças no comportamento do usuário, aciona por meio de sensores, a Tecnologia de Reconhecimento Facial Tridimensional (3D), que captura a imagem da face do usuário, validando-a e armazenando-a nos bancos de dados de imagens; havendo incertezas e divergências, mecanismos de segurança e sinais de alerta são acionados. O Sistema KUCAS proposto possui uma infra-estrutura de um *framework* F-KUCAS, um Módulo de Segurança S-KUCAS e um Algoritmo de Autenticação A-KUCAS.

Palavras-Chave: Redes de Computadores (Segurança), Processos de Autenticação, Comportamento Humano, Confiança, Biometria, Computação Ciente de Contexto.

ABSTRACT

Context-aware Computing allows to obtain and use context informations acquired through devices in the environment, with the goal to provide services. This dynamics, allied to the computer networks evolution, has been provoking deep modifications in peoples social and behavior aspects, seeing that they have the necessity to live immersed in technology and integrated with the environment, with transparency and mobility, anywhere, anytime, so that the software applications adapt themselves to the persons behavior, based on the context information captured through the environment. One of the challenges of this human – environment - technology – ubiquity interaction is to provide security. As main innovation and contribution, this thesis presents an authentication mechanism of users which makes use of environmental context information, users behavior analysis, the face recognition technology, the behavior theories of Skinner and the Mathematical Confidence of the Theory of the Evidences of Dempster-Shafer, to compose an adaptative security policy and the Known User Continuous Authentication System (KUCAS) that establishes trust levels to authenticate the user by his behavior analysis in a specific domain of the computer networks, in a period of time. The dynamics of enclosed management in this system compares the current behavior with the users previous behaviors description and with the trust restrictions. In case of indications of changes in the users behavior, the 3D Technology Face Recognition is set in motion by sensors, which capture the image of the users face, validating it and storing it in the data bases of images. If there are uncertainties and divergences, mechanisms of security and signals of alert are set in motion. The KUCAS System has an infrastructure of one framework F-KUCAS, a Security Module S-KUCAS and an Algorithm of Authentication A-KUCAS.

Keywords: Networks Computers (Security), Authentication Process, Human Behavior, Trust, Context-aware Computing.

SUMÁRIO

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas e siglas

BLUETOOTH	Protocolo de comunicação sem fio
BRIDGES	Equipamento que faz ligação entre computadores
CHAT	Salas de bate-papo na web
CONTADOR DE TEMPO	Relógio interno do sistema
CSCW	Computer Supported Collaborative Work
GIS	Geographic Information System
GPS	Software de coordenadas de localização geográfica
HARDWARE	Computador ou dispositivo
IP	Internet Protocol
Log	Registra atividades geradas por aplicações software
Login	Identificação inicial de um usuário
Logout	Identificação final do usuário
MMS	Multimedia Messaging Service
NSP	Network Service Provider
OS	Operating System
PIM	Personal Information Management
PLUG-AND-PLAY	Componente que pode compor Interfaces Padronizadas.
PTT	Postal, Telegraph And Telephone
Redes ad hoc	Redes de computadores sem fio e sem topologia fixa
SIP	Session Initiation Protocol
SMS	Short Message Service
Software	Aplicações que se executam em computadores
TCP	Transfer Control Protocol
TFA	Taxa Falsa Aceitação
TFR	Taxa Falsa Rejeição
UCE	Unsolicited Commerce Email
UDP	Protocolo de comunicação
UML	Unified Modeling Language
VOIP	Voice Over Ip
WAP	Wireless Application Protocol
WAN	Wireless Area Network
WAG	Wireless Application Gateways
WCDMA	Wideband Code Division Multiple Access
WiFi	Padrão de comunicação em redes sem fio
WIRELESS	Rede Sem Fio
WIRED	Rede Com Fio, Cabeada
WNP	Wireless Number Portability
WORKFLOW	Processo de fluxo de trabalho
WPAN	Wireless Personal Area Network
W3C	World Wide Web Consortium
3D	Imagens em Movimento em Espaço Tridimensional
3G/B3G	Terceira geração da tecnologia de telefonia celular
3GPP	Third Generation Partnership Project
4G	Quarta geração da tecnologia

1 Introdução

1.1 Introdução

A identificação e autenticação de pessoas é requisito fundamental de segurança em qualquer sistema automatizado em redes de computadores.

A identificação do usuário é feita através de um código de usuário e a autenticação e feita através de sua senha.

A autenticação contínua deve ser um processo que verifica se o usuário que se identificou no início de uma aplicação de software, ainda está apto a continuar no sistema, sem interferências humanas ou paralisações do processo.

Como principal inovação e contribuição, esta tese propõe uma política de segurança adaptativa através de um mecanismo de autenticação contínua de usuários que faz uso de informações de contexto do ambiente, da análise do comportamento do usuário, da tecnologia de reconhecimento facial, das teorias comportamentais de Skinner e da Confiança Matemática da Teoria das Evidências de Dempster-Shafer, para compor um Sistema de Autenticação Contínua de Usuários Conhecidos – KUCAS (*Known User Continuous Authentication System*), que estabelece níveis de confiança para autenticar o usuário através da análise do comportamento dele em um ambiente ou domínio específico nas redes de computadores, num determinado período de tempo.

A dinâmica de gerenciamento incluso nesse sistema compara o comportamento atual com o histórico de comportamentos anteriores do usuário e com as restrições de atribuição de confiança; caso haja indícios de mudanças no comportamento do usuário, aciona por meio de sensores, a Tecnologia de Reconhecimento Facial Tridimensional (3D), que captura a imagem da face do usuário, validando-a e armazenando-a nos bancos de dados de imagens; havendo

incertezas e divergências, mecanismos de segurança e sinais de alerta são acionados. O Sistema KUCAS proposto possui uma infra-estrutura de um *framework* F-KUCAS, um Módulo de Segurança S-KUCAS e um Algoritmo de Autenticação A-KUCAS.

O sistema KUCAS propõe a autenticação contínua de usuários no intervalo de tempo em que uma aplicação de software está ativa, ele verifica se o usuário que já tenha sido autenticado inicialmente, ainda está apto a continuar no sistema, de acordo com o nível de confiança que ele adquire; e para isto faz uma análise do comportamento e confiança atribuída para verificar se continua autenticando ou não, o usuário.

Como a confiança é dinâmica, diante das variações no comportamento da pessoa, o nível de confiança no sistema irá variar. Se diminuir a confiança do sistema no usuário, seus direitos de acesso podem ser alterados ou revogados. Um usuário já autenticado no sistema poderá ser excluído do sistema caso sua confiança caia a níveis inaceitáveis.

E com isto é possível estabelecer uma política de segurança maleável e adaptativa ao usuário, de acordo com a variação da confiança e das informações de contexto do ambiente.

Este trabalho baseia-se na confiança, no ambiente tecnológico, nas pessoas e suas características biométricas e comportamentais.

1.2 Motivação

A motivação para este trabalho são as necessidades de uma política de segurança adaptativa em autenticação de usuários.

A autora do presente trabalho tem desenvolvido, ao longo de sua vida profissional, inúmeros projetos na área de desenvolvimento de sistemas computacionais nos mais diferentes segmentos corporativos. Com a evolução das redes de computadores, da tecnologia de reconhecimento facial, bem como o emprego da confiança como critério de segurança e o barateamento das tecnologias, as empresas são levadas a investir em soluções e infra-estrutura

que proporcionem aos seus usuários acesso a produtos e serviços; portanto a questão da segurança no acesso às informações tornou-se mais relevante ainda. Nos projetos desenvolvidos fez uso de várias tecnologias e metodologias como: tecnologia de reconhecimento facial, *workflow*, arquitetura de sistemas, desenvolvimento de *framework* para segurança, entre outros, e percebeu a importância da criação de um sistema complexo de autenticação contínua que viesse contemplar grande parte das necessidades de segurança em redes de computadores com e sem fio.

Uma outra motivação para este projeto é que a Computação Ciente de Contexto (Computing aware-context) define dimensões contextuais, as quais são parâmetros disponibilizados pelos equipamentos e permitem obter informações dos mesmos, do ambiente e do usuário; a partir de sua captura e análise possibilitam a elaboração da análise comportamental de usuários.

1.3 Objetivo

O objetivo desta tese é definir um mecanismo de autenticação contínua de usuários nas redes de computadores baseando-se na análise comportamental do usuário, nas dimensões contextuais da Computação Ciente de Contexto, na biometria e na confiança matemática da Teoria das Evidências de Dempster-Shafer. A confiança não é só a dicotomia de confiar ou não confiar, a confiança é dimensional, pode-se dimensionar o quanto se confia. E assim, o mecanismo de autenticação analisa o comportamento do usuário e, aumenta ou diminui a confiança no mesmo; quando ocorre uma mudança no comportamento do usuário, o mecanismo cria restrições de confiança geradas pelo próprio usuário, definindo uma política de segurança adaptativa para cada usuário, autenticando-o ou revogando o acesso.

1.4 Justificativa

Uma justificativa para esta tese é que política de segurança não pode ser rígida e estática, mas sim, deve ser adaptativa, maleável e facilitar a autenticação de usuários em aplicações de *software* nas redes de computadores com e sem fio. Isto é cada vez mais importante, pois à medida que a tecnologia evolui, os sistemas ficam cada vez mais distribuídos e surgem mais vulnerabilidades na segurança.

Em geral, as autenticações são feitas no início de uma sessão; mas em transações longas e encadeadas, nas redes de computadores, é importante uma autenticação contínua, mas sem interferências humanas ou paralisações do processo.

A justificativa para utilizar a biometria facial, em especial, a Tecnologia de Reconhecimento Facial, é que os aspectos biométricos de uma pessoa são associados ao comportamento e características físicas da mesma, o que permite a análise comportamental, uma vez que, o comportamento de uma pessoa pode ser observado e analisado utilizando mecanismo de análise comportamental em qualquer ambiente.

Uma justificativa para o desenvolvimento de um sistema de autenticação foi o desenvolvimento do projeto "Bastet" (SANDAMANN et al., 2002) de controle de acesso e autenticação de pessoas por meio da tecnologia de reconhecimento facial, do qual a autora participou, atuando como orientadora de projeto e implementando-o no laboratório do Centro Universitário da FEI em 2002, o qual apesar de satisfatório, apresentou uma série de problemas no reconhecimento, e na autenticação, em geral, causados pela qualidade das imagens, luminosidade do ambiente e erros na calibração e treino do algoritmo.

Uma outra justificativa foi o acompanhamento da implantação de uma solução de reconhecimento facial no andar térreo do *shopping* Rio Sul, no Rio de Janeiro, no final de 2004 e começo de 2005; a grande quantidade de pessoas que foram cadastradas gerou uma incidência muito grande de falsos positivos e negativos, o qual gerou o aumento crescente das

bases de dados e problemas com o tráfego de imagens na rede, além da percepção da mudança do comportamento das pessoas perante uma tecnologia desconhecida, pois elas sentem que a privacidade é invadida; isto motivou a um estudo sobre a análise comportamental, pois foi constatado que diante do medo e da insegurança, o usuário não confia e não colabora com a tecnologia, ele se esquiva dificultando a captura das imagens da face, fazendo caretas e tornando o processo lento; também foi feito um estudo de como controlar as informações obtidas em situações com volume grande de dados e a melhor maneira de limpeza das bases de dados.

Com as experiências obtidas nestes projetos e analisando este contexto, foi idealizado um sistema de autenticação contínua que utiliza reconhecimento facial, análise comportamental e Confiança Matemática, para definir com algum grau de confiança a autenticação de um usuário. A análise das informações geradas pela tecnologia de reconhecimento facial e as informações comportamentais podem definir o nível de confiança que o sistema terá no usuário, inclusive validando sua própria identidade e autenticando-o.

1.5 Revisão Bibliográfica

Para atender as necessidades de desenvolvimento do mecanismo de autenticação contínua de usuários e por conseqüência do sistema KUCAS foi feita uma revisão bibliográfica na área de Computação Ciente de Contexto, na área da biometria, em particular, da tecnologia do reconhecimento facial e da análise comportamental; na área de segurança, visando a autenticação de usuários e o controle de acesso e segurança; e foram pesquisados trabalhos que utilizam a confiança como requisito de segurança. Alguns destes trabalhos norteiam esta tese e estão citados a seguir:

1.5.1 Computação Ciente de Contexto

A Computação Ciente de Contexto é um paradigma da computação, onde os equipamentos e dispositivos capturam as informações de contexto do ambiente e do usuário com o objetivo de disponibilizar serviços. (GOULARTE, 2003).

Trabalhos relevantes na área enfatizam a necessidade de entender e auxiliar as práticas cotidianas das pessoas e estudar o ambiente através do fornecimento de dispositivos heterogêneos que ofereçam diferentes formas de interação.

Segundo Abowd et al. (2002) a computação ciente de contexto permite gerenciar dispositivos em rede, de forma a fornecer ao usuário uma experiência holística com mobilidade e transparência.

No trabalho de Want et al. (1992) é citado, o projeto *Active Badge* do *Olivetti Research Lab's,* na área de Computação Ciente de Contexto, onde a localização e o rastreamento de pessoas é proposto utilizando crachás especiais e sensores espalhados pelo ambiente.

Schilit e Theimer (1994) definem contexto como a indicação da localização e a identificação de pessoas e objetos ao redor, situações sociais e condições ambientais como iluminação e barulho. Os autores apontam três aspectos importantes de contexto: onde o usuário está, com quem o usuário está e quais os recursos próximos do usuário.

Já Dey e Abowd (1999) afirmam que contexto é tudo o que envolve uma situação relevante para uma aplicação de software e seus usuários, pois mudaram de uma situação para outra situação, levando-se em conta se uma informação pode ser usada para caracterizar uma situação de interação, então esta informação é de contexto.

Salber *et al*. (1999) definem contexto como informações sobre pessoas ou dispositivos que podem ser usados para transformar o modo como um sistema fornece serviços,

considerando os dados emocionais, dados históricos, dados de localização, dados de interação e de foco de atenção do usuário.

Em Schilit, Theimer, (1994) é discutida a utilização da escrita manual como meio de interação com o meio e os equipamentos; e no trabalho realizado por Ishii e Ullmer (1997) objetos do mundo físico são utilizados para manipular artefatos eletrônicos, criando o conceito de interfaces tangíveis que se comunicam com o ambiente.

Nos últimos anos surgiram vários projetos de pesquisas baseados em Computação Ciente de Contexto, entre eles estão o *Georgia Tech* (DEY, ABOWD, 1999), o projeto *Ninja* (CZERWINISKI, 1999) e o projeto *Centaurus* (KAGAL, 2001). Dois projetos brasileiros se destacam na área de computação ciente de contexto, um é o *Context Kernel* (ARRUDA JUNIOR et al., 2003) desenvolvido no ICMC-USP que desenvolveu um serviço Web para armazenamento e recuperação de informações de contexto e outro descrito em Goularte et al. (2003) que apresenta uma metodologia para personalização e adaptação de conteúdo baseado em contexto para TV Digital Interativa.

Em Paula (2004) é apresentada uma metodologia de interpretação biométrica da forma como um usuário digita no teclado do computador.

Jones e Brown (2004) sugerem que contexto pode ser usado em equipamentos móveis para descrever o ambiente, pessoas ao redor do usuário, situação, estado, temperatura, entre outras.

Em Ryan e Cinotti (2005), contexto é descrito como localização, ambiente, identificação e tempo. Os autores apresentam pesquisas relevantes na área e incluem a utilização de sensores acoplados a dispositivos computacionais permitindo que a manipulação física das informações seja corretamente interpretada por aplicações de software.

Este trabalho a utiliza a Computação Ciente de Contexto, na captura das informações relevantes do usuário e dos dispositivos presentes no ambiente.

1.5.2 Biometria

1.5.2.1 Tecnologia de Reconhecimento Facial

A tecnologia de reconhecimento facial vem sendo utilizada em sistemas que efetuam identificação e autenticação de usuários, apesar do grau de incerteza, algoritmos novos surgiram nos últimos anos.

Diversos autores (PHILLIPS, RAUSS e DER, 1996), (PHILLIPS, WECHSLER, HUANG e RAUSS, 1998); (PHILLIPS, MARTIN, WILSON e PRZYBOCKI , 2000) retratam a evolução da tecnologia de reconhecimento facial desde os primórdios do desenvolvimento, os métodos existentes e avaliam o algoritmo de reconhecimento facial Face Recognition Technology (FERET), criado em 1998, no MIT/Estados Unidos, e conhecido por ser o conjunto de testes mais abrangente proposto para a tecnologia, apesar de terem sido consideradas bases de imagens estáticas.

A base de dados do FERET (PHILLIPS et. al, 1996, 2002) possui faces com variações de translação, escala e iluminação de modo consistente. Há imagens de pessoas obtidas de fotos tiradas em datas diferentes com diferença que chega até um ano. O maior teste do FERET foi baseado em imagens de 1196 pessoas diferentes. Nesse teste, os algoritmos citados acima possuem desempenho muito similar. Com imagens frontais adquiridas no mesmo dia, o desempenho daqueles algoritmos foi de mais de 95% de acerto. Para imagens obtidas com câmeras e iluminações diferentes, o desempenho foi entre 80 e 90%. Para imagens tomadas um ano depois, a taxa de reconhecimento típica foi de 50%. A diferença entre os algoritmos foi menor que 0.5%. Para testes com 200 pessoas, os três algoritmos praticamente não erraram. Entretanto, nesse experimento, mesmo um simples método de combinação por correlação pode, algumas vezes, propiciar o mesmo resultado, com a diferença de tratar-se de um método lento.

Heo et al. (2003) apresentam uma análise comparativa sobre a Tecnologia de Reconhecimento Facial atual e a tecnologia FERET (Face Recognition Technology), considerando as variações de iluminação, expressões faciais, idade, tamanho da cabeça de uma pessoa, pose e o tamanho da estrutura de banco de dados necessária para sua utilização.

O projeto *Informedia* da *Carnegie Mellon University* utiliza técnicas de reconhecimento de faces e legendas em vídeos de forma a estendê-los com metainformação contextual (WACTLAR, 2000).

Os trabalhos citados servem de base a este projeto, pois o mesmo utiliza a tecnologia de reconhecimento facial no mecanismo de autenticação contínua proposta.

1.5.2.2 Análise Comportamental de Pessoas

A Análise Comportamental de pessoas está baseada na psicologia comportamental que é um ramo científico da psicologia onde são estudadas as interações entre as emoções, pensamentos, comportamentos e estados fisiológicos. Alguns trabalhos relacionados são apenas embasamento teórico, mas foram considerados devido a natureza da informação.

Edward L. Thorndike foi o fundador dessa teoria, na qual todo comportamento de um organismo vivo tende a se repetir, se for recompensado assim que emitir o comportamento. Por outro lado, o comportamento tenderá a não acontecer, se o organismo for castigado após sua ocorrência. É a definição da LEI DO EFEITO (TODOROV, 1990).

Pela LEI DO EFEITO, o organismo irá associar as situações ocorridas com outras semelhantes, generalizando essa aprendizagem para o contexto maior da vida, ou seja, as pessoas tendem a repetir o comportamento em situações que se repetem, o que pode ser considerado no contexto de um sistema de autenticação de pessoas e nos aspectos de segurança, entre outras aplicações (WITTER, 2005).

Skinner (1967) foi um comportamentalista que influenciou e fundou o Behaviorismo, palavra originada do termo *behavior*, em inglês, que significa comportamento, e é uma das filosofias que embasam a análise experimental do comportamento humano.

Em Fawcett, Provost (1997) é apresentado um método que utiliza técnicas de *data mining* na detecção de fraudes e clonagem de celulares; baseado em informações de um grande banco de dados de transações de clientes, é possível verificar mudanças suspeitas no comportamento do usuário e que pode ser indicador de um comportamento fraudulento.

Este trabalho inova em relação aos citados ao propor uma política de segurança adaptativa baseado na análise comportamental de usuários nas redes de computadores.

1.5.3 Segurança

1.5.3.1 Autenticação

Na área de autenticação vários trabalhos relevantes surgiram nos últimos anos. Em Chen, Pearson, Vamvakas (2002) é apresentado um sistema de autenticação em ambiente distribuído que utiliza *Trusted Computing* e *Smart Cards.* Um sistema de autenticação e controle de acesso a instituições financeiras é descrito no relatório Técnico do *Federal Financial Institutions Examination Council*, que determina regras de controle de autenticação de novos clientes e de clientes existentes nas bases de dados de uma instituição financeira, no controle de acesso aos serviços de *e-banking ou* banco eletrônico (FEDERAL, 2001). Em Potter (2002) é explicada a evolução da verificação de assinatura digital em instituições financeiras como política de autenticação de clientes; e traz um compêndio sobre a evolução do sistema de pagamentos baseado em identificação por meio eletrônico e nas estratégias de autenticação baseada em computadores.

Este trabalho inova em relação aos citados por apresentar um mecanismo de autenticação que é a base da política de segurança adaptativa, proposta.

1.5.3.2 Controle de Acesso e Segurança

Em Szabó (2003) é abordado o gerenciamento de riscos na identificação de clientes em instituições financeiras, desde as questões da identificação, os aspectos legais, os tipos de métodos de identificação e autenticação utilizados e o estabelecimento de um sistema de central de identificação em vários níveis que permite reduzir os custos de administração.

Em Siau et al (2004) é apresentado um *framework* e um modelo de confiança contínua para o *mobile commerce* (*m-commerce*), onde é discutida a confiança do cliente no *m-commerce* como um processo complexo e frágil que envolve tecnologia e regras de negócios.

Este trabalho inova em relação aos citados ao propor uma política de segurança que permite o controle de acesso de forma maleável.

1.5.4 Confiança

Em Ruggiero (2002) é apresentado um modelo de segurança em redes *ad hoc* que utiliza medição e distribuição de confiança. Em Scweitzer (2004) é apresentado um modelo de confiança distribuída em redes *ad hoc*. Também em 2004 foi apresentada uma tese de doutorado que define uma plataforma de computação com confiança (MITTELSDORF).

Em Ganger (2001) é apresentado um mecanismo de autenticação por confiança que refina por métodos matemáticos e a teoria das probabilidades a decisão de autenticar ou não um usuário baseando-se em observações de localização física do mesmo, atividade, leitores biométricos e número de vezes que errou a senha.

Em Veras (2005) é apresentado a utilização da confiança na personalização de usuários no acesso a sites da Internet.

Este trabalho inova em relação aos citados por utilizar informações da análise comportamental do usuário e baseando-se nas evidências, compõe a confiança necessária para a política de segurança adaptativa.

1.6 Metodologia da Pesquisa

A metodologia da pesquisa desta tese consistiu das seguintes etapas:

1ª. Etapa: Revisão bibliográfica, pesquisa exploratória, documental e conceitual sobre os temas: segurança em redes de computadores, reconhecimento, autenticação, controle de acesso e análise comportamental. Pesquisa bibliográfica sobre computação pervasiva e ubíqua; levantamento das publicações no âmbito da Computação Ciente de Contexto.

2ª. Etapa: Pesquisa sobre a evolução da Tecnologia de Reconhecimento Facial, mecanismos de autenticação, segurança e privacidade. Estudo sobre implementação e testes de algoritmos de reconhecimento facial. Acompanhamento de implementação de algoritmos de reconhecimento facial desenvolvido por terceiros.

3ª. Etapa: Pesquisa bibliográfica sobre aplicações e definições do processo de atribuição da Confiança Matemática da Teoria das Evidências de Dempster-Shafer.

4ª. Etapa: Pesquisa sobre a Teoria Comportamental, histórico, aspectos sociais e psicológicos. Estudos e pesquisas sobre métodos matemáticos e para tratar informações obtidas sobre o comportamento de pessoas.

5ª. Etapa: Idealização de um mecanismo de autenticação contínua e como conseqüência um sistema que o implemente e que possa ser a base de uma política de segurança adaptativa ao usuário.

6ª. Etapa: Definição da Arquitetura e Modelagem do Sistema de Autenticação Contínua.

7ª. Etapa: Um estudo sobre a aplicabilidade da solução.

8ª. Etapa: Elaboração da Tese.

1.7 Contribuições e Inovações

Esse trabalho contribui para a área de segurança da informação em redes de computadores por:

i) apresentar uma abordagem sobre computação ciente de contexto, tecnologia do reconhecimento facial, análise do comportamento humano e confiança matemática, no suporte ao processo de autenticação contínua de usuários em redes de computadores;

ii) propor um sistema de autenticação contínua de usuários conhecidos que se baseia em níveis de confiança no comportamento do usuário e que venha identificar e autenticar usuários dado um domínio de aplicação específico num determinado período de tempo;

iii) definir um mecanismo de análise comportamental que permita a autenticação contínua de usuários em aplicações em redes de computadores.

iv) introduzir uma política de segurança adaptativa ao usuário.

v) propõe uma política de segurança adaptativa ao comportamento do usuário, baseando-se na análise comportamental do usuário, nas restrições de confiança geradas pelo usuário, nas restrições de confiança impostas pelo sistema KUCAS e nas informações de contexto do ambiente.

1.8 Estrutura da Tese

A Introdução apresenta o contexto, a motivação, a justificativa, a revisão bibliográfica com comentários sobre os trabalhos na área, a metodologia para elaboração deste projeto e as contribuições que ele propicia.

O Capítulo 2 apresenta a revisão bibliográfica, fundamentação teórica sobre Autenticação no ambiente da Computação Ciente de Contexto.

O Capítulo 3 faz uma abordagem sobre a Tecnologia de Reconhecimento Facial como base para a autenticação de usuários na Computação Ciente de Contexto.

O Capítulo 4 faz uma abordagem sobre o Comportamento Humano do ponto de vista da psicologia comportamental, para se obter subsídios para a análise comportamental de usuários, como base para a autenticação.

O Capítulo 5 descreve um mecanismo de análise comportamental de usuários e descreve a arquitetura de um Sistema de Autenticação Contínua de Usuários Conhecidos KUCAS (*Known User Continuous Authentication System*).

O Capítulo 6 apresenta um estudo de caso sobre a aplicabilidade do sistema KUCAS, baseado numa simulação de aplicações financeiras com dados fictícios em máquinas ATM (Automated Teller Machine).

Nas Considerações Finais são exploradas as possibilidades de trabalhos futuros, contribuições do sistema proposto, trabalhos decorrentes desta pesquisa e é feita uma conclusão final.

2 Autenticação na Computação Ciente de Contexto

2.1 Introdução

A evolução da tecnologia das redes de computadores com e sem fio traz novos desafios em relação à segurança dos dados e dos usuários.

Este capítulo aborda as características da Computação Ubíqua e da Computação Ciente de Contexto e como estas características influenciam na segurança, na autenticação e na privacidade de usuários de aplicações de software em redes de computadores com e sem fio.

2.2 Computação Ubíqua

No século XX, no início dos anos 90, Mark Weiser (WEISER,1991,1993), um cientista do Xerox Palo Alto Research Center visionou, para o século XXI, uma nova era na computação, com ambientes saturados de redes de computadores com ou sem fio, num mundo em que os dispositivos se relacionam com as pessoas, entendem as ações humanas, sentem fenômenos físicos e se comunicam uns com os outros. Ele previu que a computação se espalharia pelo ambiente em equipamentos móveis e embarcados altamente disponíveis, interagindo com os seres humanos baseados em seus comportamentos ao utilizar aplicações de software no ambiente tecnológico; de forma transparente e invisível, integrada ao ambiente.

Hoje em dia, as visões de Mark Weiser são interpretadas como o resultado da evolução das conexões das redes de computadores com e sem fio e pelo dinamismo da Computação Ubíqua.

A Computação Ubíqua e pervagante é o novo paradigma da computação distribuída e é realizada por dispositivos que atuam de forma discreta nos ambientes onde estão

implantados e tem a infra-estrutura de serviços disponível em qualquer lugar, em qualquer dispositivo e a qualquer hora (TRIPATHI, 2005). Este novo paradigma é o resultado de pesquisas e dos avanços em redes com e sem fio, redes ad hoc, redes de sensores, sistemas distribuídos, sistemas embarcados, redes de satélites, agentes móveis, autômatos, realidade virtual e inteligência artificial com técnicas que permitem a saturação do ambiente com vários dispositivos, integrando grandes computadores com computadores pessoais, invadindo a vida das pessoas e trazendo desafios à segurança (RAVI et al., 2002) (STAJANO, 2002).

As pesquisas na área da computação pervagante e ubíqua vêm evoluindo desde a década de 90, no século XX; com a introdução dos conceitos das redes de computadores móveis ad-hoc surgiu a necessidade de atender aos requisitos de transporte de dados e informações a qualquer hora e em qualquer lugar, e novos padrões foram desenvolvidos através de tecnologias de redes sem fio como Rádio Frequência, WiFi, Bluetooth, blackberry, além das tecnologias de acesso via celular (HANSMANN, 2003).

A computação ubíqua tem por característica possuir muitos dispositivos no ambiente, alguns embarcados para se conectar com redes com e sem fio e com isto surgem desafios à segurança no que se refere à dinâmica ambiental, com a proliferação de vários dispositivos no ambiente e o acesso computacional de modo transparente, sem o usuário conhecer a tecnologia que está embutida no ambiente e em diversos dispositivos móveis como o computador pessoal (PC), o Personal Digital Assistant (PDA), o celular, vestimentas e acessórios com dispositivos digitais embutidos.

A computação é ubíqua por dar mobilidade, isto é, permite acesso a recursos computacionais e serviços independentes da localização geográfica.

Na Computação ubíqua os serviços são distribuídos e com isto surgem novos desafios técnicos e preocupações com este ambiente, como segurança, vulnerabilidades, ataques, acessos indevidos, capturas de informações, garantia de privacidade, autenticação confiável,

confiabilidade das aplicações de software, capacidade de armazenamento de energia e a necessidade constante de carregamento de baterias dos dispositivos.

2.3 Computação Ciente de Contexto

A evolução da interação usuário-computador-ambiente vem concretizar as idéias lançadas por Mark Weiser, e como extensão da Computação Ubíqua surge a Computação Ciente de Contexto (Context-Aware Computing).

A Computação Ciente de Contexto estende os conceitos da Computação Ubíqua e estuda aplicações que se adaptam de acordo com sua localização de uso, que interage com as pessoas e objetos e com as mudanças que ocorrem com as pessoas e objetos ao longo do tempo (SCHILIT, THEIMER, 1994) e que adaptam seu comportamento com base em informações capturadas de um ambiente físico e/ou computacional (SANTOS et al., 2001).

Portanto, a Computação Ciente de Contexto explora as interações do ser humano com dispositivos e equipamentos computacionais de forma a aproveitar as informações contextuais presentes nessa comunicação, as quais podem ser coletadas, analisadas e servirem de subsídios para adaptação de serviços de acordo com as necessidades dos usuários e características do hardware e dos dispositivos de interação.

Um dos paradigmas da computação ciente de contexto é a capacidade de ensinar computadores a interagir com o ambiente e as pessoas, e reagir quando houver mudanças tanto das pessoas como do ambiente, de modo a continuar obtendo informações sobre a localização das pessoas, estado físico, estado emocional, histórico, comportamental, entre outros.

Com isso, projetos voltados para interfaces mais amigáveis investigam técnicas de comportamento de usuários, reconhecimento de escrita e de gestos, interação com canetas,

técnicas de voz e percepção computacional, interação com sensores e manipulação de artefatos eletrônicos (DEY, ABOWD, 1999).

A Computação Ciente de Contexto permite a obtenção e utilização de informações de contexto adquiridas de dispositivos computacionais no ambiente, informação de contexto é qualquer informação que possa ser usada para caracterizar a situação de uma entidade, sendo que entidade é uma pessoa, lugar ou objeto que é considerado relevante para a interação entre um usuário e uma aplicação; informações possíveis de se obter são localização, identificação de pessoas e objetos, lugares e horários (DEY, 2001).

Porém, há muitas outras informações contextuais A maioria dos sistemas ciente de contexto ainda não incorpora históricos e outras pessoas no ambiente além do usuário.

Em Dey (1999) e Abowd e Mynatt (2000) são propostas cinco semânticas ou cinco dimensões semânticas para especificação e modelagem de informações de contexto e que ajudam a definir qual informação é importante ou relevante.

- Who - dimensão da identificação, identifica quem é;
- Where - dimensão da localização, identifica onde está;
- What - dimensão da determinação, o quê é;
- When - dimensão temporal, quando;
- Why - dimensão de intenção, por que;

Em (TRUONG et al., 2001) é sugerida a sexta dimensão contextual, ou seja, para a captura e acesso automatizado de atividades humanas, How, a dimensão que justifica, o como;

A definição de contexto e as seis dimensões semânticas ajudam a decidir quais informações são relevantes para um sistema, porém é necessário analisar os requisitos e modelar as informações necessárias que cada dimensão pode fornecer, em geral, há uma tendência para desenvolvimento de um modelo de contexto de usuário que sobrepõe

problemas associados, e com isto há uma generalização ao classificar o contexto em aspectos temporais, estático e dinâmico.

Henricksen et al (2002) também definem contexto estático como informações que permanecem fixas durante o tempo de vida da entidade, ao passo que o contexto dinâmico pode ser de três tipos: informações de sentido, informações explícitas e informações a serem interpretadas. As informações de contexto dinâmico de sentido são aquelas capturadas por meio de sensores físicos e lógicos. Informações de contexto dinâmico explícito são aquelas fornecidas explicitamente pelo usuário, por exemplo, a senha de acesso.

Henricksen et al. (2002) propõem que os conjuntos de características, usualmente utilizados em aplicações cientes de contexto, podem ser classificados em infra-estrutura de comunicação, sistema, domínio e ambiente:

Contexto de infra-estrutura é a comunicação entre a aplicação e o dispositivo usado pelo usuário para acessar a aplicação, fornece subsídios para que se possa reportar mudanças de estado devido a falhas, adição ou remoção de um dispositivo no ambiente.

Contexto de sistema é formado pelo contexto do usuário, o estado atual dos dispositivos e serviços utilizados e deve conter informações que possibilitam saber até que ponto um dispositivo está ciente dos outros dispositivos nas suas proximidades e até que ponto uma aplicação está ciente da proximidade de outra para oferecer serviços.

Contexto de domínio se refere às informações sobre a semântica do domínio da aplicação, considerando os relacionamentos entre dispositivos e usuários.

Contexto de ambiente contém as informações sobre o endereço e localização de uma determinada entidade.

De modo geral, todos os contextos requerem cuidados em relação a invasão de privacidade e a espionagem, pois todas as informações capturadas ficam vulneráveis e podem ser disponibilizadas a outros.

Para evitar a captura das informações e uma utilização inadequada Dey (1999) sugere cinco requisitos que um software de computação ciente de contexto deve possuir:

1. Especificação de Informação de Contexto: O requisito mais importante de um software ciente de contexto é a existência de mecanismos que permitam que uma aplicação especifique quais contextos ela tem interesse e que ações devem ser tomadas quando determinado contexto for obtido.

2. Percepção Contextual: É a capacidade de detectar o contexto e apresentar as informações que o descrevem.

3. Associação de Informação Contextual: Autoriza associar informações contextuais a dados.

4. Captura de Recurso Contextual: Permite que aplicações descubram e explorem recursos e serviços relevantes para um determinado contexto.

5. Adaptação Contextual: Descreve onde o contexto causa uma ação e onde o contexto é usado para modificar ou adaptar serviços.

Em Goularte (2003) é proposta a separação do item "Adaptação Contextual" em outros dois, a saber:

1. Ações disparadas pelo Contexto: Uma ação é disparada quando um determinado conjunto de informações contextuais atinge valores específicos.

2. Mediação Contextual: Adapta serviços e dados de acordo com os limites e preferências impostos pelo contexto.

Um sistema ciente de contexto é um sistema que utiliza informações contextuais para prover informação relevante e/ou serviços ao usuário, onde a relevância depende da ação do usuário (PASCOE, 1998; DEY e ABOWD, 1999).

Entretanto, um sistema ciente de contexto não se restringe somente a mobilidade, há um contexto maior, que engloba todos os sistemas tanto em redes com ou sem fio.

A Computação Ciente de Contexto colabora com este trabalho por definir dimensões semânticas, ou dimensões contextuais que permitem obter e utilizar informações de equipamentos e dispositivos no ambiente físico e computacional. Á partir das informações contextuais obtidas é possível elaborar a análise comportamental do usuário e atribuir a ele um nível de confiança que garanta a autenticação contínua do mesmo.

2.4 Autenticação em Computação Ciente de Contexto

No âmbito da Computação Ciente de Contexto, na qual milhões de dispositivos estão interconectados em redes com e sem fio, abrem-se várias oportunidades para o acesso de usuários não autorizados a informações digitais. Neste ambiente, o controle de acesso e a autenticação são aspectos críticos para garantir a segurança. A tríade tradicional utilizada na autenticação e que garante que uma pessoa ao utilizar uma aplicação de software em redes de computadores, é conhecida por: You know (senha que seja conhecida do usuário); You have (código de acesso ao sistema que o usuário possui); You are (característica biométrica da pessoa, algo que a pessoa possui fisicamente e é único) para que a autenticação seja válida. Existe uma variedade de métodos de autenticação de usuários, e estes métodos formam a base dos sistemas de controle de acesso. As três categorias de métodos para verificação da identidade de um usuário são baseadas em algo que o usuário sabe, tal qual um código de acesso e uma senha; e alguma característica física do usuário, baseado na biometria.

Se a identidade dos usuários legítimos puder ser verificada com um grau aceitável de certeza, as tentativas de acesso ao sistema sem a devida autorização podem ser negadas. Quando um usuário legítimo é verificado, são aplicadas técnicas de controle de acesso para permitir seu acesso aos recursos do sistema.

As senhas são o mecanismo mais comum de autenticação de usuários que precisam acessar computadores e redes. Mas as senhas também podem representar uma forma de

conexão e proteção extremamente fraca, se os usuários escolherem senhas de fácil memorização, ou se por ventura ocorrer o esquecimento da mesma.

Outro mecanismo de autenticação são os cartões inteligentes, que são dispositivos do que armazenam certificações, chaves públicas e privadas, senhas e outros tipos de informações pessoais. O acesso do usuário a um sistema com um cartão inteligente oferece uma forma de autenticação forte, pois trata-se de uma identificação baseada na criptografia e na prova de posse da chave privada mantida no cartão inteligente no momento de autenticação de um usuário na rede; ou seja, é um dispositivo que envolve um componente que se tem, com um componente que se sabe. A desvantagem é que o cartão pode ser perdido.

Outra forma de autenticação é a infra-estrutura de chave pública (PKI - Public Key Infrastructure), incluindo certificados e respectivos serviços que oferecem recursos de autenticação que se baseiam na tecnologia criptográfica de chave pública. Uma PKI oferece os mecanismos para a emissão o gerenciamento do ciclo de vida de certificados digitais.

Atualmente, existem várias estratégias de autenticação de usuários sendo utilizadas em aplicações comerciais e existem vários problemas com autenticação baseada em senhas, pois a senha pode ser copiada, esquecida ou adivinhado por uma pessoa não autorizada.

Soluções alternativas como perguntas randômicas e senhas descartáveis geralmente são simples de utilização e bem aceita pelos usuários. Além disso, não requerem *hardware* adicional como outras soluções baseadas em propriedade e características. Outra vantagem é que elas podem ser integradas em sistemas baseados em rede e na Web, além de diversos sistemas operacionais.

A utilização de perguntas randômicas, porém, adiciona uma dificuldade adicional ao usuário que quiser divulgar seu segredo, pois, ao contrário de contar apenas uma palavra, terá que divulgar todas as informações constantes no questionário que serve de base para as perguntas randômicas.

Autenticação por sistemas biométricos se baseia em características fisiológicas e comportamentais de pessoas vivas. Os principais sistemas biométricos utilizados nos dias de hoje são baseados no reconhecimento de face, impressão digital, geometria da mão, íris, retina, padrão de voz, assinatura e ritmo de digitação. As vantagens desses sistemas são que eles não podem ser forjados nem tampouco esquecidos, obrigando que a pessoa a ser autenticada esteja fisicamente presente no ponto de autenticação. A desvantagem reside na falta de padrões, desconforto de usar alguns dispositivos biométricos e custo elevado dos equipamentos envolvidos.

Em geral, o processo de autenticação de usuários é bastante frágil, pois podem ocorrer interceptações, decorrentes do fato de que as informações confidenciais que são necessárias para autenticar o usuário origem junto usuário destino, poderão ser manipuladas por outros usuários ao trafegarem pela rede (STALLINGS, 1998).

Nos sistemas distribuídos, o usuário origem e o usuário destino estão interconectados através de uma rede aberta na qual vários outros usuários também têm acesso. Assim sendo toda a troca de mensagens realizada entre os dois parceiros deverá ser encaminhado através da rede, ficando, portanto, propício de ser interceptado por um outro usuário que poderá modificar ou destruir as mensagens enviadas bem como inserir mensagens falsas nesta comunicação.

Devido a esses problemas de vulnerabilidade da comunicação que possibilitam ameaças à segurança do sistema, um sistema de autenticação propício a esse ambiente deverá requerer:

Uma autenticação forte - cujo objetivo é fazer com que as informações necessárias para autenticar um usuário não sejam divulgadas durante a comunicação;

Uma autenticação mútua - a autenticação deve ocorrer nos dois sentidos, ou seja, tanto a origem deve ser autenticada no destino para que este tenha a garantia de onde a

mensagem foi originada, como o destino deve ser autenticado na origem para garantir que realmente é ele que irá receber e interpretar a mensagem enviada;

Uma autenticação contínua - a freqüência do processo de autenticação deverá ser sob demanda ou assíncrona; apenas uma autenticação inicial não é suficiente pois um intruso poderá se fazer passar por um usuário já autenticado e prejudicar a comunicação.

As ameaças de segurança em um ambiente distribuído poderão ser controladas usando criptografia para fornecer uma autenticação forte, mútua e contínua. Independentemente de qual técnica de criptografia se irá utilizar, é necessário que os parceiros da comunicação tenham conhecimento da chave criptográfica que irá ser utilizada na segurança do seu processo.

Segundo (STALLINGS, 1998), a criptografia pode ser simétrica e assimétrica.

Tanto na mobilidade e transparência da computação ubíqua, como nas dimensões contextuais da computação ciente de contexto, há necessidade de mecanismos de segurança e autenticação.

A autenticação de usuários neste contexto pode também ser baseada em chaves de acesso e senhas, um método tradicional utilizado pela maioria dos sistemas, porém, o dinamismo torna os dois ambientes muito vulneráveis, pois permite que os usuários possam estar presentes ou ausentes e observando outros usuários ou usufruindo das informações das dimensões contextuais.

A autenticação do usuário em aplicações distribuídas na Internet e nas redes de computadores com e sem fio, pode ser feita da forma tradicional com mecanismos como chaves de acesso, senhas e cartões magnéticos; o problema delas serem esquecidas pelos usuários ou roubadas, vai continuar existindo.

Como as informações são contextuais, as senhas e chaves de acesso podem ser facilmente interceptadas, uma maneira de garantir a autenticação de usuários é usufruir as

informações de contexto e utilizar uma autenticação focada em biometria, a tecnologia que mensura as informações físicas e únicas dos seres vivos, e com isto obter informações para uma efetiva análise comportamental do usuário e autenticá-lo por suas características físicas e comportamentais.

Uma outra forma de autenticação que pode ser utilizada é a análise comportamental do usuário, um mecanismo mais complexo que pode ser definido por parâmetros ou dimensões contextuais obtidos dos dispositivos no ambiente, cuja análise permite identificar os usuários das aplicações baseando-se em seus comportamentos, o atual e os anteriores.

A combinação da forma de autenticação tradicional com autenticação baseada em biometria provê um nível maior de segurança na autenticação de pessoas na computação ciente de contexto.

A autenticação pode ser combinada com outras tecnologias como troca de chaves secretas, utilização de seqüências de segredos não reutilizáveis com informação biométrica, mecanismos de gestão de chaves criptográficas; autenticação com reconhecimento facial e reconhecimento de voz, ou digital dos dedos ou palma da mão.

2.5 Segurança em Computação Ciente de Contexto

A segurança na computação ciente de contexto está relacionada com as pessoas, com o ambiente, com a arquitetura dos sistemas, com a estrutura das redes de computadores; a segurança é um desafio, mas é intrínseco aos problemas de segurança encontrados em qualquer tipo de rede e consiste em se ter mecanismos de prevenção que possibilitam apontar vulnerabilidades, minimizar os riscos de fragilidades e evitar acessos indevidos, ataques e destruições.

Os diferentes cenários da computação ciente de contexto definem as melhores práticas de segurança neste ambiente e devem estar aptos para conferir ao sistema uma operação

segura, desde a transmissão dos dados até o armazenamento dos mesmos, independente das restrições, tais como escassez de recursos de radiofreqüência, pouca memória, baixa capacidade de processamento e duração restrita de baterias (CALLAWAY, 2003), (CAM-WINGET et al, 2003).

O ambiente da Computação Ubíqua tem maior vulnerabilidade em função da mobilidade e transparência, sendo necessário cinco requisitos básicos de segurança para que um dispositivo ou sistema neste ambiente possa ser considerado seguro: disponibilidade, confidencialidade, integridade, autenticidade e não-repudio e privacidade, conforme citado em Hu e Evans (2003) e relacionado abaixo:

Disponibilidade dos serviços e recursos de um sistema sempre que forem necessários, ou seja, acesso a qualquer hora e em qualquer.

Confidencialidade das informações para que não sejam acessadas por entidades não autorizadas e que só devem estar disponíveis para aqueles devidamente autorizados, ou seja, os dados não podem ser acessados sob a interferência de oscilações numa rede sem fio e nas fragilidades de um ponto de acesso.

Integridade para que as informações não sejam modificadas ou alteradas sem consentimento enquanto trafegarem pela rede de computadores e ainda garante que o sistema tenha um desempenho correto, ou seja, os dados devem se manter íntegros, e as trocas de informações não devem ser interceptadas e nem alteradas no percurso dos dados.

A autenticidade significa verificar a identidade da pessoa ou do processo que deseja se comunicar com o sistema protegido, ou seja, deve garantir que os usuários e sistemas da rede confirmem a identidade de seus pares de comunicação.

O não-repudio é a capacidade do sistema identificar a origem da informação recebida de outra pessoa, além de garantir que a informação veio do remetente. O remetente não pode ser capaz de negar (repudiar) o envio da informação que ele de fato enviou.

Privacidade significa que a troca de mensagens entre usuários e sistemas conta com confidencialidade.

A invasão da privacidade se caracteriza pela aquisição e divulgação de informações sem autorização.

Além da garantia de sigilo de informações transmitidas, deve ser considerado o tratamento específico das informações que são armazenadas nos dispositivos portáteis (SCHNEIER, 2003).

A vulnerabilidade dos mecanismos de segurança constitui um grande risco, e pode ter sua origem numa falha de operação não intencional ou em ações maliciosas por parte de elementos da rede, por isto deve ser tratada por esquemas de criptografia, pois as ameaças contra as aplicações existem desde a captura no dispositivo móvel até os níveis da aplicação onde o roteamento é mais crítico (KARPIJOKI, 2001).

Vulnerabilidades tanto nas redes como em dispositivos móveis, como celular, PDA, notebook, palm, etc, pode permitir acesso a pessoas não autorizadas e negar o acesso aos autorizados (SCHEIER, 2003).

Numa rede com fio, os usuários são primeiramente identificados e autenticados para que possam participar de qualquer interação ou transação que envolva troca de informações, por ser um ambiente privado, para se submeter ao processo de identificação e autenticação, o usuário deve inicialmente estar conectado fisicamente a rede (WHITMAN, 2003).

Numa rede sem fio, basta que o usuário esteja dentro da área de alcance das comunicações locais para que ele possa entrar na rede. Neste caso, a vulnerabilidade do sistema se torna muito mais acentuada e cuidados adicionais devem ser tomados para que não se tenha interferência negativa impossibilitando a aplicação (SCHMIDT, 2001).

2.6 Privacidade em Computação Ciente de Contexto

A Computação Computação Ciente de Contexto vem mudando o conceito de privacidade, tornando possíveis novas oportunidades de interagir e compartilhar.

A expressão - em qualquer lugar, a qualquer momento - tanto serve para permitir a troca de informações para o bem como para o mal; a perda da confidencialidade pode ocorrer durante a transição dos dados e também no local onde ficarão armazenados (CARVALHO, CUGNASCA,GUTIERREZ, 2004).

No quesito privacidade há muita vulnerabilidade na computação ciente de contexto, pode se considerar a invasão da privacidade para ações maliciosas e a invasão de privacidade para rastrear e personalizar as preferências de usuários durante a navegação na Internet, para oferecer novos produtos e serviços direcionados para as suas reais necessidades.

A sociedade americana Association for Computing Machinery (ACM) elaborou um código de ética que contém alguns princípios como: evitar danos a terceiros; conhecer e respeitar as leis existentes, relativas ao trabalho profissional; respeitar a privacidade de terceiros; ser honesto e digno de confiança (ACM, 1992).

EPAL (Enterprise Privacy Authorization) é uma linguagem formal para definição de políticas de privacidade com objetivo de controle de acesso a informações por meio de regras detalhadas baseadas em modelos de dados e autenticação de usuários. Em uma política EPAL são definidas hierarquias de categorias de dados, de usuários e de finalidades e conjuntos de ações, obrigações e condições. Nas categorias de dados são definidas as diferentes informações coletadas de acordo com suas perspectivas de privacidade. Os usuários e seus grupos são definidos em categorias de usuários de acordo com os dados coletados os quais eles possuem acesso e no modelo de finalidades são definidos os serviços associados a cada dado coletado (BACKES et al, 2004).

Stajano (2002) lista alguns problemas preocupantes em relação à segurança e privacidade dos usuários que utilizam sistemas cientes de contexto:

- cada vez mais atividades comuns são efetuadas através de dispositivos eletrônicos móveis o que permite coletar informações de comportamento e preferências de usuários e reduzindo a privacidade;
- computação ciente de contexto adiciona a questão da escala de uso das informações, pois dados pessoais que podem ser coletadas;
- brechas e vulnerabilidades poderão legalizar a espionagem.

2.7 Contextualização

Os problemas de segurança, privacidade, controle de acesso e autenticação são preocupantes em qualquer tipo de rede.

A proposta deste trabalho é extrair das dimensões contextuais da computação ciente de contexto, informações que tanto podem favorecer a mobilidade da computação ubíqua como as interações da computação ciente de contexto.

Informações do usuário indicadas por who, informações da localização indicadas por where, informações temporais indicadas por when, informações de tarefas indicadas por what e informações de intenções indicadas por why são variáveis contextuais que contribuem com informações e serviços à política de segurança adaptativa proposta.

3 Autenticação usando Tecnologia de Reconhecimento Facial

3.1 Introdução

Este capítulo apresenta uma abordagem sobre a Tecnologia de Reconhecimento Facial, um ramo da biometria, que mensura as características físicas e únicas da face humana, como suporte para a autenticação de usuários na computação ciente de contexto.

Uma das capacidades mais impressionantes que quase todos os seres humanos possuem é o poder de reconhecimento facial, um mecanismo perceptível de capacidade da visão que é aperfeiçoado pelo cérebro humano ao longo dos anos, culminando no poder de reconhecer uma face mesmo após muitos anos ou que a face apresente alterações significativas, tais como o envelhecimento, processos de engordar e emagrecer, presença de óculos, barba, bigode, um corte ou uma cor diferente de cabelo; o reconhecimento acontece naturalmente para identificar pessoas e é utilizado ao longo da vida (BRUNELLI, POGGIO, 1993).

Aspectos físicos e psicológicos influem na identificação pelo cérebro humano. Não apenas a face, a estatura, a forma do corpo e o conjunto face-corpo são utilizados no reconhecimento, mas também as expressões faciais, expressões corporais e o contexto onde a face ou a pessoa se insere, pois denotam o estilo da pessoa e são observados para se atingir um reconhecimento efetivo (BIRNBRAUER, 1979).

As informações adicionais sobre a pessoa são passadas através das expressões faciais tais como alegria, tristeza, surpresa ou ira e permitem ao ser humano estabelecer o relacionamento social, identificar aspectos psicológicos, reconhecer o interlocutor, se adaptar e permitir a interação com outras pessoas (BAER et al., 1968).

Os seres humanos, ao se comunicarem, expressam grande parte de seu estado emocional nas expressões faciais, estas informações podem ser usadas computacionalmente

para interagir com aplicações. Técnicas de reconhecimento de expressões faciais são discutidas em LEE et al. (1996) e a influência que produzem nos relacionamentos. Mudanças sensíveis nas expressões faciais também podem ser percebidas por tecnologias de reconhecimento por meio de movimento dos lábios, mesmo sem som e reconhecimento por voz (BEYMER, POGGIO 1995).

3.2 Características de Sistemas Biométricos

Um sistema biométrico é um sistema de reconhecimento de padrões que efetua a identificação pela determinação da autenticidade da característica biométrica registrada em posse da pessoa. Normalmente um sistema deste tipo pode ser dividido em duas partes o módulo de captura da imagem e o de identificação.

No módulo de captura, as características biométricas da pessoa são obtidas por um sensor biométrico, ou câmeras, e são analisadas por um algoritmo que gera um t*emplate*. O *template* é uma representação compacta da característica biométrica que possui informações significativas para identificar a pessoa, descrevendo os dados biométricos para facilitar a comparação (ASHBOURN, 2000).

No módulo de identificação é feita uma comparação entre o template da imagem capturada e os templates das imagens nas bases de dados.

O desenvolvimento de sistemas biométricos como reconhecimento de faces, digitais (dedos, palma da mão), íris/retina, voz, modo de andar ou digitar num computador provêem uma solução superior na identificação de indivíduos e minimiza os riscos de alguém se apoderar e usar a identificação pessoal de outra pessoa; entretanto, também possuem desvantagens, pois requerem a cooperação ativa dos indivíduos. Por exemplo, reconhecimento por digital e por íris/retina necessita que a pessoa se posicione em frente a um equipamento e colabore com a leitura feita pelo mesmo; o reconhecimento pela voz, requer

que o participante fale num equipamento com um microfone e os ruídos no ambiente acabam interferindo no processo; no modo de andar também há necessidade de cooperação da pessoa e no modo de digitar além da cooperação podem ter a interferência de aspectos psicológicos como nervosismo e excitação que interferem no reconhecimento (KUPERSTEIN, 1996).

As características físicas e comportamentais do ser humano podem ser diferenciadas, comparadas, armazenadas e convertidas em códigos de autenticação para automatizar métodos para identificação de pessoas, como também pode-se combinar entre si essas tecnologias, como por exemplo, utilizar duas tecnologias ao mesmo tempo para garantir a certeza do reconhecimento como identificação por impressão digital junto com a identificação de reconhecimento da face, ou identificação pela íris com identificação pela retina, ou reconhecimento da voz com geometria da mão, entre outras, alternadamente (GOVINDARAJU, 1990).

Para implantar um sistema biométrico são necessários equipamentos especiais como câmeras digitais ou sensores e de forma generalizada, para cada caso, o hardware e o *software* devem ser otimizados para o elemento biométrico adotado (YACOOB e DAVIS,1996).

A evolução de equipamentos especiais como câmeras de vídeo digitais, redes de sensores e *software* para tratamento de imagens fez surgir muitos trabalhos na área de biometria, sendo que a maioria deles é desenvolvido para a área de segurança e são utilizados no controle de acesso, segurança de sistemas, identificação criminal e na interação de robôs com computadores e seres humanos (MURRAY, BASU,1994).

A desempenho de um sistema biométrico depende da precisão de recursos de hardware que afetam a identificação; a velocidade envolve medidas de tempo, largura de banda, complexidade computacional, escalabilidade e medidas de precisão (PANKANTI et al., 2000).

3.3 Tecnologia de Reconhecimento Facial

A tecnologia de reconhecimento facial, desde o seu surgimento em meados da década de 90 do século XX, vem se aprimorando e se aperfeiçoando mais intensamente que outras tecnologias biométricas, como por exemplo, a de reconhecimento por digitais dos dedos, da palma das mãos, ou da íris, e novos algoritmos surgiram com várias técnicas de reconhecimento de faces de pessoas utilizando imagens digitais originadas por câmeras fotográficas ou de vídeo (KIM, 2002).

A Tecnologia do Reconhecimento Facial é baseada num sinal de vídeo ou uma fotografia de uma face, o sistema deve ser capaz de comparar a face de entrada com as faces armazenadas numa base de dados para determinar se a pessoa a ser reconhecida está pré-cadastrada.

Os projetos desenvolvidos utilizando a tecnologia de reconhecimento facial são focados na detecção de características individuais e únicas da face humana, assim um sistema de reconhecimento facial deve concentrar-se nos aspectos mais relevantes e característicos de uma face, tais como os olhos, nariz ou boca, e a linha que delimita a cabeça, sendo que a testa, o queixo, cor de cabelos, cor de pele têm pouca informação útil (CHELLAPPA et al., 1995).

Apesar de ser um problema conceitualmente simples, onde as necessidades dependem da precisão das características, a resolução é bastante complexa e está essencialmente associada à dificuldade de abstrair as características que a diferenciam de outras faces; as faces formam uma classe de objetos similares, pois todas apresentam poucas diferenças substanciais e todas possuem os mesmos elementos faciais, dois olhos simétricos, nariz e boca dificultando o processo de classificação; o processo de reconhecimento deve considerar detalhes como iluminação, rotação além das variações das expressões em pequenos intervalos de tempo, como estar sorrindo, chorando, séria, exprimindo sentimento de dor ou sofrer

mudanças como estar magro, gordo, com óculos, sem óculos, com barba, sem barba, etc (FRISCHHOLZ e DIECKMAN, 2000).

Figura 1: Características de um algoritmo de reconhecimento facial
Fonte: elaborada pelo autor

Na Figura 1 é feita uma representação dos pontos de uma face que são considerados numa tecnologia de reconhecimento facial.

Na face, os olhos são o elemento mais importante, pois mesmo isolados, permitem o reconhecimento da face. O inverso também se aplica, pois uma face com os olhos ocultos torna-se difícil de identificar, exemplo disso, é a utilização de máscaras para esconder a identidade de quem as usa (ASCENSO et al., 2002).

O reconhecimento e autenticação no controle de acesso às redes de computadores com e sem fio são requisitos indispensáveis num sistema de segurança. Vários processos, tecnologias biométricas, crachás, cartões magnéticos, controle de senhas e chaves de acesso são utilizados, mas ainda não oferecem a segurança necessária, pois os processos são vulneráveis, as tecnologias biométricas baseadas nas características físicas e únicas das pessoas podem falhar, as senhas podem ser esquecidas, os crachás e cartões magnéticos podem ser perdidos ou utilizados indevidamente por terceiros (ARYANANDA, 2002).

O reconhecimento e autenticação de pessoas são o principal aspecto para a segurança da informação. É através dela que se determina a pessoa autorizada a acessar e modificar dados; a falta de autenticação inviabiliza qualquer outra forma de segurança.

A utilização da face como elemento de identificação têm várias aplicações em segurança de computadores e bases de dados.

Existem muitos métodos e algoritmos para se detectar e localizar uma face numa imagem. Detectar uma face e as suas principais características consiste em localizar os olhos, nariz, boca, contornos da face ou outros elementos faciais e normalizar a face antes da fase de reconhecimento (TEOH, 2004).

As medidas de probabilidade estatística que determinam se amostras biométricas são do mesmo individuo chamam-se taxa de falso negativo e taxa de falso positivo (PHILLIPS et al., 1996).

Um sistema de detecção de faces também pode provocar dois tipos de erros:

a) **falso-positivo**: uma imagem que não é face é apontada como sendo a face encontrada.

b) **falso-negativo**: uma imagem que é face é apontada como não face, e não é encontrada.

Falhas na Tecnologia de Reconhecimento Facial e que geram a ocorrência de falsos positivos e falsos negativos, afetam a segurança e fazem com que seja inviável utilizá-la isoladamente no reconhecimento e autenticação de pessoas.

A detecção de faces também pode ser dificultada pelos seguintes fatores:

1. **Problemas de Pose**: as imagens das faces podem variar através do ângulo de captura da imagem ou do ângulo da face da pessoa. Uma face pode estar rotacionada para o lado e obstruir alguma característica, como por exemplo, o olho ou parte da boca.

2. **Presença ou ausência de componentes estruturais**: características que modificam faces como barba, bigode, óculos, etc.

2. **Expressão facial**: a face pode ser diretamente modificada com a expressão da pessoa, um sorriso, uma cicatriz, olheiras, inchaços, os processos de engordar, emagrecer e envelhecer.

4. **Oclusão**: uma parte de uma face pode estar oculta por algum objeto ou sombra.

5. **Orientação da imagem**: uma imagem pode ter sido obtida em um ambiente não favorável, interior de um ambiente escuro, contra luz, iluminação indevida ou exagerada.

6. **Iluminação**: uma área coberta por sombras ou baixa incidência de luminosidade prejudica a captura da imagem da face; o excesso de iluminação também causa problemas, como a alta incidência de luminosidade ou raios solares podem prejudicar a imagem.

Todos estes fatores fazem com que sistemas de detecção e reconhecimento de faces funcionem parcialmente ou apresentem erros, pois provocam mudanças no aspecto da face analisada, o que pode ser amenizado e corrigido com a escolha da câmera de vídeo adequada e um lugar apropriado para colocá-la (SAVVIDES et al., 2003).

Uma imagem da face ao ser capturada traz consigo a face e a não-face, ou seja, a face, a ser reconhecida está integrada no ambiente que a rodeia e necessita ser isolada do restante da imagem para se proceder com a identificação. Alguns sistemas não distinguem a fase de extração, que pode estar integrada quer na fase de detecção quer na fase de reconhecimento.

Na autenticação biométrica o usuário se cadastra no sistema, permitindo a coleta de seus dados biométricos. Um sensor, ou câmera de vídeo digital registra as imagens da face. As imagens podem ser monocromáticas ou coloridas, capturadas por uma ou múltiplas câmeras estacionárias ou móveis.

A imagem digital é uma matriz de inteiros, onde cada inteiro representa o brilho da imagem num tempo discreto e num ponto discreto do plano de imagem, cada ponto dessa matriz é um *pixel* (NALWA,1993).

Os valores discretos assumidos pelos pontos numa imagem monocromática variam de 0 (preto) a 255 (branco), numa escala de cinza (RUBENFELD, 1999), sendo que é nesta escala de cores cinzas que é feito o reconhecimento da face.

3.3.1 Técnicas utilizadas na tecnologia de reconhecimento facial

Nos últimos anos surgiram várias técnicas de reconhecimento facial, abaixo são descritas as mais relevantes.

- **Principal Component Analysis (PCA)**

A Análise de Componentes Principais (PCA) é uma técnica estatística que pode ser usada para simplificar um conjunto de dados, pois através de uma transformação escolhe um novo sistema de coordenadas para o conjunto de dados, tal que a maior variação do conjunto de dados venha a se agrupar no primeiro eixo, chamado primeiro componente principal, a segunda maior variação no segundo eixo e assim por diante. Sobre o ponto de vista de uma transformada, o resultado obtido é uma mudança de base, uma projeção em um novo espaço, onde cada componente esteja livre de redundância e seja expressa em ordem de variação ou contribuição (ETEMAD, CHELLAPPA,1997).

PCA é um método linear que pode ser aplicado na eliminação da redundância ou detecção de padrões existentes em um conjunto de dados é também conhecido como transformada de Hotteling ou expansão de Karhunen-Loeve. O método de reconhecimento de faces utilizando a transformada de Karhunen-Loeve foi proposto por Kirby e Sirovivh em 1990 (KIRBY, 1990).

Na detecção de padrões utiliza-se a distância euclidiana entre os componentes desse novo espaço e para redução se utiliza os componentes que mais contribuem nessa variação do espaço, ou os autovetores que correspondem aos maiores autovalores da matriz de covariância

e eliminam-se as que menos contribuem para a variação, ou que tenha os menores autovalores.

Os métodos baseados em PCA estão entre os que possibilitam a obtenção dos melhores resultados em termos de reconhecimento de faces frontais, em imagens de faces com boa iluminação e pose. Apesar da qualidade dos resultados obtidos, essa técnica tem a desvantagem de ser uma tanto custosa computacionalmente, pois todos os pixels da imagem são utilizados para se obter sua representação em função da covariância entre essa imagem e todas as outras imagens da base de dados; a técnica PCA é a obtenção de um espaço, definido por vetores que representam as faces de modo eficiente e com uma dimensão mais reduzida do que o espaço de imagens (CAMPOS, 2001).

Os vetores de base deste novo espaço não são correlacionados e maximizam a variância existente entre as faces de treino utilizadas para construir o espaço. Como o espaço de imagens é altamente redundante para descrever faces já que cada *pixel* das faces está correlacionado com os *pixels* vizinhos e todas as faces apresentam semelhanças evidentes, constrói-se a matriz de covariância a partir de um conjunto de imagens de faces (CHELLAPA et al, 1995).

- **Método baseado em aparência**

Método baseado em aparência ou *Active Appearance Models* é o método que emprega o aprendizado de padrões apresentados pelas faces de um conjunto de faces ou banco de dados de faces. Ao contrário da correspondência de templates, onde templates são pré-definidos por especialistas, os “templates”, nos métodos baseados em aparência são ensinados. Em geral, métodos baseados em aparência confiam em técnicas de análises estatísticas e máquinas de aprendizados para procurar características relevantes de face e de não-face. As características de aprendizado são uma forma de distribuição de modelos ou

funções de discriminação que são, conseqüentemente, usadas para detecção de face (BRUNELLI, POGGIO, 1993).

- **Active Wavelet Network (AWN)**

Active Wavelet Network é uma técnica similar a *Active Appearance Models* que tenta minimizar os efeitos de oclusão parcial e mudanças de iluminação das faces a serem detectadas (HEO et al., 2003).

- **Filtro Gabor Wavelet**

A partir de 1993, surgiram vários outros sistemas de reconhecimento robustos com imagens não normalizadas. Em 1999 surge um método baseado em filtros de Gabor, templates e grafos para eliminar os ruídos das imagens.

O uso do Filtro de Gabor é para modelar a variação encontrada no conjunto de treino de imagens e amenizar os ruídos das imagens. No método para rastrear faces utilizando a técnica *elastic graph matching* (EGM), os filtros de Gabor, com diferentes freqüências e orientações, são aplicados em algumas posições do interior da face, formando vetores de características. A face é então representada como um grafo, em que os nós e as arestas codificam informação geométrica. O rastreamento da face é realizado mediante um procedimento de EGM em cada quadro de imagem da face (LIU, 2002).

A principal desvantagem desta abordagem é o alto custo computacional requerido, o que conduz a uma taxa de processamento inadequada para aplicações em tempo-real.

- **Segmentação de Imagens**

A segmentação subdivide uma imagem e delimita regiões de interesse para uma aplicação específica, permitindo que se encontrem diferenças entre dois ou mais objetos.

- **Processo sensível a mudanças na iluminação**

É um processo de reconhecimento facial relativo à detecção e rastreamento de características faciais em seqüências de vídeo e utiliza uma abordagem baseada em cor, sensível a mudanças na iluminação (WANG, 1997).

- **Processo baseado em bordas**

É uma técnica de reconhecimento facial baseada na Teoria de *Rough Sets* que delimita as bordas; é um processo interessante que pode ser utilizado com outros objetivos, pois falha em diversas situações, como presença de óculos, adornos na cabeça e cabelos cobrindo a testa. (VIEIRA, 2003).

- **Processos de Rastreamento 3D da Face**

Trabalhos referentes ao rastreamento 3D da face permitem determinar a pose e o foco de atenção do usuário de frente, de perfil direito e esquerdo, caso abaixe a cabeça ou levante o queixo.

As técnicas podem ser divididas em *model-based*, as quais utilizam um modelo 3D da face, são robustas e demandam maior esforço computacional e *feature-based*, que determinam a pose da face a partir da posição de determinadas características faciais e são

sensíveis à falhas quando os pontos característicos não são localizados, em virtude de oclusão da imagem da face ou da variação de iluminação (MOGHADDM et al, 2003).

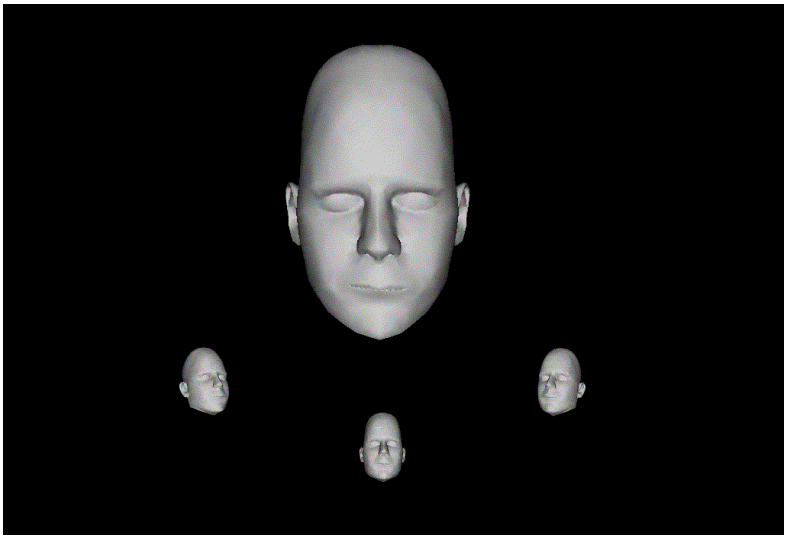


Figura 2: Sistema de Reconhecimento Facial em 3D
Fonte: CBA-Consultores Biométricos – software A4VISION

As variações de iluminação provocam alterações profundas nas imagens e a utilização do método das eigenfaces aplicado à textura da face apresenta resultados ruins devido à sensibilidade deste método às variações de iluminação.

Em Pentland et al (1994) os autores aplicam a técnica de análise em componentes principais para detectar a presença e localização de faces numa imagem.

Em Pentland e Choudhury (2000) é feito um estudo sobre a utilização da tecnologia de reconhecimento facial em dispositivos e equipamentos móveis e embarcados.

Lee et al. (1996) utilizam a informação sobre a cor da pele e do movimento característico da face numa seqüência de vídeo.

As técnicas baseadas em características geométricas utilizam a dimensão e a distância entre os elementos constituintes da face (olhos, sobrancelhas, nariz, boca, etc.) ou quaisquer

outros pontos para fazer a identificação da face, baseado no número de *pixels*. A configuração espacial dos elementos faciais é traduzida por um vetor que contém medidas dos elementos faciais tais como distâncias, ângulos e curvaturas (TURK, PENTLAND, 1991).

Em Turk, Pentland (1991) foi demonstrado que o erro residual da codificação usando eigenfaces pode ser usada tanto para detectar faces em imagens naturais como para a determinação precisa da localização, escala e orientação de faces na imagem. Também foi demonstrado satisfatoriamente que este método pode ser usado para obter o reconhecimento de faces confiável em imagens com poucas restrições. No trabalho de Pentland (1991) é elaborada uma análise de vários algoritmos utilizando o método de avaliação FERET.

A abordagem baseada na textura da imagem usa a imagem da face como um todo para o processo de reconhecimento, ou seja, as faces são representadas através de imagens ou através de características não geométricas obtidas a partir da imagem da face. Alguns destes métodos baseiam-se na correlação de templates deformáveis, outros se baseiam no uso de filtros de Gabor para se efetuar o reconhecimento.

Pentland e Choudhury (2000) discutem as dificuldades e soluções para aplicação da biometria em ambientes de baixo poder computacional e fazem uma análise comparativa entre vários trabalhos de reconhecimento facial desde 1989. Analisam o sistema KOHONEN (KOHONEN, 1996), conhecido como o primeiro sistema de reconhecimento automático de faces, que demonstrou que uma simples rede neural pode desempenhar reconhecimento de faces usando imagens de faces registradas, normalizadas e alinhadas. No sistema KOHONEN é apresentado uma rede neural que descreve faces através da aproximação dos autovetores da matriz de autocorrelação das imagens de face, os autovetores (*eigenfaces).*

Para utilização do sistema de KOHONEN é necessário fazer um alinhamento e normalização da imagem da face. Muitos pesquisadores tentaram esquemas de reconhecimento de faces baseados em atributos locais como limites, bordas, distâncias entre

pontos e outras abordagens características com o emprego de redes neurais. Enquanto muito sucesso foi obtido em bases de imagens pequenas com faces alinhadas, nenhum trabalho obteve resultados satisfatórios em problemas mais realísticos de grandes bases de dados, com localização, orientação e escala da face desconhecida.

Pentland (1994) sugere que, para que um novo algoritmo seja considerado potencialmente competitivo, esse deve ser testado com bases de dados possuindo, no mínimo, 200 indivíduos, devendo resultar em uma taxa de reconhecimento maior que 95%. Esses resultados foram válidos somente para imagens estáticas provenientes de máquinas fotográficas, hoje com algoritmos em 3D e a evolução das câmeras de vídeo já é possível um método de testes de algoritmos destinados a reconhecimento de pessoas a partir de seqüências de vídeo (WENG et al., 2000).

Nos experimentos descritos no trabalho de Phillips (1997), foram realizados testes com uma base de seqüências de imagens de 20 pessoas, sendo que o treinamento foi realizado com apenas 10 deles, pois os autores também fizeram testes de identificação. A melhor taxa de acerto obtida foi de 94,31 %. Matsuno et. al (1995) fazem um estudo sobre o reconhecimento automático de expressões faciais humanas. Schneiderman e Kanade (2000) introduzem um modelo estatístico para detecção de faces em 3D.

Em 3D, a maioria das bases de seqüências de imagens de faces disponível foi criada para testar métodos de rastreamento e de determinação da orientação tridimensional. Por isso, em geral, elas possuem poucas pessoas diferentes, ou seja, as bases de dados contém as imagens das mesmas pessoas, mas em ângulos e posições diferenciadas.

3.3.2 Tecnologia de Reconhecimento Facial em 2D

A Tecnologia de Reconhecimento Facial Bidimensional (2D), é baseada em imagens estáticas e frontais da face, no plano x-y.

Embora existam vários métodos para o reconhecimento automático de faces humanas, a grande maioria considera apenas imagens monocolores das faces, no qual é utilizada uma modelagem 2D resultado de vídeos de uma única câmera.

Na modelagem em 2D, os sistemas que conseguem trazer melhores resultados são baseados na metodologia *pictorial-based* que têm sido muito eficientes em bancos de dados compostos de faces frontais e com iluminação constante.

Um sistema baseado na metodologia *templates* é composto pela imagem completa da face (vista frontal) e um conjunto de quatro máscaras, representando olhos, nariz, boca e a região que inclui desde o queixo até as sobrancelhas.

O algoritmo de reconhecimento se baseia no cálculo da correlação (*normalized cross-correlation*) das faces existentes na base de dados, na comparação com a face a ser reconhecida. Este método detecta os pontos característicos, determinando os parâmetros da transformação que leva uma imagem frontal a uma determinada escala e posição em que os pontos se encontram. Através destes parâmetros, pode-se realizar a inversa da transformação e obter imagens normalizadas. Este processo de normalização é importante para reduzir as variações dos padrões introduzidas pelos movimentos da face, o que melhora o desempenho do sistema de reconhecimento.

As imagens utilizadas tanto para treinar quanto para testar o sistema de reconhecimento são imagens das regiões características normalizadas com relação a transformação. Para efetuar o treinamento, deve ser utilizada uma seqüência de vídeo de imagens da face da pessoa.

O reconhecimento deve ser feito utilizando análise de componentes principais (PCA), com uma base para cada região da face. Dessa forma, é criada uma base para olhos esquerdos, outra para olhos direitos, uma para o nariz e outra para a boca, obtendo-se as *eigenfeatures* (*eigenlefteyes, eigenrighteyes, eigennoses e eigenmouth*) (BELHUMEUR et al., 1997).

Após a obtenção de todas as *eigenfeatures*, essas deverão ser concatenadas de forma a criar um espaço de características formado por todas as *eigenfeatures*. Através de um algoritmo extrai-se das imagens da face, características chaves que são convertidas num código numérico que representa a identidade biométrica do usuário (FRISCHHOLZ, DIECKMANN, 2000).

No reconhecimento, uma série de cálculos matemáticos são definidos, a partir das medidas e distâncias entre vários pontos: olhos, nariz, ossos laterais da face e do queixo. As medidas são convertidas algoritmo, que passa a ser a "matriz" biométrica facial da pessoa.

A matriz obtida é comparada com um conjunto de várias outras assinaturas faciais existentes na base de dados do sistema, sendo estabelecido um limite de similaridade entre elas. O reconhecimento é feito pela comparação da matriz da pessoa a ser identificada com várias matrizes previamente arquivadas no sistema.

É feita uma comparação entre a característica biométrica e o padrão que foi registrado no banco de dados. A coincidência entre o padrão gravado e o coletado algumas vezes pode falhar.

Em geral na modelagem em 2D é necessário verificar se a face em frente à câmera é real e não apenas uma fotografia.

A seguir a seqüência de etapas de um sistema de reconhecimento facial :

Etapa 1: Localização olho: As posições dos centros dos olhos na face são determinadas.

Etapa 2: Verificação da Qualidade da Imagem: A qualidade da imagem da face é verificada para ver se está adequada para as etapas que seguem, a imagem não deve ter muitos ruídos, se a qualidade for considerada demasiado baixa, a imagem deve ser rejeitada.

Etapa 3: Normalização - A face é extraída da imagem, rotacionada e escalada tal que o centro dos olhos são posicionados para se encontrar na mesma linha horizontal do *pixel* tais que o ponto médio desta fileira está alinhado com o ponto médio entre os centros dos olhos.

Etapa 4: Pré-processamento - A imagem normalizada é pré-processada com técnicas que compreende, entre outras transformações, a eliminação de freqüências espaciais, as mais altas e as mais baixas, e faz a normalização do contraste e intensidade de iluminação.

Etapa 5: Extração da característica - na imagem pré-processada, as características relevantes são extraídas para distinguir uma pessoa de outra.

Etapa 6: Construção da referência ajustada - durante o registro as características faciais de diversas imagens de uma pessoa são extraídas, combinadas e comparadas com as faces armazenadas no banco de dados de imagens.

Etapa 7: Reconhecimento - a face é comparada com todas as outras faces armazenadas em bancos de imagens.

3.3.3 Tecnologia de Reconhecimento Facial em 3D

Nas últimas décadas, as pesquisas em biometria facial enfocaram o uso de imagens 2D para reconhecimento, porém, apesar de todo o avanço obtido, este tipo de aplicação sofre severa influência de fatores tais como: variação de luminosidade, posição e expressões faciais.

A Tecnologia de Reconhecimento Facial Tridimensional (3D) é a evolução da 2D, ou seja, com a possibilidade de capturar uma imagem da face e a rotacionar no espaço x-y-z com o objetivo de reconhecer e autenticar uma pessoa com mais segurança, em vários ângulos, tanto de perfil como face frontal.

As mudanças na aparência que ocorrem durante o movimento da face (rotações verticais ou horizontais) só podem ser exploradas em uma estrutura 3D de uma face.

No reconhecimento facial em 3D são analisadas imagens da face pelos movimentos da cabeça no espaço do eixo x-y-z, o qual permite reconhecer uma pessoa por sua face frontal, por seu perfil e se a pessoa abaixa a cabeça ou levanta o queixo (COLMENAREZ, HUANG,1995).

Alguns trabalhos vêm tentando aplicar técnicas tradicionais de reconhecimento 2D em imagens 3D, ou mesmo associar informação 2D e 3D, com algum sucesso (ATICK et al. 1996).

Recentemente, foi proposto o uso do *Mean Square Error* (MSE), obtido pelo registro de imagens 3D pelo algoritmo *Iterative Closest Point* (ICP), como medida para a qualidade do reconhecimento facial 3D. A utilização da medida, *Surface Interpenetration Measure* (SIM), para avaliação da correspondência entre imagens 3D de faces (ATICK et al.,1996).

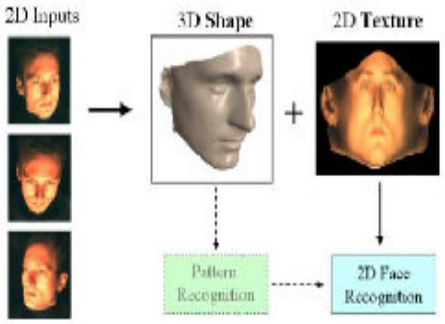


Figura 3: Comparação imagem 2D com 3D
Fonte: Mitsubishi electric research laboratories
CBA-Consultores Biométricos – (2005)

A Tecnologia do reconhecimento Facial em 3D utiliza mais de uma câmera de vídeo para a captura das imagens da face. Com avanços da microeletrônica, os custos para implementação de sistemas de digitalização de imagens foram bastante reduzidos,

possibilitando a construção de sistemas de visão *stereo* a um custo um pouco maior em relação a um sistema com apenas uma câmera.

Figura 4: Exemplos de reconhecimento facial usando geometria 3D
Fonte: elaborada pelo autor

A Figura 4 representa a captura de uma face humana, considerando-se as variações na qualidade da imagem, ruídos (sombras) e a distância. Com imagens da face em 3D as características tridimensionais das faces obtidas são formadas através de pares de imagens *stereo*.

Em Moghaddam et al. (2004) é descrito um sistema de reconhecimento e detecção de movimento e poses do corpo humano em 3D, capturadas por 51 câmeras de vídeo, num ângulo de 360 graus.

Genericamente, existem duas abordagens para o reconhecimento de faces. Na abordagem denominada *feature-based*, o reconhecimento baseia-se na configuração espacial dos elementos faciais e em suas características geométricas. Medidas como distâncias, ângulos e curvaturas de determinados elementos faciais são extraídas da imagem e utilizados para o reconhecimento.

A abordagem denominada *pictorial-based* procura fazer o reconhecimento diretamente a partir da imagem, sem procurar obter uma descrição geométrica da face.

Os métodos baseados em informação 3D podem utilizar qualquer uma das abordagens anteriores. Nestes métodos coloca-se a possibilidade da introdução de mais uma dimensão: a profundidade. O objetivo da introdução de mais uma dimensão consiste em desenvolver um sistema que funcione em condições mais flexíveis, tanto na rotação e translação como na iluminação. Os primeiros estudos consideram a generalização da técnica da análise em componentes principais através do uso de várias imagens faciais em diferentes poses ou imagens faciais tridimensionais.

A técnica conhecida como “Compensação de translações no plano XY” é utilizada em 3D e é feita calculando o ponto médio entre os olhos e movendo todos os pontos do modelo de forma que a origem das coordenadas se situe nesta linha.

A Normalização da escala é feita calculando a distância entre os olhos e escalar todos os pontos do modelo de forma que esta distância seja igual a 1.

A Compensação de rotações é feita calculando o ângulo da linha que une os olhos e a horizontal e realizar uma rotação de todos os pontos do modelo, de modo que os olhos fiquem na mesma altura.

Na análise da tecnologia de reconhecimento facial em 3D, verifica-se que a pessoa não precisa colaborar e se posicionar frontalmente para a camera de vídeo no momento da captura da imagem da face, pois a tecnologia consegue a partir de uma imagem, rotacioná-la, o que permite uma análise mesmo que a pessoa levante o queixo, ou abaixe a cabeça ou não olhe diretamente para a camera de vídeo. Um outro fator, é que o excesso ou a falta de iluminação não prejudica a tecnologia, os sensores de infravermelho acopladoas à camera de vídeo conseguem capturar a imagem mesmo em ambientes escuros.

A técnica de *eigenfaces* aplicada ao reconhecimento de faces conduz a bons resultados. A taxa de reconhecimento obtida para faces frontais, com ligeiras variações de expressão e de pose, está sempre acima dos 84%, mas ainda longe dos 100% desejável, para ser utilizado num sistema de reconhecimento de faces de pessoas.

A técnica de reconhecimento em 3D necessita de um maior processamento computacional em função da rotação e translação das imagens da face no espaço x-y-z, mas em compensação é mais eficiente e seguro do que o reconhecimento em 2D.

A taxa de reconhecimento obtida para o reconhecimento de faces frontais, com ligeiras variações de expressão e de pose, está muito próxima dos 100%, desejável para o sistema de reconhecimento de pessoas.

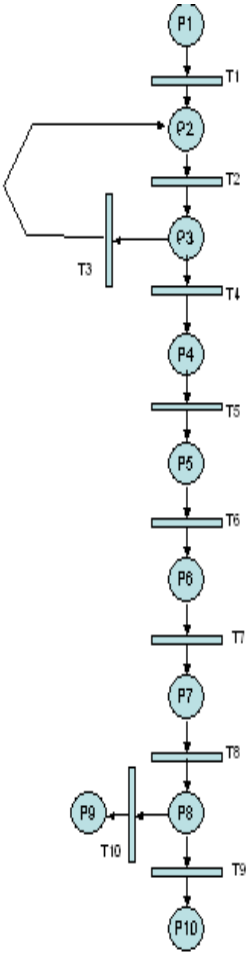


Figura 5: Simulação do Software de Reconhecimento Facial em 3D
Fonte: elaborada pelo autor

A Figura 5 representa a modelagem e simulação do software de reconhecimento facial em 3D, utilizando a Teoria das Redes de Petri (BROSSO et al, 2002), onde os lugares são representados por um círculo e as transições são representadas por retângulos, arcos conectam os lugares e as transições, conforme descrição dos mesmos na tabela abaixo.

Tabela 1: Descrição de lugares e transições da Rede de Petri

Lugares	Transições
P1.Usuário aproxima a face.	T1.Detecção do usuário OK
P2.O projetor dispara uma luz infravermelha estruturada para o teste padrão	T2.Disparo Efetuado.
P3.Câmera captura no mínimo detalhe a distorção da luz infravermelho do teste padrão.	T2.Captura OK.
P4.Utiliza a distorção da luz para calcular todos os pontos provados na superfície por meio de triangulação (3 coordenadas).	T4.Cálculos OK.
P5.Cria um molde através do entrelaçamento dos pontos calculados.	T5.Montagem OK.
P6.Calcula a sobreposição da Textura.	T6.Textura OK.
P7.Criação do molde Biométrico e armazenamento do molde numérico em um BD ordinário.	T7.Criação e armazenamento OK.
P8.Comparação do molde com um BD de Registro.	T8.Comparação OK.
P9.Usuário não cadastrado.Sai do processo.	T9.Usuário não cadastrado (Sem Acesso).
P10.Usuário reconhecido.	T10. Captura com erro ou Não efetuada

Fonte: Elaborada pelo autor.

A Tabela 1 descreve os lugares e transições da Rede de Petri da Figura 5 e indica a modelagem de um software de tecnologia de reconhecimento facial em 3D, onde são relacionados nos círculos, os lugares em que ocorre uma atividade e nos retângulas, as transições que representam os eventos que ocorrem no sistema.

3.4 Contextualização

Nos sistemas de segurança tradicionais há necessidade de validar um código de acesso com uma senha, ou uma impressão digital com uma foto da face, ou uma senha com o reconhecimento de voz, entre outras, ou seja, há necessidade de uma técnica complementar a outra para dar robustez ao sistema, pois individualmente elas apresentam incertezas como falso positivo e falso negativo (DEBAR, 1998).

Uma forma equivocada de utilização da tecnologia de reconhecimento facial em projetos de controle de acesso, em geral, é a utilização da face como chave de identificação e senha de acesso; isto pode provocar vulnerabilidades, pois a face do usuário é pública dando margens a fraudes (ASHBOURN, 2000).

A tecnologia de reconhecimento facial permite que se capture imagens da face da pessoa por câmeras de vídeo dispostas no ambiente e, portanto, as pessoas podem ser identificadas mesmo que não colaborem com a tecnologia, ou seja, apenas permanecendo ou caminhando pelo ambiente onde haja câmeras de vídeo e/ou sensores, sem precisar se posicionar em frente a uma câmera para ser identificada (KIM, 2002).

Apesar de toda evolução ela permite um índice de acerto no reconhecimento na faixa de 97%, daí a necessidade de combiná-la com outras tecnologias para dar robustez à solução.

Com a evolução das câmeras de vídeo com sensores de infravermelho, presentes no ambiente, a tecnologia de reconhecimento facial consegue manipular as informações das faces das pessoas, de modo não invasivo, o tempo todo e em todos os lugares (ZHANG et al., 2002). E com isto novas aplicações surgem para a tecnologia de reconhecimento facial, como sistemas de monitoramento de pessoas, de multidões, de ambientes e a possibilidade de numa imagem do ambiente extrair várias faces e identificá-las individualmente.

Para uma melhor definição do mecanismo de análise comportamental na autenticação de usuários foram feitos vários testes com a tecnologia de reconhecimento facial em 2D, que apesar de não ter segurança na identificação e autenticação, colaborou com a evolução da proposta do Sistema KUCAS.

Houve um teste em 2002 com o software de reconhecimento facial Bastet em 2D (SANDMANN, 2002), desenvolvido pela autora desta tese juntamente com alunos do Centro Universitário da FEI, onde foi possível perceber a importância da iluminação e da qualidade da imagem nesta tecnologia, o que ajudou na melhoria do Sistema KUCAS.

Foram elaborados vários testes com a tecnologia de reconhecimento facial em 2D e em 3D.

Abaixo são descritos alguns problemas encontrados pela autora desta tese na utilização da tecnologia de reconhecimento facial tanto em 2D como em 3D.

1) problemas com as câmeras de vídeo: as câmeras de vídeo disponibilizadas no mercado em geral são para vigilância, as quais não possuem a mesma definição de imagens que as câmeras apropriadas para a tecnologia de reconhecimento facial; o ideal são câmeras que tenham filtros e detectores de face.

2) problemas com iluminação no ambiente: em geral são instaladas soluções de reconhecimento facial em portarias de prédios e condomínios, sendo que nestes lugares há muita luminosidade que podem vir de janelas, portas de vidro, paredes espelhadas o que dificulta a captura das imagens da face; o ambiente de captura da imagem da face deve ter um fundo neutro ou opaco, para que a luminosidade não interfira no sistema.

3) aumento excessivo das bases de dados e dificuldades em administrar esse volume de imagens e informações; é necessário estipular limpezas periódicas ou salvar em outro banco de dados as imagens que são menos acessadas.

4) mudanças de equipamentos em geral causam transtôrnos; principalmente quando há necessidade de migrar bases de dados de imagens para outros lugares; e em geral é muito lento.

5) mudanças de sistema operacional devem ser bem monitoradas para evitar falhas no sistema de reconhecimento facial;

6) as variações de expressão da face da pessoa: este talvez seja um dos mais sérios problemas, pois em geral, as pessoas não se sentem à vontade frente a uma tecnologia que elas não conhecem.

7) durante a captura da imagem: a pessoa deve colaborar e se posicionar frontalmente para a câmera de vídeo e evitar mudanças bruscas nas expressões faciais no momento da captura da imagem.

Se as condições ideais não são atendidas, a tecnologia de reconhecimento facial em 2D se torna inviável, pois é quase impossível desejar que as pessoas estejam sempre com a mesma expressão facial, neutra; o fato da pessoa desviar o olhar um pouco para baixo, ou para cima, já é suficiente para não ser encontrada no banco de imagens, o que pode resultar na demora, pois é necessário um novo cadastramento e haverá aumento da base de dados, o que com o tempo vai degradando o sistema.

Nos testes com a tecnologia de reconhecimento facial em 3D os problemas se resumem aos da câmera de vídeo e do volume de informações geradas, uma vez que a incidência de falso positivo e falso negativo é muito reduzida.

Numa análise pragmática, a tecnologia de reconhecimneto facial é uma tecnologia ciente de contexto pois é possível a indexação das dimensões contextuais do ambiente, por exemplo, a dimensão who indica o usuário que terá a imagem da face capturada, a where a localização, a when a indicação de data e hora, a what a própria imagem da face do usuário e a why um processo repetivo de intenções de captura de imagens da face.

Nesta visão é possível aumentar a estrutura de variáveis e inserir a tecnologia de reconheciemento facial na estrutura de um sistema de autenticação contínua de usuário, com a missão de prestação de serviços.

4 Comportamento Humano

4.1 Introdução

Este capítulo apresenta uma abordagem sobre o comportamento humano do ponto de vista da psicologia para se obter subsídios para a análise comportamental de usuários, como base para a autenticação.

Nos capítulos anteriores foram analisadas a computação ciente de contexto e a tecnologia de reconhecimento facial. O objetivo da associação dos dois temas com a abordagem do comportamento humano é justificar a influência do comportamento do usuário nas dimensões contextuais da computação ciente de contexto e fazer uma integração com a missão de prestação de serviços da tecnologia de reconhecimento facial.

4.2 O Comportamento Humano

Na década de 30, no século XX, Skinner (1967), realizando experiências com ratos e pombos, propôs o estudo comportamental de organismos vivos a fim de descrever as leis que regem o comportamento de qualquer outro organismo, incluindo o homem. O que diferenciou sua proposta da outros cientistas foi um conjunto de procedimentos e de noções que ficou mais tarde conhecido como Análise Experimental do Comportamento (AEC).

Uma das principais inovações conceituais de Skinner está na noção de comportamento operante, que se distingue daquela de comportamento respondente. Para Skinner, o comportamento operante é emitido pelo organismo, e não produzido pelo ambiente, e o que modela o comportamento são suas conseqüências reforçadoras.

O behavorismo radical de Skinner analisa um comportamento que pode ser controlado por regras e faz um controle e uma análise de variáveis que podem vir a influenciar no

comportamento humano; de modo análogo, ao comportamento do usuário ao utilizar uma aplicação de software e interagir com um dispositivo eletro-eletrônico.

As evidências do Comportamento Humano são dados obtidos das medições das ações comportamentais de uma pessoa de forma que a ação possa ser medida no começo, meio e fim; a análise comportamental de pessoas é a base da psicologia comportamental, uma vez que é possível prever o comportamento das pessoas a partir da analise dos antecedentes do momento que ocorrem as mudanças.

O comportamento humano é um processo e como tal pode ser observado; ocorre dentro de uma margem de erro com probabilidade previsível.

A análise científica do comportamento começa pelo conhecimento e isolamento das partes de um evento, para determinar as características e as dimensões da ocasião em que o comportamento ocorre, e definir as mudanças produzidas em respostas ao ambiente, espaço, tempo e oportunidades.

Um evento comportamental inclui os estímulos anteriores a resposta, a própria resposta, o próprio comportamento e as conseqüências desta resposta sobre o comportamento futuro.

A causa de um comportamento não é necessariamente imediata, mas pode ser descrita, é mensurável, observável e perceptível através de instrumentos de medida (SKINNER, 1995).

Como a análise comportamental enfatiza implicações empíricas, é necessário avaliar todas as suposições e definir as respostas que compõe o comportamento e como elas estão relacionadas com o ambiente em que ocorre.

Em termos comportamentais, é possível estabelecer a ocorrência futura do comportamento desde que mantidas as condições estimuladoras que garantem que o comportamento a ser emitido será adequadamente reforçado.

Assim, pode-se dizer que o ambiente, o espaço virtual e o espaço físico estabelecem as condições para o comportamento ocorrer.

Quando o organismo responde a um estímulo ambiental e as conseqüências de sua resposta são premiadas, isso faz aumentar a probabilidade de respostas similares; quando as conseqüências são punitivas, diminui tal probabilidade. É deste modo que as variáveis ambientais modelam o comportamento dos indivíduos, num processo de condicionamento operante.

O conceito-chave do pensamento de Skinner é o de condicionamento operante, que é um mecanismo que premia uma determinada resposta de um indivíduo até ele ficar condicionado a associar a necessidade à ação.

Para Skinner (1967) no comportamento operante, o ambiente é modificado e produz conseqüências que agem de novo sobre ele, alterando a probabilidade de ocorrência futura semelhante.

Um comportamento operante não tem a mesma precisão de resposta, por ter também que pensar em uma atitude econômica, o ser humano sempre prefere a resposta mais simples, sempre a mesma resposta, e o comportamento operante tem uma economia de resposta.

Skinner (1967) descreve o comportamento observável, ou seja, o que é sentido e visto, sendo referência para o comportamento passado e as condições que o afetaram e as condições relacionadas com o comportamento futuro. O comportamento é uma interação entre indivíduo e ambiente, e é condicionante, ou seja, o comportamento tende a se repetir em situações semelhantes.

A unidade básica de análise do comportamento é a contingência das interações entre um organismo e seu meio ambiente, e para ser adequada, deve sempre especificar a "situação" em que o comportamento ou resposta ocorreu, a "resposta" e as "conseqüências" de tal resposta. As relações entre estes três aspectos "situação", "resposta" e "conseqüência"

constituem as contingências de reforço e a veracidade de um fato depende de concordância. O controle adequado do ambiente e a observação do comportamento das pessoas resultante no ambiente explicam a conduta das pessoas (SKINNER,1995).

Skinner defendeu a observação sistemática das contingências ambientais como base para demonstrar o controle experimental do comportamento.

Segundo Pettenger e Gooding (1977) existem várias outras linhas de pesquisa em psicologia comportamentais, sendo que as variáveis comportamentais variaram de uma linha para outra; conforme estudo preliminar, para esta pesquisa em psicologia que atenda a um sistema de autenticação contínua são sugeridos os pesquisadores abaixo.

Holland, um seguidor de Skinner, não obstante suas especificidades, diz que os comportamentos respondentes e operantes são controlados por eventos ou estímulos do ambiente em que o individuo está inserido (Witter (2005).

Staats diz que o comportamento de uma pessoa é baseado em princípios de aprendizagem estabelecidos em laboratório (STAATS, 1973).

Bandura situou os princípios de modificação de comportamento dentro da aprendizagem social, e como os processos de modificação do comportamento são afetados pelas respostas anteriores, as quais assumem o papel de estímulos e afeta a resposta (BANDURA, 1969).

Sidman dando continuidade aos estudos de Skinner faz um aprofundamento do estudo do aprendizado por regras. Isto depende da estrutura e do balanceamento das tentativas de teste, indicam ainda que as relações estabelecidas no treino e as emergentes podem ficar sob controle de estímulos contextuais presentes na situação de teste (SIDMAN, 1998).

Para Witter (2005) as variáveis ambientais interferem no comportamento da pessoa, o qual tende a se repetir, quando a pessoa vivencia condições ambientais já vividas e que deram a elas alguma vantagem.

Skinner indica variáveis comportamentais que associadas com as definições das dimensões contextuais da computação ciente de contexto garantem uma análise mais eficiente do comportamento do usuário; basicamente, o que interessa é a observação e o registro de uma única resposta, a qual pode produzir uma mudança no ambiente.

O dado básico, portanto, é a freqüência de resposta de um único usuário e a noção fundamental de que o comportamento não se encontra nem no usuário, nem fora deste, e sim na interação entre usuário e ambiente.

4.3 Análise Comportamental de usuário e a autenticação

A análise comportamental de pessoas é uma área muito ampla, este trabalho se restringe a utilizá-la para solucionar problemas de segurança na identificação da pessoa ao utilizar uma aplicação de software e sua aplicação na definição de uma política de segurança maleável e adaptativa ao usuário.

A análise comportamental de pessoas na computação ciente de contexto é baseada em mudanças significativas e transformações de processos no comportamento das pessoas, utiliza a investigação do conhecimento: de onde vem, como é armazenado, como se recupera dados de conhecimento, como o conhecimento pode ser perdido, as quais podem ser definidas como variáveis comportamentais; e utiliza-se métodos empíricos para efetuar a análise.

Em Abowd, Mynat (2000) e em Abowd et al. (2002), a captura e controle de atividades humanas é responsável pelo desenvolvimento de aplicações capazes de preservar a gravação de alguma experiência cotidiana para acesso futuro.

Sistemas que utilizam as informações de contexto dos usuários para descoberta de conhecimento se resumem em mecanismos para que o usuário possa dar seu consentimento, com relação ao uso de informação gerada por ele mesmo.

No ambiente da computação ciente de contexto, os eventos do comportamento de uma pessoa no ciberespaço, armazenados no *log*, não guardam relação entre si, e por isto devem ser isolados, pois geram muitas informações, algumas redundantes.

A análise comportamental faz parte de qualquer esforço multidisciplinar para compreender o comportamento humano e é a base do comportamento ao longo da história de vida das pessoas, as pessoas nascem com necessidades de base biológica, e aprendem outras necessidades sob a forma de motivação, e utiliza freqüentemente métodos quantitativos e qualitativos para saber se estimulo está funcionando (WITTER,2005).

4.4 Análise Comportamental

O enfoque da AEC (Análise Experimental Comportamental) proposto por Skinner implica na elaboração da análise comportamental em várias etapas para se conhecer efetivamente o comportamento da pessoa.

1. definir operacionalmente o comportamento alvo a ser analisado, medir a freqüência com que ele ocorre.

2. observar o comportamento em termos da tríplice contingência que é a expressão usada para dizer que vai observar o contexto, a resposta e a conseqüência.

3. registrar a taxa de ocorrência do comportamento (freqüência) em outras medidas de ocorrência do comportamento ao longo do processo.

4. se for o caso, introduzir a variável experimental. (No sistema KUCAS isto é aplicado quando se deseja introduzir uma nova ferramenta para o usuário, como por exemplo, um código novo no acesso).

5. comparar a freqüência do comportamento antes e depois da introdução da variável experimental ou de ocorrência de resposta.

A quantidade de informações produzidas pelas pessoas ao utilizar a tecnologia versus a capacidade de armazenamento dos recursos computacionais tem impulsionado o desenvolvimento de tecnologias capazes de tratar estes dados, transformá-los em informações úteis e extrair conhecimentos sobre o comportamento das pessoas. Desde os anos 60 do século

XX a AEC recorre a computadores e equipamentos eletrônicos especialmente criados para estudos específicos do comportamento a ser observado.

4.5 Contextualização

A computação ciente de contexto, a tecnologia de reconhecimento facial e a análise comportamental promovem a interação entre pessoas, muitas das informações são trocadas de forma implícita. Expressões faciais, gestos e tonalidade de voz podem ser utilizados para auxiliar a comunicação entre as pessoas envolvidas na interação. No entanto, na interação usuário-computador raramente há o compartilhamento de informações de contexto devido ao uso de dispositivos tradicionais de interação como o teclado, mouse, sensores e câmeras de vídeo.

Aplicações cientes de contexto devem ser capazes de adquirir informações de contexto de modo automatizado, disponibilizando-as em um ambiente computacional em tempo de execução. Estas informações são a base do comportamento do usuário.

O comportamento é baseado em informações contextuais, baseado no histórico comportamental anterior, estória anterior de reforço do comportamento e o comportamento imediato da pessoa ao interagir com uma aplicação de software e o ambiente.

No processo proposto de autenticação contínua do usuário, é utilizado conjuntamente, com a análise comportamental do usuário, a tecnologia de reconhecimento facial para a captura da imagem da face do usuário e as informações de contexto do ambiente.

5 Sistema de Autenticação Contínua de Usuários Conhecidos

Known User Continuous Authentication System – (**KUCAS)**

5.1 Introdução

O sistema KUCAS (*Known User Continuous Authentication System*) é um sistema de autenticação contínua de usuários conhecidos, destinado a sistemas cientes de contexto e baseado na análise comportamental do usuário, em suas características biométricas e na confiança, um conceito que os seres humanos adotam para atribuir crédito a uma pessoa, de acordo com o seu comportamento. A confiança em uma pessoa pode variar ao longo do tempo de acordo com o seu comportamento. Indícios de faltas ou restrições no comportamento resultam no aumento ou redução do nível de confiança previamente estabelecida.

O Sistema KUCAS é integrado com o usuário, a tecnologia e o tempo, recebendo eventos e informações através de sensores e dispositivos de controle dispostos no ambiente.

Abaixo estão relacionadas algumas definições que sustentam o Sistema KUCAS.

Usuário: é uma pessoa autenticada que possui acesso às aplicações de software num domínio específico nas redes de computadores com e sem fio.

Contexto: Contexto é qualquer informação que possa ser usada para caracterizar a situação do ambiente e do usuário.

Ambiente: É o ambiente tecnológico, a infra-estrutura necessária, num domínio específico nas redes de computadores com e sem fio, da Computação Ciente de Contexto. É onde se deseja capturar as informações do comportamento dos usuários ao interagir com aplicações de software.

Intervalo de tempo: é o intervalo de tempo desde o tempo inicial em que o usuário faz a identificação de acesso numa aplicação de software até o tempo final em que ele encerra a aplicação. Costuma ser chamado de sessão.

Comportamento: O comportamento é o conjunto de respostas que viabilizam a intenção entre uma pessoa e o ambiente tecnológico, ou seja, são as ações que o usuário efetua ao interagir com as aplicações de software e o ambiente tecnológico das redes de computadores.

Confiança: conceito atribuído ao usuário, e que pode variar de acordo com a análise comportamental do mesmo. Baseando-se nas evidências do comportamento do usuário é possível compor a confiança atribuída a ele.

Restrição de confiança: são comportamentos do usuário que foge da normalidade do mesmo. Uma restrição pode ser uma seqüência de transações não recomendadas, um valor diferente do usual, um lugar, um horário, etc. A restrição de confiança é a base da política de segurança adaptativa ao usuário.

Tecnologia do Reconhecimento Facial: Tecnologia utilizada para capturar, identificar e reconhecer imagens da face do usuário. A tecnologia de reconhecimento facial é um mecanismo biométrico que é acionado por meio de sensores no ambiente, é acionado no primeiro acesso do usuário ao sistema KUCAS e toda vez que o usuário tiver um comportamento fora da normalidade, ou fizer algo considerado restrição de confiança.

Análise Comportamental do usuário: é feita tendo por base as informações do ambiente, as respostas que integram o comportamento do usuário e as conseqüências do mesmo.

A característica do comportamento, da confiança e das restrições de confiança são elementos da "política de segurança" imposta pelo sistema.

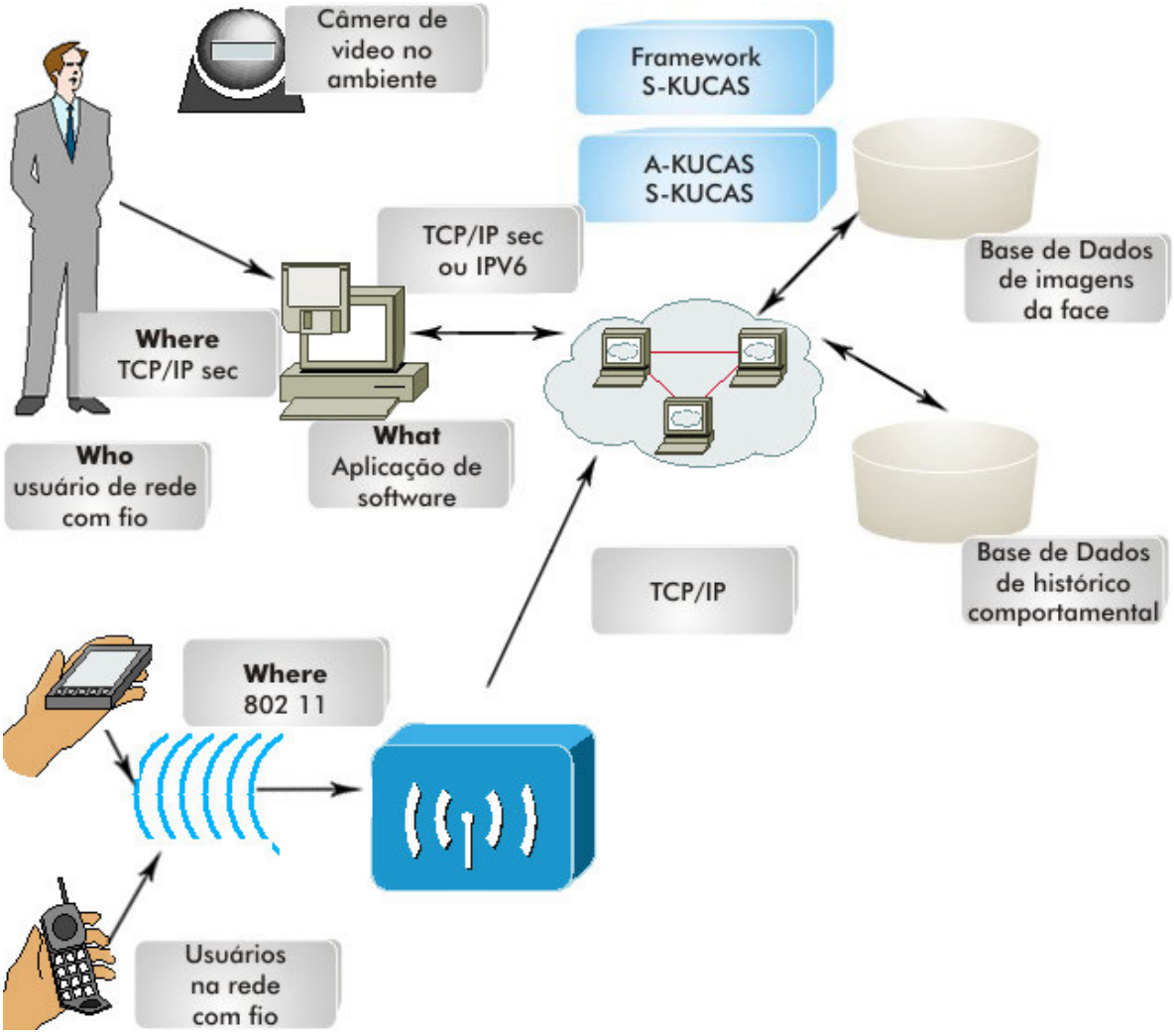


Figura 6: Visão do Sistema KUCAS
Fonte: elaborada pelo autor

A Figura 6 representa uma visão do sistema KUCAS; o usuário acessa uma aplicação de software na rede com ou sem fio, o sistema KUCAS é acionado e captura as informações do comportamento do usuário no ambiente por meio do framework F-KUCAS, o qual aciona o algoritmo A-KUCAS e o módulo de segurança S-KUCAS; conforme vai aumentado a interação do usuário com o ambiente o sistema KUCAS vai variando o nível inicial de confiança inicial atribuído ao usuário. Câmeras de vídeo no ambiente capturam as imagens da face dos usuários quando houver uma mudança comportamental do usuário ou se o comportamento atingir uma restrição de confiança imposta pelo sistema.

O sistema KUCAS possui três etapas distintas: etapa de captura das informações comportamentais do usuário no contexto do ambiente, etapa de análise comportamental do usuário e etapa de atribuição de confiança.

Cada etapa forma a estrutura do sistema KUCAS, que é descrita a seguir.

5.2 Estrutura do Sistema KUCAS

A captura de informações comportamentais do usuário no contexto do ambiente é feita a partir do momento em que o usuário se identifica e acessa uma aplicação de software até o momento em que ele encerra a mesma. As informações do usuário são capturadas utilizando-se o conceito das variáveis contextuais definidas na Computação Ciente de Contexto, citadas no capítulo 2, as quais são armazenadas em bancos de dados de históricos comportamentais. As informações obtidas são as evidências do comportamento do usuário.

A análise comportamental é baseada nas evidências do comportamento do usuário e na comparação com as informações armazenadas nas bases de históricos comportamentais do mesmo. A análise comportamental possui duas fases, a primeira é a comparação das informações obtidas no momento em que o usuário interage com a aplicação de software, com as informações comportamentais do histórico; a segunda fase é a verificação da existência ou não de restrições comportamentais que possam colaborar com a análise e permitir ou não a autenticação do usuário. A análise comportamental no sistema KUCAS baseia-se nas teorias comportamentais de Skinner, conforme estudo apresentado no capítulo 4.

A atribuição da confiança também possui duas etapas:

Na primeira vez, o sistema KUCAS, por não ter informações comportamentais suficientes, aciona a tecnologia de reconhecimento facial, captura imagens da face do usuário e as armazena nas bases de dados de históricos da face, contabiliza o comportamento na base

de históricos comportamentais e dá uma confiança mínima para que o usuário possa efetuar as transações de software, ao final contabiliza e armazenas as informações capturadas.

Na segunda etapa, ou seja, nos acessos subseqüentes ao sistema, e com o aumento da interação com o usuário, é feito primeiro uma consulta nas bases de dados de restrições de confiança, não havendo restrições é feita a captura de informações nas bases de históricos comportamentais, havendo mudanças no comportamento, a tecnologia de reconhecimento facial é acionada; se a face do usuário já estiver cadastrada e for identificada, é feito o armazenamento dos dados comportamentais, a confiança é recalculada e novas imagens da face são armazenadas; se a face do usuário não estiver cadastrada nas bases de dados de imagens, mecanismos de segurança são acionados.

Com o aumento das informações comportamentais, subsídios para uma análise das evidências do comportamento mais eficiente vão sendo gerados, e o sistema KUCAS continua efetuando a análise das evidências comportamentais e aumentando a confiança.

Se houver um comportamento que é uma restrição de confiança, a tecnologia de reconhecimento facial é acionada e a confiança recalculada.

Se houver mudança comportamental, a tecnologia de reconhecimento facial é acionada e a confiança recalculada.

Enquanto não houver mudança comportamental, o sistema não aciona a tecnologia de reconhecimento facial, apenas efetua a análise das evidências comportamentais e mantém a confiança.

Caso haja alteração comportamental, o sistema aciona a tecnologia de reconhecimento facial, caso o usuário não for identificado, o sistema aciona mecanismos de segurança.

Caso haja alteração comportamental, o sistema aciona a tecnologia de reconhecimento facial, se o usuário for identificando, o sistema recalcula a confiança e procede ao armazenamento das informações comportamentais e das imagens da face.

Atingindo um nível de confiança necessária, a tecnologia de reconhecimento facial deixa de ser utilizada, ou seja, é possível autenticar um usuário sem a verificação da face.

O Sistema KUCAS possui dois tipos diferentes de autenticação:

1. **Autenticação inicial**: a pessoa informa o código de acesso e a senha com a qual tem acesso às aplicações de software no Sistema KUCAS.

2. **Autenticação contínua**: garante a autenticidade da pessoa durante a comunicação e ao longo do processamento da aplicação de software; o sistema consulta as bases de dados periodicamente, sem a necessidade de um pedido de confirmação de autenticação, tudo é feito de forma ubíqua; uma autenticação contínua que se prolonga durante o intervalo de tempo em que o usuário interage com a aplicação de software.

5.3 Captura das informações comportamentais

A captura das informações comportamentais do usuário se dá a partir do momento em que o usuário se identifica por meio de um código de acesso e senha, seleciona a aplicação de software desejada e começa a interagir com o sistema. O usuário deve ser conhecido, ou seja, possuir um código de acesso e senha e ter sido previamente cadastrado para acesso à aplicação de software.

5.3.1 Definição das variáveis comportamentais

Para se obter informações comportamentais do usuário utiliza-se uma categorização de dimensão de contexto que define algumas variáveis, conforme citado no capítulo 2, que auxiliam na captura das informações comportamentais do usuário. As dimensões contextuais a serem consideradas são aqui denominadas de variáveis comportamentais de contexto, com as quais deve-se capturar o máximo de informações do usuário e em torno dele, no ambiente.

• **Who** (quem): Indica a dimensão de contexto de identificação de uma pessoa; pode se incorporar á informação referente a outras pessoas, também presentes no ambiente;

• **Where** (onde): Indica a dimensão de contexto de localização, ou seja, a localização da pessoa e dos dispositivos de hardware que estão sendo utilizados por ele. Na Computação Ciente de Contexto esta dimensão é muito utilizada em associação com a dimensão de identidade (who) e a temporal (when) com o intuito de prover informações sobre a localização e a identidade da pessoa em um determinado tempo;

• **When** (quando): Indica a dimensão de contexto temporal para indexação de registros capturados ou para informar a duração de tempo em que uma pessoa permanece em um determinado local;

• **What** (o quê): Indica a dimensão de contexto responsável por identificar a atividade do usuário no momento. Dispositivos cientes de contexto devem suportar interpretações de atividades humanas.

• **Why** (por que): Indica qual a intenção do usuário. Esta dimensão é muito complexa para ser obtida do ambiente. No sistema KUCAS, ela pode ser obtida por meio da análise comportamental do usuário, em interações que se caracterizarem como hábito do usuário.

No capítulo 2 desta tese é apresentada a dimensão de contexto How (como), mas ela possui um alto grau de complexidade para o sistema KUCAS na forma atual, é necessário que ele evolua mais para responder a esta dimensão no que se refere à análise comportamental.

As informações das dimensões contextuais serão agregadas a outras variáveis obtidas conforme o tipo da aplicação de *software* que o usuário utiliza e qual o momento de autenticação em que o usuário se encontra.

As variáveis comportamentais são as informações que se obtém ao longo do tempo em que o usuário está acessando uma transação de software. Essas informações já existem muitas vezes nos sistemas tradicionais sendo conhecidos como registros de Log.

A captura das informações comportamentais e análise do comportamento são feitas em tempo real.

5.3.1.1 Variável who

O primeiro passo é identificar o usuário e definir as variáveis e premissas que serão usadas na investigação das evidências do comportamento do usuário.

O Sistema KUCAS adota a variável de contexto **who** para a identificação do usuário.

Deve haver um código de usuário para identificação e uma senha para autenticação. A informação é obtida no momento inicial em que o usuário se identifica no acesso à aplicação de software.

Neste momento, a aplicação chama a API de comunicação do sistema KUCAS, a qual faz a ligação entre a aplicação e o framework F-KUCAS.

A identificação do usuário é feita através da aplicação, onde ele informa um código de usuário e a autenticação e feita através de sua senha. O usuário pode fornecer outras informações durante a interação com o sistema, mas as principais informações são obtidas através de consulta ao cadastro de usuários, tais como idade, endereço, nível de escolaridade.

A variável **who** é o conjunto de informações do usuário que utiliza uma aplicação de software.

who = Ui sendo i o índice da ocorrência de comportamento.

O sistema KUCAS foi modelado com a UML (Unified Modeling Language) (FOWLER, 2000) tanto para fazer a representação das classes das variáveis comportamentais, como para a definição das suas funcionalidades e arquitetura.

Por definição a variável **who** é denominada classe de usuários. A classe de usuários está associada com outras variáveis, agrupadas em duas classes, a classe **conf** e a classe **imag**.

A classe **conf** é a classe das variáveis comportamentais "nível de confiança" atribuída ao usuário e classe **imag** é a classe das variáveis "imagem da face" do usuário.

As classes de variáveis **who, conf e imag** conferem a identificação do usuário.

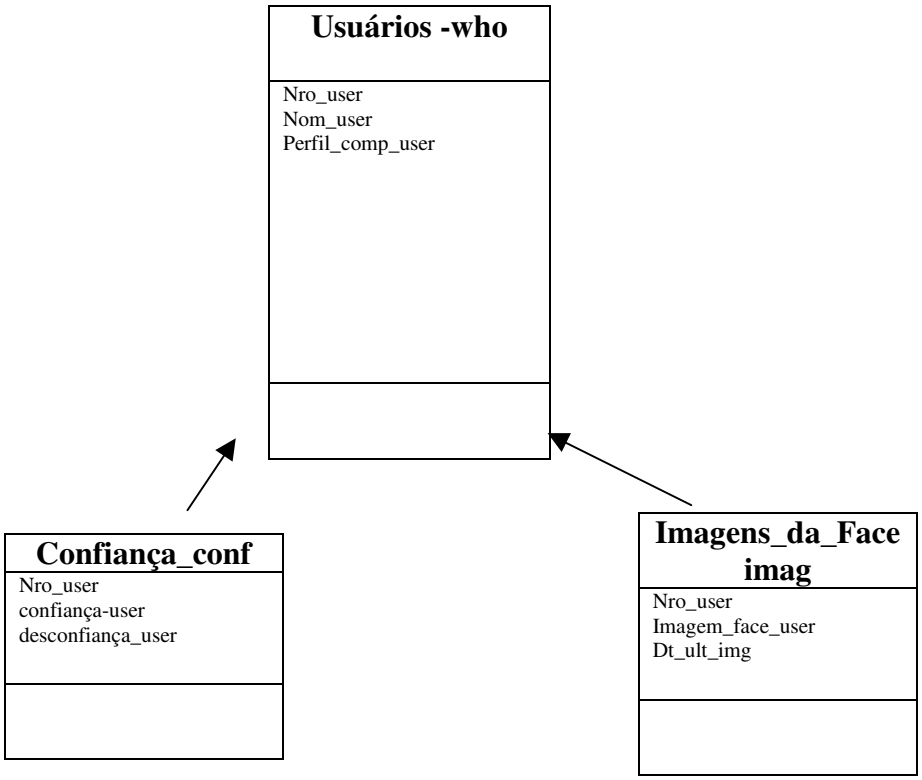


Figura 7: Diagrama de Classes da Variável who
Fonte: elaborada pelo autor

A Figura 7 representa o diagrama de classe da variável de identificação **who**, ou seja, de associação das classes **who, conf** e **imag.** A classe usuário se associa com a classe Imagens_da_face e com a classe Confiança_conf, as quais contém informações sobre a imagem da face do usuário e o nível de confiança atribuído a ele, respectivamente.

Do ponto de vista de modelo, a variável **who** pode conter todas essas informações, mas não deve ser esquecido que existe o cadastro de usuários feito previamente que contém informações pessoais, as quais não são indicadas aqui para não haver duplicação de dados.

As variáveis nomeadas para atender a classe de usuários **who** estão definidas na Tabela 2.

Tabela 2: Variáveis da classe de usuários who

Nome da variável	Descrição da variável
nro_user	Chave de identificação do usuário
nom_user	Nome do usuário
perfil_comp_user	Nível de confiança atribuída ao usuário
imagem_face_user	Imagem da face do usuário
dt_ult_img	Data da última captura da imagem da face
confiança-user	Nível de confiança atribuído ao usuário
desconfiança_user	Nível de desconfiança atribuído ao usuário

Fonte: Elaborada pelo autor.

A Tabela 2 representa o contexto da identificação do usuário; através das variáveis apresentadas é possível identificar o nível de confiança atribuído ao usuário, a imagem de sua face e data da última captura da imagem da face.

5.3.1.2 Variável where

A variável comportamental **where** é denominada classe de localização e fornece o endereço dos equipamentos e periféricos no qual o usuário está executando uma aplicação de software.

where = Li sendo i o índice da ocorrência de comportamento.

Figura 8: Diagrama de classes da variável de localização where
Fonte: elaborada pelo autor

As variáveis nomeadas para atender a classe de localização where estão definidas na tabela abaixo:

Tabela 3: Variáveis da classe de localização where

Nome da variável	Descrição da variável
Cod_Disp	Código do equipamento ou periférico ou dispositivo onde aplicação de software está sendo executada pelo usuário
End_local	Endereço do equipamento
Bairro_local	Bairro
CEP_local	Código de Endereçamento Postal
Cidade-local	Cidade
País_local	País
Nro_seq-local	Número seqüencial que indica quantas vezes o equipamento foi utilizado pelo usuário neste local.
Coord-GPS	Coordenada de localização GPS

Fonte: Elaborada pelo autor.

A Tabela 3 representa o contexto da localização do equipamento ou periférico que o usuário utiliza, através das variáveis apresentadas é possível identificar o local onde o usuário utilizou a transação de software e se está ou não nas proximidades de seu endereço informado na variável **who**.

5.3.1.3 Variável when

A variável comportamental **when** é denominada classe temporal e representa os horários de início e fim em que o usuário interage com a aplicação de software.

when = Ti sendo i o índice da ocorrência de comportamento.

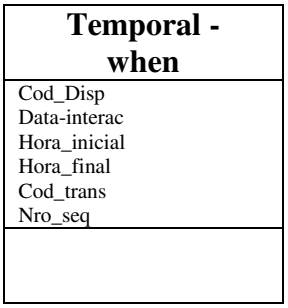


Figura 9: Diagrama de classes da variável temporal when
Fonte: elaborada pelo autor

As variáveis que compõem a classe da variável temporal **when** estão definidas na tabela abaixo:

Tabela 4: Variáveis da classe temporal when

Nome da variável	Descrição da variável
cod_disp	Código do dispositivo ou equipamento
data_interac	Data da interação do usuário com a aplicação de software
hora_inicial	Hora inicial da utilização
hora_final	Data final da utilização
cod_trans	Código da transação utilizada (variável do contexto what)
nro_seq	Número seqüencial que indica quantas vezes o equipamento foi utilizado pelo usuário.

Fonte: Elaborada pelo autor.

A Tabela 4 representa as variáveis da classe temporal **when** e a combinação das mesmas permite uma análise dos horários em que o usuário utiliza a aplicação de software,

num determinado dispositivo, num determinado lugar. A combinação de todas estas variáveis permite fazer o cruzamento de várias informações de contexto como, por exemplo, qual o tempo gasto num local e qual o tempo gasto numa aplicação de software.

5.3.1.4 Variável what

A classe de variável comportamental **what** representa a aplicação de software com as quais o usuário interage.

what = Si sendo i o índice da ocorrência de comportamento.

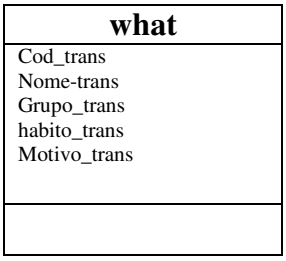


Figura 10: Diagrama de classes da variável transacional what
Fonte: elaborada pelo autor

As variáveis nomeadas para atender a classe transacional, ou seja, as classes de aplicações de software **what** estão definidas na tabela abaixo:

Tabela 5: Variáveis de aplicações de software what

Nome da variável	Descrição da variável
cod_trans	Código da transação de software
nome_trans	Nome da transação de software
grupo_trans	Grupo das transações
nro_seq_trans	Número seqüencial que indica quantas vezes a transação foi utilizada pelo usuário
valor_trans	Valor da transação

Fonte: Elaborada pelo autor.

A Tabela 5 representa o contexto das aplicações de software definidas pela variável **what,** através das variáveis apresentadas é possível identificar qual a aplicação de software utilizada, e o valor da mesma.

5.3.1.5 Variável why

Segundo Witter (2005) o ser humano associa as situações ocorridas com outras semelhantes, generalizando essa aprendizagem, ou seja, as pessoas tendem a repetir o comportamento em situações que se repetem, o que é chamado de intenções ou o hábito.

O hábito ou as intenções que o usuário possui de fazer sempre as mesmas interações com as aplicações de software é representado pela classe de variável comportamental **why.**

why = Ji sendo i o índice da ocorrência de comportamento.

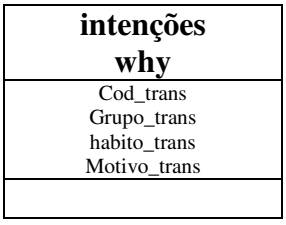


Figura 11: Diagrama de classes da variável de intenções why
Fonte: elaborada pelo autor

As variáveis nomeadas para atender a classe de intenções why estão definidas na tabela abaixo:

Tabela 6: Variáveis da classe de intenções why

Nome da variável	Descrição da variável
Cod_trans	Código da transação de software
Grupo_trans	Grupo das transações
Habito-trans	Habito que o usuário possui de interagir com a aplicação de software
motivo_trans	Motivo da interaçõ

Fonte: Elaborada pelo autor.

A Tabela 6 representa o contexto das intenções do usuário em relação a uma aplicação de software e é definida pela variável why, através das variáveis apresentadas é possível identificar quais as intenções do usuário.

5.3.1.6 Variável rest

Enquanto as variáveis comportamentais who, where, when, what e why representam o comportamento do usuário, é necessário definir a classe de variáveis comportamentais **rest** que representa os comportamentos não aceitáveis, ou seja, restrições de confiança no acesso a aplicações de software. A restrição também pode ser atribuída a uma seqüência de comportamentos que um usuário não pode fazer. A restrição pode ser a lugares onde o usuário não pode acessar a aplicação de software, de horários, de utilização de certos tipos de periféricos ou dispositivos, de limites de valores entre outras, que podem ser definidas pelo sistema ou pelo usuário.

A variável comportamental **rest** representa as restrições comportamentais que um usuário determina ou que o sistema KUCAS pode definir para ele conforme o comportamento.

rest = {Rj, Rj+1, ..., Rn} para $j \geq 0$ sendo j o índice da ocorrência de restrição.

Figura 12: Diagrama de classes da variável de restrições rest
Fonte: elaborada pelo autor

As variáveis nomeadas para atender a classe de restrições comportamentais rest estão definidas na tabela abaixo:

Tabela 7: Variáveis da classe de restrições rest

Nome da variável	Descrição da variável
Cod_rest	Código da transação de software
Cód-user	Grupo das transações
Cod-trans	Habito que o usuário possui de interagir com a aplicação de software
Valor-trans	Motivo da interaçõ
Desc-Rest	Descrição da restrição comportamental

Fonte: Elaborada pelo autor.

A Tabela 7 representa o contexto das restrições comportamentais do usuário em relação a uma aplicação de software e é definida pela variável **rest**, através das variáveis apresentadas é possível identificar as restrições comportamentais do usuário.

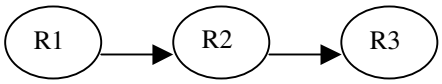


Figura 13: Máquinas de Estados Finitos de Seqüência de Restrições de Confiança
Fonte: elaborada pelo autor

A Figura 13 representa uma máquina de estados finitos de uma seqüência de restrições de confiança, no exemplo, se o usuário fizer um comportamento que represente a R1, em seguida a restrição R2 e em seguida a restrição R3, o sistema KUCAS bloqueia o usuário.

Cada classe de variáveis comportamentais who, where, when, what, why, rest, imag e conf é composta por atributos e operações, sendo que os atributos definem o estado da classe e as operações definem o comportamento das classes.

O cruzamento das informações contidas nestas classes permite efetuar a análise do comportamento do usuário, pois representam a evidência do comportamento dele. Sendo

possível definir quem utilizou determinada aplicação de software, a localidade em que o usuário a utilizou, se está nas proximidades do seu endereço ou distante, qual o horário em que a aplicação foi utilizada e se fazendo uma comparação com as bases de históricos é possível saber se o valor da aplicação está entre os valores normalmente utilizados pelo usuário, permitindo definir restrições comportamentais, bem como, se o usuário já possui algum hábito.

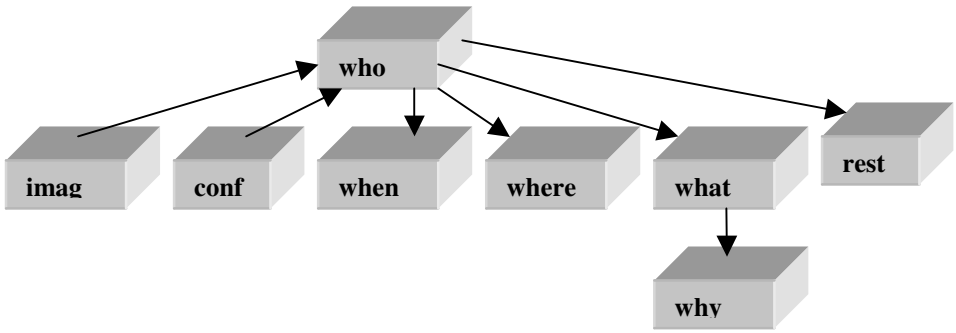


Figura 14: Diagrama das classes das variáveis comportamentais
Fonte: elaborada pelo autor

5.3.1.7 Matriz Comportamental do Usuário

O vetor de variáveis comportamentais do usuário Bi é uma sextúpla definida como:

Bi = {who, where, when, what, why, rest }, onde:

who é a classe de usuários ou conjunto das variáveis comportamentais who;

who = Ui para i = 1 sendo representado pelo conjunto de variáveis de contexto who

U: X → B

Onde X define o domínio de tempo para os instantes de observação (discretos) e

B define o espaço dos comportamentos who de usuários. Assim, dado x ε X então U(x) define o comportamento no instante x.

where é a classe de localização ou conjunto das variáveis comportamentais where;

where = Li para i = 1 sendo representado pelo conjunto de variáveis de contexto where.

U: L → B

Onde X define o domínio de tempo para os instantes de observação (discretos) e

B define o espaço dos comportamentos **where** de usuários. Assim, dado x ε X então L(x) define o comportamento no instante x

when é a classe temporal ou conjunto das variáveis comportamentais when;

when = Ti para i = 1 sendo representado pelo conjunto de variáveis de contexto when.

U: T → B

Onde X define o domínio de tempo para os instantes de observação (discretos) e

B define o espaço dos comportamentos **when** de usuários. Assim, dado x ε X então T(x) define o comportamento no instante x

what é a classe de aplicações de software que o usuário interage ou conjunto das variáveis comportamentais what;

what = Si para i = 1 sendo representado pelo conjunto de variáveis de contexto where.

U: S → B

Onde X define o domínio de tempo para os instantes de observação (discretos) e

B define o espaço dos comportamentos **what** e usuários. Assim, dado x ε X então S(x) define o comportamento no instante x.

why é a classe de intenções do usuário, ou o comportamento que é hábito, ou variáveis comportamentais why;

Sendo que $\mathbf{H(x) = \bar{B}i}$ pode ser o comportamento médio, ou um comportamento que o usuário costuma fazer e que pode ser considerado um hábito.

why = Hi para i = 1, sendo representado pelo conjunto de variáveis de contexto **why**.

U: H → B

Onde X define o domínio de tempo para os instantes de observação (discretos) e

B define o espaço dos comportamentos **why** de usuários

Assim, dado x ε X então H(x) define o comportamento no instante x

rest é a classe de restrições comportamentais do usuário ou variáveis comportamentais rest.

rest = {Ri, Ri+1, ...Rn} para $i \geq 0$, sendo representado pelo conjunto de variáveis de contexto de restrição de confiança.

rest = Ri para i = 1 sendo representado pelo conjunto de variáveis de contexto **rest.**

U: R → B

Onde X define o domínio de tempo para os instantes de observação (discretos) e

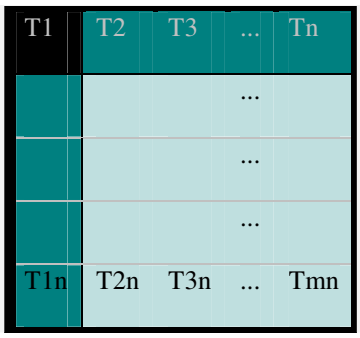
B define o espaço dos comportamentos **rest** de usuários.

Assim, dado x ε X então R(x) define o comportamento no instante x.

$$\mathbf{\Omega\,(x) = \cup\ Bi}$$

De posse de **Ω(x)** que reúne os valores de todas variáveis comportamentais é elaborada a matriz comportamental do usuário.

Tabela 8: Matriz comportamental do usuário

who	where	when	what	why	rest	Confiança	Incer-teza
User1	Local1	Data_hora1			Rest1		

Fonte: Elaborada pelo autor.

A Tabela 8 representa a matriz de variáveis comportamentais do usuário que compõe a base de comportamentos atuais e históricos, na matriz é indicado o usuário, o lugar, o período de tempo, com qual aplicação de software interagiu, se algum comportamento virou hábito (why) e as restrições de confiança que ele já efetuou.

O comportamento é a ação do usuário aos estímulos recebidos, capturar o comportamento significa armazenar as informações das variáveis comportamentais who, where, when, what, why e rest numa estrutura de dados representada pela Matriz comportamental do usuário. Quanto maior for o número de informações capturadas, mais criteriosa será a análise comportamental.

Todo comportamento do usuário é armazenado como um *log*.

A captura do comportamento do usuário ou das variáveis comportamentais do usuário é feita de forma implícita, ou seja, o usuário não sabe, não percebe e não precisa colaborar com a forma como estas informações estão sendo coletadas. A informação é coletada a partir das ações que ele realiza ao acessar aplicações de software nas redes de computadores. Esses acessos podem ser obtidos no arquivo de *log* dos servidores e por meio da monitoração do sistema KUCAS nas bases de histórico de comportamento do usuário.

Na primeira vez que o usuário utiliza o sistema KUCAS, as informações comportamentais são nulas, por isto são consideradas as premissas iniciais, como informações cadastrais previamente adquiridas e as informações de contexto do ambiente, who, where, when, what, as quais serão utilizadas para armazenar as informações do usuário.

O Comportamento do usuário é uma combinatória de n dimensões.

A Matriz comportamental do usuário contém um conjunto de eventos, os quais são manipulados. A análise do comportamento é o resultado das extrações e manipulações destes eventos associados com as restrições comportamentais, num determinado período de tempo $\Delta t = xf - xi$, onde xf é a hora final e xi é a hora inicial da interação com o usuário.

5.4 Analogia entre a teoria comportamental de Skinner

O enfoque da AEC (Análise Comportamental Experimental) proposto por Skinner neste momento é aplicado ao sistema KUCAS para efetiva análise do comportamento do usuário. Conforme etapas a seguir,

1. definir operacionalmente o comportamento alvo a ser analisado, medir a freqüência com que ele ocorre, ou seja, capturar a variável what e comparar com as restrições e as bases de histórico comportamental.

2. observar o comportamento em termos da tríplice contingência que é a expressão usada para dizer que vai observar o contexto, a resposta e o que vai acontecer, ou seja, esperar a ação do usuário na interação com a aplicação de software num determinado período de tempo capturando a informação recebida e aguardando que a aplicação envie estímulos para que o usuário evolua o comportamento.

3. registrar a taxa de ocorrência do comportamento (freqüência) em outras medidas de ocorrência do comportamento ao longo do processo, ou seja, os dados são armazenados na matriz comportamental do usuário.

4. se for o caso, introduzir a variável experimental. (No sistema KUCAS isto é aplicado quando se deseja introduzir uma nova ferramenta para o usuário, como por exemplo, um código novo no acesso). Neste caso não foi definida nenhuma variável experimental que poderia ser um campo novo na aplicação.

5. comparar a freqüência do comportamento antes e depois da introdução da variável experimental ou de ocorrência de resposta. Neste momento, é feita a comparação das restrições e do comportamento anterior do usuário.

5.5 Análise do comportamento

Para efetuar a análise do comportamento do usuário deve-se considerar o comportamento do usuário **Ω (x)**

E as restrições comportamentais R(x) podem ser definidas como:

R(x) = SBi pode ser uma seqüência de comportamentos

ou

R(x) = SBix pode ser um subconjunto isolado de comportamentos

ou

R(x) = Bix pode ser um comportamento isolado

5.6 Atribuição do nível de Confiança

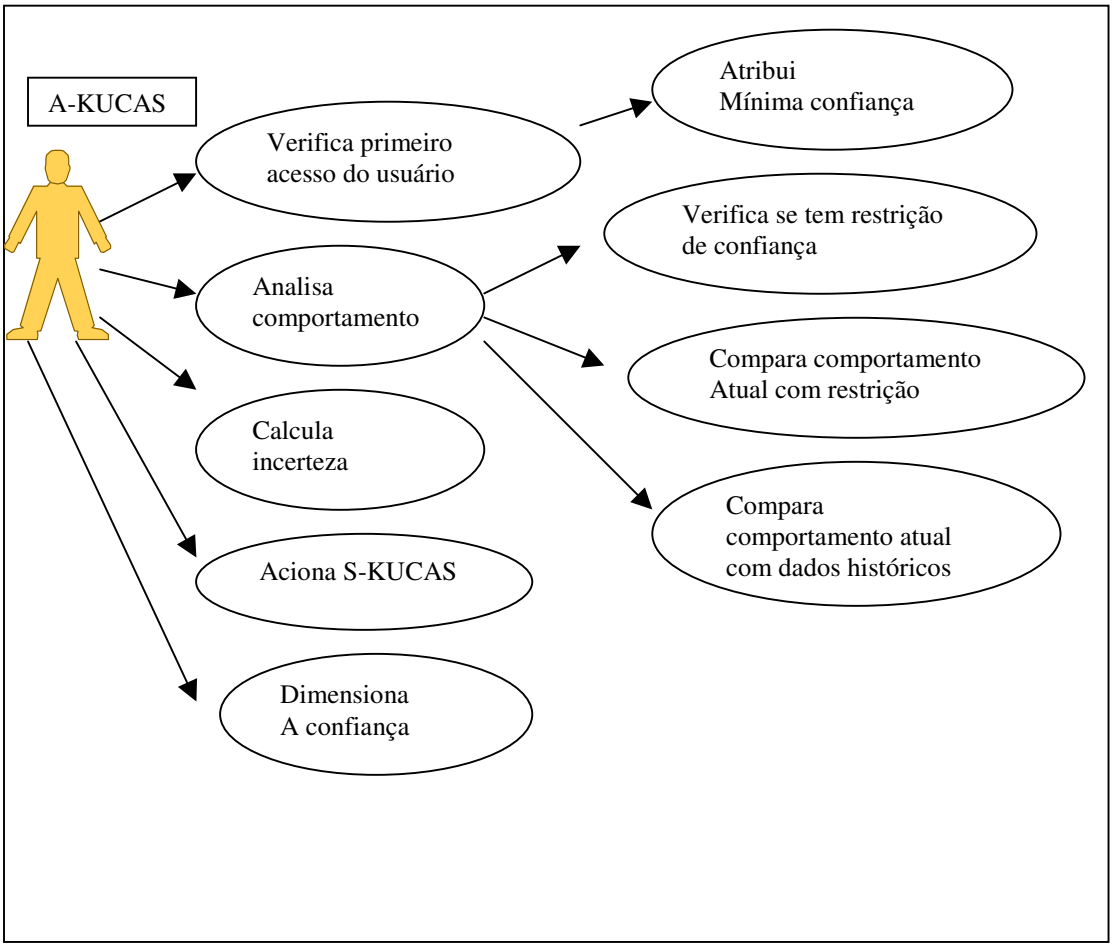


Figura 15: Diagrama de Casos de Uso do A-KUCAS
Fonte:elaborada pelo autor

O modelo proposto é baseado na Confiança Matemática da Teoria das Evidências de Dempster-Shafer (DEMPSTER, 1967) e (SHAFER, 1976 e é aplicada no Sistema KUCAS para ajudar na tomada de decisão de autenticar ou não o usuário.

A confiança é um conceito abstrato, revela uma crença na sinceridade /autenticidade de uma pessoa em outra pessoa.

Diante da dúvida e da incerteza, freqüentemente é necessário tomar decisões baseadas em evidências, as quais nem sempre são precisas. Nestes casos, utilizamos a confiança, um

critério pessoal que nada mais é do que uma métrica que adotamos para avaliar as evidências que temos diante de nós.

O conceito de Confiança é uma característica comum aos seres humanos e está diretamente relacionado à percepção, ao conhecimento e a reputação que uma pessoa tem a respeito da outra (SCHWEITZER, 2004).

Este tipo de abordagem pode ser empregado, não somente para seres humanos, mas, também em ambientes computacionais onde existem interações entre seus membros, como é o caso de ambientes de redes de computadores e na interação com aplicações de software. Para utilizar este tipo de abordagem em ambientes de redes de computadores é necessário desenvolver um modelo de confiança adequado ao usuário e a interação com o ambiente. Este modelo deve incorporar valores mínimos e valores de atribuição da confiança.

O Sistema KUCAS não se baseia somente na dicotomia da constatação ou não de um fato, mas no quanto se confia neste fato, por isto, estipula-se intervalos de confiança baseado na análise do comportamento do usuário e nas restrições de confiança geradas pelo próprio usuário.

Com o passar do tempo e de acordo com a análise comportamental, o nível de confiança no usuário pode sofrer variações, e assim, o Sistema KUCAS ao longo da interação com o usuário, determina as evidências para aumentar ou diminuir a confiança que se tem no mesmo.

Quando existem várias evidências independentes é possível realizar algumas inferências gerais relacionadas a cada uma dessas evidências e derivar vários conjuntos alternativos de hipóteses de uma simples coleção de evidencias, cada um desses conjuntos tem um grau de confiança associado, chamado de intervalo de crença ou intervalo de confiança matemática (UCHÔA et al, 2004).

Dado um conjunto universo X, uma Medida de Confiança é a função:

$\lambda : P(X) \rightarrow [0,1]$

Tal que $\lambda(\phi) = 0$ e $\lambda(X) = 1$, para todos os possíveis subconjuntos de $X \in P(X)$,

O número 0 deve ser atribuído ao conjunto vazio, uma vez que o conjunto vazio corresponde à hipótese falsa.

Uma função $\lambda \rightarrow [0,1]$ é chamada de função de confiança se ela for relativa a alguma atribuição de probabilidade $m: \rightarrow [0,1]$.

A função de confiança representa a quantidade total de confiança na evidência que aponta para um determinado conjunto de hipóteses e, como é probabilidade, varia entre 0 e 1.

Associado a cada medida de confiança está uma medida de desconfiança, Df, definida pela equação:

$Df(X) = 1 - \lambda(X)$, para todo $X \in Df$

A desconfiança também varia no intervalo de 0 a 1 e mede até que ponto a evidência em favor de "não confiar" valida a confiança em "confiar".

Por similaridade: $\lambda(X) = 1 - Df(X)$

As medidas de confiança e desconfiança são então mutuamente duais.

A medida de desconfiança também pode ser definida como independente da medida de confiança.

$Df: P(X) \rightarrow [0,1]$

Tal que $Df(\phi) = 0$ e $Df(X) = 1$

Então, Medidas de Confiança e Desconfiança podem ser caracterizadas pela função:

$M: P(X) \rightarrow [0,1]$ tal que $m(\phi) = 0$

Esta é uma função probabilidade, onde para cada conjunto $X \in P(X)$, o valor de $m(X)$ expressa a proporção com que cada elemento atende a uma requisição de um elemento particular de X.

Se há evidências verdadeiras em favor de ”não confiar”, então λ (X) = 1 e Df(X) = 0. Isto implica que o único valor possível para λ (X) = 0.

Dado λ (X) pode não evidenciar totalmente o quanto se pode confiar.

As evidências vão sendo coletadas e observadas na análise comportamental e elas definem a confiança. A confiança pode variar dependendo do usuário, da localização, do tempo e das restrições de confiança que o usuário pode fazer.

Portanto, a Confiança baseia-se em duas medidas não complementares: Medida de Confiança e Medida de Desconfiança. As relações de confiança são definidas em pares. Essa medida de confiança é expressa por uma dupla (mC, mD), onde mC e mD podem assumir valores entre (0,1) e expressam respectivamente, a mínima confiança e a mínima desconfiança de um em relação a outro.

Pode existir uma incerteza na atribuição da confiança, pois nem sempre o complemento da confiança expressa a desconfiança.

O Sistema KUCAS baseado nas evidências do comportamento estabelece se confia no usuário com valores no intervalo (mC, mD), onde mC é a mínima confiança e mD é a mínima desconfiança.

Mas na incerteza, pode se não se ter valores para atribuir nem a confiança e nem a desconfiança.

Baseado nestas condições pode-se definir a associação de quatro funções. A função confiança (λ), a função potencial de confiança (Pf), a função desconfiança (Df) e a função incerteza da confiança (If) .

A função confiança (λ), expressa o valor mínimo de confiança.

A incerteza (If) e a função potencial de confiança (Pf) expressam a máxima confiança que é atribuída ao usuário, com $0 \leq Pf \geq 1$.

Pf = Max λ = Min λ + If

A função desconfiança é dada por:

Df = 1 – Pf

A confiança, a desconfiança e a incerteza expressam todas as possibilidades de atribuição de confiança a um usuário, desta forma:

λ + Df + If = 1, tal que , { λ, Df, If} e

(If) = 1- (λ + Df) é a incerteza.

5.6.1 Valor inicial de Confiança

Uma característica comum a todas as formas tradicionais de mensuração da confiança, é que ela é vista como unidimensional. Confiança é freqüentemente mensurada, no plano individual, como uma variável dicotômica (confia, não confia) e tem uma operacionalização muito frágil, por isto é necessário complementá-la com os resultados obtidos com a análise comportamental e com a tecnologia de reconhecimento facial.

A confiança é baseada em informações comportamentais, na análise comportamental e nas informações de contexto provenientes do ambiente e da tecnologia de reconhecimento facial, e com isto é possível inferir um valor mínimo de confiança inicial e dar prosseguimento ao processo de autenticação do Sistema KUCAS.

A heurística do valor inicial da confiança é determinada por um modelo definido pelo comportamento do usuário, pela atividade que ele está fazendo no momento, pela localização do usuário e pelo horário.

Sendo λ =(mC , mD), onde mC e mD indicam respectivamente os valores da mínima confiança e da mínima desconfiança.

Por definição, o Sistema KUCAS, na primeira vez que o usuário interage com o sistema, utiliza um modelo de atribuição da confiança mínima:

λi = (mCi , mDi), onde λi é a confiança inicial e sendo **mCi** a mínima confiança inicial e **mDi** a mínima desconfiança inicial.

Então,

λi é a confiança inicial no usuário e que representa os valores iniciais da mínima confiança (mC) e da mínima desconfiança (mD) que o sistema atribui a um usuário, conforme o modelo indicado abaixo:

- Confiança inicial padrão => λi = (1.00 , 0.00)
- Confiança inicial critica => λi = (0.00 , 1.00)

Neste caso é proposto um modelo, mas a confiança inicial também pode ser definida conforme o usuário, sua localização, o horário em que ocorre o comportamento atual e conforme seu histórico comportamental.

5.6.2 Atribuição do nível de Confiança

Nas vezes subseqüentes, com a base de históricos comportamentais repletos de informações, o nível de confiança pode ser modificado dependendo da análise comportamental do usuário, para isto o sistema KUCAS extrai automaticamente o nível da confiança do usuário, monitorando as suas ações.

Então, o comportamento do usuário é definido pela função:

$\Omega(x) = \cup$ **Bi**

Sendo **Bi** o histórico do comportamento e **Bj** o comportamento atual, o sistema KUCAS verifica se o comportamento atual é uma restrição à confiança causada pelo comportamento do usuário ou definida pelo sistema.

Sendo **Ri** uma restrição á confiança.

Se **Ri** $\subseteq$ **Bj** , ou seja, a restrição à confiança ocorreu, então houve um comportamento anormal, a confiança será reduzida e a aplicação de software será bloqueada.

Se não ocorreu restrição, o sistema KUCAS verifica no histórico de comportamentos **Bi** se já houve alguma vez um comportamento igual ou semelhante a **Bj,** se sim, a confiança se mantém e o sistema KUCAS continua autenticando o usuário na aplicação de software.

Se **Bj** nunca ocorreu antes, então é acionado o módulo de segurança S-KUCAS que aciona a tecnologia de reconhecimento facial.

Se o usuário foi identificado, é calculada a incerteza da confiança If(Bj) do usuário, baseado no comportamento atual. A confiança do usuário é mantida, pois não se sabe se a tecnologia de reconhecimento facial deu falso positivo ou falso negativo e o usuário contínua utilizando a aplicação de software.

Se o usuário não foi identificado, é calculada a incerteza da confiança If(Bj) do usuário, baseado no comportamento atual. A confiança do usuário é diminuída, ou seja, diminui-se a confiança e aumenta-se a mínima confiança. O comportamento **Bj** é cadastrado como uma restrição de confiança, ou seja, é um comportamento não normal do usuário.

Neste caso, o acesso à aplicação de software é bloqueada.

Se houve uma mudança comportamental e uma restrição comportamental foi verificada, significa que a **Ω (x)** variou negativamente e que o nível de confiança no usuário diminui, assim:

Se **λ** = f(mC, mD) e seja **δ** um valor constante a ser acrescido e/ou diminuído da confiança.

mC’ = mC - **δ**

mD’ = mD + **δ**

então:

λ = (mC - **δ**, mD + **δ**) , ou seja, o sistema KUCAS diminui **δ** na mínima confiança e acrescenta **δ** na mínima desconfiança, armazena as informações obtidas e não contínua a autenticar o usuário.

Se houve uma mudança comportamental e não foi verificada nenhuma restrição comportamental, significa que a **Ω (x)** variou positivamente e que o nível de confiança no usuário aumentou, assim:

$\lambda' = f(mC', mD')$

$mC' = mC + \delta$

$mD' = mD - \delta$

então:

$\delta = (mC + \delta, mD - \delta)$, ou seja, o sistema KUCAS acrescenta δ na mínima confiança e diminui δ na mínima desconfiança e contínua a autenticar o usuário.

Como os valores da confiança e da desconfiança pertencem ao intervalo (0,1), é necessário controlar os valores atribuídos à confiança para que se houver número negativo, este seja igual a zero e se houver número maior que 1, este seja igual a 1 (DEMPSTER, 1967).

Se $mC > 1.0$, então: $mC = 1.0$

Se $mC < 0$, então: $mC = 0$

Se $mD > 1.0$, então: $mD = 1.0$

Se $mD < 0$, então: $mD = 0$

Se não houve mudança comportamental a função **Ω (x)** não variou e portanto o sistema KUCAS mantém o nível de confiança atribuído anteriormente ao usuário.

Conforme demonstrado, a atribuição do nível de confiança é feita lentamente e de forma linear.

Em (PLATZER, 2004) a atribuição do nível de confiança é feita de modo exponencial, ou seja, quando se perde a confiança é rápido, e para atribuir confiança, é lento e pode ser representado pela equação exponencial

$$y = f(x) = e^{-1/x} \qquad \text{para todo } x \in (0, \infty [.$$

Se for acionada a tecnologia de reconhecimento facial, o sistema KUCAS verifica a incerteza da confiança:

If(Bj) = 1 – (mC + mD) = μ

If(Bj) = μ é a incerteza atribuída ao usuário em relação ao comportamento **Bj**.

Na confiança do usuário será indicado que houve uma incerteza. É feita uma incerteza na atribuição da confiança, pois nem sempre o complemento da confiança expressa a desconfiança. A confiança assume uma dimensão, ou seja, é multidimensional, pois se pode confiar, não confiar e não ter elementos para avaliar a confiança.

λ (x) = (Mc ; mD; μ) em Δ t

O sistema KUCAS de autenticação contínua de usuários atribui uma confiança mínima ao usuário inicialmente, e com o tempo de uso transcorrido, baseando-se na análise dos dados comportamentais capturados e nas restrições, o sistema vai variando a confiança atribuída inicialmente. Da mesma forma, como as pessoas confiam nas outras, dando uma credibilidade relativa inicial e, por fim, analisando as evidências atuais e as restrições para saber se continuam emprestando confiabilidade ou, convenientemente, optando por deixar de prestá-la; desta forma, define-se uma política de segurança adaptativa ao usuário.

Para o controle da mudança comportamental do usuário no Sistema KUCAS é necessária a interação de varias aplicações de software que enviam mensagens de alertas, acionam sensores e tecnologias que garantem a autenticação do usuário no sistema KUCAS.

No apêndice A é descrito a estrutura do algoritmo A-KUCAS.

5.7 Arquitetura do Sistema KUCAS

O Sistema KUCAS é integrado ao usuário, ao ambiente e à tecnologia por meio de sensores, dispositivos e câmeras de vídeo.

Para suportar as necessidades computacionais, o sistema KUCAS possui uma arquitetura distribuída em cinco camadas: camada de aplicação, camada de interface, camada do framework, camada comportamental e camada de dados.

O sistema KUCAS é composto por um framework de serviços F-KUCAS, um algoritmo de autenticação A-KUCAS e um módulo de segurança S-KUCAS.

Ao ser acionado o sistema KUCAS chama o *framework* F-KUCAS inicia as atividades, aciona o algoritmo A-KUCAS e armazena as informações comportamentais e de imagens da face do usuário obtidas.

O algoritmo A-KUCAS manda informações para os API's pertencentes ao *framework* F-KUCAS, os quais têm várias funções, entre elas, gerar os *logs* do Sistema KUCAS, acessar as bases de dados de comportamentos e de imagens da face, mandar mensagens de alertas ao Sistema KUCAS, acionar o Módulo de Segurança S-KUCAS quando houver mudanças comportamentais da pessoa.

O Módulo de Segurança S-KUCAS, quando acionado, ativa sensores, câmeras de vídeo e aciona a Tecnologia de Reconhecimento Facial.

Tabela 9: Camadas do Sistema KUCAS

CAMADA	FUNÇÕES
Camada de Aplicação	Permite a entrada de dados nos sistema. Interage com a Camada de Interface.
Camada de Interface	Estrutura de redes que interage com o *Framework* F-KUCAS.
Camada do Framework	Contém o *Framework* F-KUCAS, o algoritmo A-KUCAS, aplicações de *software* e o módulo de Segurança S-KUCAS.
Camada Comportamental	E acionada pela Camada do Framework e está orientada como interface de comunicação ou interação com a Camada de Dados.
Camada de Dados	Dá suporte ao acesso aos dados das imagens das faces e dados comportamentais do usuário.

Fonte: Elaborada pelo autor.

A Tabela 9 apresenta a arquitetura cliente-servidor do Sistema KUCAS, distribuída em cinco camadas.

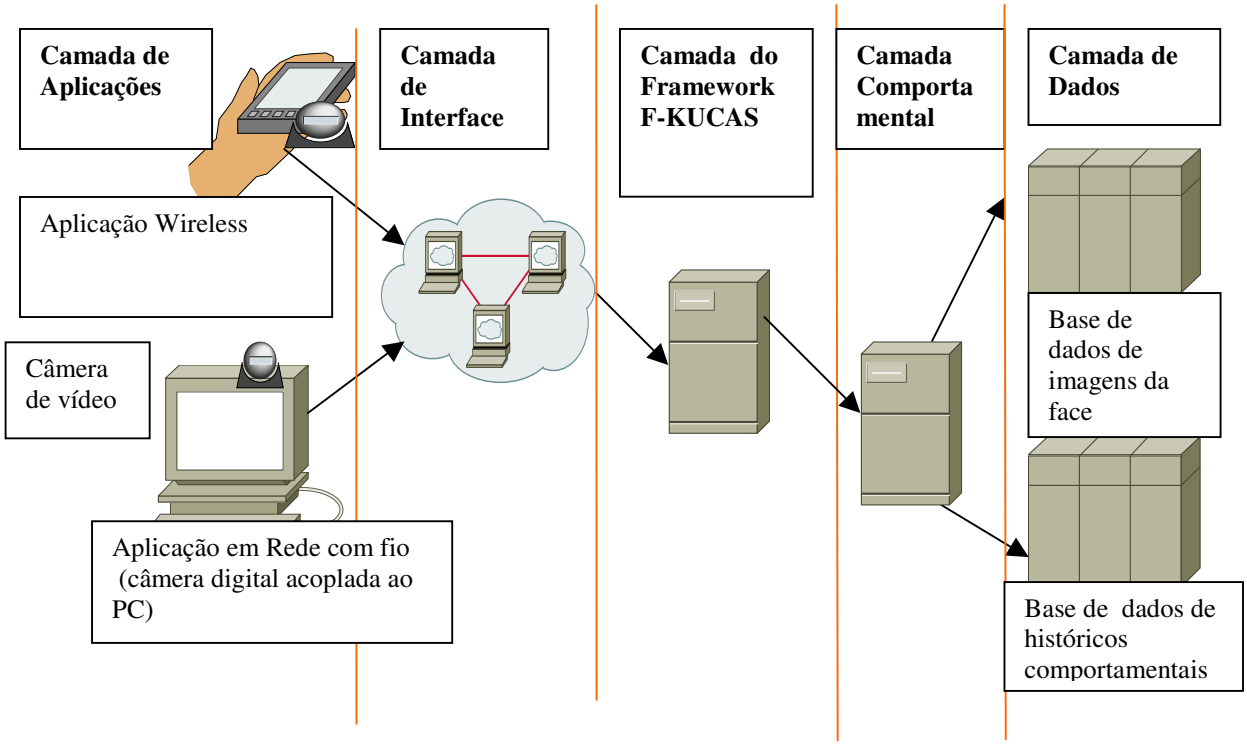


Figura 16: Arquitetura de camadas do Sistema KUCAS
Fonte: elaborada pelo autor

Conforme descrito na Tabela 10 e representado na Figura 16.

1) **Camada de Aplicação**: Camada que contém as aplicações que permitem a interação com o Sistema KUCAS. Esta camada tem a funcionalidade de prover a comunicação com o usuário do Sistema KUCAS. Esta camada recebe as informações do usuário e processa a interação com o *framework* F-KUCAS. A camada de aplicação entra em contato com a camada comportamental, por meio da Camada de Interface, para obter informações de como iniciar a coleta de dados para efetuar a análise das evidências comportamentais.

2) **Camada de Interface**: é uma estrutura de redes com ou sem fio e é responsável pela ligação entre a camada de Aplicação e a Camada Comportamental.

3) **Camada do *Framerwork***: é uma camada que contém o *framework* F-KUCAS, de serviços, e todos seus módulos ou API's de software e que aciona o Algoritmo de Autenticação Contínua A-KUCAS e o módulo de segurança S-KUCAS.

4) **Camada Comportamental**: Camada Comportamental através de regras e aplicações ou API de software provê a integração entre as camadas anteriores e a camada de dados. Esta camada é composta por várias aplicações ou API's que determinam as regras da análise das evidências comportamentais e aciona o algoritmo A-KUCAS que utiliza os princípios da Confiança Matemática para determinar a autenticação contínua do usuário.

5) **Camada de dados**: Camada de Dados contém os dados das imagens da face e do histórico comportamental dos usuários que ficam armazenados em bancos de dados. Um banco de dados contém as imagens das faces e outro banco contém o histórico comportamental das pessoas. Quando a camada de aplicação recebe da camada comportamental as informações, esta entra em contato com a camada de dados, e uma aplicação de software é acionada para atualizar e recuperar informações nos bancos de dados.

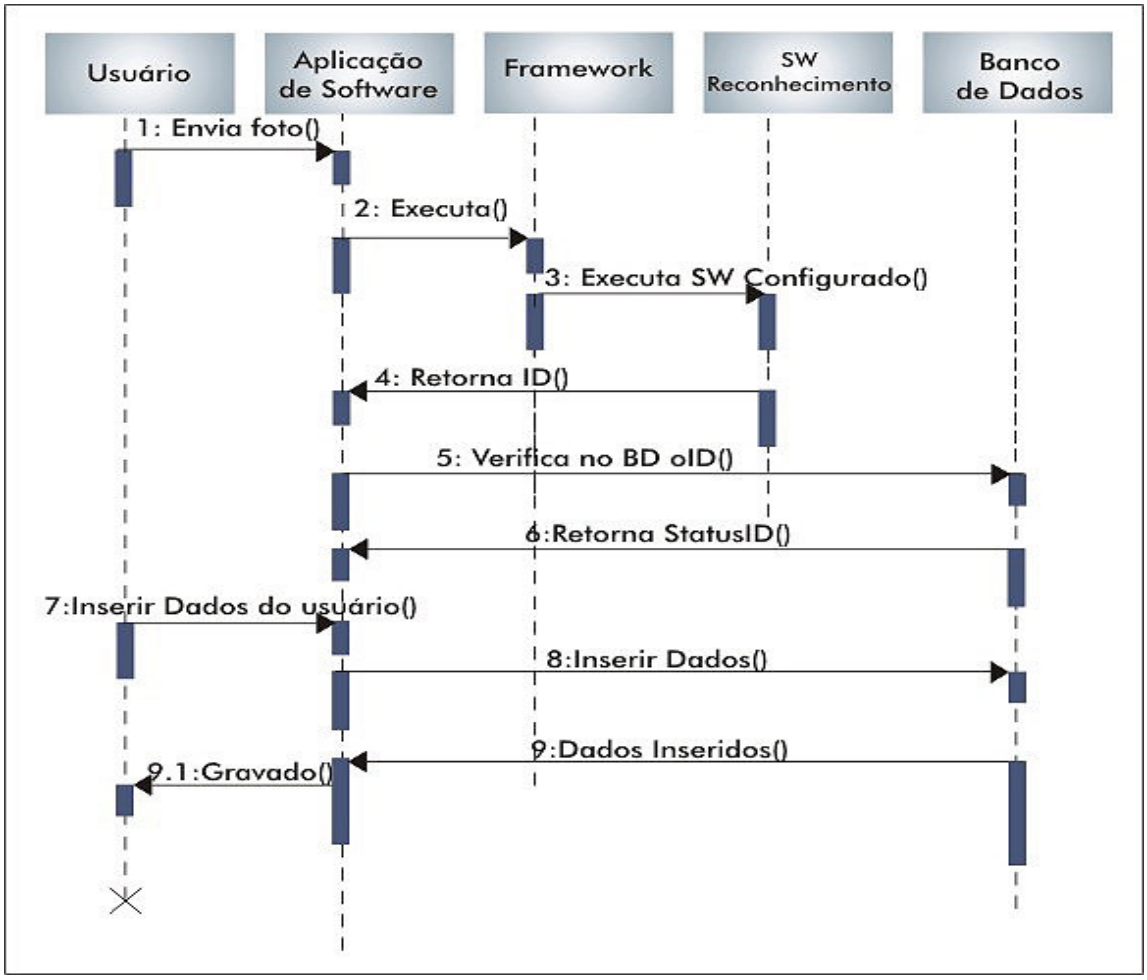


Figura 17: Esquema do Sistema KUCAS
Fonte: elabora pelo autor

A Figura 17 mostra como as mensagens de objetos do sistema KUCAS interage em uma situação, num determinado período de tempo. Sendo que a comunicação pode ser assíncrona, imprevisível e ocorrer em um tempo qualquer; ou síncrona, previsível, ocorrendo em tempo específico.

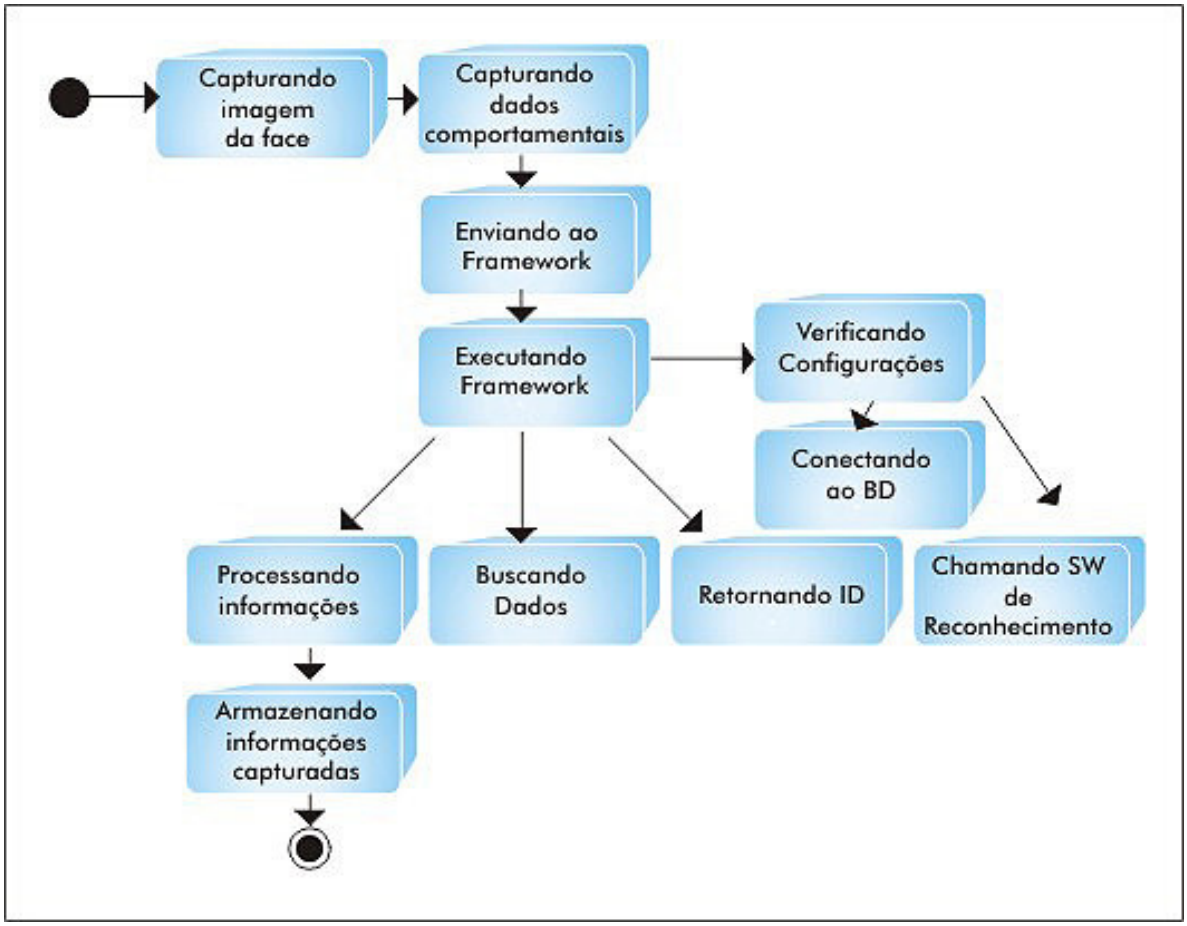


Figura 18: Estados do Sistema KUCAS
Fonte: elaborada pelo autor

A Figura 18 representa a fase de ativação do sistema e as mudanças do estado inativo para o estado ativo.

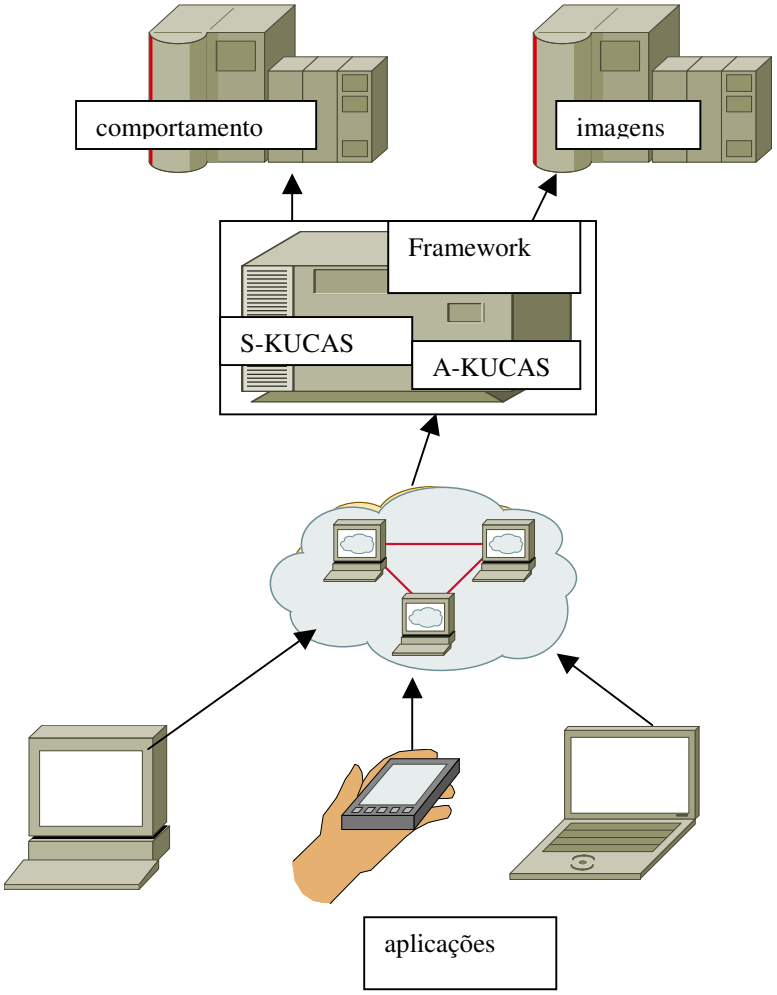


Figura 19: Arquitetura Física do Sistema KUCAS
Fonte: elaborada pelo autor

A Figura 19 representa a arquitetura de implantação do sistema KUCAS.

5.8 *Framework* F-KUCAS

O Sistema KUCAS, através de seu *framework*, F-KUCAS, acessa a base de dados de histórico comportamental e inicia um processo de análise das evidências do comportamento do usuário baseando-se no histórico de comportamentos anteriores, o Sistema KUCAS envia uma mensagem de alerta ao Módulo de segurança S-KUCAS, o qual aciona um mecanismo que captura uma imagem da face da pessoa utilizando uma câmera de vídeo e sensores

instalados no ambiente em que a pessoa está, a imagem da face é transmitida ao *framework* F-KUCAS, o qual aciona uma aplicação ou API que por meio da Tecnologia de Reconhecimento Facial em 3D, processa a verificação nas bases de dados de imagens da face e verifica se a pessoa em frente a câmera de vídeo é a mesma contida na base de dados de imagens da face.

Se a imagem capturada da face do usuário da aplicação está contida na base de dados de imagens da face, o Sistema KUCAS contabiliza na base de dados de histórico comportamental, os dados do usuário e mantém a autenticação contínua.

Se a imagem capturada da face do usuário da aplicação não está contida na base de dados de imagens da face, o Sistema KUCAS aciona uma aplicação de software no *framework* (F-KUCAS) que aplica a Confiança Matemática para validar a continuação do acesso à aplicação ou o término da mesma; ao mesmo tempo em que gera *logs* da atividade do usuário no sistema.

Durante todo este processo uma aplicação de software no *framework* F-KUCAS registra os *logs* com as informações das atividades do usuário. Estes *logs* contêm informações como local, dia e hora do acesso, tempo gasto em cada aplicação, endereço IP da máquina ou dispositivo do usuário, transação iniciada e dados informados, entre outras.

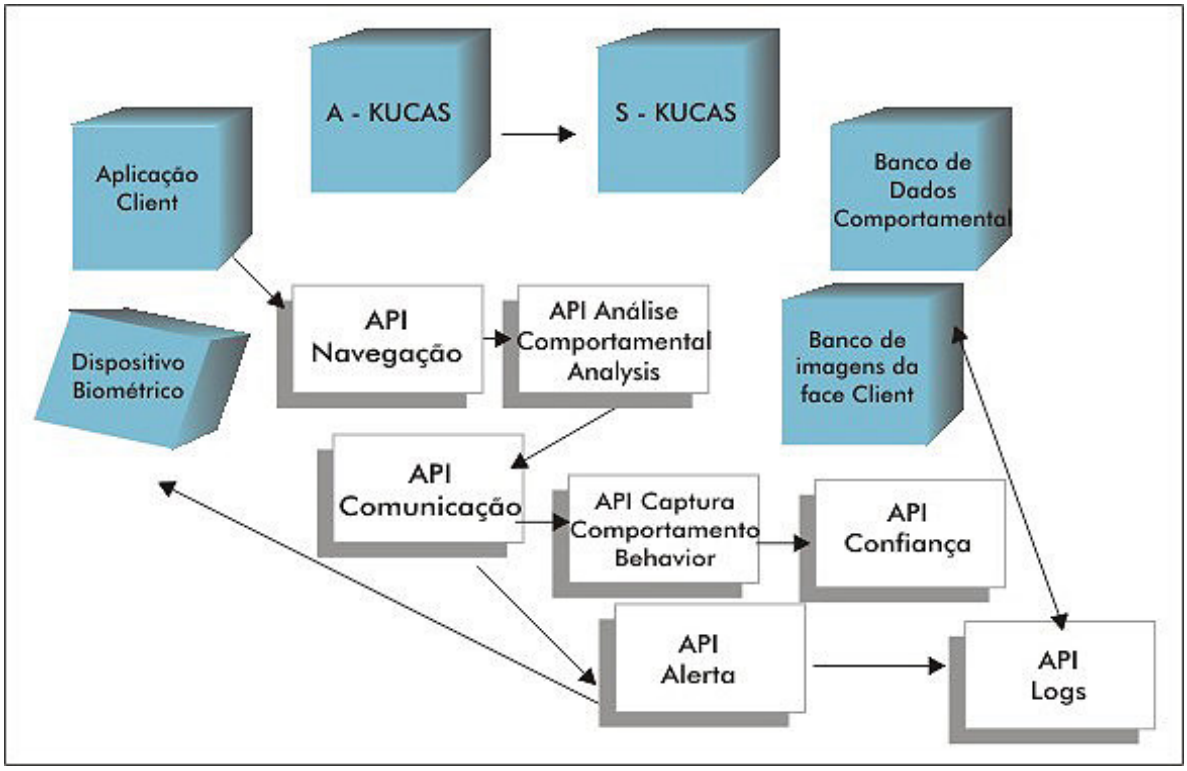


Figura 20: Arquitetura Modular do Framework F-KUCAS
Fonte: elaborada pelo autor

O *framework* F-KUCAS representado graficamente na Figura 20 possui uma arquitetura modular que permite o acréscimo de qualquer outro dispositivo, e objetiva permitir a evolução tecnológica e escalabilidade do sistema KUCAS, sem provocar grandes alterações no mesmo, a cada manutenção ou evolução tecnológica.

O *framework* F-KUCAS é composto por diversas aplicações de serviços que são API ou aplicações de *software*, que se encarregam de fazer a distribuição do serviço, enviar mensagens de alertas e acionar sensores. Contém ainda o Algoritmo A-KUCAS e o Módulo de Segurança S-KUCAS.

O *framework* F-KUCAS é composto por várias API's (*Application Program Interface*), API de software, a saber:

API de Navegação: é um API de software que implementa um método padrão (verificaMensagens), invocado pelo componente que faz a interação com o usuário para obter informações de chegadas de dados comportamentais e imagens de uma face.

API de Análise do Comportamento: é um API que implementa um método analiseComportamento, invocado pelo componente que faz a interação com o usuário para obter informações do comportamento do usuário. O resultado obtido não é uma análise comportamental, mas as evidências de um comportamento. O resultado desta interação é repassado ao API de Comunicação.

API de Comunicação: é um API que recebe a chamada para o método obtemRastrosUsuarios, definido em sua interface. Neste ponto o API faz a comunicação com as bases de dados deve entrar em contato com o API de coleta de comportamento e recuperar o comportamento armazenado por eles.

API de Captura do Comportamento: é um API que recebe chamada para seu método capturaComportamento, retornando o comportamento requisitado pela aplicação de software de analise comportamental. Este API interage com a API de Confiança.

API de Confiança: é um API que recebe a chamada para o método estipularNivelConfianca que será o responsável pela determinação do grau de confiança a ser adotado no sistema de autenticação.

API de Alertas: é um API que envia alertas sobre mudança comportamental no usuário da aplicação.

API de *Logs*: é um API que grava nos bancos de dados informações geradas no uso da transação de software.

API de Limpeza: é um API que verifica constantemente o volume de informações armazenadas e compara as datas do dia e do armazenamento, com o objetivo de efetuar uma limpeza nas bases de dados comportamentais e de imagens da face e manter a base de dados com um número limite de informações que atenda a análise comportamental, controlando o espaço para armazenamento das informações e a quantidade ocupada pela memória.

5.9 Algoritmo A-KUCAS

A-KUCAS é um algoritmo que analisa o comportamento do usuário, utiliza um mecanismo já citado anteriormente para efetuar a análise comportamental do usuário e atribuir a ele o nível de confiança.

O algoritmo A-KUCAS é modular, aberto, independente de hardware e tem escalabilidade para suportar as mudanças na arquitetura do sistema KUCAS e no framework F-KUCAS.

No algoritmo A-KUCAS os eventos são modelados através de um objeto ativo que monitora esta condição de ocorrência de um evento, e percebe quando este se torna verdadeiro. O Objeto recebido é considerado uma mensagem e pode conter atributos e operações. Um objeto chama uma operação de um outro objeto, através de uma mensagem síncrona. Esta mensagem passa informação através de parâmetros e valores de retorno. Um período de tempo também é um evento.

A captura das variáveis comportamentais é efetuada por várias API's (*Application Program Interface*), ou API's residentes no framework, como a **API de Navegação** (verificaMensagens) que faz a interação com o usuário para obter informações do comportamento do usuário; a **API de Comunicação** faz a comunicação com as bases de dados deve entrar em contato com o API de coleta de comportamento e recuperar o comportamento armazenado por eles; a **API de Captura do Comportamento** que recebe chamada para seu método capturaComportamento, retornando o comportamento requisitado pela aplicação de software de analise comportamental; **API de *Logs*** que armazena nos bancos as informações nos *logs* e em arquivos de históricos comportamentais.

O algoritmo A-KUCAS utiliza a **API de Confiança** que reside no framework F-KUCAS e é um API que recebe a chamada para o método estipularNivelConfianca, o qual é o

responsável pela determinação do nível de confiança a ser adotado no sistema de autenticação.

5.10 Módulo de Segurança S-KUCAS

S-KUCAS é um módulo de segurança que é acionado, pelo API de Alertas, residente no framework F-KUCAS, quando há uma variação no nível de confiança atribuído ao usuário.

O módulo S-KUCAS efetua uma interação com o ambiente, aciona a tecnologia de reconhecimento facial e câmeras de vídeo por meio de sensores, captura imagens do ambiente e da face do usuário; também aciona a tecnologia de reconhecimento facial e bloqueia o acesso do usuário ao sistema quando necessário.

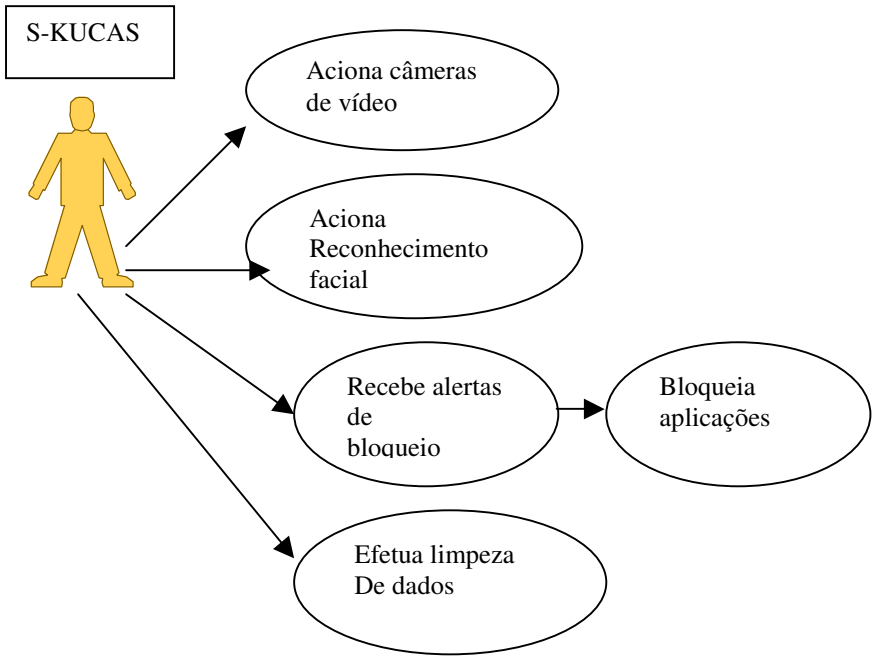


Figura 21: Diagrama de casos de uso do S-KUCAS
Fonte: elaborada pelo autor

6 Estudo de Caso

6.1 Introdução

Neste capítulo é feito um estudo de caso da aplicabilidade do mecanismo de análise comportamental e do Sistema KUCAS, proposto no capítulo 5, numa simulação com dados hipotéticos no uso de uma aplicação financeira de software em Máquinas de Auto-Atendimento ATM (*Automated Teller Machine*).

Figura 22: ATM (*Automated Teller Machine*)
Fonte: Fort Hays State University

As máquinas ATM são utilizadas por instituições financeiras e estão distribuídas em várias localidades; são máquinas multitarefas e oferecem serviços bancários de consulta de saldos de aplicações financeiras, extratos de movimentações, depósito de valores, saque de valores, pagamento de contas e tributos, pagamento de boletos de cobrança com código de barras ou fichas de compensação, solicitação e impressão de talões de cheques, transferências de valores entre contas de um mesmo banco, transferência de valores entre bancos entre outros serviços. As ATM's são consideradas a invenção tecnológica que de forma mais significativa, mudou os hábitos das pessoas no cotidiano, havendo milhões de equipamentos instalados em todo o mundo.

Para a simulação proposta, uma premissa básica, é que o acesso às aplicações no ATM é feito por clientes da instituição financeira, ou seja, um usuário conhecido que através de uma tela principal informa a senha e o código de acesso ou cartão magnético e senha; o usuário escolhe num menu de opções, qual a aplicação financeira de software que deseja utilizar.

Na tabela abaixo são indicadas as possíveis aplicações financeiras disponíveis ao usuário num ATM.

Tabela 10: Relação de aplicações de software disponíveis no ATM

Aplicação de Software
DEPÓSITO COM CARTÃO PARA PRÓPRIA CONTA CORRENTE
DEPÓSITO COM CARTÃO PARA PRÓPRIA CONTA POUPANÇA
DEPÓSITO COM CARTÃO PARA TERCEIROS CONTA CORRENTE
DEPÓSITO COM CARTÃO PARA TERCEIROS CONTA POUPANÇA
DEPÓSITO SEM CARTÃO CONTA CORRENTE
DEPÓSITO SEM CARTÃO CONTA POUPANÇA
DEPÓSITO IDENTIFICADO
CONSULTA DE SALDO
EMISSÃO DE EXTRATO
TALÃO DE CHEQUES
PREFEITURA/ORGÃOS – PAGAMENTO (ISS/IPTU)
PAGAMENTO CONTAS DE CONSUMO
PAGAMENTO CONTAS DE TRIBUTOS MUNICIPAIS
IPVA – IMPOSTO SOBRE VEÍCULOSAUTOMOTORES
DPVAT – SEGURO OBRIGATÓRIO
LICENCIAMENTO DE VEÍCULOS
GPS – GUIA DE PREVIDÊNCIA SOCIAL
TRANSFERÊNCIA C/C PARA C/C
TRANSFERÊNCIA C/C PARA C/P
TRANSFERÊNCIA C/C PRÓPRIA PARA OUTRO BANCO
TRANSFERÊNCIA C/C TERCEIROS PARA OUTRO BANCO
RETIRADA/SAQUE
APLICAÇÕES/INVESTIMENTOS
FINANCIAMENTOS/EMPRÉSTIMOS
CAPITALIZAÇÃO
CONTRATAÇÃO DE SEGURO

Fonte: Elaborada pelo autor.

Para a simulação hipotética em um ATM é necessário a definição dos requisitos básicos de ATM, a definição funcional da máquina de auto-atendimento, as necessidades de

conectividade, as necessidades de infra-estrutura de *hardware* e *software*, quem é o usuário e qual aplicação de software ele vai utilizar no ATM.

6.2 Estrutura de um ATM

A estrutura de um ATM é composta por diferentes equipamentos de *hardware*, diversos *software* e sistemas operacionais. Na máquina ATM se executam as aplicações de *software* de transações financeiras sendo que a lógica de negócio reside no computador central da instituição financeira.

Tanto os sistemas de comunicação como os sistemas operacionais variam segundo o tipo de equipamento e conforme o fabricante, podendo ser MS/DOS, MS/Windows NT, MS/Windows 2000, OS/2, Unix e Linux. Os protocolos de comunicação são TCP/IP ou SNA.

As máquinas ATM são conectadas via computador central a um software gerenciador transacional através de uma estrutura de redes de computadores, a qual pode ser uma rede externa ou uma rede local.

Rede Externa: É a rede de computadores que concentra as máquinas ATM's que estão localizadas em pontos remotos como *shopping centers*, supermercados, postos de combustíveis, ruas e etc. Estas máquinas ATM's utilizam remotamente protocolos de comunicação do tipo LLCC2, X.25, BSC3. Possuem largura de banda compartilhada com um concentrador de terminais, e em geral, o *gateway* de comunicação é proprietário e permite a conexão entre as agências da instituição financeira e o Computador Central.

Rede Local: È a rede de computadores que concentra as máquinas ATM's que estão localizados nas agências das instituições financeiras, e tem processo transacional similar ao de um caixa na instituição financeira. Neste tipo de rede as conexões são de 64 e 128 kb e as linhas de comunicação a 9600 Kb.

O ATM possui uma aplicação de software responsável pela camada de apresentação e algumas regras de consistência com o objetivo de reduzir o tráfego de mensagens na rede com o computador central. Os equipamentos possuem bases de dados locais para apoio e armazenamento de tabelas diversas; também possuem bases de dados denominadas *logs*, as quais armazenam registros de todas as transações efetuadas.

A configuração básica de um ATM contém um cadastro com informações do endereço de localização do equipamento, horário de funcionamento, valores de parâmetros e limites, tipo de terminal e fabricante.

Em relação às inovações nos ATM's, pode-se citar a possibilidade de acesso a Internet e a utilização de ATM's wireless, uma alternativa para regiões com acessos difíceis, ou carência de redes de telefonia fixa ou falta de infra-estrutura de redes de comunicações. (FINEP, 2005)

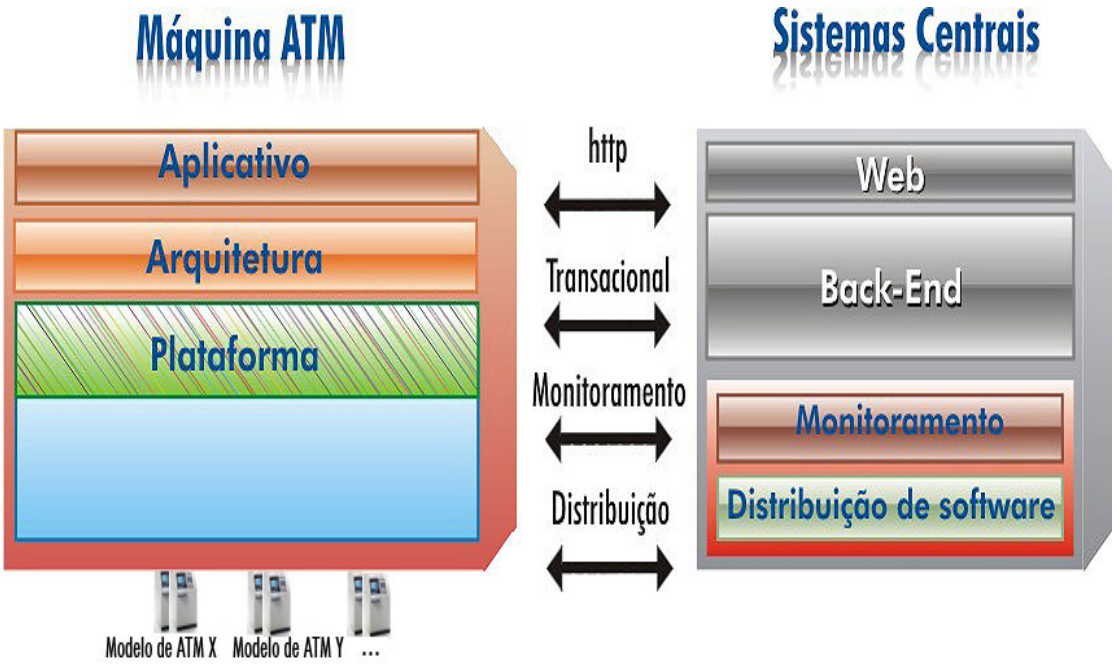


Figura 23: Estrutura do ATM
Fonte: elaborada pelo autor

A Figura 23 ilustra uma estrutura de uma máquina ATM onde, distingui-se:

1. O *Back-End* é o local onde se executam as aplicações financeiras de software e onde reside a lógica de negócios e um possível ambiente de serviços da instituição financeira.

2. O próprio equipamento do auto-atendimento que suporta a aplicação gerencia os dispositivos.

3. O componente de monitoramento fornece informações sobre o estado dos equipamentos.

4. O componente de distribuição é o responsável pela distribuição de novas versões das aplicações de software.

6.3 Segurança em ATM

ATM utiliza padrões de criptografia, a saber:

Criptografia por Software: pode ser feito por chave fixa ou por chave variável.

Criptografia por hardware: é necessário a instalação no equipamento de um teclado criptográfico, que possui dois índices de chaves, no índice A é gravada a Master key (TMK) e no índice B a Working KEY (TWK). A Master Key (TMK) é uma chave gerada por um teclado criptográfico do computador central e tem como base o número do terminal do equipamento.

Alguns equipamentos ATM permitem a leitura de cartões com *chip* de memória, no qual se concentram as informações do usuário, além de leitora de cartões especifica, o equipamento possui um módulo de segurança, que é um hardware onde é inserido um *chip* de segurança para validação dos cartões de clientes, num processo de autenticação do cartão. A interface com esse módulo é feita por aplicação de software especifica de cada fabricante. Por contingência, quando ocorre algum problema com o modulo de segurança ou quando o mesmo não é inicializado, a aplicação lê os cartões com chip pela tarja magnética.

6.4 Autenticação em ATM

A estrutura do ATM dispõe de vários tipos de autenticação para as transações dos cartões, mediante identificação do usuário, senha, palavras chaves, identificação criptografada de letras, uma senha secundária, digitação do dia, mês e ano do nascimento.

6.5 Gravação de *log*

A estrutura do ATM têm funcionalidades para a gravação de um *log* que é o *registro* e armazenamento de todas as transações efetuadas, possui funcionalidades de consulta a este *log* gerado, através do painel do operador. O *log* é gravado constantemente na máquina ATM mesmo que exista restrição de espaço, sendo que o número de movimentos armazenados pode ser customizado de fabricante para fabricante.

6.6 Simulação do Sistema KUCAS

Neste estudo de caso, é feita uma simulação para a viabilidade da aplicabilidade do Sistema KUCAS.

A aplicação de software considerada para a simulação é a de saque no ATM.

O sistema KUCAS define algumas restrições básicas e outras que podem ser customizadas de acordo com o ambiente, o equipamento e regras de negócios da instituição. A vantagem da definição de restrições é que não é necessário acessar constantemente a base de históricos comportamentais, o que garante o desempenho e rapidez do sistema KUCAS.

Por exemplo, uma restrição da instituição, o usuário não pode digitar a senha mais do que três vezes, pois é feito um bloqueio da mesma; ou o usuário só tem acesso a determinadas aplicações de software.

Na simulação proposta, são definidas as seguintes restrições: aplicações que o usuário pode utilizar, locais que o usuário pode fazer saques sob restrições de horário ou de valor, tipos de periféricos que o usuário pode utilizar e a seqüência de transações que o usuário pode submeter.

Após o usuário se identificar e escolher no menu principal qual a transação desejada, o Sistema de Autenticação Contínua de Usuários Conhecidos - KUCAS é inicializado e aciona o framework F-KUCAS.

Na etapa de inicialização do sistema KUCAS:

- aciona-se um contador de tempo;

- verifica-se se o usuário faz acesso pela primeira vez;

- se sim, o sistema KUCAS atribui ao usuário a confiança mínima para que ele possa interagir com a aplicação de software escolhida, o framework aciona o módulo S-KUCAS de segurança que captura e armazena uma face do usuário.

Sendo: $\lambda = (mC; mD; If)$, sendo

mC a mínima confiança, mD a mínima desconfiança e If a incerteza.

Seja λo o valor inicial da confiança, valores pré definidos aleatoriamente no intervalo 0 e 1, sendo que:

Na primeira vez a confiança λ é dada por $\lambda o = (0.01 ; 0.09 ; 0.00)$ e é mínima.

Cada captura do comportamento do usuário é feita por API's residentes no framework F-KUCAS, o qual aciona o algoritmo A-KUCAS, que efetua a análise comportamental do usuário da seguinte maneira:

Verifica-se se há restrições de confiança armazenadas. Se sim, e o comportamento atual do usuário é uma restrição, o framework F-KUCAS aciona o módulo de segurança S-KUCAS o qual aciona a tecnologia de reconhecimento facial e efetua o reconhecimento do usuário.

Se o usuário não for reconhecido pela tecnologia de reconhecimento facial, o módulo S-KUCAS efetua o bloqueio da aplicação e diminui a confiança no usuário.

Para esta simulação, atribui-se um valor hipotético $\mu = 0.01$ para variar a confiança.

Então, $\lambda = (mC - 0.01; mD + 0.01; If)$

Se o usuário foi reconhecido pela tecnologia de reconhecimento facial, o sistema continua autenticando o usuário, sem bloquear a aplicação, mas diminui a confiança por ter atingido uma restrição.

Neste caso, $\lambda = (mC - 0.01; mD + 0.01; If)$ e a restrição comportamental existente é excluída, deixa de ser uma restrição para este usuário.

Se o comportamento está dentro das normalidades, sem restrições, o sistema KUCAS, aumenta a confiança que já tinha no usuário e continua a autenticá-lo.

Então, $\lambda = (mC + 0.01; mD - 0.01; If)$

Quando não há restrições impostas, considera-se que o usuário possui um comportamento que está dentro das normalidades, sem restrições, neste caso, o sistema KUCAS, verifica no histórico dos comportamentos anteriores, por meio de pesquisa e comparação, se o usuário já efetuou aquele comportamento.

Se sim, o sistema continua a autenticá-lo, mantém a confiança original e atualiza a dimensão contextual why, pois este comportamento está se repetindo e pode ser um hábito do cliente, que será armazenado.

Se não, o framework F-KUCAS aciona o módulo de segurança S-KUCAS o qual aciona a tecnologia de reconhecimento facial e efetua o reconhecimento do usuário;

Se o usuário não for reconhecido o módulo S-KUCAS efetua o bloqueio da aplicação e diminui a confiança do usuário.

Ou seja, $\lambda = (mC - 0.01; mD + 0.01; If)$

Se o usuário foi reconhecido, o sistema continua autenticando o usuário, sem bloquear a aplicação, e não altera a confiança, pois não foi atingida nenhuma restrição. Neste caso, pode se considerar que o sistema KUCAS não invade a privacidade do usuário.

Toda vez que a tecnologia de reconhecimento facial for acionada, independente do reconhecimento ter sido feito, o sistema KUCAS atualiza, a incerteza do nível de confiança do usuário.

A incerteza é calculada, pois é uma situação onde não se consegue ter informações seguras para se aumentar ou diminuir a confiança no usuário.

Então,

$\lambda = [mC - 0.01; mD + 0.01; (If = (1- (mC + mD)]$

Sendo possível variar a confiança utilizando as restrições, não havendo restrições é possível variar a incerteza da confiança e por ela ir determinando o nível de confiança do usuário.

Se for detectado alguma restrição para o usuário, o sistema KUCAS,em tempo real, aciona o módulo S-KUCAS de segurança que efetua a captura da imagem da face do usuário, aciona a tecnologia de reconhecimento facial. Se a tecnologia de reconhecimento facial retornar uma posição de “não reconhecido”, o acesso do usuário á aplicação de software é bloqueado pelo módulo S-KUCAS.

O intervalo de tempo entre a análise do comportamento e o reconhecimento facial não demora mais do que frações de segundos, pois o bloqueio deverá ocorrer antes da próxima aplicação de software ser efetuada por ele.

O usuário interage com a aplicação e o sistema KUCAS, por intermédio do framework F-KUCAS captura as informações fornecidas pelo usuário.

O sistema KUCAS acessa as bases de dados do histórico do comportamento do usuário, se for o primeiro acesso do usuário, o sistema KUCAS aciona o módulo de segurança

S-KUCAS que aciona sensores e a câmera de vídeo que está no ambiente, captura uma imagem da face do usuário, esta imagem é encaminhada ao framework, que por meio de aplicações e API aciona a Tecnologia de Reconhecimento Facial e valida ou não a imagem da face. Após a identificação facial, o Sistema KUCAS permanece capturando as informações de contexto das variáveis who, where, when e what. Ao final, o sistema armazena as informações recebidas e atribui um nível de confiança mínimo, pois é o primeiro acesso do usuário.

O usuário pode acessar as transações financeiras de uma instituição que disponibiliza um ATM em qualquer lugar a qualquer hora, desde que não haja limite de horário estabelecido.

Nos acessos seguintes, o sistema KUCAS captura as informações utilizando o framework F-KUCAS, e calculando as evidencias do comportamento do usuário.

O módulo S-KUCAS só é acionado se a análise comportamental do usuário atingir alguma restrição for negativa, pois neste caso, o sistema não autentica o usuário e aciona a tecnologia de reconhecimento facial e se aciona mecanismos de bloqueio da aplicação.

Se não atingir nenhuma restrição, o sistema KUCAS não aciona a tecnologia de reconhecimento facial.

Sistema KUCAS verifica constantemente e atualiza o nível de confiança para determinar se o usuário continua no acesso a aplicação de software ou se o sistema aciona mecanismos de bloqueio da aplicação.

No apêndice A é possível visualizar o pseudo-código do algoritmo A-KUCAS.

Tabela 11: Transações para simulação do KUCAS

Transação de Software	Código	Grupo
RETIRADA/SAQUE	t7	R001

Fonte: Elaborada pelo autor.

As transações financeiras são agrupadas por grupos para agilizar a recuperação das informações**.** Para a visualização do cenário, o diagrama a seguir permite visualizar a interação do usuário com a aplicação de software no ATM.

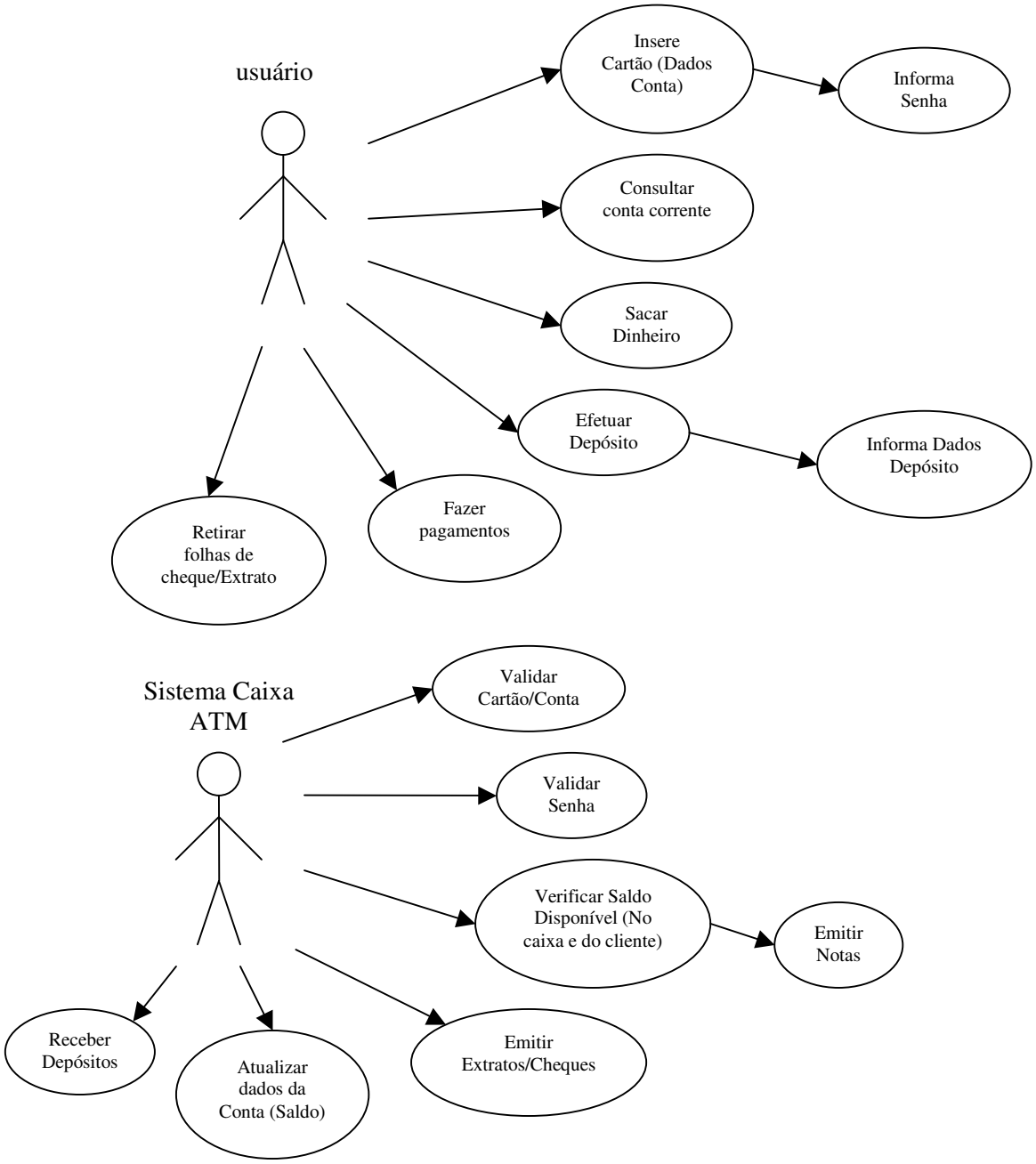


Figura 24: Diagrama de Casos de Uso – cenário do usuário em um ATM
Fonte: elaborada pelo autor

O Diagrama de Sequências abaixo representa a sequência de troca de informações numa aplicação de saque, no Sistema KUCAS.

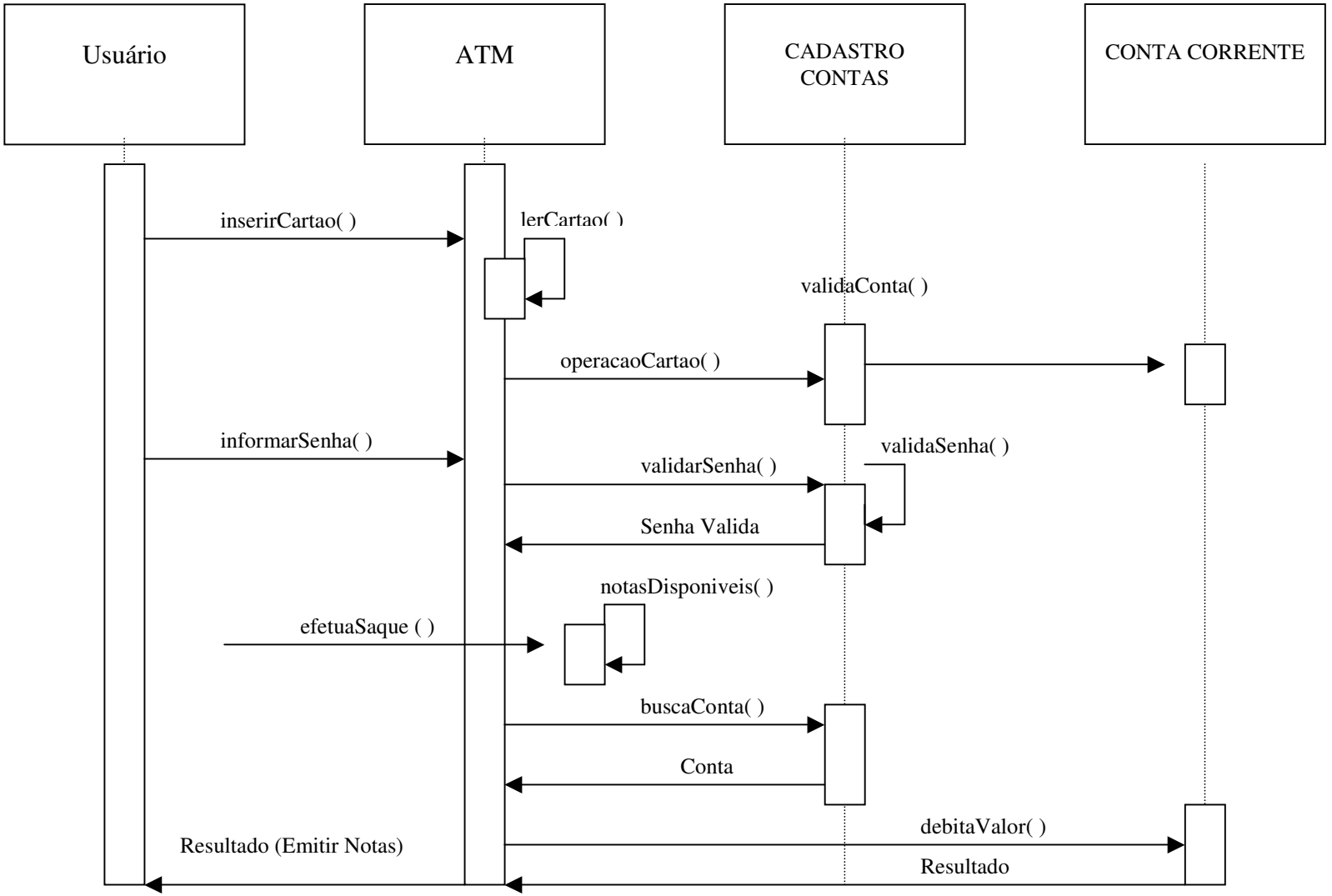


Figura 25: Seqüência de uma aplicação financeira de saque

Fonte: elaborada pelo autor

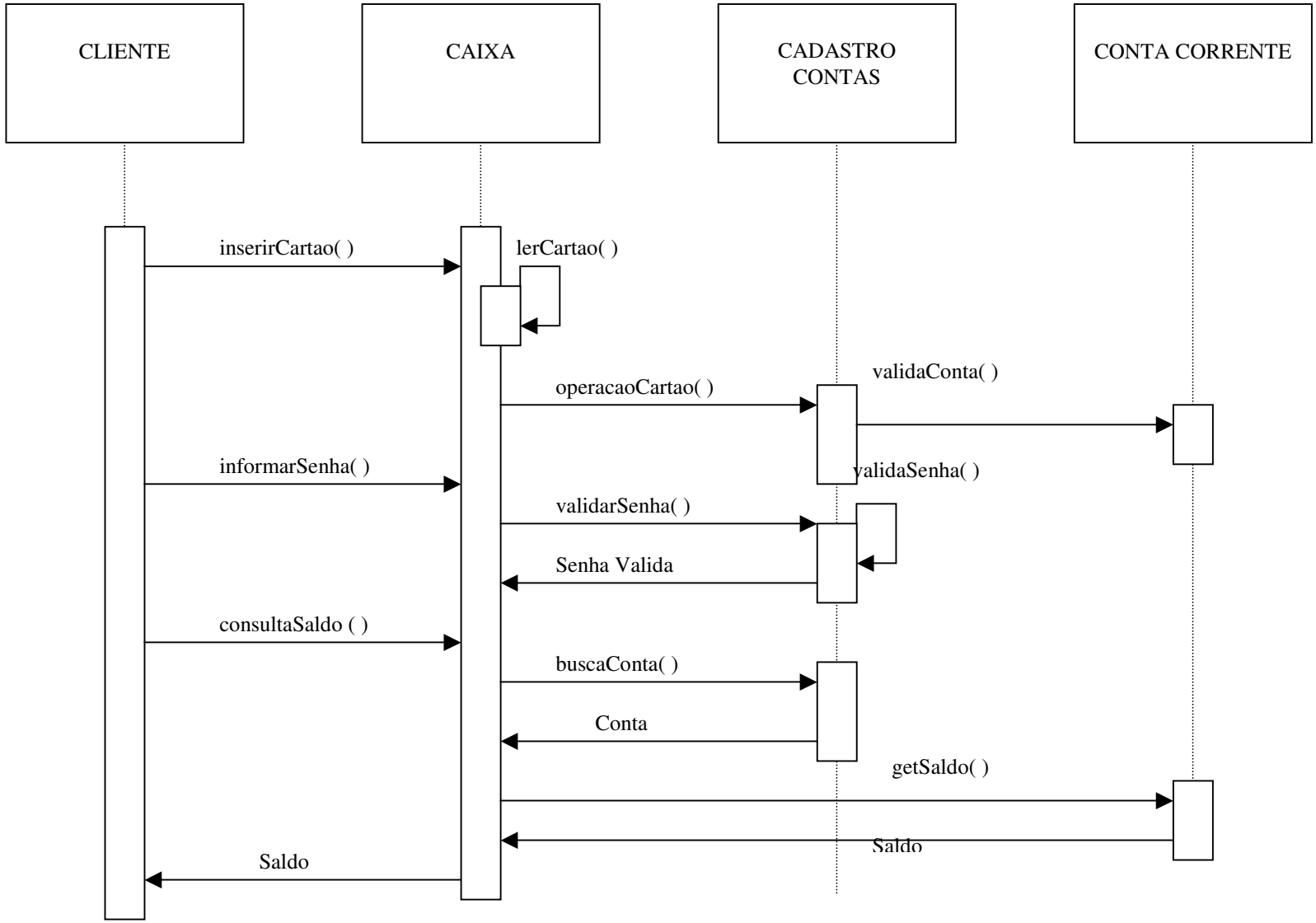


Figura 26: Seqüência de uma aplicação financeira de consulta de saldo

Fonte: elaborada pelo autor

6.6.1 Captura das variáveis comportamentais

As variáveis comportamentais são as informações que se obtém ao longo de um intervalo de tempo Δt que compreende o tempo entre o acesso e a saída do usuário na aplicação de software, ou seja, o tempo de duração da sessão.

O primeiro passo é identificar o usuário, verificar se existem restrições de confiança para ele e capturar as variáveis do ambiente, como horário, localização, acessos permitidos, valores permitidos de saque, entre outras.

6.6.1.1 Captura da variável who

Seja o usuário definido por User1.

Abaixo indica-se as variáveis **who** capturadas.

Tabela 12: Classe usuários Who

Nome da variável	Conteúdo
Nro_user	3550271
Senha_user	******
Imagem_face_user	JPG
Dt_ult_img	20060306
confiança-user	0.1
desconfiança_user	0.9

Fonte: Elaborada pelo autor.

A Tabela 12 representa o contexto do usuário, através das variáveis apresentadas é possível identificar o nível de confiança atribuído ao usuário, qual a imagem de sua face, qual a data da última captura da imagem da face, qual a senha e a chave de identificação. A variável Senha-user, que indica a senha do usuário, é um campo protegido nas bases de dados, e como definição da política de segurança, tentativas de acesso ao sistema com senhas erradas pode dar margem a um comportamento duvidoso e faz diminuir o nível de confiança atribuído

ao usuário. Pode-se considerar que algumas informações são provenientes do chip do cartão de acesso, utilizado pelo usuário.

6.6.1.2 Captura da variável where

A variável comportamental **where** é o conjunto de variáveis do endereço do equipamento e periférico no qual o usuário está executando uma transação de software.

As variáveis nomeadas para atender a classe de localização **where** estão definidas na tabela abaixo:

Tabela 13: Classe localização Where

Nome da variável	**Descrição da variável**
Cod_Disp	M1898AP81
End_local	Rua Melbourne
Bairro_local-	Assunção
CEP_local	05085060
Cidade-local	São Paulo
País_local	Brasil
Nro_seq-local	1
Coord-GPS	Alt11log221

Fonte: Elaborada pelo autor.

A Tabela 13 representa o contexto da localização do equipamento ou periférico que o usuário utiliza, através das variáveis apresentadas é possível identificar o local onde o usuário utilizou a transação de software e se está ou não nas proximidades de seu endereço informado na variável who.

6.6.1.3 Captura da variável when

A variável comportamental when é o conjunto dos horários em que o usuário interage com a transação de software, que identifica o início e o fim de uma transação de software.

As variáveis nomeadas para atender a classe de variáveis de horários when estão definidas na tabela abaixo:

Tabela 14: Classe temporal When

Nome da variável	**Descrição da variável**
Cod_Disp	M1898AP81
Data_inicial	060306
Data_final	060306
Cod_trans	T3
Nro_seq	1

Fonte: Elaborada pelo autor.

A Tabela 14 apresenta uma série de variáveis, e a combinação das mesmas permite uma análise dos horários em que o usuário utiliza a aplicação de software, num determinado dispositivo, num determinado lugar. A combinação de todas estas variáveis permite fazer o cruzamento de várias informações de contexto como, por exemplo, qual o tempo gasto num local e qual o tempo gasto numa aplicação de software.

6.6.1.4 Captura da variável What

A variável comportamental **what** representa o conjunto de transações de software que o usuário utilizou.

As variáveis nomeadas para atender a classe de transações what estão definidas na tabela abaixo:

Tabela 15: Classe transacional What

Nome da variável	Descrição da variável
Cod_trans	t7
Nome_trans	Saque em espécie
Grupo_trans	Grupo das transações
Nro_seque_trans	R001
Valor_trans	1000,00

Fonte: Elaborada pelo autor.

A Tabela 15 representa o contexto das transações definidas pela variável what, através das variáveis apresentadas é possível identificar qual a transação utilizada, qual o valor da transação. A combinação das variáveis de who, where, when e what permite definir quem utilizou determinada transação, onde o usuário utilizou a transação, se está nas proximidades do seu endereço ou distante, qual o horário em que a transação foi utilizada e comparando com as bases de históricos é possível saber se o valor da transação está entre os valores historicamente utilizados pelo usuário.

As informações obtidas do usuário User1 interagindo com uma transação de saque de valores.

6.6.1.5 Verificando variável rest

Abaixo as restrições de confiança existentes cadastradas para o usuário.

Tabela 16: Tabela de Restrições de Confiança

Nome da variável	**Restrição**
Cod_rest	R1
Cód-user	6339786
Tipo_rest	Saques em transação t7 não pode ser superior a
Valor-trans	R$ 1.050,00
Desc-Rest	Limitação de saque

Fonte: Elaborada pelo autor.

A Tabela 16 indica a restrição de confiança existente para o comportamento do usuário.

É feita uma comparação do comportamento atual com as restrições. Neste caso, o usuário está fazendo um saque de R$ 1.000,00 e tem restrição caso o saque seja superior a R$ 1.050,00.

Para esta simulação suponhamos que o valor definido no sistema Kucas para a variação da confiança seja o valor 0.01.

Neste caso a confiança aumenta, pois o usuário não teve um comportamento fora da normalidade, e o usuário é autenticado.

Supondo-se que o mesmo usuário faça um segundo acesso e efetue e um saque de R$ 1000,00. O sistema KUCAS autentica o usuário, aumenta a confiança e atualiza a variável **why** por ser indício de um hábito.

Supondo-se que o mesmo usuário faça um terceiro acesso e efetue um saque de R$ 2000,00. O sistema KUCAS aciona a tecnologia de reconhecimento facial, calcula a incerteza IF = 1 – (0.02 + 0.89) = 0.10; se o usuário for reconhecido, o sistema Kucas diminui a confiança passando a ser (0.01;0.88), pois o usuário fez um comportamento que atinge a

restrição; autentica o usuário, afinal, ele foi reconhecido, mesmo num comportamento de restrição. Neste caso, o sistema Kucas não aumenta a restrição de valor para R$ 2.000,00 automaticamente, pois existe uma restrição inicial de limite de R$ 1.000,00.

Se o usuário não for reconhecido, o sistema Kucas calcula a incerteza, diminui a confiança e bloqueia o acesso à aplicação.

De posse das variáveis comportamentais é montada uma matriz comportamental do usuário.

6.7 Matriz Comportamental do Usuário

Tabela 17 : Matriz comportamental

Who	Where	When	What	Why	Rest	Conf	If incerteza
3550271	M1898AP81	06032006 05:53 - 06:00	T7 Saque 1000		T7Saquemaior1050	(0.01;0.90)	-
3550271	M1898AP81	06032006 06:05 – 06:09	T7 Saque 1000	Saque 1000	T7Saquemaior1050	(0.02;0.89)	-
3550271	M1898AP81	06032006 06:11 – 06:14	T7 Saque 2000 limite atinge restrição, mas é reconhecido, então é autenticado	Saque 1000	T7Saquemaior1050	(0.01;0.88)	0.01
3550271	M1898AP81	06032006 06:11 – 06:14	T7 Saque 2000 limite atinge restrição. Não é reconhecido, então o acesso é bloqueado	Saque 1000	T7Saquemaior1050	(0.01;0.88)	0.01

Fonte: Elaborada pelo autor.

A Tabela 17 representa a matriz comportamental do usuário, um log com o registro de todo o seu comportamento, restrições cadastradas, confiança adquirida e incertezas calculadas.

O sistema Kucas vai variando a confiança e autenticando continuamente, ou não, um usuário conforme seu comportamento.

Em relação à restrição pode-se considerar duas possibilidades:

1-Restrição pode ser definida previamente pelo sistema ou pelo usuário, como por exemplo, três tentativas inválidas de senha, bloqueiam o acesso; ou saque de valores após um determinado horário.

2-Restrições que o próprio usuário gera baseada em seus comportamentos anteriores, como por exemplo, o usuário faz saques constantes de valores médios de R$ 1000,00; ele não tem restrições previamente cadastradas; num outro dia ele faz um saque de R$ 1500,00, neste caso, o sistema vai acionar a tecnologia de reconhecimento facial, pois ele mudou o comportamento, e se ele for reconhecido, o sistema autentica o usuário e permite o saque desejado, mas cria uma restrição de que saques maiores de R$ 1500,00 deverão ser acionados a tecnologia de reconhecimento facial. Ou seja, todos os comportamentos anteriores são analisados, havendo mudanças na média, cria se uma restrição. Havendo restrições previamente definidas pelo usuário, elas se sobrepõem às restrições do comportamento.

7 Conclusões e Trabalhos Futuros

7.1 Considerações Finais

Neste trabalho foi apresentado um procedimento tecnológico-corpóreo-contextual para efetuar a análise comportamental de usuários baseado em confiança e utilizando-se as dimensões definidas na computação ciente de contexto, com o objetivo de dar robustez ao desenvolvimento do sistema de autenticação contínua de usuários KUCAS, definido neste projeto.

Como inovação surge uma política de segurança adaptativa ao usuário e que varia de acordo com as restrições de confiança ao comportamento do usuário.

Conforme proposto, esta tese apresenta uma abordagem sobre a computação ciente de contexto como base para utilização de suas definições num sistema de autenticação contínua. Apresenta um levantamento sobre a tecnologia do reconhecimento facial e os mecanismos utilizados de modo a fornecer um entendimento sobre a utilização desta tecnologia no sistema KUCAS. Apresenta um estudo teórico sobre a análise comportamental na psicologia e faz uma analogia com a utilização em autenticação. Procura aperfeiçoar um estudo sobre a variação dos níveis de confiança em um sistema de autenticação contextual e para isto apresenta um resumo teórico sobre a confiança matemática da teoria das evidências de Dempster-Shafer.

A análise comportamental foi baseada nas teorias de SKINNER (1967) – adequadamente aplicáveis no presente contexto – sendo que as definições de comportamento, citadas no capítulo 4, serviram de base teórica para a definição das variáveis comportamentais associadas com as definições da computação ciente de contexto.

O Sistema KUCAS lida com diferentes situações para o comportamento, e adota o particularmente no devido contexto, o behavorismo radical de Skinner, ou seja, analisa um

comportamento que pode ser controlado por regras e faz um controle, neste caso perfeitamente legítimo, e uma análise de variáveis que podem vir a influenciar no comportamento humano-moral-corporal.

O comportamento humano tem uma margem de probabilidade de incerteza, em diversos aspectos físicos e psicológicos, pode ser manipulado pela própria pessoa em sua individualidade e sofrer variações ao longo do tempo, mas ele é intransferível e de foro íntimo, possui um caráter de sigilo pessoal, o usuário não tem como perder ou esquecer o comportamento, como esquece uma senha; ninguém pode roubá-lo e usá-lo indevidamente. A confiança é baseada no comportamento atual e nos anteriores, então considera-se que a confiança dada ao usuário, não pode ser perdida, nem esquecida e nem roubada.

No estudo de caso envidaram-se esforços no sentido de validar o mecanismo de análise comportamental e verificar o quanto possível sua aplicabilidade e funcionalidade na dimensão social aqui evidenciada.

A forma de determinar as restrições comportamentais pode variar; pode-se criar um arquivo contendo as informações de restrições e compará-las, ou utilizar mecanismos matemáticos e estatísticos. Para os testes, foi utilizado o procedimento sócio-tecnológico de extração da informação e comparação.

Em relação à tecnologia de reconhecimento facial, esta vem evoluindo e melhorando no mundo todo. Por segurança, e como resultado de vários testes, conforme citados no capítulo 3, a modalidade em 3D é a melhor e a que mais se adapta a proposta do sistema de autenticação KUCAS. No entanto, dentre as inúmeras variáveis, a tecnologia em 3D esbarra ainda com um fator que é preponderante em qualquer tipo de investimento e, sobretudo no campo da informática, que é o do impedimento financeiro, uma vez que se trata de ação que demanda a liberação de altas verbas para que se possa efetuá-la com maior margem de acerto e eficiência, o que inviabiliza tráfego constante de imagens nas redes.

Foram feitos vários testes com a tecnologia de reconhecimento facial em 2D, que apesar de não ter segurança na identificação e autenticação, colaborou para uma melhor definição da proposta do Sistema KUCAS, uma vez que a idéia inicial era idealizar um sistema de autenticação contínua com a tecnologia de reconhecimento facial; com os testes da tecnologia de reconhecimento facial foi visível a sua fragilidade em sistemas de autenticação de usuários, por isto o interesse em complementá-la com análise comportamental e a confiança.

É de suma importância mencionar um teste realizado em 2002 com o software de reconhecimento facial Bastet em 2D, desenvolvido pela juntamente com alunos do Centro Universitário da FEI, onde foi possível perceber a importância da iluminação e da qualidade da imagem nesta tecnologia, o que permitiu detectar sensível melhora do Sistema KUCAS. Em 2004 e 2005 também foram feitos testes com outro software de mercado de reconhecimento facial em 2D; os problemas vivenciados nestes testes, como a troca de versão de sistema operacional, troca de versão de software, acúmulo de informações nas bases de dados de imagens, qualidade das imagens geradas pelas câmeras de vídeo, incidência muito alta de falsos positivos e falsos negativos. Outrossim, como agravante, surgiram erros na definição da topologia da rede, os quais tornaram possível a benéfica definição de escolha da tecnologia de reconhecimento facial em 3D como a mais indicada e ainda atingir índice de melhoria da arquitetura do framework F-KUCAS.

Os esforços para elaboração deste projeto foram canalizados no sentido de utilizar a tecnologia de reconhecimento facial, mas na impossibilidade, o sistema KUCAS por ser modular, permite que a mesma seja substituída por outras tecnologias biométricas.

Também é possível inserir no sistema KUCAS outras tecnologias biométricas para se obter informações do usuário, como, por exemplo, considerar se o usuário está sozinho ou na companhia de outras pessoas conhecidas do sistema. Pode-se instalar uma balança no

ambiente e comparar o peso do usuário com as informações cadastrais, além de ser possível identificar o usuário pela voz, pela palma da mão e pelo modo como digita as informações solicitadas.

Ao utilizar a confiança no Sistema KUCAS, cria-se uma forma de se aceitar riscos e conceder privilégios a quem se confia, e por isto, a autenticação é viável. Dando autonomia para o sistema confiar ou não, no usuário, e autenticá-lo nas aplicações de software em redes de computadores.

A atribuição da confiança foi feita de modo linear e a mesma pode variar por ambiente tecnológico, por sistema, por localização, por horário e pela atividade que o usuário está fazendo. Conforme o sistema KUCAS vai sendo utilizado, e com o aumento das informações comportamentais, o usuário pode ser identificado por seus hábitos (comportamentos repetitivos) e o mecanismo de autenticação do sistema KUCAS terá informações para prever as intenções comportamentais do usuário.

Convém salientar que o mecanismo de autenticação proposto pode evoluir para atribuir a confiança de forma exponencial, ou seja, se houver uma mudança brusca no comportamento do usuário, a confiança diminui rapidamente, de modo exponencial, sendo lenta a sua recuperação.

A proposta de um teste em equipamentos ATM elevou-nos a um novo patamar de visualização otimizada do mecanismo de autenticação proposto na simulação.

A computação ciente de contexto, conforme a prospecção que realizamos, pode vir a permitir a exploração de informações que possibilitam expandir o relacionamento entre atividades humanas e serviços computacionais no sentido de facilitar a interação do usuário com o computador, o que permite ao Sistema KUCAS coletar informações e armazená-las.

Para obter as informações de contexto relevantes ao Sistema KUCAS procurou-se tornar efetiva uma categorização de tipos de contexto, a qual auxiliou na análise

comportamental do usuário, por meio das dimensões de contexto, iniciando por Who (quem) que permite a identificação da identidade do usuário. No que tange ao dispositivo Where (onde) que permite a identificação da localização, é utilizada em associação com a dimensão de identidade who e a respeito da temporal when reafirma-se que o intuito deverá ser fornecer novas funcionalidades às aplicações. When (quando) que permite a identificação do contexto temporal, poderá ser utilizado para informar a duração do tempo em que o usuário permaneceu no auto-atendimento (ATM) e pode ser utilizada para indicar quando o usuário permanece em um determinado local ou sessão da aplicação do software. What (o quê) que oportuniza a identificação da dimensão responsável por identificar a atividade do usuário e torna possível considerar todas as atividades que o usuário faz na aplicação de software. Why (por que) denota a intenção do usuário, este contexto foi associado com o comportamento repetitivo do usuário que pode caracterizar um "hábito". A dimensão de contexto How (como) não foi considerada, mas projeta uma atenuante uma vez que é muito complexa a obtenção de informações contextuais, ficando dessa maneira, impossível determinar com exatidão o como – modo em que ocorre - da ação de um usuário.

Em relação à privacidade, o sistema KUCAS invade a individualidade – podendo ferir direito humanos - dos usuários, mas adotando-se com critérios muito bem estabelecidos uma política de segurança bem definida, com contratos, acompanhada de explicações dos benefícios do sistema, pode evitar transtornos.

O Sistema KUCAS contribui com o paradigma da autenticação, ou seja, da tríade tradicional que garante a autenticação de uma pessoa (you know - senha); (you have – código de acesso); (you are – aspectos biométricos do usuário) e contribui com o item comportamento, como parte da autenticação.

Em relação à aplicabilidade do Sistema KUCAS, ele pode ser utilizado em qualquer aplicação em redes de computadores com e sem fio, desde que a aplicação esteja preparada

para interagir com uma API de comunicação entre a aplicação e o sistema KUCAS; deve se considerar também a capacidade de processamento do dispositivo para instalar a API.; deve se considerar também uma API adequada para cada sistema operacional.

Em relação a escalabilidade, o sistema KUCAS possui uma arquitetura modular e em camadas, isto permite a evolução do mesmo além de permitir acrescentar outros dispositivos e sensores, bem como trocas de sistema operacional e da tecnologia do reconhecimento facial.

O Sistema KUCAS é viável tanto em aplicações de software longas e encadeadas como nas curtas, sendo possível fazer uma autenticação contínua do usuário ao longo do tempo em que ele estiver utilizando as aplicações.

Numa visão social pode-se dizer que o Sistema KUCAS autentica aquele no qual confia, e que, conforme vimos, é um mecanismo de segurança, e se os usuários souberem que são autenticados baseados na confiança e no comportamento deles, talvez pudessem ser reduzidos os índices de ataques às aplicações como roubo de valores e de informações nas redes de computadores e aos dispositivos em geral.

7.2 Trabalhos Futuros

Como extensão deste trabalho, pode ser dimensionada uma exploração de melhoria na proposta do algoritmo A-KUCAS. Urge que o módulo S- KUCAS seja conduzido a um melhor redimensionamento de segurança para um efetivo acionamento das redes de sensores que ativam as câmeras de vídeo no ambiente. A arquitetura do framework F-KUCAS necessita de uma criteriosa revisão, de modo a permitir a incorporação de novos elementos técnicos, sendo necessário detalhar mais a arquitetura do sistema, detalhar as API's sugeridas, redefinir as funções de cada API e detalhar o módulo de segurança S-KUCAS.

Ainda dentro desta perspectiva futurística há a necessidade de efetuar um número mais intenso de testes que possam fornecer mais informações para medir a maturidade do

framework – para que o *framework* possa atingir sua maturidade e conseqüente aumento da usabilidade. Faz-se necessário que o mesmo seja testado intensamente de modo a permitir a criação de um conjunto maior de serviços a serem distribuídos.

Ainda em relação ao *framework* F-KUCAS é necessária a customização do mesmo para permitir diferentes formatações e definições das imagens da face dos usuários, originadas de vários tipos de câmeras de vídeo, de modo a agilizar o processo de reconhecimento facial e transferir para si a atividade de melhoria da imagem, antes de enviá-la para a tecnologia de reconhecimento facial.

Uma outra perspectiva futura é utilizar mecanismos de inteligência artificial e conduzir a uma evolução do Sistema KUCAS para um procedimento baseado em conhecimentos.

Aplicações possíveis do sistema KUCAS são sistemas de controle de acesso de pessoas, sistemas de avaliação de ensino a distância, entre outras.

Testes efetivos da utilização de aplicações de software nas redes sem fio.

Testes exaustivos com vários tipos de usuários que permitam refinar e melhorar a proposta.

REFERÊNCIAS

ABOWD, G. D., MYNATT, E. D. **Charting past, present, and future research in ubiquitous computing**. In: ACM Transactions on Computer-Human Interaction (TOCHI, 2000), v. 7, n. 1, pp. 29–58., 2000.

ABOWD, G.D., MYNATT, E.D., RODDEN, T. **The Human Experience**. In: Pervasive Computing, v.1, n.1, pp. 48-57, 2002.

ACM Press, ISBN 1-58113-142-9, 1999, pp 263-270, disponível em http://doi.acm.org/10.1145/313451.313556. acessado em 22/08/2005 e ACM Code of Ethics and Professional Conduct Adopted by ACM Council 10/16/92. disponível em http://www.acm.org/constitution/code.html acessado em 01/08/2005

ACOSTA, E; TORRES L.; ALBIOL, A. - **An Automatic Face Detection and Recognition System for Video Indexing Applications.** Proceedings of IEEE 27th Conference on Acoustics, Speech and Signal Processing (ICASSP 2002), Vol. 4, pp. 3644-3647, 2002

ARRUDA JUNIOR,C.R.E.; BULCÃO NETO, R.F.; PIMENTEL, M.G.C. **Open context-aware storage as a Web Service**. 1st International Workshop on Middleware for Pervasive and Ad Hoc Computing (MPAC). Rio de Janeiro, 2003.

ARYANANDA, L. **Recognizing and Remembering Individuals: Online and Unsupervised Face Recognition for Humanoid Robot**, Proceedings of the 2002 IEEE/RSJ International Conference on Intelligent Robots and Systems(IROS 2002), pp.1202-1207, Vol.2, 2002

ASCENSO, J.; VALENTIM, J., PEREIRA, F. - **Informação de Textura e de Geometria 3D** - Instituto Superior Técnico - Instituto das Telecomunicações – Lisboa – Portugal, 2002.

ASHBOURN, J. - **The distinction between authentication and identification**, 2000. Disponível em: <http://homepage.ntlworld.com/avanti/authenticate.htm>. acessado em 22/08/2005

ATICK, J. J., GRIFFIN P. A., REDLICH A. N. , **Statistical approach to shape and shading: reconstruction of 3D face surfaces from single 2D images**, Neural Computation, Vol. 8, 1996.

BACKES, M.; BAGGA, W.; KARJOTH,G.; SCHUNTER, M. **Efficient Comparison of Enterprise Privacy Policies**, 19th ACM Symposium on Applied Computing, Special Track "Security", Nicosia, Cyprus, March 2004.

BAER, D. M.; WOLF, M. M.; RISLEY, T. R. **Some current dimensions of applied behavior analysis**. Journal of Applied Behavior Analysis, 1, pp. 91-97. , 1968.

BANDURA, A. **Principles of Behavior Modification**. Holt, Rinehart and Winston, New York. 1969

BELHUMEUR P. N. H.; KRIEGMAN D.J., **Eigenfaces vs. Fisherfaces: recognition using class specific linear projection**, Pattern Analysis and Machine Intelligence, IEEE Transactions., 1997

BEYMER, D. ; POGGIO, T. **Face Recognition from one example view**. A.I. Memo 1536, Massachusetts Institute of Technology, September 1995.

BIRNBRAUER, J. S. **Applied behavior analysis, service and the acquisition of knowledge**. The Behavior Analyst, 2, pp.15-21., 1979

BOHN, J.; COROAMĂ, V., LANGHEINRICH, M., FRIEDEMANN, M., ROHS, M. **Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing**, Institute for Pervasive Computing, ETH Zurich, Switzerland, acessado em 24/02/2004 em http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf

BROSSO, I.; BRESSAN, G.; RUGGIERO, W.V. **Evaluation of E-business applications performance** . In: 2nd WSEAS Int. Conf. on Simulation, Modeling and Optimization (ICOSMO 2002), 2002, Skiathos. Proceedings of the WSEAS International Conferences, 2002. v. 1. p. 1971-1976.

BRUNELLI R.; POGGIO, T. , **Face recognition: features versus templates**, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. 10, Outubro 1993, pp. 1042-1052

CALDER, B. J. ; MALTHOUSE, E. C. - Journal Of Consumer Psychology, 13(4), 387–394, Lawrence Erlbaum Associates, Inc. **The Behavioral Score Approach to Dependent Variables** ND 2003, também disponível em http://www.mediamanagementcenter.org/research/reports/rbs.pdf acessado em 28/07/2005

CALLAWAY; E. **Wireless Sensor Networks: Architectures and Protocols**. CRC Press, August 2003

CAMPOS, T.E. **Técnicas de Seleção de Características com Aplicações em Reconhecimento de Faces** - Dissertação de Mestrado - Instituto de Matemática e Estatística da Universidade de São Paulo, Maio, 2001

CAM-WINGET N., HOUSLEY R., WAGNER D., WALKER J. **Wireless networking SECURITY: Security flaws in 802.11 data link protocols**. Communications of the ACM, Volume 46 Issue 5, 2003

CARVALHO, T.C.M.B; CUGNASCA, C. E.; GUTIERREZ, M. **Computação Pervasiva**- anotações de aula. Escola Politécnica da Universidade de São Paulo, 2004.

CASSANDRAS, C. G. ; **Discrete Event Systems Modeling and Desempenho Analysys** , Aksen Associates IRWIN 1993 isbn 0-256-11212-6, 1993

CBA – Consultores Biométricos Associados – disponível em http://www.consultoresbiometricos.com.br

CHELLAPPA, R.; WILSON, C., SIROHEV, S **Human and machine recognition of faces: A survey**. In Proceedings of IEEE, vol. 83, pp. 705-740, May 1995

CHEN, L.; PEARSON, S.; VAMVAKAS,A.; **A Trusted Biometric System** – Internal Accession Date Only of Hewlett-Packard Company, 2002 também disponível em http://www.hpl.hp.com/techreports/2002/HPL-2002-185.pdf acessado em 11/10/2005

COLMENAREZ, A. J.; T. S. HUANG, **Frontal-View Face Detection**, Proceedings of the SPIE, vol. 2501, no.1, pp. 90-95, 1995

CZERWINISKI, S., et al. **An Architecture for a secure service discovery**, Mobicom, 1999.

DARRELL, T.; B. MOGHADDAM; PENTLAND A. - **Active Face Tracking and Pose Estimation in an Interactive Room**, Proceedings of the 1996 IEEE Computer Society Conference on Computer Vision and Pattern Recognition , pp. 67-72, 1996.

DEBAR, H.; DACIER, M.; WESPI, A. - **Towards a taxonomy of intrusion detection systems** - IBM Zurich Research Laboratory, Ruschlikon, Switzerland, 1998.

DEMPSTER, A. P. - **Upper and Lower Probabilities Induced by a Multi-valued mapping**, Annals of Mathematical Statistics, Vol.38, pp.325-339, 1967.

DEY, A. K., ABOWD, G. D. **Towards a Better Understanding of Context and Contet-awareness**. 1st International Symposium on Handheld and Ubiquitous Computing (HUC'99), Junho, 1999 também disponível no Gvu technical report GIT-GVU-99-22, College of Computing, Georgia Institute of Technology, 1999.

DEY, A. K. **Understanding and using context**. Personal and Ubiquituos Computing, 5(1). Special issue on Situated Interaction and Ubiquitous Computing. 2001

ETEMAD, K. ; CHELLAPPA, R. **Discriminant analysis for recognition of human face images**, Journal of the Optical Society of America , vol. 14, pp. 1724-1733, 1997.

FAWCETT, T.; PROVOST, F. **Adaptive Fraud Detection** – Data Mining and Knowledge Discovery 1, 291-316, Kluwer Academic Publishers, 1997.

FEDERAL - Authentication in a Electronic Banking Environment – Technical Report of Federal Financial Institutions Examination Council, 2000 K Street, NW, Suite 310 . Washington, DC 20006., August 8, 2001.

FINEP - Relatório Setorial disponível em: http://www.finep.gov.br/PortalDPP/relatorio_setorial/impressao_relatorio.asp?lst_setor=20 acessado em 05/10/2005.

FOWLER, Martin, SCOTT, Kendall. **UML distilled.** A brief guide to the standart object modeling language. Addison Wesley Longman Inc. , 2000.

FRISCHHOLZ R. W.; DIECKMANN U. **BioID: A Multimodal Biometric Identification System** In: IEEE Computer Society, v. 33, n.2, pp.64-68, February 2000.

GANGER, G.R. **Authentication Confidences** Carnegie Mellon University, School of Computer Science CMU-CS-01-123, abril, 2001.

GOULARTE, R., SANTOS, R. F., MILAGRES, F. G., MOREIRA, E. S. **Um Serviço de personalização automática de conteúdo para TV interativa**. In: Anais do WebMidia 2003 - IX Simpósio Brasileiro de Sistemas Multimídia e Web, Salvador, Novembro, 2003, v.2, n.1, pp. 547-550.

GOVINDARAJU, V.; SRIHARI, S.N; SHER , D.B., **A computacional model for face location**, Proc. 3rd Int. Conf. on Computer Vision, pp.718-721, 1990.

HANSMANN, U. **Pervasive Computing Handbook**. The Mobile World. Springer Verlag; 2nd edition, August 2003.

HENRICKSEN, K., INDULSKA, J. and RAKOTONIRAINY, A. **Modeling Context Information in Pervasive Computing Systems.** *Proc. Pervasive Computing*, Zurich,Switzerland, LLNCS 2414:167-180, NAGHSHINEH, F.M. M. (ed) Springer Verlag, 2002

HEO, J.; ABIDI, B.; PAIK, J.; ABIDI, M. **Face recognition: evaluation report for FaceIt® Identification and Surveillance** – Proc. of SPIE 6th. International Conference on Quality Control by Artificial Vision – 2003 - Vol. 5132, pp.551-558, Gattinburg, TN, May 2003, também disponível em http://imagin.utk.edu/publications/papers/2003/heo-qcav03.pdf acessado em 22/08/2005

HU L.; EVANS, D., **Secure aggregation for wireless networks**, In Workshop on Security and Assurance in Ad hoc Networks, January 2003, disponível em http://www.cs.virginia.edu/~evans/pubs/wsaan-abstract.html. acessado em 22/08/2005

ISHII,H.; ULLMER, B. **Tangible bits: towards seamless interfaces between people, bits and atoms** – Proceedings of CHI'07, pp. 234-241, 1997 também disponível em IBM Systems Journal, vol. 39 nos. 3 e 4, 2000.

JOHNSTON, J. M. - **Distinguishing between applied research and practice**. The Behavior Analyst, 19, 35-47, 1996

JONES, G.J.F.;BROWN, P.J. **Context-aware retrieval for ubiquituous computing environments -** Invited paper in *Mobile and ubiquitous information access*, Springer Lecture Notes in Computer Science, Vol. 2954, pp. 227-243, 2004

KAGAL, L.; UNDERCOFFER JEFFREY, A. J., VIGIL T., **Enforcing security in ubiquitous environments**, tech. rep., University of Maryland, Baltimore County, 2001

KAGAL, L.; et al. **Centaurus: a framework for intelligent services in a mobile environment**, ISWSAWC, April 2001.

KARPIJOKI V. - **Security in ad hoc networks**, in Seminar on Network Security, 2001.

KAUFMANN, M.; JAMESON - **A Modelling both the context and the user**. Personal and Ubiquitous Computing, 5:29–33. 2001

KIM T.; LEE S.; LEE J.; KEE,S. ; KIM S., **Integrated approach of multiple face detection for video surveillance**, Proceedings, IEEE 16th Conference on Pattern Recognition, pp. 394-397, vol.2, 2002.

KIRBY M. S., **Application of the Karhunen-Loeve procedure for the characterization of human faces**, Pattern Analysis and Machine Intelligence, IEEE Transactions., vol. 12, no. 1, pp. 103-108, 1990.

KLOSTERMAN, A.J.; GANGER,G. **Secure Continuous Biometric-Enhanceed Authentication**, Carnegie Mellon University, 2004

KOHONEN, W., **Neural Information Processing in Real-World Face Recognition Applications**, IEEE Expert, vol. 11, no. 4, pp. 7-8, August 1996

KUPERSTEIN, M., **Face Recognition: the Oldest Way to Verify ID is Now the Newest**, Defense and Security Electronics, vol. 28, no. 3, pp. March 1996.

LEE C. H., KIM J. S., PARK K. H., **Automatic face location in a complex background using motion and color information**, Pattern Recognition, Vol. 29, No. 11, 1996, pp. 1877-1889., 1996

LIU H. CHENGJUN , **Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition**, Image Processing, IEEE Transactions, Wechsler, 2002.

MATSUNO, K; LEE C. W.; KIMURA S.; TSUJI S., **Automatic Recognition of Human Facial Expressions**, Proceedings of the 1995 IEEE International Conference on Computer Vision, pp. 352-357, 1995.

MILAGRES, F.G. **Segurança Baseada em Informações de Contexto para Redes Sem Fio**. Dissertação de Qualificação de Mestrado. Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. São Carlos, 2003.

MILLER, S., NEUMAN, C., SCHILLER, J., AND J. SALTZER, **Kerberos Authentication and Authorization System**, MIT Project Athena, Cambridge, MA, December 1987 também disponível em http://web.mit.edu/kerberos, acessado em 11/02/2006.

MITTELSDORF, A.W. **Uma plataforma para computação com confiança baseada em monitor de máquinas virtuais e atestamento dinâmico** tese de doutorado, Universidade de São Paulo, 2004.

MOGHADDAM, B.; LEE, J.; PFISTER, H.; MACHIRAJU, R., **Silhouette-Based 3D Face Shape Recovery**, Graphics Interface, June 2003 (Graphics Interface, TR2003-081)

MOGHADDAM, B.; LEE, J.H.; PFISTER, H.; MACHIRAJU, R., **Model-Based 3D Face Capture with Shape-from-Silhouettes**, IEEE International Workshop on Analysis and Modeling of Faces and Gestures (AMFG), pp. 20-27, October 2003 (IEEEXplore, TR2003-084)

MOGHADDAM, B; LEE, J.; PFISTER, H.; MACHIRAJU, R., **Finding Optimal Views for 3D Face Shape Modeling**, IEEE International Conference on Automatic Face and Gesture Recognition (FG), pp. 31-36, May 2004 (IEEEXplore, TR2004-024)

MURRAY, D.; BASU A., **Motion Tracking with an Active Camera**, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 16, no. 5, pp. 449-459, May 1994.

NALWA, V.S.A., **Guided Tour of Computer Vision**, AT&T, 1993.

PANKANTI S.; BOLLE M.R.; JAIN A. **Biometrics: The Future of Identification** In: IEEE Computer Society, v. 33, n.2, pp.46-49, February 2000.

PASCOE, J. **Adding generic contextual capabilities to wearable computers**. In: International Symposium on Wearable Computers, 1998, pp. 92–99.

PAULA, M. **Avaliação de Padrão de digitação como mecanismo de autenticação** – dissertação de mestrado em engenharia elétrica- Escola Politécnica da USP, 2004.

PENTLAND, A.; MOGHADDAM, B.; STARNER, T.**View-based and modular eigenspaces for face recognition.** In IEEE Conference on Computer Vision and Pattern Recognition, 1994.

PENTLAND A. S.; CHOUDHURY T. **Face Recognition for Smart Environments** In: IEEE Computer Society, v. 33, n.2, pp.50-55, February 2000.

PETTENGER, O.; GOODING, C. T. **Teorias da aprendizagem na prática Educacional**. São Paulo: EPU, 1977.

PHILLIPS, P., RAUSS, P., DER, S. **FERET (Face Recognition Technology) Recognition Algorithm Development and Test Report** (ARL-TR-995): U.S. Army Research Laboratory. 1996.

PHILLIPS, P; WECHSLER , H., HUANG, J. AND RAUSS, P. **The feret database and evaluation procedure for face recognition algorithms, Image and Vision Computing** , vol. 16, no. 5, pp. 295-306, 1998.

PHILLIPS P.J.; MARTIN A.; WILSON C.L.; PRZYBOCKI M. **An Introduction to Evaluating Biometric Systems** In: IEEE Computer Society, v. 33, n.2, pp.56-63, February 2000.

PHILLIPS P. J.; GROTHER P.; MICHEALS R.; BLACKBURN D.; TABASSI, M.; BONE, E. J. M. - **FRVT 2002 Evaluation Report**, Technical Report, http://www.frvt.org. acessado em 22/08/2005

PHILLIPS P. J.; MOON, H.; RAUSS, P.; RIZVI, S. **The feret evaluation methodology for face recogniotn algorithms**. In IEEE Proceedings of Computer Vision and Pattern Recognition, pages 137-143, June 1997.

PLATZER, C **Trust-based Security in Web Services**. Master's Thesis – Technical University of Vienna, Maio, 2004.

POTTER, E. J.; **Customer Authentication: The Evolution of Signature Verification in Financial Institutions**. In Journal of Economic Crime Management, Summer 2002, Volume 1, Issue 1, 2002; também disponível em: www.jecm.org

RATHA, N.K.; CONNELL, J. H.; BOLLE, R. M. **Enhancing security and privacy in biometrics-based authentication systems** – IBM Systems Journal – volume 40, number 3, 2001

RAVI, S.; RAGHUNATHAN, A.; POTAPALLY, N. **Securing Wireless Data: System Architecture Challenges** - International Symposium on System Synthesis (ISSS),October,2002 - http://www.princeton.edu/~sravi/papers/2002_isss_invited.pdf acessado em 22/08/2005

RYAN, N.; CINOTTI, T.S.; Raffa, G., **Smart environments and their applications to cultural heritage** – Proceedings UBICOMP/2005, Tkio, Japão, 11/setembro de 2005.

RUBENFELD, M., WILSON, C. **Gray Calibration of Digital Cameras -** NIST Mugshot Best Practice. NIST IR-6322, 1999

RUGGIERO, W.V. **Modelo de Segurança em redes Ad-Hoc**.
Tese (Livre Docência) – Escola Politécnica, Universidade de São Paulo, 2002.

RUGGIERO, W.V. - **Medição e Distribuição de Confiança em redes Ad-Hoc** – (versão em português) - International Conference on Wireless Security, Las Vegas, Estados Unidos, 2002.

SALBER,. D.; DEY, A.K; ABOWD, G. D **The context toolkit: aiding the development of context-enabled applications** Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit, Pittsburgh, Pennsylvania, United States, Pages: 434 – 441, 1999, ACM Press New York, NY, USA ISBN:0-201-48559-1

SANDMANN, H.; SENAGA, M.; BROSSO, I. **Bastet – Tecnologia de Reconhecimento Facial**, In Proceedings of WORKCOMP'2002 – ITA - Instituto Tecnológico da Aeronáutica – São José dos Campos/SP - Brasil, Outubro, 2002.

SANTOS JR., J. B., GOULARTE, R., MOREIRA, E. S., FARIA, G. B. **The Modeling of Structured Context-Aware Interactive Environments**. In: Transactions of the SDPS Journal of Integrated Design and Process Science, v. 5, n. 4, Dezembro, 2001. pp. 77–93.

SAVVIDES, M.; VIJAYA KUMAR, B.V.K.; KHOSLA PRADEEP - **Illumination normalization using logarithm transforms for face authentication**, Lecture Notes in Computer Science, Springer-Verlag Heidelberg, volume 2680/2003, January 2003.

SCHEIER, B. **Thinking Sensibly About Security in an Uncertain World**. Copernicus Books, Ed.1, 2003

SCHILIT, B., THEIMER, M. **Disseminating active map information to mobile hosts**. In: IEEE Network, v.8, n.5, 1994. pp. 22–32.

SCHMIDT M., **Subscriptionless mobile networking: Anonymity and privacy aspects within personal area networks**, tech. rep., Institute for Data Communications Systems, University of Siegen, Germany, 2001.

SCHNEIDERMAN, H. ; KANADE, T., **A Statistical Method for 3D Object Detection Applied to Faces and Cars**, Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, Vol. 1, pp. 746-751, 2000.

SCHNEIER, B. **Beyond Fear. Thinking Sensibly About Security in an Uncertain World**. Copernicus Books, Ed. 1. 2003.

SCHWEITZER, C.M. **Mecanismo de Consolidação de Confiança Distribuída para Redes Ad Hoc**. Tese de Doutorado. Escola Politécnica da Universidade de São Paulo, 2004.

SHAFER, G. **A mathemathical theory of evidence**. Princeton, Princeton University Press, 1976.

SIAU, K.; SHENG, H.; NAH, F.; DAVIS, S. **A qualitative investigation on consumer trust in mobile commerce ,** International Journal of Electronic Business , vol.2, no. 3, pp.283-300, 2004

SKINNER, B.F. **Ciência e Comportamento Humano**. São Paulo: Martins Fontes. (1967)

SKINNER, B. F. **Questões Recentes na Análise Comportamental** (2ª ed.). São Paulo: Papirus Editora. (Original publicado em 1989), 1995.

SIDMAN, M. . **Coercion and its fallout**. Boston, MA:, 1989, Authors Cooperative. Portuguese translation: M. A. Andery & T. M. Sério (translators), *Coerção*. Campinas (Brazil): Editorial Psy, 1998.

STAATS, A.W.; STAATS, C.K. **Comportamento humano complexo: uma extensão sistemática dos princípios da aprendizagem.** Trad. Carolina M. Bori. São Paulo, Ed. Pedagógica e Universitária / Ed. da Universidade de São Paulo, 1973. (Coleção Ciências do Comportamento)

STAJANO, F. **Security for Ubiquitous Computing**. John Wiley & Sons Ed. 1, 2002.

STALLINGS, W. **Cryptography and Network Security-Principles and Practice** – Prentice Hall, second edition, 1998.

SZABÓ, K.; **Customer Authentication, as a matter of risk in Financial Services** Periodica Polytechnica Ser.Soc.Man. SCI Vol. 11, no.1, pp. 13-26, 2003

TEOH, A. - **Nearest Neighbourhood Classifiers in a Bimodal Biometric Verification System Fusion Decision Scheme** , Journal of Research and Practice in Information Technology, Vol. 36, No. 1, February 2004

TRIPATHI, A.K. **Reflections on Challenges to the Goal of Invisible Computing -** ACM Ubiquity — Volume 6, Issue 17 (May 17 - May 24, 2005)

TODOROV, J. C. **The K&S in Brazil**. *Journal of the Experimental Analysis of Behavior*, 54, 151-152., 1990

TRUONG, K.N., ABOWD, G.D., BROTHERTON, J.A. ***Who*, What, When, Where, How: Design Issues of Capture & Access Applications**. Georgia Institute of Technology Technical Report GIT-GVU-01-02. January 2001.

TURK M.; PENTLAND A . **Face Recognition Using Eigenfaces**, Proceedings of IEEE Conference on ComputerVision and Pattern Recognition (CVPR/91), pp. 586-591, 1991.

UCHÔA , J.Q.; PANONTIM S. M.; NICOLETTI, M. C. **Elementos da Teoria de Evidência de Dempster-Shafer** - Universidade Federal de São Carlos (UFSCar), 2004 disponível em http://www.dc.ufscar.br/~carmo/relatorios/dempster.pdf acessado em 21/07/2005

VERAS, A. L. M.; RUGGIERO, W. V. **Proposta de modelo para acompanhamento e análise de comportamentos de usuários em aplicações seguras na Web**. In: CONFERÊNCIA IADIS IBERO-AMERICANA WWW/INTERNET 2005, 2005, Lisboa. Acta da Conferência IADIS Ibero-Americana WWW/Internet 2005. Lisboa: IADIS, 2005. v. v1, p. 499-502..

VIEIRA, R. C. ; TENORIO, M. B. ; ROISENBERG, M. ; BORGES, P. S. S – **Comparação entre Redes Neurais Artificiais e Rough Sets para a classificação de Dados** – VI Brazilian Conference on Neural Networks – VI Congresso Brasileiro de Redes Neurais, pp. 175-178, Junho 2-5, 2003 – Centro Universitário da FEI, São Paulo - SP - Brazil.

YACOOB, Y.; L. S. DAVIS, **Recognizing Human Facial Expressions from Long Image Sequences using Optical Flow**, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 6, pp. 636-642, June 1996.

WACTLAR, H. **Informedia – Search and Summarization in the Video Medium** - Proceedings of Imagina 2000 Conference, Monaco, January 31 - February 2, 2000.

WANG, H.; CHANG, S., **A highly efficient system for automatic face region detection in MPEG video**, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 7, No. 4, Agosto 1997, pp. 615-625

WANT, R.; HOPPER,A.; FALCAO, V.; GIBBONS, J.**. The Active Badge Location System.** ACM Transactions on Information Systems, 10(1), 1992.

WAYMAN J. L. **Federal Biometric Technology Legislation** In: IEEE Computer Society, v. 33, n.2, pp. 76-80., February 2000

WEISER, M. **The computer for the 21st century**, Scientic American , vol. 265, no. 3, pp. 66-76; . 94-104, 1991.

WEISER, M. **Some Computer Science Issues in Ubiquitous**. In: Communications of the ACM, v.6, n.7, pp. 75-84, 1993.

WENG J., EVANS C., HWANG W., **An Incremental Learning Method for Face Recognition under Continuous Video Stream**, Proceedings of the Fourth IEEE International Conference on Automatic Face and Gesture Recognition, pp.251-256, 2000

WHITMAN, M. E. **Enemy at the Gate: Threats to Information Security**. In: Communications of the ACM, v.46, n.8, pp. 91-95, Agosto, 2003.

WITTER,G.P. **Metaciência e Psicologia**, Editora: ALINEA e à TOMO, ISBN: 8575161075, 2005

ZHANG Z., ZHU L., LI S., ZHANG H., **Real-Time Multi-View Face Detection**, Fifth IEEE International Conference on Automatic Face and Gesture Recognition, May, 2002, pp.149-154.

ZHOU, L.; HAAS Z. J., **Securing AD HOC networks**, IEEE Networks, 1999.

APÊNDICE A

Esquema do algoritmo do Sistema A-KUCAS (pseudo-portugues).

<A-KUCAS>
<Identifica login do usuário>
<ok>
<aciona contador de tempo>
<captura variável de contexto comportamental who>
<captura variável de contexto comportamental where>
<captura variável de contexto comportamental when>
<verifica se usuário já utilizou o sistema>
<primeira vez>
<atribui o nível de confiança mínima para o usuário>
<aciona módulo S-KUCAS>
<captura imagem da face do usuário>
<aciona tecnologia de reconhecimento facial>
<armazena imagens da face do usuário>
<define restrições de confiança do usuário ou do sistema se houver>
<não é a primeira vez>
<captura variável de contexto comportamental what>
<verifica se tem restrições comportamentais de confiança>
<sim, tem restrições comportamentais de confiança>
<compara comportamento atual com as restrições de confiança>
<verifica se atingiu alguma restrição comportamental>
<sim, atingiu restrição de confiança>
<aciona o módulo de segurança S-KUCAS>
<captura imagem da face do usuário>
<ativa tecnologia do reconhecimento facial>
<calcula a incerteza>
<verifica se a face capturada é a do usuário da aplicação>
<não>
<aciona módulo de segurança S-KUCAS e bloqueia a aplicação de software>
<sim>
<continua autenticando o usuário>
<diminui a confiança>
<não atingiu restrições de confiança>
<mantém a confiança>
<armazena comportamento atual nas bases de dados comportamentais>
<usuário autenticado
<não tem restrições de confiança no comportamento atual>
<compara comportamento atual com base de históricos>
<sim, tem comportamento igual ao atual >
<criar o hábito why>
<armazena o comportamento nas bases de dados
<aumenta a confiança>
<não tem comportamento igual ao atual>
<aciona o módulo de segurança S-KUCAS>
<aciona tecnologia de reconhecimento facial>
<calcula a incerteza>

<verifica se face do usuário igual das bases de dados>
<sim>
<mantém a confiança>
<armazena comportamento atual nas bases de dados>
<não>
<bloqueia transação>
<encerra contador de tempo>
<atualiza variável who>
<verifica volume de informações comportamentais armazenadas>
<aciona modulo_limpeza no framework>
</A-KUCAS>