UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

Uma Proposta de Autenticação de Usuários para Ensino a Distância

por

MAURICIO FIORESE

Dissertação submetida à avaliação, como requisito parcial para
a obtenção do grau Mestre em
Ciência da Computação

Prof. Dra. Liane M. R. Tarouco
Orientadora

Porto Alegre, abril de 2000.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Fiorese, Mauricio

Uma Proposta de Autenticação de Usuários para Ensino a Distância/Mauricio Fiorese – Porto Alegre: PPGC da UFRGS, 2000.

90f.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR – RS, 2000. Orientadora: Tarouco, Liane M. R.

1. Educação a distância. 2. Redes de computadores. 3. Segurança. 4. Autenticação de usuários. 5. Controle de acesso. 6. Dispositivos biométricos. I. Tarouco, Liane M. R. II. Título.

Agradecimentos

Gostaria de deixar meus sinceros agradecimentos a todos que de alguma forma contribuíram para o êxito deste trabalho, e em especial:

- a Deus, pela luz, pela força, coragem e perseverança ao longo de todo este período;
- à minha orientadora, Dr. Liane M. R. Tarouco, pela atenção concedida, pela orientação e pela oportunidade de desenvolvimento desta dissertação de mestrado;
- aos professores do PPGC da UFRGS pelo valioso conhecimento que me forneceram e especialmente ao professor Raul F. Weber, pelas dicas e aconselhamentos ao longo desta etapa;
- ao CNPq, pela bolsa de estudo;
- a meus pais e familiares, pelo apoio em todos os sentidos ... este trabalho é dedicado a vocês!
- a minha namorada Melissa, pela compreensão e confiança, por toda a força e apoio ao longo deste período, e pelos importantíssimos "Boa Sorte!";
- aos meus colegas de mestrado, pelo prazer de suas amizades, conversas e trocas de conhecimentos, futebol, e outras coisas mais;
- a todos meus amigos, especialmente ao Rodrigo de Vit, Anderson Maciel, Alessandro Boeira e Fábio Vazquez. Valeu Galera !!!!

Sumário

Lista de Abreviaturas

API:	Application Program Interface
BioAPI:	Biometric Application Program Interface
CERT:	Computer Emergency Response Team
CGI:	Common Gateway Interface
PPGC:	Programa de Pós-Graduação em Computação
CPF:	Cadastro de Pessoas Físicas
DBMS:	DataBase Management System
DNS:	Domain Name Server
FAR:	False Acceptance Rate
FBI:	Federal Bureau of Investigation
FRR:	False Rejection Rate
HA-API:	Human Authentication - Application Program Interface
HTML:	Hypertext Markup Language
HTTP:	HyperText Transfer Protocol
IP:	Internet Protocol
JDK:	Java Development Kit
JDBC:	Java DataBase Connectivity
JNL:	Numerical Library for Java
JSDK:	Java Servlet Development Kit
MD5:	Message Digest 5
NCSA:	National Center for Supercomputing Applications
ODBC:	Open DataBase Connectivity
OEM:	Original Equipment Manufacturers
PC:	Personal Computer
PIN:	Personal Identification Number
RFC:	Request for Comments
RISC:	Reduced Instruction Set Computers
SAM:	Security Accounts Manager
SAPI:	Speech Application Programming Interface
SDL:	Specification and Description Language
SDL/GR:	Specification and Description Language / Graphic Representation
SDL/PR:	Specification and Description Language / Plain Representation

SDK:	Software Development Kit
SMTP:	Simple Mail Transfer Protocol
SQL:	Structured Query Language
SSL:	Secure Sockets Layer
TACACS:	Terminal Access Controller Access Control System
TCP/IP:	Transmission Control Protocol / Internet Protocol
UFRGS:	Universidade Federal do Rio Grande do Sul
UML:	Unified Modeling Language
URL:	Uniform Resource Locator
VLSI:	Very Large Scale Integrated
WWW:	World Wide Web

Lista de Figuras

Lista de Tabelas

Resumo

Este trabalho investiga diferentes estratégias e técnicas de autenticação de usuários visando determinar quais podem ser integradas em um ambiente de educação a distância.

Diversas soluções de autenticação existentes no mercado foram analisadas para se determinar as mais adequadas. Buscou-se as soluções consideradas factíveis de utilização, seja pelo custo ou quantidade de equipamentos extras envolvidos, seja pela simplicidade operacional ou pelo grau de certeza das medidas efetuadas.

A partir desta análise foi delineado um modelo de autenticação que integra várias técnicas de autenticação a fim de chegar a um nível de segurança maior que senhas, utilizadas na maioria dos sistemas de educação a distância.

O sistema funciona como um *proxy*, cuja função é controlar o acesso à páginas *Web* através da combinação de senhas, perguntas randômicas, dispositivos biométricos e checagem randômica, ao mesmo tempo que gera *logs* da atividade do aluno no curso. Estes *logs* conterão informações como dia e hora do acesso, tempo dispendido em cada página, endereço IP da máquina do aluno, entre outras. Estas informações podem ser utilizadas tanto para avaliar o aluno, como para gerar seu perfil estatístico, que servirá para gerar alertas na medida em que os dados do perfil sofrerem mudanças acima dos limites estabelecidos, durante a atividade do aluno.

Um protótipo do sistema foi implementado para validar a solução delineada ao longo do trabalho.

A integração dos métodos de autenticação, que identificam o aluno e a máquina em que ele está trabalhando, com as rotinas de avaliação do procedimento de educação a distância, foi um dos principais resultados alcançados.

Palavras-Chave: Educação a distância, redes de computadores, segurança, autenticação de usuários, controle de acesso, dispositivos biométricos

Title: *"A Solution for User Authentication for Distance Learning"*

Abstract

This work investigates different strategies and techniques of user authentication in order to determine which ones may be integrated in a distance learning environment.

Several authentication solutions available on the market are analyzed in order to find the most appropriate. The criteria used to determine the best solutions involve cost or amount of equipments involved, operational simplicity, and degree of confidence or results obtained.

Based on this analysis, an authentication model that integrates several authentication techniques is delineated in order to obtain greater security than those used in most distance learning systems, based only on passwords.

This system works like a proxy whose function is to control access to Web pages through the combination of passwords, random queries, biometric devices and random checks, at the same time that it generates logs of student's activity during a course. These logs contain information about day and hour of access, time spent on each page, IP address of the student's machine and so on. This information can be used both to evaluate the student and to generate his/her statistical profile. This profile is used to give an alarm when the data of the profile undergo changes above the established limits, during the student's activity.

A prototype of the system has been implemented to validate the solution designed.

The integration of the authentication methods, which identifies both the student and the machine where he/she is working, with the evaluation routines of the distance learning procedure, is one of the main reached results.

Keywords: Distance Learning, computer networks, security, user authentication, access control, biometric devices.

1 Introdução

Hoje em dia, existe um aumento da dependência de sistemas de computador em quase todos os aspectos dos negócios, comércio e educação, e por isso muitas organizações estão confiando na efetividade de seus sistemas para terem sucesso. O aumento da ênfase em segurança de computadores significa que apenas pessoas autorizadas poderão acessar as informações armazenadas nos sistemas. Neste contexto, destaca-se a importância da autenticação de usuários.

A definição mais geral de autenticação dentro de sistemas de computação engloba a verificação da identidade, autenticação da origem e conteúdo da mensagem. O conceito de verificação de identidade, especificamente, aplica-se a usuários humanos, sistemas de computação e processos executando nesses sistemas. A autenticação pelo conhecimento de uma informação secreta ou a pela posse de um dispositivo físico de autenticação único são igualmente válidos para todos os tipos de entidades descritos acima. Por outro lado, autenticação biométrica apenas tem sentido no contexto de seres humanos [KIM95].

Mecanismos de autenticação confiáveis são críticos para a segurança de qualquer sistema de informação automatizado [NAT94]. Quando um usuário legítimo é verificado, são aplicadas técnicas de controle de acesso para permitir seu acesso aos recursos do sistema. 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.

Existe uma variedade de métodos para executar autenticação de usuários, os quais 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 ele sabe, tal qual uma senha; algo que o ele possui, tal qual um *token* de autenticação; e alguma característica física do usuário, tal qual a impressão digital ou padrão de voz. De modo a usar estas características para verificar a identidade de um indivíduo, os sistemas de computadores usam *software, hardware* ou a combinação dos dois [FIO98].

Com o advento da Internet, especialmente da WWW (*World Wide Web)* e do hipertexto, muito se tem investido no estudo e exploração da rede de computadores como uma ferramenta eficiente para o ensino [OSW97].

O objetivo dos sistemas de ensino a distância é proporcionar material instrucional para um número maior de alunos potencialmente espalhados em uma grande área. Desta forma, permite-se, por exemplo, que novos conhecimentos cheguem a alunos isolados dos grandes centros de ensino e que professores sejam compartilhados eficientemente por diversos alunos localizados em diferentes locais [MAC99].

Atualmente, existem várias estratégias de autenticação de usuários sendo utilizadas em aplicações comerciais. Porém, em ambientes de ensino a distância as restrições de ordem econômica e operacional são diferentes. Deve-se tanto buscar uma solução de menor custo, quanto uma maior simplicidade de procedimentos.

No ambiente de educação a distância, a autenticação é especialmente importante durante procedimentos de avaliação, embora também deva ser complementada por análise do comportamento ou padrão de uso do usuário durante sua utilização em condições normais de estudo. A qualificação do educando para atribuição de notas ou conceitos, em algumas situações, exige a verificação de que o avaliando seja ele próprio [RUT99]. Em [RIT97], também é demonstrada esta preocupação através da seguinte questão: "Como se ter certeza de que o aluno X é realmente o aluno X que ele diz ser?"

A maioria dos sistemas de educação a distância disponíveis no mercado tentam resolver o problema da autenticação do aluno através da combinação nome/senha, dentre eles o *Learnig Space, Virtual-U, WebCt, TopClass e o AulaNet* [LOP99]. Porém, existem vários problemas com autenticação baseada em senhas. Ela baseia a autenticação de um indivíduo em algo que pode ser copiado, esquecido ou adivinhado por uma pessoa não autorizada [BRO98]. Além disso, existem vários métodos que um intruso pode usar para atacar sistemas baseados em senhas [KES99], dentre eles adivinhação da senha (*password guessing*), ataque do dicionário (*dictionary attack*), monitoramento do tráfego na rede (*sniffing*), engenharia social, cavalos-de-tróia e cópia de anotações. Os CERTs (*Computer Emergency Response Teams*) estimam que aproximadamente 80% dos incidentes de segurança registrados são relacionados às senhas fracas.

O avanço da biometria, aliado à redução dos preços dos equipamentos, fez com que nos últimos anos surgissem dúzias de sistemas biométricos a baixo custo, abrindo a possibilidade de uso de dispositivos mais incrementados sem a necessidade de grandes investimentos.

No decorrer deste trabalho, várias estratégias de autenticação existentes serão analisadas com vistas a se determinar quais as que podem ser integradas em um ambiente de educação a distância. Buscar-se-ão aquelas que sejam factíveis de utilização, seja pelo custo ou quantidade de equipamentos extra envolvidos, seja pela simplicidade operacional ou pelo grau de certeza das medidas efetuadas.

Vale ressaltar que existe uma diferença entre autenticação para fins de educação a distância e para sistemas comerciais, ou seja, o sistema tem que ter algum mecanismo de proteção contra a "personificação" do usuário com a sua conivência, isto é, o aluno pede para outra pessoa fazer a prova em seu lugar. Deste modo, buscar-se-ão métodos que procurem minimizar este problema ou pelo menos dificultar este procedimento. Sabe-se, porém, que por mais sofisticada que seja a solução, sempre poderão existir métodos para enganar o sistema.

Este trabalho propõe-se a estudar as diferentes técnicas e mecanismos de autenticação de usuários aplicáveis em um cenário de educação à distância, analisando suas características e tendências futuras, e propondo um modelo mais completo, econômico e factível que satisfaça as características de segurança requeridas por este cenário.

A integração dos métodos de autenticação, que identificam o aluno e a máquina em que ele está trabalhando, com as rotinas de avaliação do procedimento de educação a distância, será um dos principais resultados esperados.

Após esta breve introdução, é apresentado, no capítulo 2, o estado da arte em termos de autenticação de usuários, assim como uma análise comparativa entre as principais soluções encontradas no mercado. O capítulo 3 descreve o modelo de autenticação proposto. No capítulo 4 são descritos os aspectos relacionados à implementação, implantação do protótipo e uma avaliação do sistema e, finalmente, o capítulo 5 contém as conclusões finais do trabalho.

2 Autenticação de Usuários

O crescimento das redes abertas fez com que surgissem vários problemas de segurança, que vão desde o roubo de senhas e interrupção de serviços até problemas de personificação, onde uma pessoa faz-se passar por outra para obter acesso privilegiado.

Com isso, surgiu a necessidade de autenticação, que consiste na verificação da identidade tanto dos usuários quanto dos sistemas e processos. Os mecanismos de autenticação de usuários dividem-se em três categorias: baseados no conhecimento (o que se sabe), baseados em propriedade (o que se possui) e baseados em características (o que se é) [YOU96].

2.1 Soluções de Autenticação Baseadas no Conhecimento (O que se sabe)

A autenticação pelo conhecimento é o modo mais utilizado para fornecer uma identidade a um computador, no qual destaca-se o uso de segredos, como senhas, chaves de criptografia, PIN (*Personal Identification Number*) e tudo mais que uma pessoa pode saber. Porém, como visto na introdução deste trabalho, existem vários problemas com a autenticação baseada em senhas.

Vários métodos foram propostos para tentar tornar a autenticação baseada em senhas mais segura, entre eles o uso de geradores randômicos de senhas, checagem pró-ativa [BIS95], utilização de senhas descartáveis (*one-time passwords)* e sistemas de desafio/resposta (*chalenge/response systems*), modificações no processo de *login* [MAN96] e combinação com outros mecanismos de autenticação de usuários como *smartcards* [WU96].

2.1.1 Senhas Descartáveis (*One-Time Passwords)*

Uma senha descartável é aquela que só é usada uma vez no processo de autenticação. Com isso, evita o ataque da captura e repetição da senha, porque a próxima conexão requererá uma senha diferente. Existem muitas implementações de senhas descartáveis baseadas em *software* e *hardware*. As implementações baseadas em *hardware*, utilizam dispositivos especiais como *smartcards* e *tokens*.

As senhas descartáveis podem ser classificadas em duas categorias: sincronizadas no tempo e desafio/resposta. No método de autenticação baseado em tempo sincronizado, computa-se uma nova senha a cada 30 segundos, de acordo com um algoritmo pré-definido que utiliza o dia, a hora e um segredo. Em sistemas baseados em desafio/resposta, o sistema envia um desafio para o usuário (geralmente um número ou um *string*), que retorna uma resposta baseada em um algoritmo pré-definido.

O S/KEY, definido pela RFC 1760, é um sistema que implementa senhas descartáveis. A cada conexão é usada uma senha diferente, impedindo ataques baseados

na captura ou adivinhação de senhas. Existem várias implementações compatíveis com S/KEY que podem ser encontradas na Internet.

2.1.2 Perguntas Randômicas (*Random Queries)*

Perguntas randômicas é um método de autenticação baseado em desafio/resposta. Em uma primeira etapa, faz-se um cadastro do usuário, no qual ele responde a um questionário com perguntas variadas como a bebida favorita, o número da identidade, CPF, data de aniversário, lugar de nascimento, etc.

No momento da conexão, o usuário entra com sua identificação. O sistema, então, escolhe uma pergunta do questionário de forma aleatória e desafia o usuário. Se sua resposta coincidir com a previamente armazenada no questionário, a conexão é permitida e lhe são atribuídos os direitos de acesso correspondentes.

Empresas de cartão de crédito geralmente utilizam este método para autenticar seus usuários em ligações telefônicas. A vantagem é que ele pode ser totalmente implementado em *software*, não necessitando de *hardware* adicional.

2.1.3 Análise das Soluções Baseadas no Conhecimento

O mecanismo de autenticação mais popular e usado nos sistemas de computação é a autenticação através de senhas. As vantagens deste tipo de autenticação são:

- Onde o usuário estiver, o segredo estará com ele;
- O segredo pode ser facilmente modificado, se necessário;
- O segredo é facilmente inserido através do teclado, não necessitando de dispositivos especiais;

Entretanto, este tipo de autenticação tem algumas limitações: as senhas podem ser adivinhadas, roubadas ou esquecidas.

Soluções alternativas, como perguntas randômicas e senhas descartáveis, geralmente são de simples utilização e bem aceitas pelos usuários, baratas e fáceis de implementar. Além disso, não requerem *hardware* adicional como outras soluções baseadas em propriedade e características. Outra vantagem que vale destacar é que elas podem ser integradas em sistemas baseados em rede e na *Web*, além de diversos sistemas operacionais. Elas evitam vários ataques e problemas baseados em senha, mas não impedem que um aluno divulgue seu segredo para outro fazer o curso em seu lugar.

A utilização de perguntas randômicas, porém, acrescenta uma dificuldade adicional ao aluno que quiser divulgar seu segredo, pois, ao contrário de contar apenas uma palavra (como no caso de senhas), terá que divulgar todas as informações constantes no questionário que serve de base para as perguntas randômicas.

A integração de soluções baseadas em conhecimento com dispositivos biométricos oferece dois níveis de autenticação, e pode ser uma solução interessante para evitar o problema acima citado.

Outras soluções não computacionais também têm sido propostas. Segundo o professor Sigulem [SIG99], da Escola Paulista de Medicina, a solução utilizada naquela instituição na determinação da identidade do aluno para fins de avaliação em um ambiente de educação a distância, foi sobrecarregar o aluno com quatro ou mais horas de trabalho por dia. Através da análise dos trabalhos, consegue-se determinar a identidade do aluno, assim como seu rendimento, porém isto requer muita dedicação e acompanhamento. O custo desse acompanhamento individual pode tornar esta solução inviável.

Algumas instituições obrigam seus alunos a distância a comparecerem em uma sala de aula para avaliação de forma presencial. Outras utilizam centros de certificação, especializados nesse tipo de avaliação. Porém, devido à distância geográfica envolvida em cursos de educação a distância, estas soluções podem ser inviáveis.

2.2 Soluções de Autenticação Baseadas na Propriedade (O que se tem)

As soluções de autenticação baseadas na propriedade caracterizam-se por um objeto físico que o usuário possui. Este objeto pode ser um cartão inteligente (*smartcard*), uma chave ou um *token (*dispositivo eletrônico semelhante a uma calculadora, usados para calcular senhas descartáveis). As desvantagens deste tipo de autenticação são que os objetos físicos podem ser perdidos, roubados ou esquecidos e o custo adicional do *hardware*. A vantagem baseia-se no princípio de que a duplicação do objeto de autenticação poderá ser mais cara que o valor do que está sendo guardado.

É comum ver-se a combinação de autenticação por propriedade com autenticação baseada em senhas, fornecendo dois fatores de autenticação. Sem os dois, um usuário não pode ser autenticado na conexão a um sistema ou aplicação. Com a crescente utilização de cartões inteligentes já é possível obter-se três fatores de autenticação, através de sua combinação com senhas e dispositivos biométricos.

2.2.1 Mecanismos de Autenticação Baseados em *Tokens*

Tokens são dispositivos semelhantes a uma calculadora de mão e que não necessitam de dispositivos de leitura/escrita adicionais. Eles fornecem autenticação híbrida, usando tanto "algo que o usuário possui" (o próprio dispositivo), como "algo que o usuário conhece" (um PIN de 4 a 8 dígitos). Sistemas de autenticação por *tokens* baseiam-se em um dos seguintes esquemas: autenticação por desafio/resposta ou autenticação sincronizada no tempo.

Nos sistemas baseados em desafio/resposta, o usuário insere sua identificação no sistema. O sistema apresenta, então, um desafio randômico como, por exemplo, na forma de um número de sete dígitos. O usuário, por sua vez, digita seu PIN no *token* e informa o desafio apresentado pelo sistema. O *token*, gera a resposta correspondente

cifrando o desafio com a chave do usuário, a qual ele informa ao sistema. Enquanto isso, o sistema calcula a resposta apropriada baseado no seu arquivo de chaves de usuários. Quando o sistema recebe a resposta do usuário, ele a compara com a resposta que acabou de calcular. Se forem idênticas, a conexão é permitida e são atribuídos ao usuário os direitos de acesso correspondentes.

Quando são utilizadas calculadoras de desafio/resposta, é dado a cada usuário um dispositivo que foi unicamente chaveado. Ele não pode utilizar o dispositivo de nenhum outro usuário para seu acesso. O sistema deve ter um processo ou processador para gerar um par de desafios/resposta a cada tentativa de conexão, baseado nos dados informados pelo usuário. Cada desafio é diferente, para que a observação de uma troca de desafios/resposta com sucesso não traga informações suficientes para uma conexão subseqüente. A desvantagem deste esquema é o número de mensagens trocadas entre o usuário e o servidor.

A grande maioria dos fabricantes de *tokens* utilizam autenticação por desafio/resposta. A empresa *Security Dynamics Inc (http://www.securitydynamics.com)*, porém utiliza o esquema sincronizado no tempo, do qual, manipula sua patente. Neste esquema, um algoritmo proprietário que roda tanto no *token* quanto no servidor, gera números idênticos que mudam no decorrer do tempo. Quando deseja entrar no sistema, o usuário informa seu PIN de quatro dígitos seguido por um número de seis dígitos mostrado no momento pelo *token*. Ao receber o PIN, o servidor localiza a chave do usuário e calcula qual deveria ser a senha de acesso para aquele momento, comparando-a com a que o usuário enviou. Se forem iguais, libera o acesso à rede. Um dos problemas desta técnica é que ela exige uma sincronização entre o *token* e o servidor. Para solucioná-lo, ambos devem ser sincronizados pelo horário de Greenwich.

2.2.1.1 *SecureID*

SecureID é um sistema de dois fatores de autenticação desenvolvido e comercializado pela *Security Dynamics, Inc.* Ele é utilizado para identificar usuários de redes e sistemas e prevenir acesso não autorizado.

Cada usuário do *SecureID* tem uma senha ou PIN memorizada e um *token* com um visor de cristal líquido. O *token* mostra um novo valor pseudo-randômico, chamado de *tokencode*, em um intervalo de tempo fixo, normalmente de 60 segundos. O usuário combina o fator memorizado com o *tokencode*, pela simples concatenação ou entrando com o valor no teclado do *token*, que cria a senha requerida para liberar o acesso ao recurso protegido.

Basicamente, o sistema é composto por três componentes: o *token* propriamente dito, um *software* cliente, e um *software* servidor para autenticação e gerenciamento centralizado.

O *token* contém um microprocessador de 8 bits, um relógio, um visor de cristal líquido, uma bateria e, em alguns modelos, um teclado. A unidade é acomodada em um compartimento que, se aberto, apaga a memória. A figura 2.1 apresenta alguns modelos de *tokens SecureID*.

FIGURA 2.1 - Modelos de *tokens SecureID*

O *software* cliente consiste em uma modificação do sistema de autenticação do *host* para que ele possa se comunicar com um *ACE/Server*. Atualmente, existem versões do *ACE/Server* para uma variedade de sistemas operacionais, incluindo *Windows NT, Sun Solaris, IBM AIX e HP-UX* [SEC99].

Dentre as vantagens apresentadas pelo fabricante do *SecureID* [SEC99] destacam-se: facilidade de uso; autenticação dos usuários na rede, sistemas, aplicações ou nível de transação; e o fato de não necessitarem de leitores adicionais. As principais desvantagens são que, como todos os dispositivos de *tokens*, eles podem ser roubados; e a necessidade de não deixar as baterias acabarem.

As suas principais aplicações são na proteção de linhas de acesso discadas, na segurança de *hosts* e aplicações, e na segurança de redes TCP/IP (*Transmission Control Protocol / Internet Protocol)* e TACACS (*Terminal Access Controller Access Control System*).

A *Security Dynamics, Inc*, também oferece uma solução para acesso à aplicações baseadas na *Web*. O *Secure Web Application Access* funciona integrado ao *ACE/Server* e o *SecureID,* e proporciona autenticação do usuário, cifragem da informação que passa através da rede com SSL (*Secure Sockets Layer*) e controle de acesso à aplicações de intranets e extranets. A empresa fornece agentes/ACE para *Windows NT Internet Information Server e Netscape Enterprise Server* com *UNIX, Sun Solaris, HP-UX e AIX* [SEC99].

2.2.2 Análise das Soluções Baseadas na Propriedade

As soluções de autenticação baseadas na propriedade caracterizam-se pela posse de um objeto físico. Sua vantagem consiste no princípio de que a duplicação desse objeto será mais cara que o valor do que está sendo guardado. As desvantagens são que os objetos físicos podem ser perdidos ou esquecidos e o custo adicional do *hardware*.

Dentre as soluções baseadas em *tokens*, o *SecureID*, da *Security Dynamics, Inc*, é líder no mercado com mais de quatro milhões de *tokens* vendidos no mundo inteiro [FLE99] . Por possuir dois fatores de autenticação (PIN e o *token*) esta solução apresenta um bom nível de segurança. Uma vez que uma nova senha é gerada a cada 60 segundos, o sistema evita ataques como: adivinhação da senha, ataque do dicionário e monitoramento do tráfego na rede. Outra característica importante na comparação com outros produtos são a facilidade de uso e o fato de não requerer *hardware* adicional.

A existência de versões do *ACE/Server* para vários sistemas operacionais, assim como soluções para Internet, facilita sua portabilidade.

Em termos de integração com outras aplicações, a *Security Dynamics, Inc*, mantém um sistema de parcerias, no qual é disponibilizado um *toolkit* para a criação de agentes específicos para cada aplicação.

Segundo [FLE99], o custo aproximado de um *token SecureID* é de US$ 70,00. O servidor *ACE/Server* tem um custo de aproximadamente US$ 400,00 dólares mais um pequeno valor por usuário.

O problema da utilização de mecanismos de autenticação baseados na propriedade para aplicações de ensino a distância é que, assim como as senhas podem ser divulgadas para outras pessoas, os *tokens* também podem ser emprestados. Aliado ao custo do produto, conclui-se esta solução seja inviável para essas aplicações.

2.3 Soluções de Autenticação Baseadas em Características (O que se é)

Uma área que está melhorando tecnologicamente e simplificando o processo de identificação de pessoas é a biometria. Sistemas biométricos são métodos automatizados para a verificação ou o reconhecimento de uma pessoa com base em alguma característica física, tal como a impressão digital ou o padrão de íris, ou algum aspecto comportamental, tal como a escrita ou o padrão de digitação [KIM95]. Ainda que os sistemas biométricos não possam ser usados para estabelecer um "sim/não" na identificação pessoal, como as outras tecnologias tradicionais, eles podem ser usados para alcançar uma identificação positiva, com um alto grau de confiança e uma taxa de erro em torno de 0,001%.

Teoricamente, qualquer característica humana, física ou comportamental, pode ser usada para a identificação de pessoas, desde que satisfaça os seguintes requerimentos [JAI97]:

- Universalidade: significa que todas as pessoas devem possuir a característica;
- Singularidade: indica que esta característica não pode ser igual em pessoas diferentes;
- Permanência: significa que a característica não deve variar com o tempo;
- Mensurabilidade: indica que a característica pode ser medida quantitativamente.

Na prática, existem outros requerimentos importantes:

- Desempenho: refere-se à precisão de identificação, os recursos requeridos para conseguir uma precisão de identificação aceitável e ao trabalho ou fatores ambientes que afetam a precisão da identificação;
- Aceitabilidade: indica o quanto as pessoas estão dispostas a aceitar os sistemas biométricos;

- Proteção: refere-se à facilidade/dificuldade de enganar o sistema com técnicas fraudulentas.

A tabela 2.1 relaciona os requerimentos acima com algumas técnicas biométricas.

TABELA 2.1 – Comparação de tecnologias biométricas quanto aos requerimentos

Biométricos	Universalidade	Singularidade	Permanência	Mensurabilidade	Desempenho	Aceitabilidade	Proteção
Face	Alto	Baixo	Médio	Alto	Baixo	Alto	Baixo
Impressão Digital	Médio	Alto	Alto	Médio	Alto	Médio	Alto
Geometria da Mão	Médio	Médio	Médio	Alto	Médio	Médio	Médio
Veias da Mão	Médio	Médio	Médio	Médio	Médio	Médio	Alto
Íris	Alto	Alto	Alto	Médio	Alto	Baixo	Alto
Retina	Alto	Alto	Médio	Baixo	Alto	Baixo	Alto
Assinatura	Baixo	Baixo	Baixo	Alto	Baixo	Alto	Baixo
Voz	Médio	Baixo	Baixo	Médio	Baixo	Alto	Baixo

2.3.1 Componentes de um Sistema Biométrico

Um sistema biométrico padrão possui os seguintes componentes:

- Um dispositivo de medida, o qual forma a *interface* do usuário. A facilidade de uso é um fator importante para os biométricos: o dispositivo deve ser instintivo e deixar pouca possibilidade para erros. Ele deve ser satisfatório para o uso de uma grande quantidade de pessoas, incluindo aquelas destreinadas;

- Um *software* de operação, incluindo o algoritmo matemático que irá checar a medida contra um modelo (*template*). Os algoritmos mais recentes dependem menos da modelagem estatística e mais da programação dinâmica, das redes neurais, e da lógica fuzzy (*fuzzy logic*). Isto aumenta sua flexibilidade; eles são menos suscetíveis a rejeitar alguém por causa de uma sujeira, por exemplo, se o resto do modelo estiver de acordo;

- Um *hardware* e sistemas externos: a usabilidade, confiança e o custo do sistema irá freqüentemente depender tanto destes sistemas externos como dos dispositivos de medida. Alguns sistemas (tais como checagem de impressão digital) são

intrinsecamente bem adaptados para o uso em sistemas distribuídos, enquanto outros (tal como reconhecimento de voz) são mais apropriados para sistemas centralizados.

2.3.2 Como Funcionam os Sistemas Biométricos

O mecanismo de autenticação por biometria tem dois modos: registro e verificação. Para o uso inicial da biometria, cada usuário deve ser registrado pelo administrador do sistema. Este, verifica se cada indivíduo registrado é um usuário autorizado. O processo de registro consiste no armazenamento de uma característica biológica do indivíduo (física ou comportamental) para ser usada, posteriormente, na verificação da identidade do usuário.

A característica biológica é tipicamente adquirida por um dispositivo de *hardware*, o qual está no *front end* do mecanismo de autenticação por biometria. O componente do *front end* para estes sistemas é um dispositivo conhecido como sensor. Quando uma característica física é apresentada ao sensor, ele produz um sinal que é modulado em resposta às variações da quantidade física sendo medida. Se, por exemplo, o sensor for um microfone usado para capturar um padrão de voz, ele irá produzir um sinal cuja amplitude varia com o tempo em resposta à variação da freqüência em uma frase falada.

Pelo fato dos sinais produzidos pela maior parte dos sensores serem analógicos por natureza, é necessário converter estes sinais para digitais, para que possam ser processados por um computador. Ao invés de usar todos os dados do sensor, os sistemas biométricos freqüentemente processam estes dados para extrair apenas as informações relevantes ao processo de autenticação. Uma vez que a representação digital foi processada para o ponto desejado, ela é armazenada. A característica biológica armazenada na forma digital é chamada de modelo (*template*). Muitos dispositivos biométricos capturam amostras múltiplas durante o processo de registro para contabilizar graus de variação na medida destas características.

Uma vez que o usuário está registrado, os dispositivos biométricos são usados na verificação da identidade do usuário. Quando o usuário necessitar ser autenticado, sua característica física é capturada pelo sensor. A informação analógica do sensor é então convertida para sua representação digital. A seguir, esta representação digital é comparada com o modelo biométrico armazenado. A representação digital usada na verificação é chamada de amostra (*live scan).* A amostra, tipicamente, não confere exatamente com o modelo armazenado. Como geralmente há alguma variação na medida, estes sistemas não podem exigir uma comparação exata entre o modelo original armazenado e a amostra corrente. Ao invés disso, a amostra corrente é considerada válida se estiver dentro de um certo intervalo estatístico de valores. Um algoritmo de comparação é usado para determinar se um usuário quando verificado é o mesmo que foi registrado.

O algoritmo de comparação produz um resultado de quão perto a representação digital está do modelo armazenado. Se o resultado for um valor aceitável, uma resposta afirmativa é dada. A aceitação difere para cada dispositivo biométrico. Para alguns, o administrador do sistema pode configurar o nível do valor de aceitação. Se este nível for muito baixo, o dispositivo biométrico falha por ser um mecanismo de autenticação

válido. Se este nível for muito alto, os usuários podem ter problemas na autenticação. Este padrão de comparação é fundamental para a operação de qualquer sistema biométrico, e assim deve ser considerado um fator primário quando avalia-se um produto biométrico específico.

Outro aspecto que afeta a autenticação por biometria é a recuperação do modelo pelo algoritmo de comparação. O modelo pode ser usado na identificação ou na verificação de usuários. Muitos dispositivos usam a verificação, mas alguns usam a identificação.

A identificação biométrica é um processo um-para-muitos, onde uma amostra é submetida ao sistema, que a compara com todos os modelos da base de dados, a fim de verificar se esta coincide com qualquer um destes modelos e, em caso positivo, determina a identidade do usuário a quem aquele modelo pertence [ROE98].

A verificação biométrica é um processo um-para-um, onde o sistema verifica a identidade de um usuário comparando a amostra com um modelo específico. Através de uma identificação fornecida, o sistema localiza o modelo desejado e o compara com a amostra apresentada. Se houver coincidência entre a amostra e o modelo armazenado, o sistema confirma que o usuário realmente possui a identidade afirmada [ROE98]. Por exemplo, um usuário irá digitar o seu nome e então adquire-se uma amostra para a verificação. O algoritmo de comparação usará apenas o modelo armazenado àquele nome. Verificações biométricas são, tipicamente, mais rápidas do que a identificação porque elas não precisam comparar a amostra com todo o banco de dados de modelos.

2.3.3 Falsa Aceitação e Falsa Rejeição

Na escolha de um sistema de autenticação biométrico, o desempenho deve ser levado em conta. Este pode ser categorizado por duas medidas: a taxa de falsa aceitação (*FAR – False Acceptance Rate)* e a taxa de falsa rejeição (*FRR – False Rejection Rate).* A FAR, também chamada de erros do tipo 2, representa a percentagem de usuários não-autorizados que são incorretamente identificados como usuários válidos. A FRR, também chamada de erros do tipo 1, representa a percentagem de usuários autorizados que são incorretamente rejeitados.

O nível de precisão configurado no algoritmo de comparação tem efeito direto nessas taxas. O modo como estas são determinadas é fundamental para a operação de qualquer sistema biométrico e assim deve ser considerado um fator primário na avaliação de sistemas biométricos. Deve-se ter cuidado com os números de FRR e FAR dos fabricantes, porque estes são extrapolados por pequenos conjuntos de usuários e a condição de extrapolação é, algumas vezes, errada [NAT94]. Os dispositivos biométricos físicos tendem a ter uma melhor taxa de falsa aceitação por causa da estabilidade da característica medida e porque as características comportamentais são mais fáceis de serem duplicadas por outros usuários.

A configuração do valor limite para tolerância a estes erros é crítica no desempenho do sistema. A falsa rejeição causa frustração e a falsa aceitação causa fraude.

Muitos sistemas podem ser configurados para fornecer detecção sensível (baixa FAR e alta FRR) ou detecção fraca (baixa FRR e alta FAR). A medida crítica é conhecida como taxa de cruzamento (*crossover rate)*. Ela é o ponto onde o FAR e o FRR cruzam-se. Muitos sistemas biométricos comerciais têm taxas de cruzamento abaixo de 0,2%, e alguns abaixo de 0,1%. A taxa aumenta com a freqüência do uso, com os usuários acostumando-se com o sistema e o sistema tornando-se mais afinado com o nível de variação esperado. A figura 2.2 mostra as taxas de falsa aceitação e falsa rejeição.

As taxas FAR e FRR podem ser obtidas através de protocolos "uma tentativa" ou "três tentativas". No protocolo "uma tentativa" os usuários têm apenas uma chance de passar no teste biométrico. Os dados são coletados em apenas uma oportunidade e então são analisados. A partir disso vem a rejeição ou aceitação. No "três tentativas", o usuário tem até três chances antes que seja definitivamente rejeitado. Se as medidas consecutivas são estatisticamente independentes, isto melhora a FRR sem, no entanto, deteriorar a FAR. Entretanto, dependendo do tipo de aplicação, este protocolo de "três tentativas" pode não ser aceitável por uma questão de tempo ou até mesmo por conveniência [CAR97].

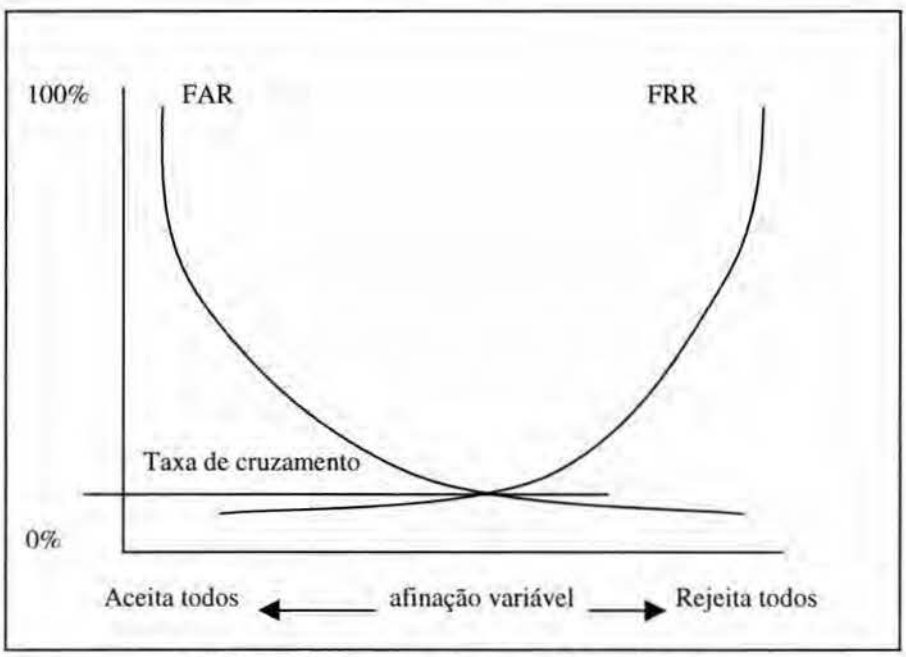

FIGURA 2.2 - Falsa aceitação x falsa rejeição

2.3.4 Métodos de Autenticação Biométricos

Os sistemas biométricos baseiam-se em características físicas e comportamentais de pessoas. Uma característica física deve ser relativamente estável, tal como a impressão digital, estrutura da mão, padrão de retina, padrão de íris ou alguma característica facial. Assim são basicamente imutáveis ou variam pouco no decorrer do

tempo. Em contrapartida, uma característica comportamental reflete o estado psicológico de uma pessoa (isto é, pode ser afetada por problemas como estresse, fadiga, gripe, etc.). Entretanto, ela possui alguns elementos psicológicos que podem ser usados na identificação de uma certa característica. Por exemplo, o método de identificação baseado em comportamento mais comum é a assinatura de uma pessoa, usada pela sociedade há décadas. Outros comportamentos usados incluem o ritmo de digitação e o padrão de voz.

Muitos sistemas precisam modificar o modelo de referência original a cada vez que ele é usado. Isto ocorre porque muitas características comportamentais mudam no decorrer do tempo, e assim, depois de muitos acessos com sucesso, o modelo pode ser diferente (às vezes significativamente) do modelo inicial, produzindo melhor desempenho na identificação de um usuário inválido. Os esquemas que utilizam este método trabalham melhor apenas quando usados regularmente.

Em geral, desde que o grau de variação entre as pessoas seja maior em uma característica comportamental do que em uma característica física, é mais difícil para desenvolvedores dos sistemas baseados em comportamento o ajuste da variação individual. Entretanto, sistemas que medem atributos físicos tendem a ser maiores e mais caros, e seu uso em algumas aplicações pode ser considerado ameaçador aos usuários. Os dispositivos biométricos baseados em comportamento são geralmente menores em tamanho, sua implementação é mais barata e seu uso é mais amigável. Ambas as técnicas fornecem um meio de autenticação de usuários muito mais confiável que os mecanismos de segurança baseados em senhas ou cartões.

Por causa destas diferenças, nenhum sistema biométrico irá servir para todas as necessidades e, para serem efetivos, é necessário aplicar diferentes técnicas em diferentes situações. Por exemplo, um sistema de verificação de voz pode ser usado em um escritório, enquanto um sistema de reconhecimento de retina pode ser usado no controle de acesso à áreas de segurança máxima [KIM95].

2.3.4.1 Reconhecimento da Face

O uso de reconhecimento de face é o método mais natural de identificação biométrica. O uso das características da face para identificação automática é uma tarefa difícil porque a aparência facial tende a mudar a todo tempo. As variações podem ser causadas por diferentes expressões faciais, mudanças no estilo do cabelo, posição da cabeça, ângulo da câmara, condições de luz, etc. Apesar das dificuldades envolvidas, o reconhecimento facial já foi abordado de diversas maneiras, variando de sistemas de reconhecimento de padrões por redes neurais até varreduras infravermelhas de pontos estratégicos (como posição dos olhos e da boca) na face.

Muitos sistemas de reconhecimento de face utilizam um computador com uma câmera para capturar as imagens da face. Estes sistemas utilizam medidas da face como distâncias entre os olhos, nariz, queixo, boca e linha dos cabelos como meio de verificação. Alguns sistemas também podem executar testes "animados" para evitar que o sistema seja fraudado por uma fotografia.

Variáveis como óculos de sol, bigode, barba, expressões faciais entre outras, podem causar falsas rejeições nesses sistemas.

A seguir serão analisados dois produtos que implementam a tecnologia de reconhecimento de faces: *Miros TrueFace (www.miros.com)* e *Visionics FaceIt (www.faceit.com)*. Esta análise baseou-se em testes realizados com cópias de avaliação e informações adquiridas nos *sites* dos fabricantes destes produtos.

2.3.4.1.1 *Miros TrueFace*

O *TrueFace* é um *software* de reconhecimento de face baseado na tecnologia de redes neurais. Isto possibilita que ele se adapte melhor a variações na imagem da face como posição da cabeça e condições de iluminação.

Algumas das principais vantagens do *TrueFace* são [BIO99]:

- A aplicação é passiva para o usuário, isto é, não requer uma ação voluntária como a colocação do dedo em um leitor de digitais. Basta ele olhar para a câmera para ser verificado, tornando-o assim, fácil de usar.
- A cada tentativa de acesso, é gravada a imagem do usuário, para fins de auditoria;
- É rápido e barato: A verificação demora de 1 a 5 segundos e utiliza câmeras comuns com resolução de 320x240 pontos;
- Possui soluções para *desktop*, redes cliente-servidor, intranets e Internet.
- É fácil de integrar: Possui um SDK (*Software Development Kit)* com bibliotecas para *Windows e Sun Solaris.*

A compatibilidade com várias plataformas e a facilidade de uso fazem do *TrueFace* um bom sistema de segurança. A instalação do *hardware* em uma máquina *Windows NT* é relativamente simples de realizar-se, pois o *TrueFace* opera com diversas câmeras e não requer uma placa de captura de vídeo. Porém, a câmera não é inclusa no pacote.

Os administradores podem rastrear a atividade e controlar o acesso aos domínios e às estações *Windows NT.* Ao contrário de outras soluções, o *TrueFace* não se limita aos ambientes *"Wintel".* Estão disponíveis versões para as estações de trabalho *Sun* e a API (*Application Program Interface*) que pode ser utilizada para atrelar o mecanismo a outras plataformas e dispositivos.

A inscrição de novos usuários é muito simples; qualquer pessoa capaz de operar um computador pode gerenciá-lo. Primeiro, o TrueFace tira várias fotos da face do usuários, criando-lhe uma conta na base de dados. Em seguida, focaliza a câmera em um lado do rosto e depois no outro, para fazer com que seja mais difícil enganar o sistema.

Além de seus recursos de segurança de *login*, o *TrueFace* permite a reprodução de fotos dos usuários rapidamente. Ele pode, então, criar um registro do evento e documentar sua verificação - entrada bem sucedida ou acesso negado, por exemplo. Segundo [GUN99], em testes de laboratório foi possível quebrar a segurança do sistema com uma máscara (produzida em uma impressora em cores) com o rosto de um usuário

registrado. O *TrueFace* não realiza o teste de expressões como o *FaceIt*, que será apresentado na próxima seção. Porém é possível aumentar a sensibilidade dos limiares padrão. Nos testes realizados, isto evitou que o mascarado continuasse driblando o *software* [GUN99].

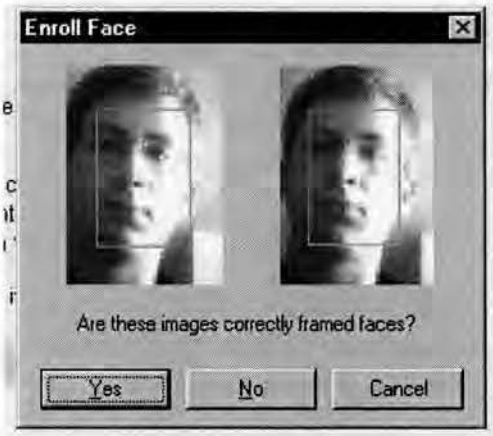

FIGURA 2.3 - Cadastro de um usuário no *TrueFace Web*

Em termos de solução para *Web*, a *Miros* oferece o *TrueFace Web*. Ele faz com que a face do usuário seja sua chave para permitir o acesso a um *Web site*. Quando o usuário tenta acessar o *Web site*, lhe é automaticamente enviado uma página onde ele tem que entrar com sua identificação. O navegador do usuário, então, recebe um cliente *TrueFace* (controle Active-X ou Netscape plug-in), o qual executa a captura da imagem, cifragem e transmissão para o *TrueFace Web Server*. Usando o reconhecimento de face, o servidor analisa a identificação e, se aprovada, a página segura é transmitida ao navegador do usuário normalmente. A figura 2.3 mostra uma etapa do cadastro de um usuário no *TrueFace Web*.

O sistema também permite que sejam feitos cadastros pela Internet, armazenando várias imagens que serão utilizadas para posterior identificação.

Por fim, o sistema possui proteção contra algumas formas comuns de fraude: ele grava a imagem da face de tentativas mal sucedidas de acesso ao *site*, notificando a administração do servidor. Ele também detecta a tentativa de uso de fotos de usuários autorizados.

A tabela 2.2 apresenta as principais características do *TrueFace* [MCD99]:

TABELA 2.2 – Principais características do Miros TrueFace

Tempo de cadastro	De 5 a 30 segundos
Tempo de verificação	De 1 a 5 segundos
Taxa de falsa rejeição (FRR)	Menor que 0.2%
Taxa de falsa aceitação (FAR)	Baixa

Tamanho do modelo	De 1000 a 1100 bytes
Facilidade de uso	Muito fácil. Basta olhar para a câmera.
Influência do Ambiente	Necessita de luz em todas as partes da face
Hardware adicional	Câmera com resolução de 320x240 pontos
Software adicional	*Microsoft SQL Server 6.5*
Facilidade de integração / API	Possui uma API de fácil utilização. Uma aplicação simples necessita de 5 a 10 chamadas
Nível de invasão	Nenhum. As pessoas aceitam muito bem a presença da câmera
Uso em redes / *Web*	Possui produtos para redes (*TrueFace Network*) e para *Web* (*TrueFace Web*)
Sistemas Operacionais	*Windows 95/98 e NT, Sun Solaris*
Banco de dados	*Microsoft SQL Server 6.5*
Preço	US$ 2.995,00 para 25 usuários ≅ US$120,00 / Usuário

2.3.4.1.2 *Visionics FaceIt*

O *FaceIt* é um pacote de *software* para reconhecimento de face que permite que um computador conectado a uma câmera localize e reconheça a face de um usuário. O *FaceIt* proporciona maior controle granular sobre os níveis de segurança (e uma segurança maior) que o *TrueFace*, embora sua configuração seja uma tarefa mais difícil de ser realizada.

Algumas das principais vantagens do *FaceIt* são: [VISC99]:

- Facilidade de uso e rapidez;
- Não utiliza nenhum *hardware* proprietário. Só necessita de uma câmera que capture 5 quadros por segundo e com resolução de 320 x 240 pontos.
- Registro da face a cada tentativa de acesso ao sistema, para fins de auditoria;
- Possui soluções para *desktop*, redes cliente-servidor, intranets e Internet.
- Compatível com a HA-API (*Human Authentication - Application Program Interface)* . Possui um SDK para *Windows 95/98 e Windows NT* e componentes Active-X para aplicações na *Web*;

O *software* funciona com ou sem senhas, e pode ser combinado com qualquer produto de fala compatível com SAPI 3.0 (*Speech Application Program Interface)*, para solicitar comandos verbais aos usuários. Embora possa ser executado em praticamente qualquer máquina equipada com processador Pentium, os requisitos de vídeo são os seguintes: uma câmera compatível com *Vídeo for Windows* que capture ao menos cinco quadros por segundo a uma resolução de 320 x 240 pontos com 16 bits de cores.

A instalação do aplicativo é simples e pode-se utilizar o produto com ou sem uma base de dados de suporte. A *interface* com o usuário é bem projetada, mas o processo de inscrição não é tão integrado com o *Microsoft User Manager* quanto outros produtos existentes.

Para cadastrar uma pessoa, deve-se capturar várias imagens com a câmera e definir as informações sobre os usuários e seus direitos de acesso. Também pode-se fazer um teste opcional de expressões e piscares de olhos, reduzindo assim a possibilidade de alguém enganar o sistema com uma fotografia. A figura 2.4 apresenta uma etapa do cadastro do usuário no *FaceIt*.

FIGURA 2.4 - Cadastro de um usuário no FaceIt

Além de oferecer o controle padrão de *login* e acesso aos arquivos, o *FaceIt* pode ser configurado para tirar uma foto instantânea automática de qualquer pessoa que passe na frente da máquina enquanto ela estiver sozinha.

Para soluções na *Web*, a empresa disponibiliza o *FaceIt Active-X*, que pode ser inserido em uma página *Web* com a lista de faces autorizadas a acessar esta página, sendo mantidas no servidor *Web*.

Tal como o *TrueFace*, o *FaceIt* protege-se contra fraudes, registrando a face de tentativas de acesso negadas e evitando o uso de fotografias através de testes de "animação" (expressões e piscares de olhos).

A combinação de captura de imagens, verificação de expressões e barreiras de senhas do *FaceIt* proporciona um alto nível de segurança. A tabela 2.3 apresenta as principais características do *FaceIt* [VIS99a]:

TABELA 2.3 – Principais características do Visionics FaceIt

Taxa de falsa rejeição (FRR)	Menor que 1%
Taxa de falsa aceitação (FAR)	Menor que 1%
Tamanho do modelo	De 1000 a 1500 bytes
Facilidade de uso	Muito fácil
Influência do Ambiente	Necessita de luz em todas as partes da face
Hardware adicional	Câmera que captura pelo menos 5 quadros por segundo com resolução de 320x240 pontos e 16 bits de cor
Software adicional	Não necessita
Facilidade de integração / API	Compatível com a HA-API. Possui um SDK para *Windows 95/98 e Windows NT* e componentes Active-X para aplicações na *Web*
Nível de invasão	Nenhum. As pessoas aceitam muito bem a presença da câmera
Uso em redes / *Web*	Possui produtos para redes (*FaceIt NT*) e um componente Active-X para uso na *Web*
Sistemas Operacionais	*Windows 95/98 e NT*
Banco de dados	Não necessita
Preço	Aproximadamente US$100,00 / Usuário

2.3.4.2 Impressão Digital

A estabilidade e a individualidade da impressão digital são largamente reconhecidas e técnicas baseadas em impressão digital têm sido usadas desde o final do século dezenove.

Na verificação de uma impressão, muitos sistemas analisam a posição de detalhes chamados de *minutiae*, tais como terminações e bifurcações dos sulcos. Sistemas modernos também verificam outras características para identificação única, tais como arcos e voltas que aparecem no dedo. Por exemplo, alguns dispositivos contam o número de cumes entre um *minutiae* para formar o modelo de referência, enquanto outros o tratam como um problema de processamento de imagens, e aplicam circuitos integrados de grande escala customizados (*VLSI – Very Large Scale Integrated)*, redes neurais, lógica fuzzy (*fuzzy logic*) e outras tecnologias para resolver o problema.

Um modelo de referência padrão de uma impressão digital requer aproximadamente 500 bytes. Alguns fabricantes afirmam que com o uso de compressão, o modelo pode chegar a 50 bytes. A verificação da impressão digital leva em média de 1 a 2 segundos [BIO99a].

Numa imagem de impressão digital obtida por um dispositivo, existem em média 30 a 40 *minutiae*. O FBI (*Federal Bureau of Investigation)* americano comprovou que não existem dois indivíduos que possuam mais do que 8 *minutiae* comuns [BIO98].

Nos dispositivos de impressão digital, o leitor deve minimizar a rotação da imagem. Ele deve compensar uma ligeira variação na imagem armazenada. Existem, também, problemas quando o usuário tem pequenos ferimentos no dedo, sujeira ou ressecamento da pele. Uma freqüente limpeza pode reduzir a percentagem de falsas rejeições.

Existem três tipos de leitores de digitais: [BIO99b].

- Ópticos: O dedo é colocado sobre um plataforma de vidro e uma imagem do dedo é capturada. Estes dispositivos tornaram-se pequenos e baratos;
- Ultra-som: O dedo é colocado sobre uma plataforma de vidro e uma varredura de ultra-som é efetuada;
- Baseados em chip: O usuário coloca seu dedo direto em um chip de silício.

Sistemas de identificação de digitais utilizam somente os leitores ópticos. Sistemas de verificação (executam verificação um-pra-um) utilizam todos os três.

Impressões digitais têm sido utilizadas em várias aplicações como controle de acesso, caixas automáticos de bancos, registros de saúde, entre outras. Algumas de suas principais vantagens são a rapidez e a confiança, o baixo preço e o pequeno tamanho dos leitores e o fato de ele ser considerado pelos usuários como pouco intrusivo. Entretanto, algumas pessoas acham que, sendo requerido sua impressão digital, estão sendo tratadas como criminosas [BIO99b].

2.3.4.2.1 *Identicator BioLogon*

O *Identicator BioLogon (www.identicator.com)* é um *scanner* compacto de impressões digitais projetado para implementações OEM (*Original Equipment Manufacturers*). Ele foi testado como recurso interno do *Key Tronic Secure Scanner Keyboard*, um teclado para PC com o *scanner Identicator DFR-200* embutido à esquerda das teclas. A *KeyTronic* vende este modelo com o *software Identicator BioLogon*.

O teclado *KeyTronic* é conectado nas portas paralelas, do teclado e do mouse. O *software* acresce (ao invés de substituir) as senhas de *logon* de seus usuários, o que é ideal para a segurança, mas nem tanto para a comodidade, se este for o motivo da aquisição do *scanner*. A figura 2.5 apresenta o teclado *KeyTronic*.

FIGURA 2.5 - Teclado *KeyTronic*.

O *Identicator 1.01* é facilmente operado: ele funciona pela simples adição de modelos biométricos a campos extras da base de dados SAM (*Security Accounts Manager)* do *Windows NT*. Isto significa que o sistema trabalha dentro da arquitetura de segurança padrão do *Windows NT* e é replicado, automaticamente, pelos *Backup Domain Controllers*. O *software* também engloba, de forma inteligente, o *User Manager for Domains*, adicionando um botão de cadastro biométrico às telas básicas do gerenciamento de usuários.

O processo de inscrição é amigável, incluindo um assistente passo-a-passo que solicita ao usuário uma impressão digital e a verifica. Na versão 2.0 do *software* (a ser disponibilizada em breve), o *Identicator* pretende implementar uma opção combinada de cartão inteligente/*scanner* de impressões digitais, além da capacidade de efetuar o *logon* sem a senha texto do Windows NT.

Para resumir, o *BioLogon* é uma solução de segurança avançada e fácil de ser usada. Por ser extremamente pequeno, os OEMs podem integrá-lo a seus produtos de várias maneiras. E graças ao simples, porém eficaz, *software* da *Identicator*, os administradores de redes têm um leque igualmente amplo de opções para incorporar a autenticação de impressões digitais em suas redes. O preço nos Estados Unidos é de US$ 150,00.

2.3.4.2.2 *American Biometric BioMouse Plus*

O *American Biometric BioMouse Plus (www.abio.com)* representa a segunda geração de *scanners* de impressões digitais. Ele combina a tecnologia de reconhecimento das digitais com um leitor de cartões inteligentes embutido, garantindo maior segurança e flexibilidade. Esta solução apresenta quase 100% de segurança quando o sistema está ativo. Entretanto, há um segundo procedimento de *logon* que permite a um determinado usuário acessar o sistema muito facilmente, utilizando apenas um cartão inteligente e um PIN. Este processo, aliado à arquitetura de *software* pesada e ao alto custo, impede que o produto seja considerado uma solução ideal.

Um dos seus grandes atrativos é a compatibilidade com várias plataformas. É possível instalar o *BioMouse Plus* em qualquer cliente *Windows* (desde o *Windows 3.1 ao Windows NT*) assim como em grande parte dos clientes *Unix*. O pacote inclui diversos componentes para o estabelecimento de segurança local e ao nível dos domínios: um servidor de autenticação, um emissor de cartões inteligentes, um programa para cadastro de usuários e um programa para manutenção de senhas. A figura 2.6 apresenta o dispositivo de leitura do *BioMouse Plus*.

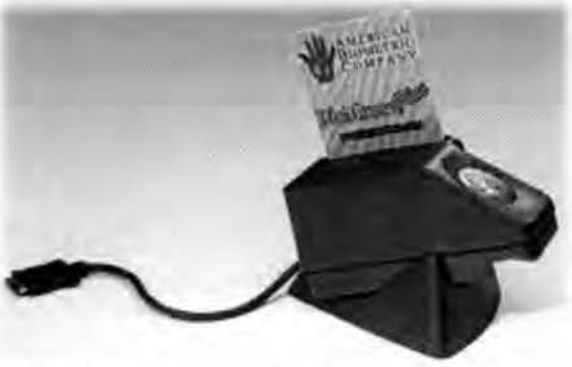

FIGURA 2.6 - Dispositivo de leitura do *BioMouse Plus*

A base de dados do servidor de autenticação não é integrada ao SAM do *Windows NT*, tampouco é replicada. Isto representa risco de caos entre os usuários caso esta máquina entre em pane.

Para cadastrar um usuário, o administrador emite um cartão inteligente utilizando o emissor que o acompanha. Depois, o dedo do usuário é inscrito no servidor de autenticação. Uma vez concluído este processo, uma sessão inicial de manutenção de senha deve ocorrer, para que a senha do usuário seja transferida para seu cartão inteligente.

No geral, o *American Biometric BioMouse Plus* precisa de alguns aprimoramentos. Embora o funcionamento do *hardware* seja confiável, o *software* é de difícil manutenção [PLA99]. A tabela 2.4 apresenta as principais características do *American Biometric BioMouse Plus* [WEL99]:

TABELA 2.4 – Principais características do *American Biometric BioMouse Plus*

Tempo de cadastro	De 20 a 30 segundos
Tempo de verificação	1 segundo
Taxa de falsa rejeição (FRR)	Não disponível
Taxa de falsa aceitação (FAR)	De 0,1% a 0,0001%, configurada pelo usuário
Tamanho do modelo	De 350 a 650 bytes
Facilidade de uso	Fácil de usar e instalar

Hardware adicional	O *hardware* está incluso no preço
Software adicional	Não necessita
Facilidade de integração / API	Possui um SDK em C/C++. O preço do BioMousePlus *toolkit* é de US$895,00
Nível de invasão	Baixo. É só colocar o dedo no leitor.
Uso em redes / *Web*	Permite *login* em *Windows NT e Novell*
Sistemas Operacionais	*Windows 95/98 e NT, Sun Solaris, Linux e Solaris Sparc* 2.5
Banco de dados	Proprietário
Preço	US$ 299,00 por instalação

2.3.4.2.3 *Identix TouchSafe Personal*

O *Identix TouchSafe Personal (www.identix.com)* é um *scanner* de impressões digitais que pode ser conectado à porta serial do computador. Ele vem acompanhado do *software IDXsecure* para *Windows NT*, da própria empresa. Ao fornecer uma camada adicional de verificação de usuários para *logins* do *Windows NT*, ele visa reforçar a segurança de *desktops* e redes. A figura 2.7 apresenta a solução *Identix TouchSafe Personal.*

FIGURA 2.7 - *Identix TouchSafe Personal*.

O *TouchSafe* apresenta um circuito interno que inclui um processador RISC (*Reduced Intruction Set Computers*) de 32 bits integrado, que tem como objetivo comparar mais rapidamente as digitais processadas pelo *scanner* com os modelos dos

usuários. Como opção, ele também é capaz de trabalhar com uma leitora de cartões inteligentes.

O *software* que acompanha, o *IDXsecure*, permite que os administradores configurem estações de trabalho de forma que seja necessária a verificação de digitais para *login* em uma rede *Windows NT*. Uma base de dados proprietária mantém os modelos das digitais cadastrados no disco rígido local da estação, obrigando os administradores a cadastrarem os usuários pessoalmente em cada uma das máquinas que eles possam utilizar.

Tanto o cadastro quanto a verificação de digitais podem ser convenientemente acessadas a partir de uma única tela. Os dez dedos podem ser inscritos. Um programa de administração independente (o *Administration*) permite definir o nível de segurança (o número máximo de usuários), o limiar para a detecção de dedos falsos (correspondência de 67% ou 100%) e o número permitido de tentativas de verificação antes da rejeição do *login*.

Em suma, o *Identix TouchSafe* possui um *hardware* admirável e pode ser uma boa opção para a segurança de algumas máquinas. Entretanto, outros produtos oferecem melhores recursos para redes [GUN99]. A tabela 2.5 apresenta as principais características do *Identix TouchSafe* [IDE99]:

TABELA 2.5 – Principais características do *Identix TouchSafe*

Tempo de cadastro	Menor que 20 segundos
Tempo de verificação	1 segundo
Taxa de falsa rejeição (FRR)	Menor que 2%
Taxa de falsa aceitação (FAR)	Menor que 0,001%
Tamanho do modelo	118 bytes
Facilidade de uso	Fácil de usar e instalar
Software adicional	*IDXSecure*
Facilidade de integração / API	Possui um SDK vendido a um preço de US$ 2.000,00
Nível de invasão	Baixo. É só colocar o dedo no leitor.
Uso em redes / *Web*	Permite *login* em *Windows NT*
Sistemas Operacionais	*Windows 95/98 e NT*
Banco de dados	Proprietário
Preço	US$ 499,00 por instalação

2.3.4.3 Geometria da Mão

A geometria da mão tem sido usada em aplicações desde o começo de 1970. Ela baseia-se no fato de que virtualmente não existem duas pessoas com mãos idênticas e de que o formato da mão não sofre mudanças significativas após certa idade [BIO98]. Existem diversas vantagens no uso da forma tridimensional da mão da pessoa como um dispositivo de identificação. Primeiramente, é razoavelmente rápida. Leva menos que 2 segundos para capturar a imagem de uma mão e produzir a análise resultante. Secundariamente, requer pouco espaço de armazenamento. É também requerido pouco esforço ou atenção do usuário durante a verificação, e os usuários autorizados são raramente rejeitados.

As dimensões da mão, tal como tamanho do dedo, largura e área são as principais características usadas nas análises. Para a captura, o usuário posiciona sua mão no leitor, alinhando os dedos, e uma câmara posicionada acima da mão captura a imagem. Medidas tridimensionais de pontos selecionados são tomadas e o sistema extrai destas medidas um identificador matemático único na criação do modelo. Um típico modelo requer cerca de nove bytes de armazenamento.

Um dos problemas com sistemas que utilizam a geometria da mão é causado pela rotação da mão quando colocada no leitor. Isto resolve-se usando pinos de posicionamento dos dedos. O sistema também deve levar em conta os diferentes tamanhos das mãos em diferentes usuários, e seu desempenho não deve ser prejudicado por sujeira e cortes na mão da pessoa. A figura 2.8 apresenta um leitor de geometria da mão.

FIGURA 2.8 - Leitor de geometria da mão

É quase impossível secretamente obter informações sobre a geometria da mão de uma pessoa, ao menos que haja sua cooperação. O sistema é fácil de ser usado, não requer treinamento complexo e pode ser utilizado por qualquer pessoa desde que não tenha deficiência relacionada com algum aspecto físico da mão. Quanto à estabilidade, deve-se ressaltar que a geometria da mão muda de acordo com a idade e, ocasionalmente, com a perda ou ganho de peso.

Existem alguns produtos que utilizam autenticação baseada em geometria da mão disponíveis no mercado. A empresa *BioMet Partners (www.biomet.ch)* disponibiliza o *FingerFoto*, baseado na geometria do dedo. Algumas características deste produto são [BMP99]: o tempo de cadastro e de a verificação na base de 1 segundo, FRR e FAR de 0,1%, o tamanho do modelo de 20 bytes, é fácil de ser usado e a necessidade do *Finger Geometry Biometry OEM Camera* na realização das leituras do dedo.

A Universidade de Michigam desenvolveu um sistema de acesso a *Web* baseado em geometria de mão [JAI98]. Nesse sistema, é utilizada a autenticação básica fornecida pelo NCSA (*National Center for Supercomputing Applications*) na restrição do acesso à *Web*, mas utiliza dados biométricos da geometria da mão ao invés de senhas para autenticação. Apesar de ser apenas um protótipo, demonstrou-se que sistemas de autenticação baseados em geometria de mão podem ser usados para controlar o acesso a paginas *Web*.

2.3.4.4 Reconhecimento de Retina

Algumas pesquisas têm provado que o padrão de veias da retina é a característica com maior garantia de unicidade que uma pessoa pode ter [AND99]. Os analisadores de retina medem esse padrão de vasos sangüíneos usando um laser de baixa intensidade e uma câmara. Nesta técnica, deve-se colocar o olho perto de uma câmara para obter uma imagem focada.

A análise de retina é considerada um dos métodos biométricos mais seguros. A FAR é nula e as fraudes até hoje são desconhecidas. Olhos falsos, lentes de contato e transplantes não podem quebrar a segurança do sistema [CAR97].

Recentes pesquisas médicas mostraram, entretanto, que as características da retina não são tão estáveis como pensava-se anteriormente: elas são afetadas por doenças, incluindo doenças das quais o paciente pode não estar ciente. Muitas pessoas ficam temerosas em colocar seu olho próximo a uma fonte de luz e aos problemas que isto possa causar. Como resultado, esta técnica impulsionou o caminho da utilização da análise da íris, que é menos invasiva. A figura 2.9 apresenta um exemplo de analisador de retina.

FIGURA 2.9 - Analisador de retina

As principais características dos analisadores de retina são [AND99]: tempo de verificação de 1,5 segundos, FRR de 12,4% (1 tentativa) e 0,4% (3 tentativas), FAR de 0%, tamanho do modelo de 40 bytes, difícil de usar e muito invasivo. Este método não é vulnerável à fraudes: falsos olhos, lentes de contato e transplantes não quebram a segurança do sistema.

2.3.4.5 Reconhecimento de Íris

Íris é o anel colorido que circunda a pupila do olho. Cada íris possui uma estrutura única que forma um padrão complexo e pode ser usada para identificar um indivíduo. A captura da imagem é feita por uma câmara em preto e branco. O usuário olha para a câmara de uma distância de aproximadamente 30 cm ou mais por poucos segundos. O sistema acomoda usuários de lentes de contato sem dificuldades, embora o sensor deva ser montado ou ajustado de modo a ser satisfatório para usuários de diferentes alturas, incluindo aqueles em cadeiras de roda.

Um sistema de reconhecimento de íris automatizado compara o novo padrão de íris capturado com o padrão de íris armazenado em uma base de dados para decidir se eles foram originados do mesmo olho. Estas imagens são processadas encontrando a íris dentro da imagem e depois extraindo suas características, alinhando o padrão com o armazenado na base de dados e combinando o conjunto de características para determinar se este foi originado do mesmo olho. O modelo da íris ocupa aproximadamente 512 bytes.

Sistemas automatizados de identificação e verificação baseados na tecnologia de reconhecimento de íris, não são invasivos e requerem menos interação do usuário do que outros sistemas biométricos. O reconhecimento de íris é uma nova tecnologia, onde a baixa FAR é a principal vantagem.

A empresa *IrisScan, Inc (www.iriscan.com)*, possui a patente sobre a tecnologia de reconhecimento de íris. As principais características dos produtos da *IrisScan* são [FID99]: tempo de cadastro menor que 30 segundos; tempo de verificação entre 1 e 2 segundos; FAR e FRR de 0,00001%; tamanho do modelo de aproximadamente 512 bytes; é fácil de ser usado; influência de ambientes com umidade; em termos de integração, é compatível com a HAAPI (*Human Authentication - Application Program Interface*) e BioAPI (*Biometric Application Program Interface*); baixo nível de invasão, pois as imagens são capturadas em uma distância de 20 centímetros; funciona em redes *Windows NT*, e no futuro na *Web*; disponível para sistema operacional *Windows NT*; possui banco de dados proprietário; e preço de US$ 5.000 para o *System 2100* e US$ 995 por unidade para o *PCIris*. A figura 2.10 mostra o kit de instalação do *PCIris*.

FIGURA 2.10 - Kit de instalação do *PCIris*

2.3.4.6 Reconhecimento de Voz

O reconhecimento de voz é um dos sistemas menos invasivos e a forma mais natural de uso é o sistema de reconhecimento de fala.

O som da voz humana é produzido pela ressonância na região vocal, em função de seu comprimento e do formato da boca e das cavidades nasais. Para a captura do som, o usuário posiciona-se diante de um microfone e pronuncia uma frase previamente selecionada, ou uma frase qualquer. Este processo é repetido várias vezes até que seja possível construir um modelo. Todos os sistemas que analisam a voz estão amplamente baseados na tecnologia de processamento de fala. A forma da onda das frases é medida usando-se análises de Fourier para encontrar o espectro de freqüências que amostram as características da voz.

A tecnologia de reconhecimento de voz é fácil de usar e não requer grandes esforços na educação do usuário. Entretanto, deve-se cuidar para garantir que o usuário fale em um tempo apropriado e em voz clara.

Uma vez que as pessoas formam seus padrões de fala através da combinação de fatores físicos e comportamentais, a imitação é impossível. Entretanto, existem problemas com as condições do ambiente onde se encontram os sensores, uma vez que é difícil filtrar o ruído de fundo. Outros problemas incluem a variação da voz devido às condições físicas do usuário, como gripes e resfriados, estados emocionais como o estresse, e duplicação através de um gravador. A imitação, porém, não é um problema como se poderia pensar, porque os aspectos da voz medida pelos sistemas não são os mesmos que os seres humanos costumam perceber.

Existem diversos fabricantes de produtos de reconhecimento de voz, entre eles a *VeriVoice (www.verivoice.com), T-Netix,(www.tnetix.com), Keyware (www.keywareusa.com) e Veritel Corp (www.veritelcorp.com)*. As principais características dos produtos da *Verivoice* são [VER99]: tempo de cadastro: 3 minutos; tempo de verificação em torno de 0,5 segundos em um Pentium Pro de 200MHhz; FAR e FRR de 1,7%; tamanho do modelo de 2 a 5 Kbytes; é fácil de ser usado; influência de ambientes com ruídos; baixo nível de invasão; funciona em redes *Windows NT*; está disponível para sistema operacional *Windows NT/95/98 e Solaris 2.5*. A figura 2.11 apresenta uma etapa do cadastro de voz no produto *VoiceGuardian, da Keyware.*

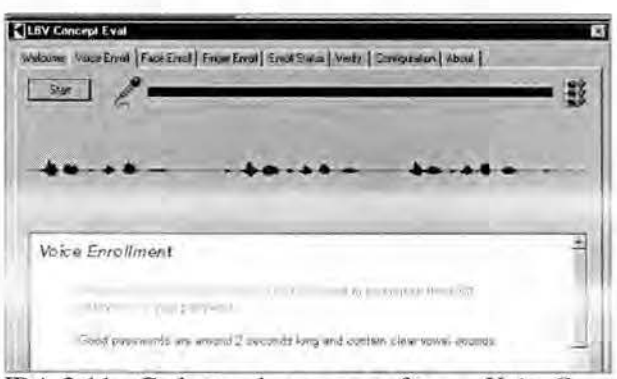

FIGURA 2.11 - Cadastro de voz no software *VoiceGuardian*

2.3.4.7 Reconhecimento de Assinatura

O ritmo necessário para escrever uma assinatura pode ser usado em um sistema de identificação automático. Esta técnica já é muito usada e popular, uma vez que todos os cheques são verificados usando-se as assinaturas.

Existem dois métodos de identificação: um método examina a assinatura já escrita, comparando-a, como uma imagem, com um modelo armazenado. A maior desvantagem deste método é que ele não pode detectar fotocópias das assinaturas. O outro método estuda a dinâmica da assinatura. Este esquema analisa o processo dinâmico da realização de uma assinatura – ritmo de escrita, contato com a superfície, tempo total, pontos de curva, laços, velocidade e aceleração. Os dispositivos utilizados para análise dinâmica são canetas óticas e superfícies sensíveis. A figura 2.12 apresenta um dispositivo de análise dinâmica de assinaturas.

FIGURA 2.12 - Dispositivo de análise dinâmica de assinaturas.

Como todas as características comportamentais, as assinaturas estão sujeitas ao humor do usuário, ao ambiente, à caneta , ao papel, e assim por diante. As assinaturas de algumas pessoas são muito consistentes, enquanto as de outras variam muito.

O modelo de assinatura tem tipicamente 1 Kbyte. Isto facilita seu uso online e com cartões inteligentes. Outras características são: possui baixa FAR, FRR em torno de 10%, é fácil de usar e tem um tempo de verificação entre 5 a 10 segundos.

2.3.4.8 Ritmo de Digitação

Como a assinatura, o ritmo de digitação exibe o mesmo fator neurofísico que pode ser utilizado na identificação única de um indivíduo. Esquemas de ritmo de digitação analisam o modo como um usuário digita em um terminal, monitorando o teclado 1000 vezes por segundo.

O método normal é a utilização das latências de digitação – o tempo entre a digitação de duas teclas. Certos dígrafos, ou digitação de duas letras adjacentes,

freqüentemente, apresentam padrões de tempo únicos que podem ser usados para caracterizar um indivíduo.

O procedimento geral de identificação e verificação requer que o usuário gere um perfil ou modelo. Na operação, a verificação requer a geração de um perfil de digitação, que é comparado com o modelo. Se existir uma grande diferença entre os dois perfis, o usuário terá seu acesso negado. Uma das vantagens deste método é que o usuário não percebe quando está sendo autenticado, ao menos que ele tenha sido informado anteriormente. Outra vantagem é que o cadastro e a verificação não são invasivos.

Em [RU97] é apresentado um sistema de controle de acesso baseado em ritmo de digitação que utiliza lógica *fuzzy* para analisar os padrões de digitação, e demonstra que esta técnica pode ser usada para identificar usuários legítimos.

2.3.5 Análise das Soluções Baseadas em Conhecimento

Os avanços da biometria aliados a PCs mais rápidos tornaram possível e econômico o uso de uma variedade de tecnologias de autenticação biométrica em redes e *desktops*. Os sistemas biométricos baseiam-se em características físicas e comportamentais de pessoas. Os principais sistemas biométricos utilizados nos dias de hoje baseiam-se no reconhecimento de face, impressão digital, geometria da mão, íris, retina, padrão de voz, assinatura e ritmo de digitação. As vantagens dos biométricos 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.

A tabela 2.6 apresenta uma comparação entre vários produtos que implementam as diferentes tecnologias de autenticação biométrica segundo alguns fatores de teste sugeridos pelo Biometric Consortium [BIC99].

TABELA 2.6 – Comparação de produtos biométricos

Produtos / Características	TrueFace	FaceIt	BioMouse Plus	TouchSafe Personal	PCIris	VeriVoice
Tempo de cadastro	5 a 30s	n.i.	20 a 30s	< 20s	< 30s	180s
Tempo de verificação	1 a 5s	1s	1s	1s	1 e 2s	0,5s
FRR	< 0,2%	< 1%	n.i.	<2%	0,00001 %	1,7%
FAR	Baixa	< 1%	0,1% a 0,0001% - configurável	< 0,001%	0,00001 %	1,7%

Tamanho do modelo	1000 a 1100 bytes	1000 a 1500 bytes	350 a 650 bytes	118 bytes	512 bytes	2 a 5 Kbytes
Facilidade de uso	Fácil	Fácil	Fácil	Fácil	Fácil	Fácil
Influência do ambiente	Necessita de luz	Necessita de luz	n.i.	n.i.	Problem as c/ umidade	Problemas c/ ruídos
API	Possui	Possui	Possui	Possui.	Possui	Possui
Uso em redes / *Web*	Sim/Sim	Sim/Sim	Sim/Não	Sim/Não	Sim/Não	Sim/Não
Sistemas operacionais	*Windows 95/98/NT, Solaris*	*Windows 95/98/NT*	*Windows 95/98/NT, Solaris, Sparc 2.5 e Linux*	*Windows 95/98/NT*	*Windows NT*	*Windows 95/98/NT, Solaris 2.5*
Banco de dados	*SQL Server*	Proprietário	Proprietário	Proprietário	Proprietá rio	Proprietário
Preço	US$ 120/usuário	US$ 100/usuário	US$ 299 / instalação	US$ 499 / instalação	US$ 995	n.i.

n.i: não informado

Dentre os métodos de autenticação analisados, o que demonstrou ser mais interessante para o uso em sistemas de educação a distância foi o reconhecimento de face. Os produtos analisados que implementam esta tecnologia são o *TrueFace* e o *FaceIt*. Ambos são rápidos e fáceis de usar. Em ambos sistemas é requerida uma câmera digital para a captura das imagens, mas pressupõe-se que este dispositivo de *hardware* esteja disponível em ambientes de educação a distância.

Dentre as principais características dos sistemas citados acima, destacam-se: são rápidos e fáceis de usar, possuem soluções para redes e para *Web* e podem ser integrados à aplicações através de APIs. Ambos possuem versões para *Windows 95/98/NT*, porém o *TrueFace* também é compatível com *Sun Solaris*.

Uma importante característica que ambos implementam e que é especialmente importante para aplicações remotas, é que a cada tentativa de acesso é gravada uma imagem do usuário para fins de auditoria. O custo dos produtos fica na base de US$100 a U$120 por usuário, porém os produtos somente são vendidos com um mínimo de 25 licenças [MCD99] [VIS99a].

Os sistemas baseados em impressão digital são mais indicados na utilização em *desktops* embora possam funcionar em rede. Os produtos analisados ainda não possuem soluções para *Web*, tornando-os inviáveis para uso remoto. Porém os fabricantes já anunciaram que pretendem disponibilizar suporte à *Web* em suas próximas versões, o

que é um indicativo de que em um curto espaço de tempo será possível utilizá-los em procedimentos de educação a distância. Eles poderiam ser utilizados em centros de certificação para autenticar localmente o aluno na realização de uma prova a distância.

Em geral, os produtos de impressão digital são fáceis de usar. Por serem extremamente pequenos, é comum encontrarem-se leitores de digitais integrados em teclados e *mouses*. A maioria é compatível com *Windows 95/98/NT*, sendo que alguns deles apresentam também versões para *Sun Solaris e Linux*. O custo varia de US$150 a US$499 por instalação.

Outras soluções, como reconhecimento de retina, íris e geometria da mão, necessitam de equipamentos extras, o que mantém seu custo elevado, sendo mais indicados, então, em aplicações bancárias e no controle de acesso a áreas protegidas.

Não foram encontradas soluções disponíveis gratuitamente ou a um baixo custo que viabilizasse sua aquisição para utilização neste projeto. Algumas alternativas que podem ser consideradas são a análise de predicado, a qual identifica o aluno por seu estilo de escrita [TUC99], e a utilização da câmera digital na realização de checagens randômicas, onde, em tempos aleatórios, captura-se uma foto do aluno, a qual deve ser enviada para um diretório remoto para conferência posterior por parte do professor.

Em termos de segurança, a integração de múltiplos dispositivos biométricos reduz a possibilidade de fraudes. Esta parece ser uma tendência dos sistemas de identificação [JAI99]. Técnicas biométricas multimodais, as quais combinam múltiplos dispositivos biométricos para uma identificação, podem ser usadas para superar as limitações individuais de cada dispositivo. Experimentos de integração de vários dispositivos foram efetuados com resultados muito positivos tanto em tempo de resposta, como em precisão [JAI99] [HON98].

Outra tendência que se percebe é a combinação de biometria com *smartcards*. Prova disso é o anúncio do *BioSMART* [BII99], o primeiro *smartcard* integrado com um sistema de verificação de impressão digital. Armazenando o modelo no *smartcard*, o *BioSMART* fornece um sistema de identificação pessoal portátil. Além disso, reduz os custos administrativos associados com a manutenção do banco de dados de modelos.

Por fim, percebe-se que a biometria é uma tecnologia emergente. Empresas de pesquisa indicam que a demanda européia por dispositivos biométricos irá exceder US$ 133 milhões no ano 2001 [BIO99a]. Segundo relatório da ICSA, em janeiro de 1998, existiam 330 produtos biométricos conhecidos, dos quais 223 eram comerciais. Em dezembro de 1998, o número de produtos biométricos conhecidos passou para 513, tendo um crescimento de 55%, enquanto os produtos biométricos comerciais chegaram a 330, com crescimento de 48% [ICS99]. Os dados são mostrados no gráfico da figura 2.13. Este crescimento, aliado à queda dos preços dos dispositivos biométricos, leva-nos a crer que em pouco tempo poderemos ter produtos biométricos mais viáveis de integração com aplicações de ensino a distância.

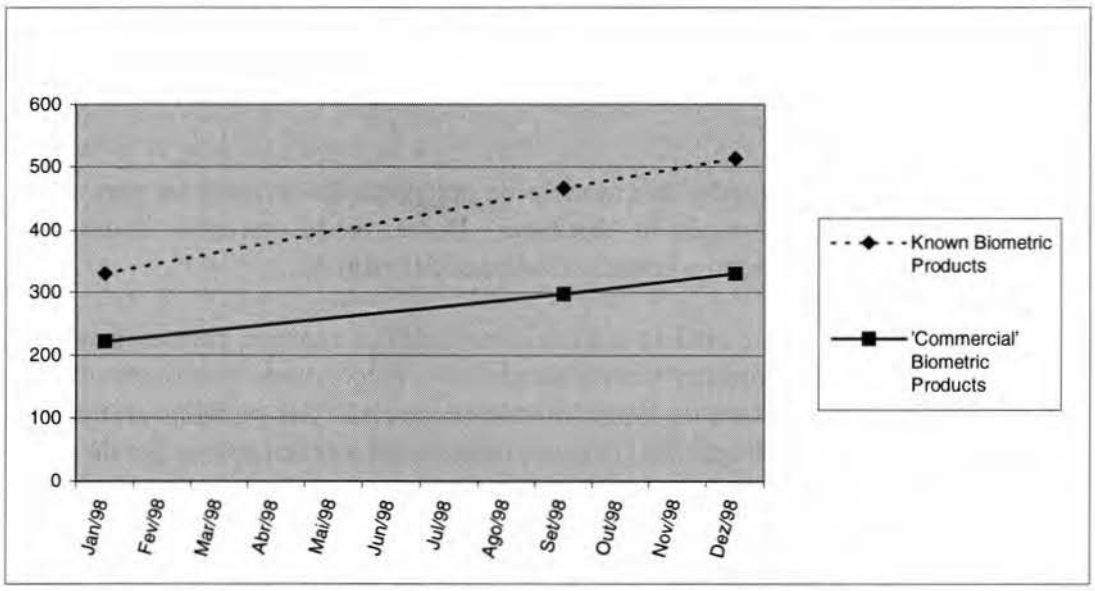

FIGURA 2.13 - Número total de produtos biométricos

3 Modelo de Proposto

Este trabalho propõe um modelo de autenticação de usuários para ser utilizado em aplicações de educação a distância. Deste modo, envolve todas as rotinas relacionadas à autenticação e geração dinâmica das páginas.

De acordo com a análise realizada no capítulo anterior, procurou-se selecionar as soluções viáveis, tanto em termos de custo e dispositivos extras envolvidos, como em termos de simplicidade de procedimentos e precisão das medidas efetuadas. Assim, foi proposto um modelo que integra essas técnicas de autenticação a fim de chegar a um nível de segurança maior do que senhas.

O sistema funciona como um *proxy*, cuja função é controlar o acesso às páginas *Web* através da combinação de senhas, perguntas randômicas, dispositivos biométricos e checagem randômica, ao mesmo tempo que gera *logs* da atividade do aluno no curso. Esses *logs* conterão informações como dia e hora do acesso, tempo dispendido em cada página, endereço IP da máquina do aluno, entre outras. Esses dados poderão ser utilizados na avaliação do aluno e também na geração de seu perfil estatístico, que servirá para gerar alertas, na medida em que os dados do perfil sofrerem mudanças acima dos limites estabelecidos, durante a atividade do aluno.

Para que apenas pessoas autorizadas possam acessar as páginas, as mesmas serão geradas dinamicamente através de um CGI (*Common Gateway Interface)* no servidor. Esse mesmo CGI será o responsável pela autenticação e pela geração dos *logs* citados acima.

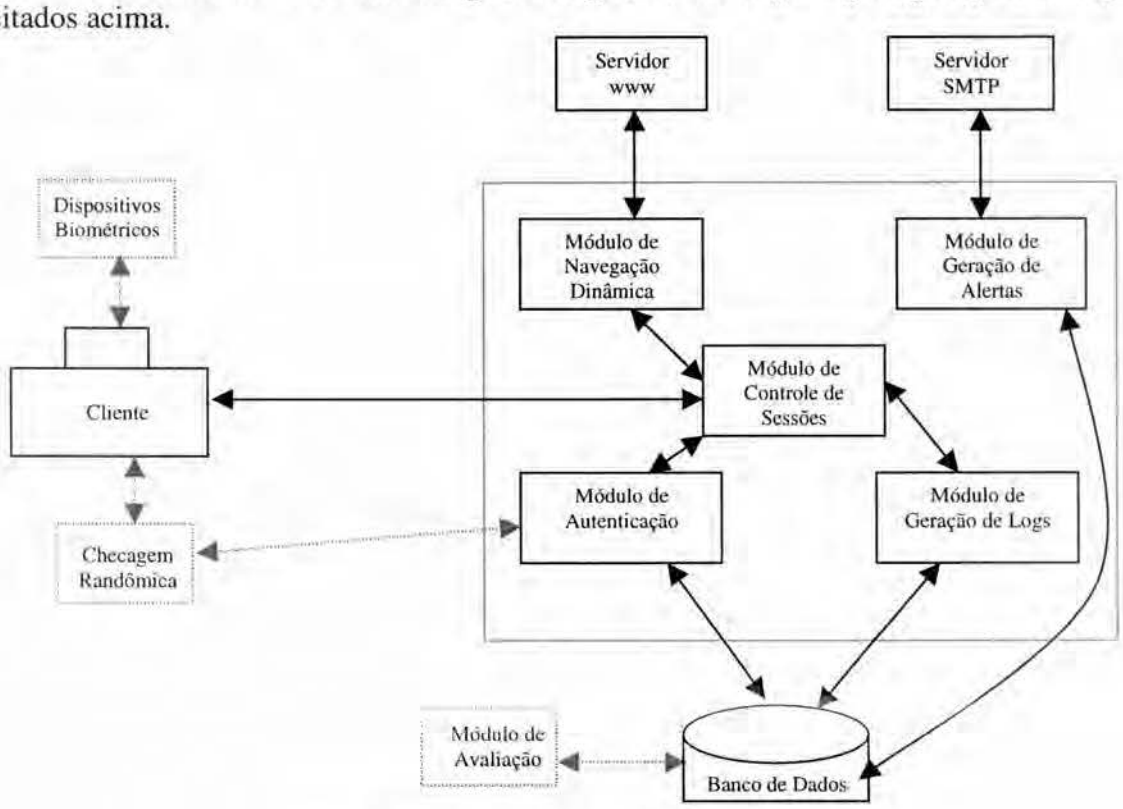

FIGURA 3.1 - Arquitetura do modelo proposto

O sistema é composto pelos seguintes módulos: módulo de autenticação, módulo de navegação dinâmica, módulo de controle de sessões, módulo de geração de alertas e módulo de geração de *logs*. A figura 3.1 apresenta a arquitetura do modelo proposto.

3.1 Módulo de Autenticação:

Este módulo integra diferentes soluções de autenticação de usuários de modo a suprir as deficiências individuais de cada uma. Estas soluções se completam, formando um todo mais seguro que o oferecido com o uso individual de cada uma.

A primeira técnica utilizada são as senhas. Por questões de segurança, apenas os *hashs* MD5 dessas senhas são armazenados no banco de dados. Isso evita que o sistema seja comprometido em caso do banco de dados ser violado. Quando o usuário entra no sistema, o mesmo busca o *hash* na base de dados e compara-o com o *hash* da senha informada, liberando o acesso caso forem idênticos.

A utilização de perguntas randômicas é uma técnica que visa dificultar o acesso de pessoas não cadastradas ao sistema. Estas perguntas baseiam-se em dados pessoais de alunos válidos que são previamente cadastrados. No momento da conexão, busca-se na base de dados uma dessas perguntas pessoais de forma aleatória, a qual é devolvida ao aluno na forma de um desafio. Se ele responder corretamente, estará autenticado no sistema. A figura 3.2 apresenta alguns exemplos de perguntas randômicas pessoais que podem ser utilizadas. É importante se destacar que as perguntas apresentadas na figura 3.2 são apenas exemplos. Caberá ao administrador do sistema realizar o cadastro das perguntas que julgar necessárias, em ferramenta própria, desenvolvida neste trabalho.

Um meio de melhorar a eficiência das perguntas randômicas é a inserção de perguntas com respostas dinâmicas, isto é, com respostas geradas pela atividade do usuário, como por exemplo: "Qual a data de sua última conexão?" Ao contrário das respostas estáticas, as dinâmicas mudam a cada sessão, aumentando o grau de segurança.

1 - Qual é a sua cidade natal?
2 - Qual é o primeiro nome de sua mãe?
3 - Em que ano você nasceu (AAAA)?
4 - Qual é o primeiro nome de seu pai?

FIGURA 3.2 - Exemplos de perguntas randômicas

O uso de dispositivos biométricos pretende adicionar a característica pessoal do aluno no processo de autenticação. Um dispositivo que pode ser utilizado é o reconhecimento de faces. Ele necessita apenas uma câmera digital, freqüentemente encontrada em ambientes de ensino a distância. Porém podem ser utilizados outros dispositivos biométricos que possam funcionar pela *Web*.

Por fim, a utilização de checagem randômica complementa a autenticação possibilitando que se faça uma verificação visual do usuário que estiver utilizando o procedimento de educação a distância. Nesta técnica, é necessário instalar uma aplicação no cliente que em tempos aleatórios extraia uma foto do usuário através de uma câmera digital e a envie para um diretório remoto para posterior conferência. Assim o professor pode conferir se a pessoa que está na frente da câmera é a mesma que passou pelos outros processos de autenticação. A aplicação que roda no cliente para extração das fotos comunica-se com o módulo de autenticação, de modo que o usuário somente poderá concluir a autenticação se esta rotina estiver ativa.

Para acessar o sistema, o aluno deve primeiramente iniciar a aplicação de checagem randômica em seu computador. A seguir, acessar, com seu navegador, a página de *login*. Neste momento lhe serão requisitados os dados de autenticação (nome, senha e/ou extração do dado biométrico). Estes dados serão enviados para o módulo de autenticação, que verificará se são válidos. Se os dados forem válidos, o sistema buscará na base de dados uma pergunta pessoal aleatória e desafiará o usuário. Se ele responder corretamente a pergunta, estará autenticado no sistema, e lhe será apresentada a página inicial com os cursos em que está matriculado. Uma resposta ou dado inválido, em qualquer etapa deste processo, negará o acesso do aluno ao sistema.

3.2 Módulo de Navegação Dinâmica

O módulo de navegação dinâmica é responsável por apresentar as páginas do curso aos alunos. Para isso, ao receber uma requisição, ele abre uma conexão URL (*Uniform Resource Locator*) com o servidor WWW destino, busca a página e a devolve para o navegador do cliente, de forma transparente.

Os métodos analisados para realizar o controle de acesso dos alunos às páginas do curso foram a geração de páginas dinâmicas, autenticação básica dos servidores WWW e alterações no servidor WWW.

A autenticação básica dos servidores WWW utiliza somente senhas, o que foi considerado insuficiente devido aos problemas relacionados às senhas apresentados no capítulo dois. A fim de obter independência de plataforma e de servidor WWW, descartou-se modificações em um servidor, optando-se assim pela geração dinâmica de páginas. Além disso, esta técnica possibilita que se obtenha um controle mais apurado das atividades dos usuários.

No momento em que este módulo busca a página no servidor remoto, ele modifica seus *links* de modo que toda a requisição do cliente passe pelo sistema. A figura 3.3 apresenta um trecho do código HTML (*Hypertext Markup Language*) de uma página modificada.

É importante salientar que a navegação somente é possível após o aluno ter passado pelo processo de autenticação. Na medida em que o usuário navega pelo curso, armazena-se várias informações, tais como a seqüência de navegação, informações de cada página, entre outras, que serão utilizadas na geração dos *logs* do sistema.

```
<li><a href="javascript:envia('x500.htm')"><big>Padrão X.500</big></a></li>
<li><a href="javascript:envia('nomes.htm')"><big>Nomes</big></a></li>
<li><a href="javascript:envia('dib.htm')"><big>BID - Base de Informações do Diretório
</big></a></li>

<script language="javascript">
function envia(url1)
{
  document.form1.URL.value=url1
  document.form1.submit()
}
</script>
<form name=form1 ACTION="http://127.0.0.1/servlets/ProxyServlet"
```

FIGURA 3.3 - Fonte do arquivo HTML com *links* modificados

3.3 Módulo de Controle de Sessões

O HTTP (*Hypertext Transfer Protocol*) é um protocolo sem estados *(stateless)*, ou seja, não fornece nenhum meio de um servidor reconhecer que uma seqüência de requisições é do mesmo cliente. Assim, é necessário que cada cliente forneça um identificador único que permita que o servidor identifique-o. Esse é o trabalho do módulo de controle de sessão

Existem várias técnicas que podem ser utilizadas no controle de sessão. Dentre as mais comuns, destacam-se campos de formulários escondidos, reescrita de URL e *cookies* [HUN98].

A técnica de campos de formulário escondidos (*hidden form fields*) consiste em adicionar este tipo de campos em um formulário HTML, os quais não são mostrados pelo navegador do cliente. Eles são enviados ao servidor no momento em que o formulário que os contém é submetido. A figura 3.4 apresenta um exemplo de campo escondido. Campos de formulários escondidos são suportados por todos os navegadores e não exigem pré-requisito adicional do servidor.

```
<FORM ACTION="cgi-bin/Exemplo" METHOD="POST"
...
<INPUT TYPE=hidden NAME="sessionid" VALUE="43rddd5d">
...
</FORM>
```

FIGURA 3.4 - Campos escondidos em um formulário HTML

Na técnica de reescrita de URL (*URL Rewriting*), cada *link* que o usuário possa clicar é dinamicamente modificado ou reescrito, de modo a incluir informações adicionais. Estas informações podem ser na forma de caminho (*path*), parâmetros ou alguma URL específica. Devido ao limitado espaço disponível para a reescrita de uma

URL, as informações adicionadas são usualmente limitadas a um identificador de sessão. Por exemplo, a figura 3.5 mostra a reescrita de uma URL para passar o identificador de sessão 123.

http://servidor:porta/servlet/Rewritten	original
http://servidor:porta/servlet/Rewritten?sessionid=123	parâmetros adicionados
http://servidor:porta/servlet/Rewritten/123	caminho modificado

FIGURA 3.5 - Reescrita de URL

A última técnica de controle de sessão estudada envolve o uso de *cookies*. Um *cookie* é um pedaço de informação enviado pelo servidor *Web* para um navegador que pode ser lido posteriormente pelo servidor. Quando um navegador recebe um *cookie,* ele o salva e depois o envia para o servidor cada vez que o navegador acessa uma página naquele servidor, sujeito à certas regras. Uma vez que o valor do *cookie* pode identificar unicamente um cliente, eles podem ser usados para controle de sessão.

O módulo de controle de sessão utiliza uma combinação de *cookies* e campos de formulários escondidos para permitir que o sistema associe um pedido a um usuário. Na verdade, o controle de sessão do sistema utiliza *cookies.* Os campos de formulários escondidos são utilizados para passar informações da sessão para o módulo de avaliação (desenvolvido por outro aluno do PPGC da UFRGS)[HAC2000] .

O funcionamento do módulo de controle de sessão é simples: no momento em que o usuário acessa a página de *login* e envia suas informações é criado um *cookie* contendo um identificador para aquela sessão. Este identificador de sessão é armazenado em memória e associado ao nome do usuário. Em todas as requisições subseqüentes, o sistema verifica este *cookie*. Se ele for válido, ele verifica a associação com o nome do usuário em memória e mantém a sessão. Ao término da sessão ou na ocorrência de uma etapa de autenticação inválida, o *cookie* é invalidado e sua referência é retirada da memória. Com isso, qualquer requisição subseqüente é redirecionada para a página de *login,* para a criação de um novo *cookie.*

3.4 Módulo de Geração de Logs

O módulo de geração de *logs* é responsável por armazenar informações sobre a atividade dos usuários no sistema. Estas informações referem-se às sessões e à seqüência de páginas acessadas. Dentre as informações da sessão, destacam-se a data e hora de acesso, tempo despendido em cada sessão, endereço IP e DNS da máquina cliente, e agente do usuário - *HTTP_USER_AGENT* (contém o nome e a versão do navegador do usuário). Além disso, este módulo também armazena a seqüência de navegação do usuário, contendo informações sobre cada página acessada, tais como título da página, URL, data e hora de acesso, tamanho da página e taxa e tempo de leitura. A figura 3.6 apresenta uma parte do *log* gerado no final de uma sessão.

A geração das informações contidas no *log* do sistema inicia no momento em que o usuário finaliza a fase de autenticação. A partir daí, qualquer operação efetuada é armazenada. No momento em que o usuário encerra sua sessão, o sistema armazena as informações do *log* na base de dados.

As informações contidas no *log* são utilizadas pelo módulo de avaliação para avaliar o aluno. O módulo de geração de alertas também utiliza essas informações para a composição do perfil do aluno.

Final da Sessão

Identificador da Sessão: *3fd973a1b2de4000.7.942246768660*
Código do Curso: *cmp124*
Usuário: *mfiorese*
Máquina: *127.0.0.1 (127.0.0.1)*
Agente do Usuário: *Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt; zaz5eng)*
Inicio da Sessão: *10 de Novembro de 1999 13:13:01 GMT-02:00*
Final da Sessão: *10 de Novembro de 1999 13:13:52 GMT-02:00*
Tempo total: *0:0:51 hs*

Seqüência de Navegação:
Tutorial de X.500 (http://127.0.0.1/x500/index.htm) [2260 bytes]
Tempo decorrido: 0:0:16 hs - Taxa de Leitura: 141.0 bytes/s

Serviços de Diretório (http://127.0.0.1/X500/servicos.htm) [4204 bytes]
Tempo decorrido: 0:0:21 hs - Taxa de Leitura: 200.0 bytes/s

FIGURA 3.6 - *Log* gerado no final de uma sessão

3.5 Módulo de Geração de Alertas

Este módulo é responsável pela análise da utilização do sistema pelos usuários e pela geração de alertas na medida em que seu comportamento desvia-se do perfil gerado durante a atividade desses usuários no sistema. Desta forma, o módulo de geração de alertas é visto como um complemento da autenticação.

O perfil do usuário é extraído através de consulta aos *logs* do sistema. Dentre as variáveis selecionadas para a composição deste perfil destacam-se:

- Horário de conexão: horário em que o usuário acessa o sistema;
- Duração da sessão: tempo em que o usuário ficou conectado;
- Taxa de leitura: relação entre o tamanho da página e o tempo em que o usuário permaneceu nela (em Kbytes/seg);
- Dia da semana: freqüência do dia em que é feito o acesso;
- Agente do usuário: freqüência dos agentes do usuário (contém o nome e a versão do navegador);

- Endereço IP da máquina: freqüência dos endereços IP das máquinas utilizadas no acesso ao sistema pelo usuário

Para que o professor possa configurar e ajustar os limites de cada variável na geração de alertas, o sistema disponibilizará uma ferramenta chamada "Configurar Alertas". Através dela, o professor poderá ajustar as regras de geração de alertas do modo que melhor lhe convier. A figura 3.7 apresenta uma visão da ferramenta Configurar Alertas.

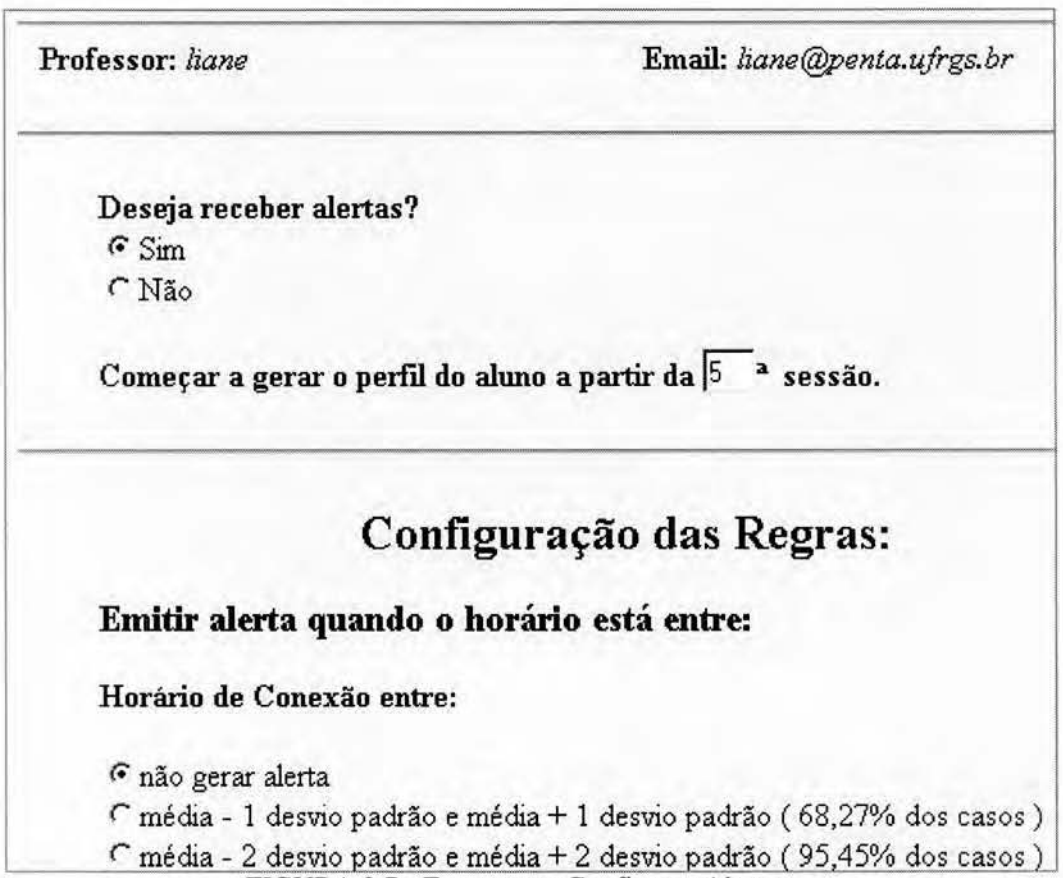

FIGURA 3.7 - Ferramenta Configurar Alertas

Com as variáveis "*horário em que o usuário acessa o sistema*", "*duração da sessão*" e "*taxa de leitura*", determina-se a média aritmética (figura 3.8) e o desvio padrão (figura 3.9).

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}$$

FIGURA 3.8 - Fórmula da média aritmética

$$s = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}}$$

FIGURA 3.9 - Fórmula do desvio-padrão

Com isso, o professor poderá configurar estas variáveis para estarem dentro de determinados intervalos. Estes intervalos foram escolhidos de acordo com a propriedade mátemática do desvio-padrão para distribuições normais [SPI79]:

- 68,27% dos casos estão incluídos entre $\bar{x} - s$ e $\bar{x} + s$;
- 95,45% dos casos estão incluídos entre $\bar{x} - 2s$ e $\bar{x} + 2s$;
- 99,73% dos casos estão incluídos entre $\bar{x} - 3s$ e $\bar{x} + 3s$;

Sempre que uma variável estiver fora dos limites configurados pelo professor, envia-se uma mensagem alertando-o do ocorrido.

3.6 Escopo da Implementação

Este trabalho propõe um modelo de autenticação de usuários a utilizar-se em aplicações de ensino a distância. Assim, serão implementadas rotinas relacionadas à autenticação, controle de sessão, geração dinâmica das páginas, geração de alertas e *logs*.

Uma vez que as páginas serão geradas dinamicamente, a *interface* com o usuário também ficará contida neste trabalho.

Em termos de integração com o sistema de avaliação (desenvolvido em [HAC2000]), serão incluídos na *interface* do sistema os *links* de chamada das ferramentas de avaliação. O identificador de sessão será passado às rotinas de avaliação através de campos escondidos.

No que refere-se à autenticação, a inviabilidade econômica para aquisição dispositivos biométricos e seu respectivo *software*, impediram sua utilização neste trabalho. A dificuldade de manipulação das APIs das câmeras digitais no desenvolvimento de uma rotina de checagem randômica também inviabiliza sua implementação neste projeto. Assim, dispositivos biométricos e checagem randômica apenas constarão no modelo e em trabalhos futuros.

Por fim , em termos de navegação dinâmica, se optou por utilizar apenas um subconjunto do HTML para a validação do modelo. Desta forma, apenas serão modificados os *links* relacionados a *tag* HREF para páginas HTML e texto.

4 Implementação do Protótipo

A fim de validar o modelo proposto no capítulo anterior, implementou-se um protótipo de um sistema de autenticação de usuários para ensino a distância. Este capítulo apresenta as tecnologias utilizadas nessa implementação, os requisitos necessários e detalhes da implantação do sistema, sua especificação em SDL (*Specification and Description Language*), modelo de dados, diagrama de classes, descrição das *interfaces*, integração com o sistema de avaliação e, por fim, uma avaliação do protótipo.

4.1 Ambiente de Implementação

O protótipo foi totalmente desenvolvido utilizando-se a linguagem *Java*. Os motivos que levaram a escolha dessa linguagem são sua portabilidade, sua segurança, sua robustez e a disponibilidade de bibliotecas para acesso a banco de dados e ao trabalho em rede. As tecnologias *Java*, fundamentais para o desenvolvimento do protótipo, foram as *Servlets* e a conectividade com banco de dados via *JDBC (Java DataBase Connectivity)*, descritas a seguir.

4.1.1 *Servlets*

As *servlets* fornecem um mecanismo simples e consistente para estender a funcionalidade de um servidor *Web*. Uma *servlet* pode ser pensada como uma pequena aplicação que roda no servidor.

A API utilizada na escrita das *servlets* não se preocupa em como ela é carregada, com o ambiente em que ela rodará ou com o protocolo usado no envio e recebimento de informações. Isto faz com que as *servlets* possam ser incorporadas em vários servidores *Web* diferentes.

As *servlets* provêem um método baseado em componentes independente de plataforma, para construção de aplicações baseadas na *Web*, sem as limitações de desempenho dos programas CGI.

Por serem escritas em *Java*, as *servlets* têm acesso a toda sua API. Elas também têm acesso à biblioteca HTTP, com chamadas específicas e todos os benefícios do *Java*, inclusive portabilidade, desempenho, reusabilidade e proteção contra *crash*.

Algumas das principais vantagens do uso de *servlets* em relação às CGIs são:

- Independência de plataforma: as *servlets* podem rodar em qualquer plataforma sem a necessidade de serem reescritas ou compiladas novamente.;

- Desempenho: carrega-se um novo programa CGI para cada requisição ao servidor. Isto quer dizer que se tivermos 10 requisições simultâneas, teremos 10 programas iguais na memória. As *servlets* são carregadas apenas uma vez e para cada nova requisição a *servlet* gera uma nova *thread*. O método *init()* da *servlet*, assim como nas *applets*, ocorre apenas na primeira vez que a classe é carregada. É geralmente no método *init()* que, por exemplo, estabelece-se uma conexão ao banco de dados. Cada uma das *threads* geradas pode usar a mesma conexão aberta no método *init()*. Este tipo de tratamento melhora o desempenho da *servlet*, já que a conexão ao banco de dados é feita apenas uma vez e todas as outras requisições usam esta conexão. A figura 4.1 apresenta o ciclo de vida da *servlet*.

- Extensibilidade: com *Java* é possível criar aplicações muito mais modulares, tirar proveito da orientação a objetos e utilizar o grande número de APIs disponíveis pela *Javasoft* (*www.javasoft.com.br*) e terceiros.

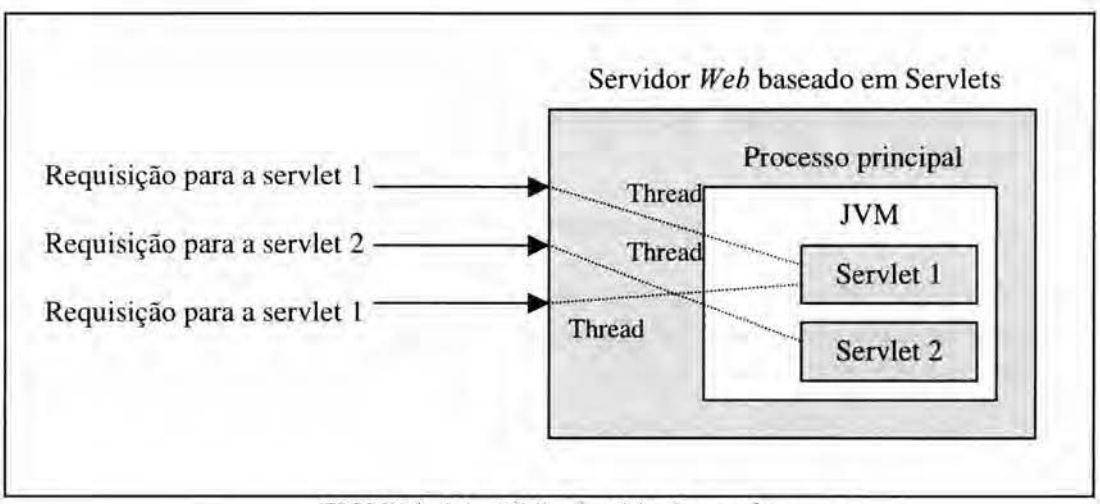

FIGURA 4.1 - Ciclo de vida da *servlets*

4.1.2 JDBC

A JDBC é uma API que permite o acesso a qualquer fonte de dados através de programação *Java*. Ela consiste em um conjunto de classes e *interfaces* escritas em *Java*, fornecendo conectividade para uma grande variedade de bancos de dados SQL, planilhas eletrônicas ou arquivos.

Com a utilização de JDBC, é fácil enviar um comando SQL para qualquer banco de dados relacional. Em outras palavras, não é necessário escrever um programa para acessar um banco de dados *Sybase* e outro para acessar um banco de dados *Oracle* e assim por diante.

Com o JDBC é possível executar três tarefas:

1. Estabelecer uma conexão com o banco de dados;
2. Enviar comandos SQL;
3. Processar os resultados.

A figura 4.2 apresenta um fragmento de código *Java* que executa as tarefas citadas acima.

```
Connection con = DriverManager.getConnection (
                    "jdbc:odbc:wombat", "login", "password");
   Statement stmt = con.createStatement();
   ResultSet rs = stmt.executeQuery("SELECT a, b, c FROM Table1");
   while (rs.next()) {
       int x = getInt("a");
       String s = getString("b");
       float f = getFloat("c");
   }
```

FIGURA 4.2 - Código *Java* mostrando acesso JDBC

Um banco de dados individual é acessado através de um *driver* JDBC específico. Existem *drivers* para quase todos os bancos de dados populares, alguns sendo disponíveis gratuitamente.

Os *drivers* JDBC classificam-se em quatro categorias:

- JDBC-ODBC *bridge:* Este tipo de *driver* fornece acesso JDBC via *driver* ODBC (*Opend DataBase Connectivity*). Ele requer que o *driver* ODBC esteja disponível na máquina do cliente;

- *Native*-API *driver:* Este tipo de *driver* converte chamadas JDBC em chamadas para a API do cliente para *Oracle, Sybase, Informix* ou outro DBMS (*DataBase Management System*);

- JDBC-*Net driver:* Este tipo de *driver* converte as chamadas JDBC em um protocolo de rede independente do DBMS, o qual é convertido para um protocolo DBMS por um servidor;

- *Native Protocol pure Java*: Este tipo de *driver* converte as chamadas JDBC em um protocolo de rede usado diretamente pelo DBMS.

4.1.3 Implantação

O protótipo do sistema foi implantado na máquina penta2 da rede da UFRGS (endereço IP: 143.54.1.30, DNS: penta2.ufrgs.br e rede: 143.54.1.0). Esta máquina é uma Sparc - ULTRA 1, com 64 Mb de memória e rodando sistema operacional Solaris 2.5.1 para Sparc.

Para que o sistema seja instalado corretamente, são necessários os seguintes produtos:

- **JDK 1.1:** O *Java Development Kit* é um conjunto de ferramentas desenvolvidas pela *Sun Microsystems* que são utilizadas na criação de programas *Java*. Atualmente encontra-se na versão 1.2. Existem versões do JDK para diferentes plataformas como *Microsoft Windows 95/98* e *Windows NT*, *Solaris 2.x for SPARC* e *x86*, *Apple MacOS*, entre outros. A versão utilizada na implantação foi a 1.1.5 para *Solaris*.

  O JDK pode ser obtido gratuitamente no endereço: http://www.java.sun.com/products/jdk/1.1/index.html .

- **JSDK 2.0:** O *Java Servlets Development Kit* é um conjunto de ferramentas desenvolvidas pela *Sun Microsystems* que são utilizadas no desenvolvimento de *servlets Java*. Atualmente encontra-se na versão 2.1. Existem versões do JSDK para diferentes plataformas como *Microsoft Windows 95/98 e NT, Solaris 2.x for SPARC e x86, Apple MacOS*, entre outros. A versão utilizada na implantação foi a 2.0 para *Solaris*.

  O JSDK pode ser obtido gratuitamente no endereço: http://www.java.sun.com/products/servlet/download.html

- ***Apache Web Server 1.3.9:*** O *Apache Web Server* é uma implementação do protocolo HTTP realizada pelo *Apache Group*. Atualmente encontra-se na versão 1.3.9, a qual utilizou-se na implantação.

  O *Apache Web Server* pode ser obtido gratuitamente no endereço: http://www.apache.org/dist/

- ***Apache JServ 1.0***: O *Apache JServ* é um *plug-in* que adiciona o suporte a *servlets* ao *Apache Web Server*. O *JServ* foi desenvolvido 100 % em *Java*, sendo compatível com o *Java* versão 1.1 e *Servlets* versão 2.0. Atualmente encontra-se na versão 1.0 a qual utilizou-se na implantação.

  O *Apache JServ* pode ser obtido gratuitamente no endereço: http://www.apache.org/jserv/dist/

- ***MySQL 3.22:*** O *MySQL* é um servidor de banco de dados SQL multi-usuário e multi-tarefa. Ele é uma implementação cliente/servidor que consiste em um *daemon mysqld* e diferentes clientes e bibliotecas. Atualmente encontra-se na versão 3.22, a qual utilizou-se na implantação.

  O *MySQL* é gratuito para plataformas *Unix* e *OS/2*. Para plataformas *Microsoft* existem versões de avaliação de 30 dias. O *MySQL* pode ser encontrado no endereço http://www.mysql.com/ .

- **Driver JDBC *mm.mysql.jdbc-1.2b*:** *MM.MySQL* é um JDBC-*Net driver* licenciado pelo GNU. Ele possibilita que sejam feitas conexões ao banco de dados *MySQL* por aplicações e *applets Java*. O *MM.MySQL* JDBC *driver* pode ser obtido gratuitamente no endereço http://www.worldserver.com/mm.mysql/ .

- ***JNL Statistics class*:** O *JNL Statistics class* é uma classe que contém uma coleção de funções de estatísticas, tais como média aritmética e desvio padrão. Esta classe é

fornecida gratuitamente pela *Visual Numeric* no endereço: http://www.vni.com/products/wpd/jnl/

4.2 Especificação do Sistema em SDL

A proposta da SDL é a descrição do comportamento real do sistema independentemente da linguagem utilizada na implementação A especificação do sistema implementado em SDL encontra-se no Anexo 1.

4.3 Modelo de Dados

O modelo de dados contém o diagrama entidade-relacionamento e a descrição de todas as tabelas utilizadas pelo sistema. Este modelo dados encontra-se no Anexo 2.

4.4 Diagrama de Classes

O diagrama de classes ilustra as especificações para classes e *interfaces* (por exemplo, *interfaces Java*) em uma aplicação. Informações típicas que este diagrama contêm são:

- Classes, associações e atributos;
- *Interfaces*, com suas operações e constantes;
- Informações de tipos de atributos;

O diagrama de classes encontra-se no Anexo 3.

4.5 Descrição das Interfaces

A *interface* do sistema foi desenvolvida utilizando-se HTML. No endereço http://www.penta2.ufrgs.br/~mfiorese/proxy/login.htm tem-se acesso à página de *login* do sistema. A figura 4.3 apresenta a tela inicial do sistema.

Ao entrar na página inicial do sistema o usuário deve preencher os campos "Username" e "Senha" e apertar no botão "Entrar". Se esses dados de autenticação forem corretos, o sistema apresentará uma página contendo uma pergunta randômica, apresentada na figura 4.4. No caso dos dados serem incorretos, o sistema negará o acesso ao usuário (figura 4.5).

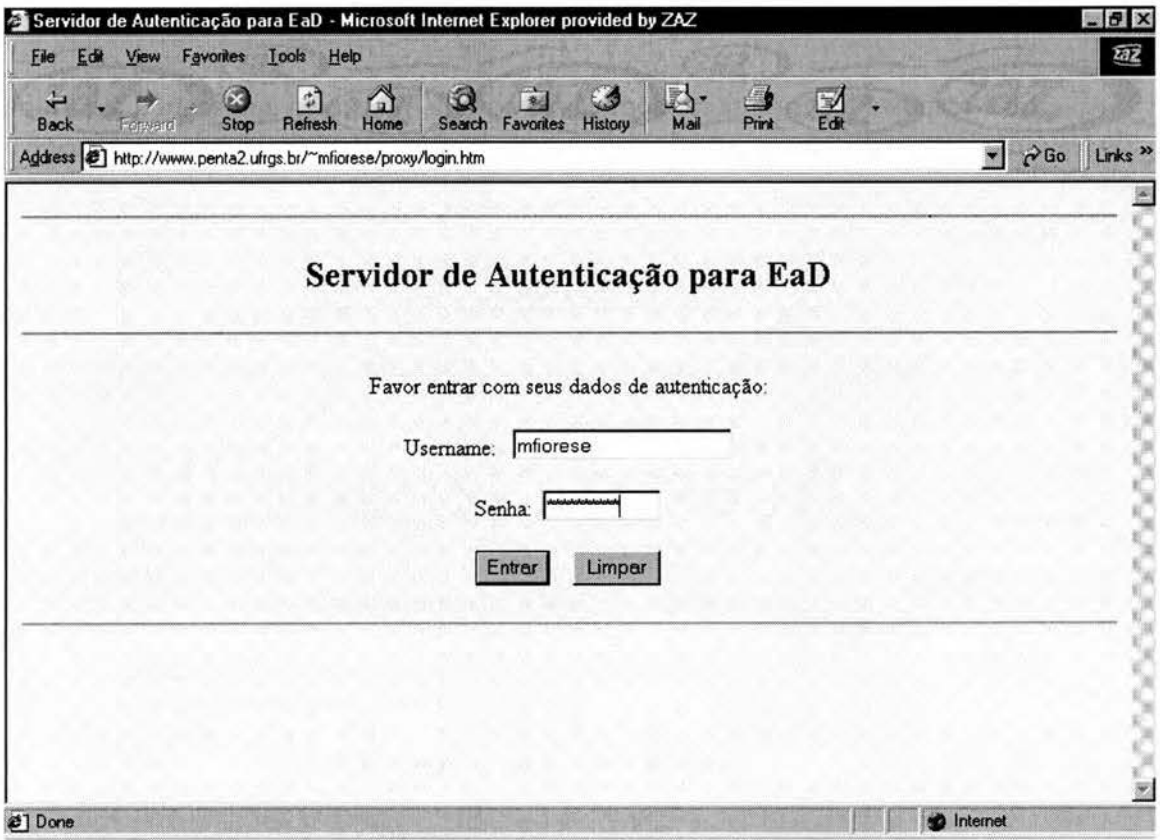

FIGURA 4.3 - Tela de *login* do sistema

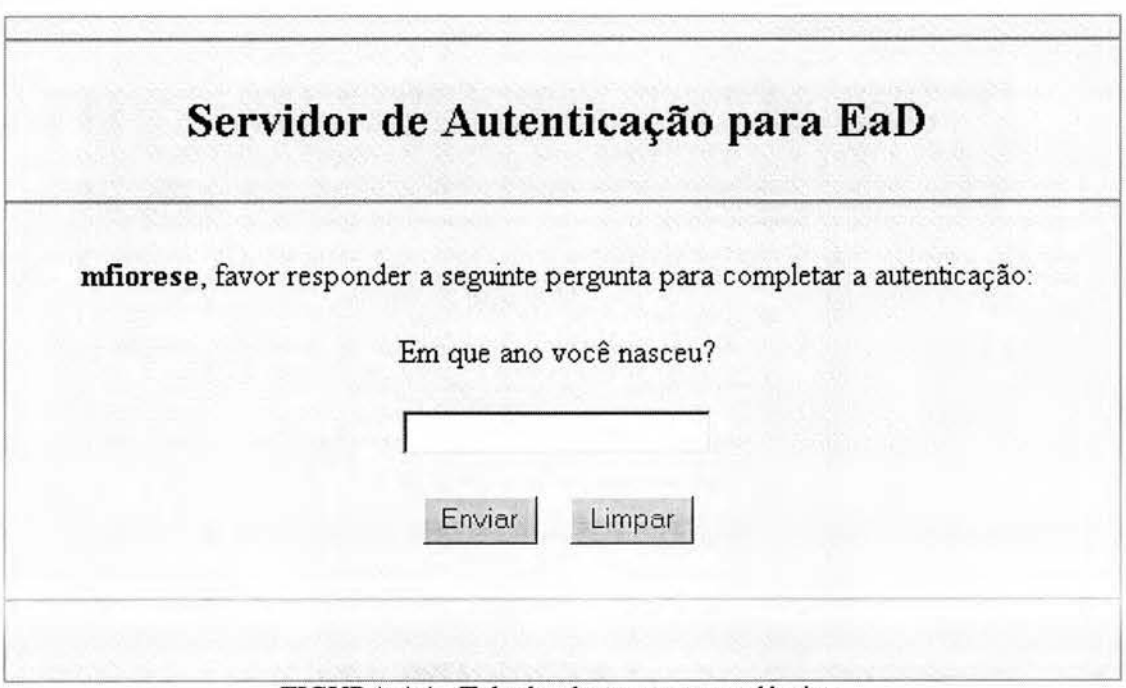

FIGURA 4.4 - Tela do da pergunta randômica

A página contendo a pergunta randômica possui uma caixa de texto que deve ser preenchida com a resposta. Após, deve-se apertar o botão Enviar.

Se a resposta à pergunta randômica for correta, o sistema apresenta a tela inicial do sistema. Essa tela varia de acordo com o tipo de usuário: administrador, professor ou aluno.

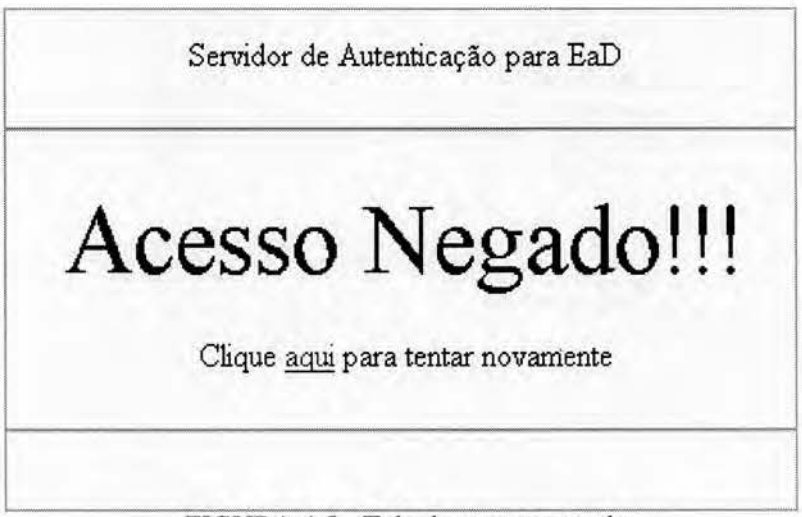

FIGURA 4.5 - Tela de acesso negado

Se o usuário for um administrador, a tela inicial apresentará um *menu* contendo ferramentas de administração, tais como "Cadastro de Alunos", "Professores" e "Administradores", "Cadastro de Cursos", "Cadastro de Matrículas", "Cadastro de Perguntas" e "Perfil do Professor". A figura 4.6 apresenta uma tela de alteração de cursos pelo administrador.

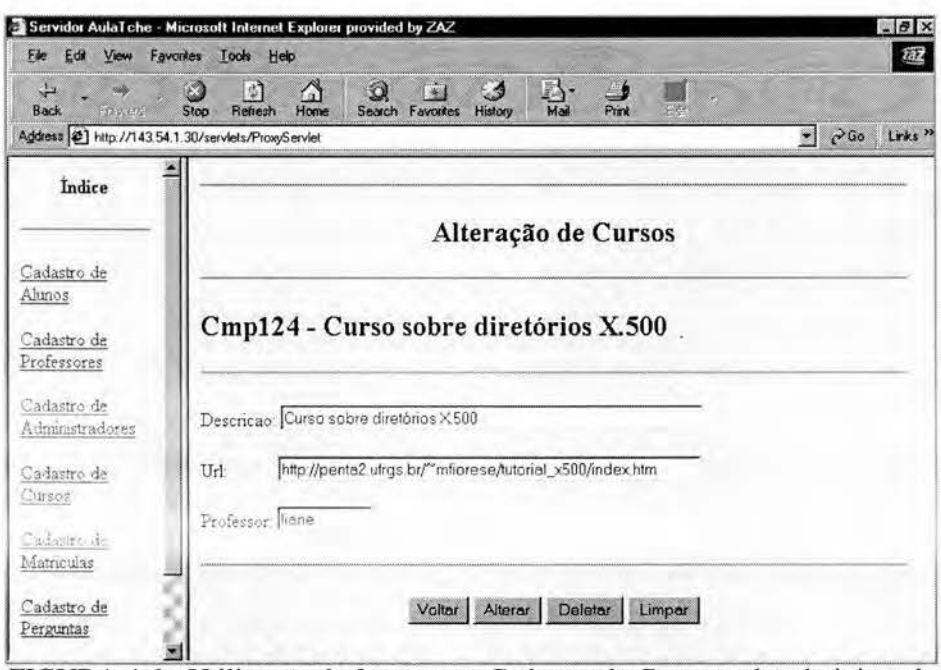

FIGURA 4.6 - Utilização da ferramenta Cadastro de Cursos pelo administrador

Se o usuário for um professor, a tela inicial apresentará uma página contendo os cursos ministrados por ele, semelhante à tela apresentada na figura 4.9. Após escolher o curso, será apresentado um *menu* contendo as ferramentas destinadas aos professores, tais como "Conteúdo", "Agenda", "*Chat*", "Correio Eletrônico", "Lista de Discussão", "Ponto de vista", "Votação", "Avaliação", "Perfil do Aluno" e "Configurar Alertas". A figura 4.7 apresenta uma tela da utilização da ferramenta "Configurar Alertas" pelo professor.

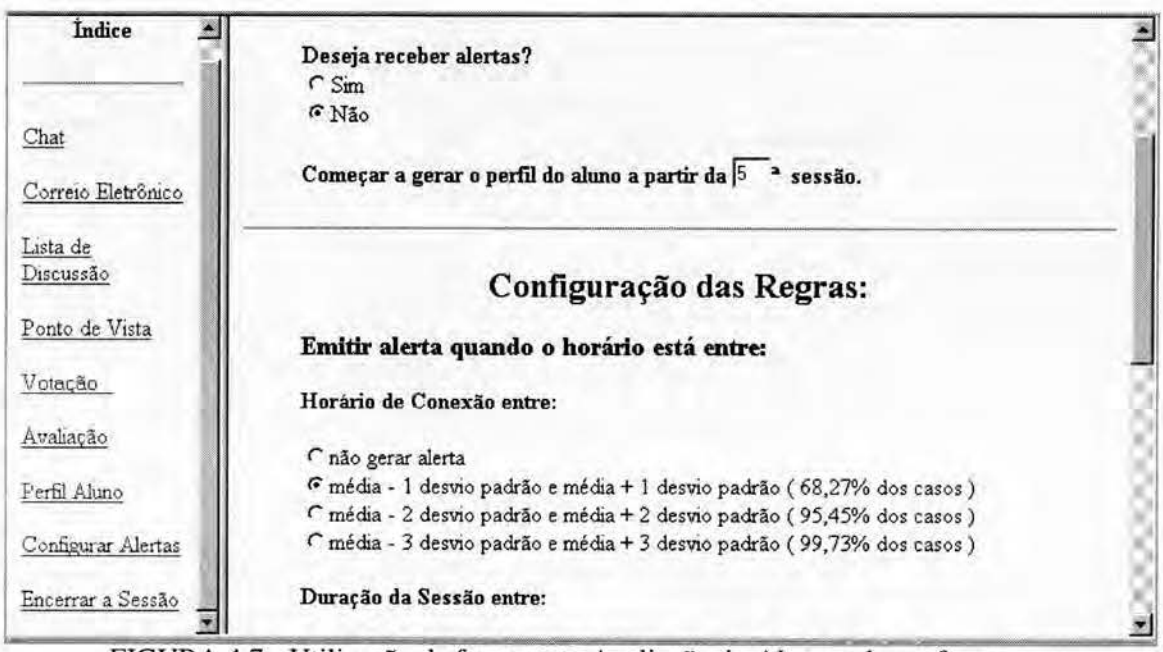

FIGURA 4.7 - Utilização da ferramenta Avaliação do Aluno pelo professor

Na página de "Configuração de Alertas" o professor configura as regras de geração de alertas. Primeiramente, ele indica se quer ou não receber alertas e a partir de qual sessão do usuário começará a ser gerado seu perfil. Em seguida ele configura as regras para cada variável, tais como "Horário de Conexão", "Duração da Sessão", "Taxa de Leitura", "Freqüência dos Dias", "Freqüência dos Endereços IPs", entre outras. Após determinar as regras, o professor deve apertar o botão "Configurar" para que as alterações sejam efetuadas.

Outra ferramenta interessante, disponível no *menu* do professor é "Perfil Aluno". Através dela o professor pode examinar o perfil do aluno gerado através dos *logs* de todas as sessões efetuadas por ele assim como rastrear uma determinada sessão. A figura 4.8 apresenta a ferramenta "Perfil Aluno".

Por fim, se o usuário for um aluno, a tela inicial apresentará uma página contendo os cursos em que ele está matriculado (figura 4.9). Ao selecionar um curso, lhe será apresentado *menu* contendo as ferramentas destinadas aos alunos, tais como "Conteúdo", "Agenda", "*Chat*", "Correio Eletrônico", "Lista de Discussão", "Ponto de Vista", "Votação", "Boletim", assim como a página inicial do curso escolhido. A figura 4.10 apresenta esta tela.

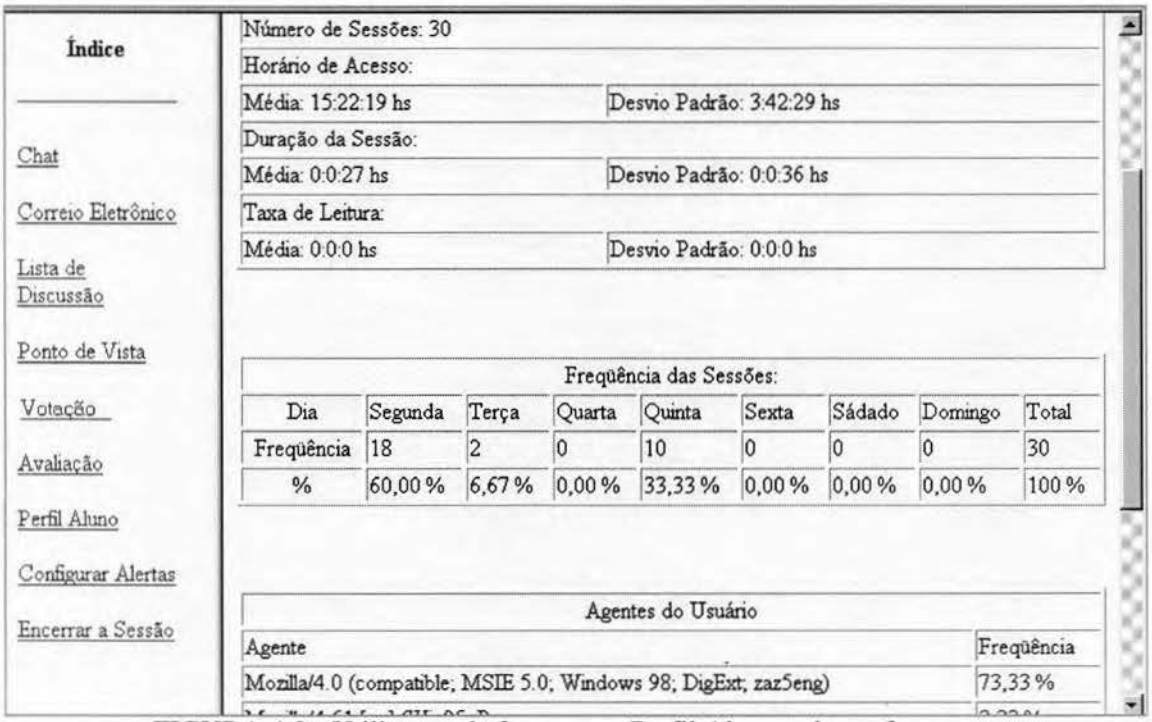

FIGURA 4.8 - Utilização da ferramenta Perfil Aluno pelo professor

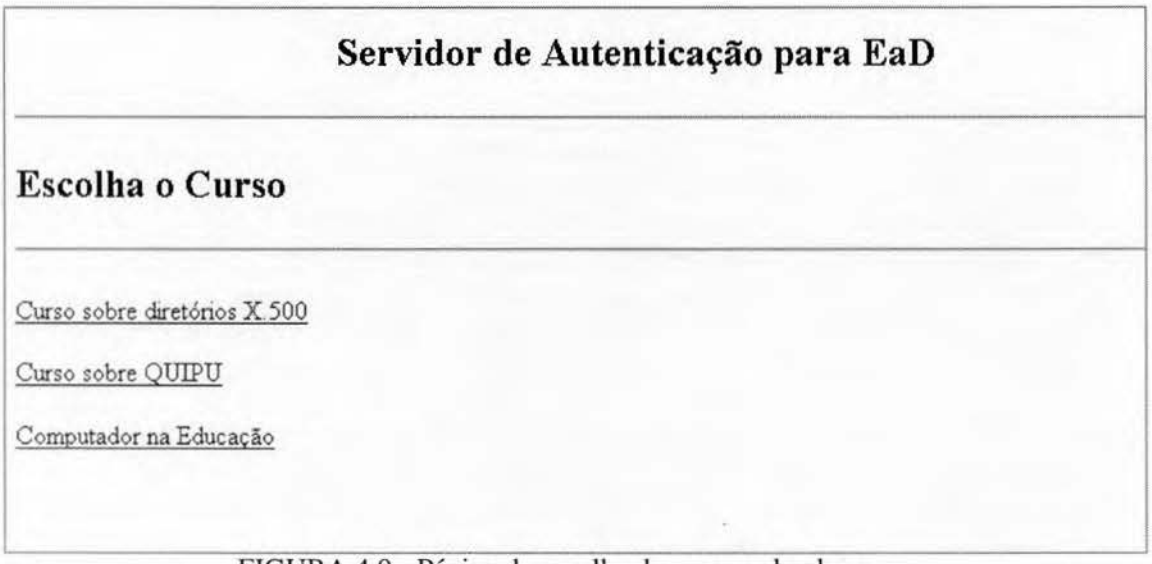

FIGURA 4.9 - Página de escolha do curso pelo aluno

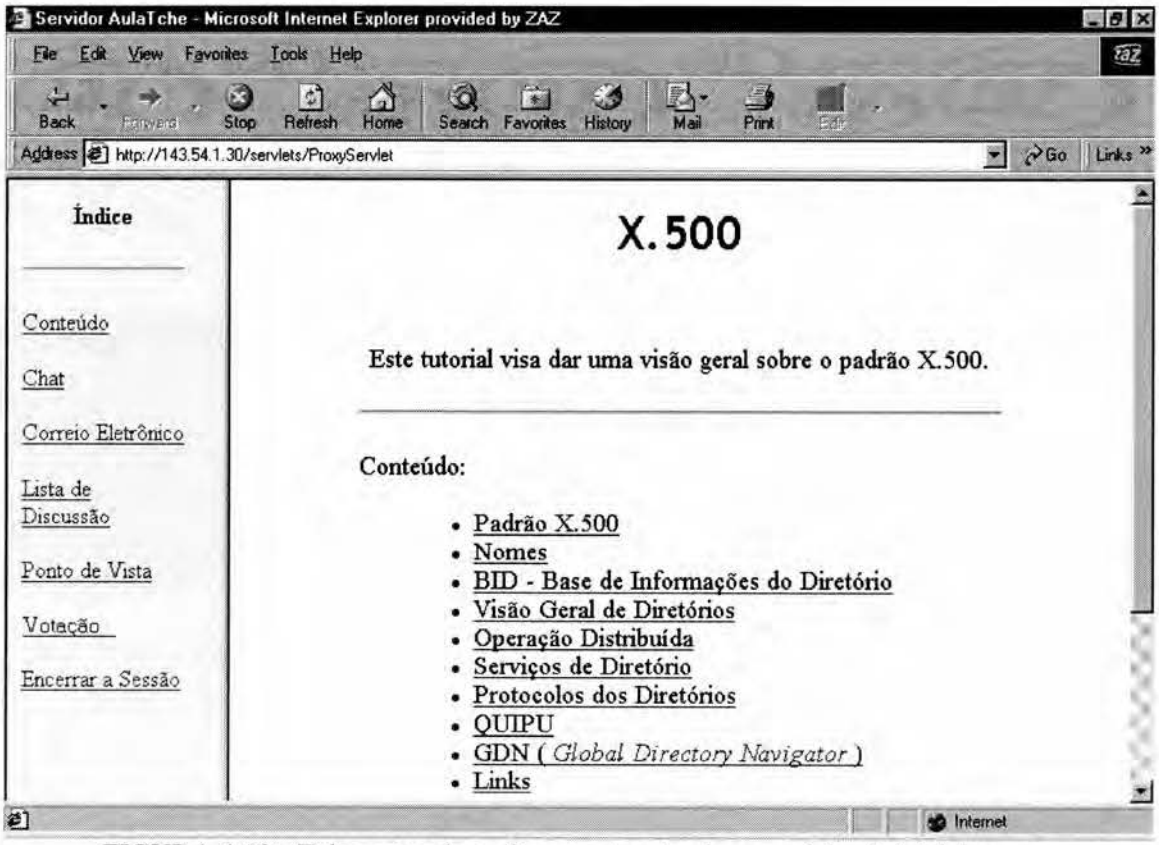

FIGURA 4.10 - Tela contendo as ferramentas do aluno e página inicial do curso

A tela acima contém dois *frames*. À esquerda apresenta-se o *menu* de ferramentas. À direita, a página inicial do curso escolhido pelo aluno.

Quando o usuário desejar sair do sistema, ele deve *clicar* no *link* "Encerrar Sessão", do *menu* à esquerda. Neste momento, será fechada a sessão e lhe será apresentado o resumo da sessão assim como sua sequência de navegação. Estas mesmas informações serão armazenadas nos *logs* do sistema e no banco de dados. A figura 4.11 apresenta a tela apresentada ao término da sessão.

FIGURA 4.11- Página de final de sessão

No momento em que o aluno encerra sua sessão, a rotina de geração de alertas verifica se o perfil do aluno está de acordo com o perfil do aluno ao longo de todo o curso, de acordo com as regras determinadas pelo professor através da ferramenta Configurar Alertas. Se o perfil da sessão estiver fora dos limites determinados pelo professor e o sistema estiver configurado para emitir alertas, será enviada uma mensagem ao professor alertando-o do ocorrido. A figura 4.12 apresenta uma mensagem enviada pelo sistema ao professor.

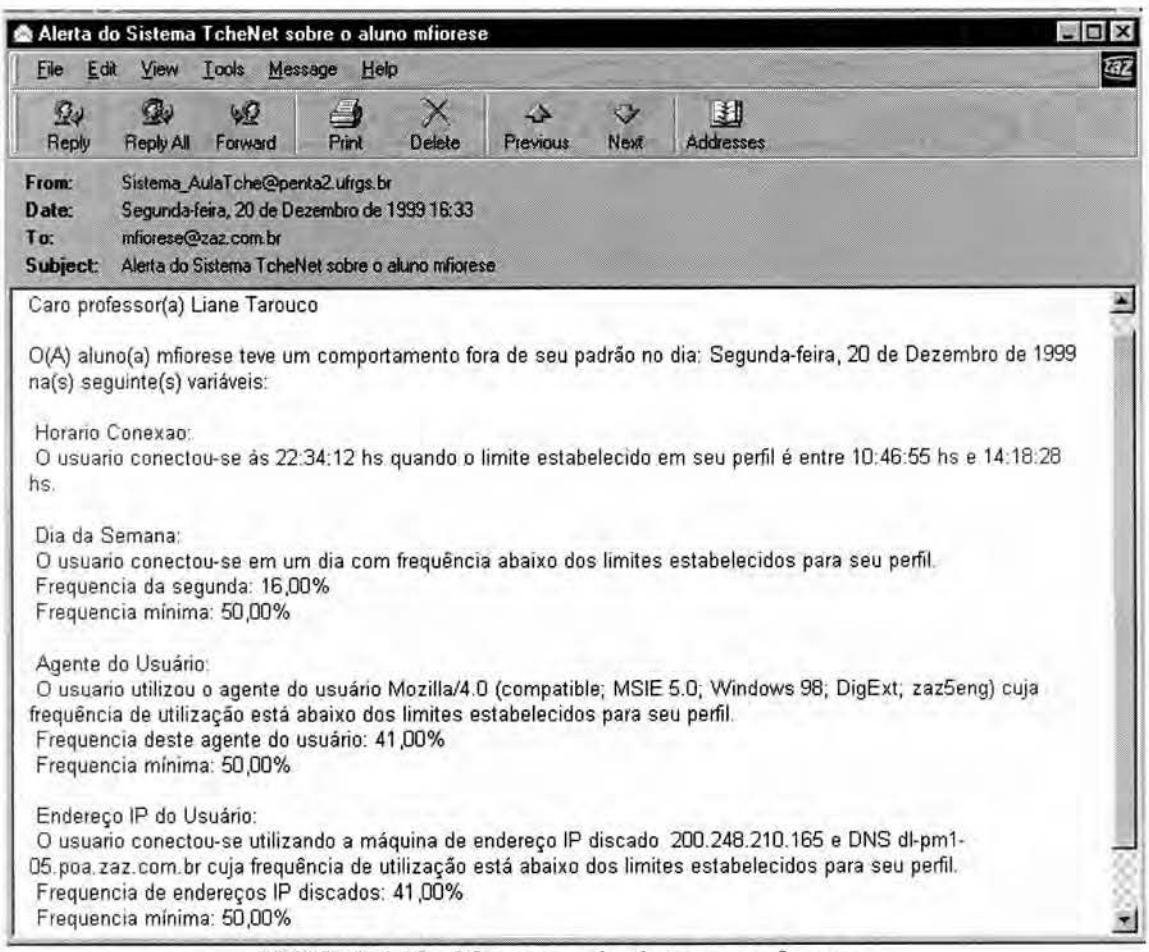

FIGURA 4.12 - Mensagem de alerta ao professor

4.6 Integração com o Sistema de Avaliação

O sistema desenvolvido nesta dissertação de mestrado foi integrado com o sistema de avaliação, desenvolvido pelo aluno Luciano Hack do PPGC da UFRGS [HAC2000].

Uma vez que o sistema de autenticação é o responsável pela geração das páginas dinâmicas, ele responsabilizou-se pela geração da *interface*. Assim, as ferramentas desenvolvidas pelo sistema de avaliação incorporaram-se nessa *interface*. São elas: "Agenda", "*Chat*", "Correio Eletrônico", "Lista de Discussão", "Ponto de Vista", "Votação", "Avaliação" e "Boletim" constantes nos *menus* do professor (figura 4.7) e do aluno (figura 4.10). A figura 4.13 apresenta a ferramenta "Correio Eletrônico", desenvolvida pelo sistema de avaliação, sendo acessada pelo aluno.

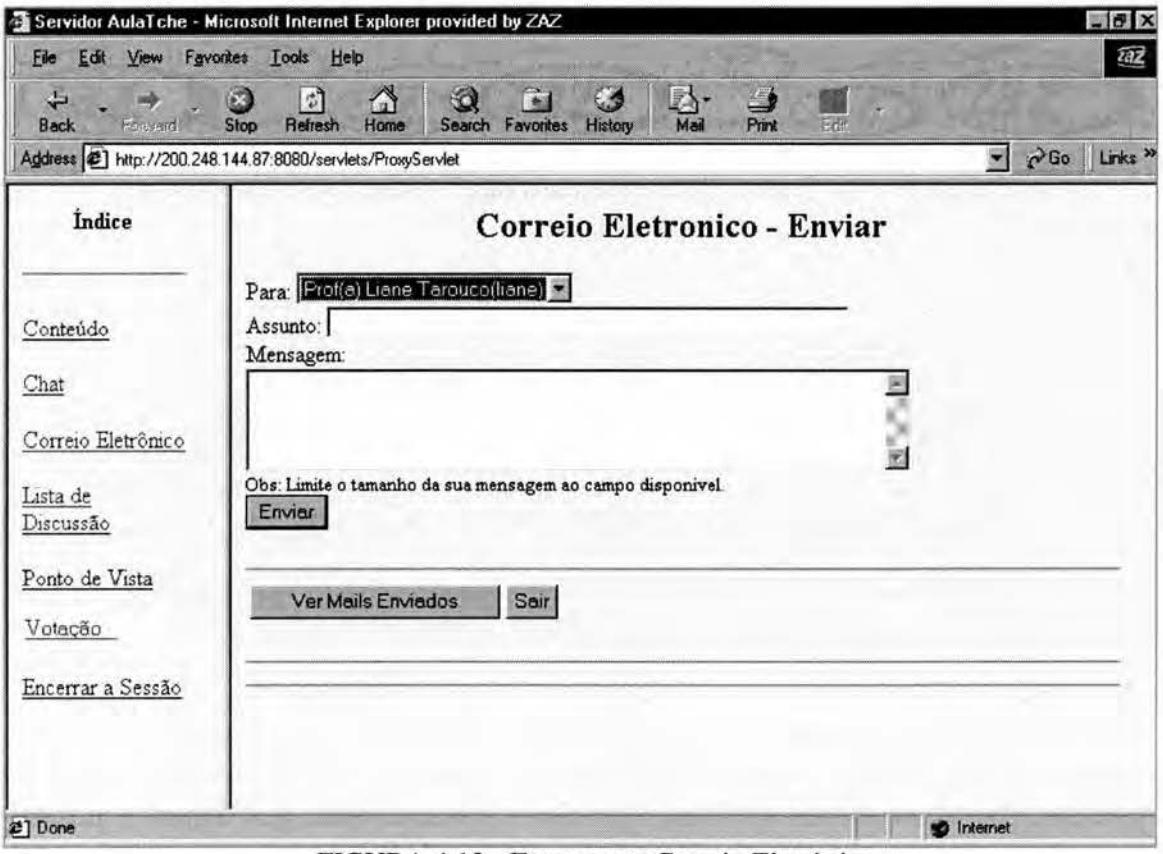

FIGURA 4.13 - Ferramenta Correio Eletrônico

Vale ressaltar que, como as ferramentas de avaliação foram inseridas na *interface* do sistema, elas só podem ser acessadas após o usuário passar pela fase de autenticação.

Uma vez que o controle de sessão foi feito pelo sistema de autenticação desenvolvido em *Java* e que o sistema de avaliação foi desenvolvido em *Pearl*, houve a necessidade de passar o identificador de sessão através de um campo escondido HTML (*hidden field)*. Este campo chama-se "jservsessionid" e pode ser visto na figura 4.14.

Quando um usuário é autenticado corretamente, o sistema insere uma tupla (id_pessoa, id_sessao, cod_curso) em uma tabela chamada "AUTENTICACOES". Com isso, o sistema de avaliação pode consultar esta tabela utilizando o campo "id_sessao", que é único, e assim consegue recuperar o identificador do usuário e o código do curso.

Quando o usuário encerra a sessão, suas informações constantes na tabela "AUTENTICACOES" são removidas. A figura 4.15 apresenta uma consulta à tabela "AUTENTICACOES" no momento em que um usuário está conectado.

```
</script>
<form name=FormGoTo ACTION="http://200.248.144.87:8080/servlets/ProxyServlet" METHOD="POST">
<input TYPE="hidden" NAME="URL">
<input TYPE="hidden" Name="Operation" value="3">
<input TYPE="hidden" Name="jservsessionid" value="3fe4ad90c5826223.1.943963696670">
</form>
```

FIGURA 4.14 - Fonte HTML contendo o campo escondido jrunsessionid

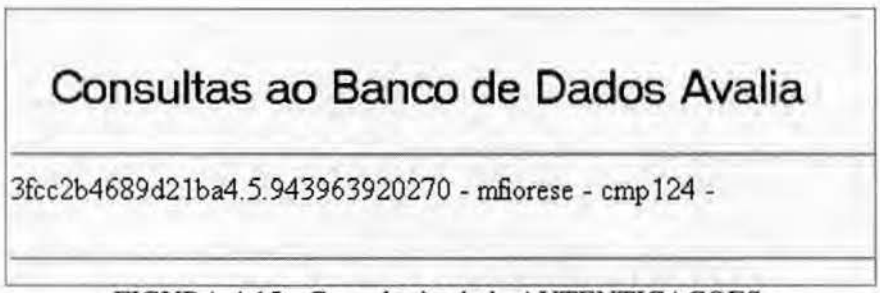

FIGURA 4.15 - Consulta à tabela AUTENTICACOES

Com vistas a facilitar a integração entre os dois sistemas, os dados utilizados pelo sistema de avaliação, gerados pelo sistema de autenticação (*logs* da utilização do sistema), são armazenados em banco de dados. Assim, basta que sejam realizadas consultas às devidas tabelas para obter acesso a essas informações.

4.7 Avaliação do Protótipo

A fim de avaliar o protótipo, o mesmo foi apresentado para alunos do mestrado do PPGC da UFRGS junto com um questionário que deveria ser enviado por email contendo as principais impressões sobre o sistema. As principais caracterísitcas destacadas foram:

- facilidade de uso: pelo fato da *interface* ser desenvolvida em HTML, sua utilização tornou-se simples e intuitiva;
- portabilidade: por ser desenvolvida em linguagem *Java* e utilizar navegadores *Web* para visualização, adapta-se praticamente a todas as plataformas;
- baixo custo: todos os *softwares* necessários são gratuitos e estão disponíveis na Internet;
- maior segurança: acredita-se que a integração de senhas com perguntas randômicas e geração de alertas melhorou a segurança do sistema.

As principais limitações estão ligadas à rotina de navegação dinâmica. Na implementação do protótipo utilizou-se apenas um subconjunto da linguagem HTML, com isso, algumas funcionalidades não são suportadas:

- Não suporta *frames*, imagens mapeadas, abertura de janelas e páginas com permissões;

- O sistema só modifica os *links* para documentos do tipo HTML, CGI e TXT. Caso os *links* forem para documentos do tipo AVI, DOC, etc., ele os abre, porém não os registra nos *logs*;

- Existem muitas alternativas para especificação de URLs, como por exemplo: http://servidor/diretorio/pagina.htm, diretório/página.htm, página.htm, etc. Procurou-se abranger o maior número de casos, porém nem todas as combinações são suportadas;

- A modificação dos *links* ocorre para as *tags* "HREF". No caso de formulários, o "ACTION" não é modificado. Assim, a requisicão referenciada pelo "ACTION" não é armazenada nos *logs* do sistema;

- No caso de uma máquina acessar o sistema através de *proxy:* foram utilizadas rotinas em *JavaScript* para a captura do endereço IP e DNS da máquina do cliente que só funcionam com o navegador *Netscape Navigator*. No caso da utilização do *Internet Explorer*, o endereço IP e DNS capturado é o do *proxy*

Algumas considerações sobre o sistema e sugestões de melhorias destacadas na avaliação englobam:

- O sucesso das perguntas randômicas está relacionado com a escolha das perguntas, a qual é tarefa do administrador do sistema;

- O rastreamento das sessões dos alunos foi considerado mais útil na avaliação do aluno do que na segurança do sistema;

- A geração de alertas foi considerada de grande utilidade para os professores. Porém, cabe a eles a otimização das regras de alertas, evitando o recebimento de muitos alertas em caso de pequenas mudanças no comportamento ou que somente recebam mensagens quando o comportamento for extremamente diferente;

- Não houve problemas de integração com o sistema de avaliação, apesar das *interfaces* serem ligeiramente diferentes;

- Dentre as sugestões de melhoria destacam-se: desenvolvimento de um *help on-line*, pequenas mudanças na *interface* e integração de dispositivos biométricos;

5 Conclusão

O objetivo deste trabalho foi estudar as diversas tecnologias de autenticação de usuários existentes no mercado, analisá-las, definindo um modelo de autenticação para utilizar-se em aplicações de educação a distância. Um protótipo deveria ser implementado a fim de validar o modelo delineado ao longo do trabalho e o mesmo deveria integrar-se ao sistema de avaliação desenvolvido por Hack [HAC2000].

Para alcançar o objetivo acima, primeiramente realizou-se uma análise comparativa em termos de custo e desempenho de diversas soluções de autenticação existentes no mercado, detalhada no capítulo dois. Como resultado desta análise, delineou-se um modelo de autenticação de usuários que integra soluções consideradas viáveis, tanto em temos de custos como em termos de simplicidade operacional.

O modelo proposto, descrito no capítulo três, integra senhas, perguntas randômicas dinâmicas, dispositivos biométricos e checagem randômica. Como complemento, extrai o perfil de utilização do sistema por um usuário e gera alertas na medida em que o comportamento deste usuário desvia-se de seu perfil.

A fim de validar o modelo delineado ao logo do trabalho, desenvolveu-se um protótipo que implementa a maior parte das rotinas definidas no modelo, assim como integra as rotinas de avaliação desenvolvidas em [HAC2000].

No desenvolvimento do protótipo, inicialmente, pensou-se em dar preferência a métodos de autenticação que envolvessem o uso de câmera digital, uma vez que elas são comuns em estações de ensino a distância. Porém, a inviabilidade econômica na aquisição dos *softwares* de autenticação necessários, impediu o uso neste trabalho. Este também foi o motivo da não utilização de outros dispositivos biométricos. Em relação à checagem randômica, a dificuldade de manipulação das APIs das câmeras digitais também impediu sua implementação. Assim, dispositivos biométricos e checagem randômica apenas constarão no modelo e em trabalhos futuros.

O sistema desenvolvido funciona como um *proxy*. Após a fase de autenticação, ele busca as páginas requisitadas em um servidor WWW, modifica seus *links* de modo que toda nova requisição passe por ele, e envia a resposta para o cliente. Porém, nada impede que um usuário acesse diretamente às páginas sem passar pelo sistema. Para resolver este problema, é necessário que apenas o sistema tenha permissão de acesso à essas páginas. Em contrapartida, o sistema ficou aberto, isto é, não é necessário que as páginas do curso estejam no servidor no qual roda a aplicação.

Uma das maiores dificuldades encontradas foi em relação à rotina de navegação dinâmica, responsável pela modificação dos *links*. A fim de validar o protótipo, foi utilizado um subconjunto do HTML, assim, o sistema não suporta algumas propriedades do HTML conforme visto na seção 4.7.

Outra dificuldade foi a integração com o módulo de avaliação [HAC2000]. Este módulo foi implementado utilizando CGIs em Pearl. Com isso, não foi possível a utilização do controle de sessão disponível com as *Servlets Java*. A solução foi a criação de tabelas dinâmicas contendo dados dos usuários e a passagem de parâmetros através de campos escondidos.

Em termos de segurança, o sistema segue a idéia de [JAI99] em que o autor propõe integrar métodos de autenticação a fim de suprir as deficiências individuais de cada um. Sabe-se, porém, que por mais sofisticada que seja a autenticação, sempre poderão existir métodos para burlar o sistema, porém ele tende a ser mais seguro que com o uso individual de senhas, encontrado na maioria dos sistemas de educação a distância.

A fim de evitar o monitoramento do tráfego (*sniffing*), recomenda-se que seja instalado o módulo de SSL (*Secure Sockets Layer*) no servidor Apache. Alguns testes foram executados com sucesso, porém, devido à escassez de tempo, este módulo não foi instalado na penta2. Vale ressaltar que este módulo é disponível gratuitamente no endereço http://www.apache-ssl.com.

Por fim, os objetivos deste trabalho foram cumpridos. O avanço dos mecanismos de autenticação de usuários, principalmente no que se refere a biometria, aliado à redução no preços dos equipamentos, fez com que surgissem dezenas de produtos a baixo custo, possibilitando seu uso sem a necessidade de grandes investimentos. Desse modo, a análise comparativa realizada neste trabalho contribui para que possamos ter uma visão mais realista desses produtos, de suas caracterísitcas, custo e possibilidades de uso.

Esta análise possibilitou a definição de um modelo de autenticação para aplicações de ensino a distância. Dentre os vários artigos publicados na área, não foi encontrado nenhum material a respeito da autenticação dos usuários. Desta forma, este trabalho contribui, não como uma solução para os problemas de autenticação em educação a distância, mas como uma proposta de um modelo, que pela integração de métodos de autenticação, tende a ser mais seguro que com o uso único de senhas, encontrado na maioria dos sistemas de educação a distância. Além disso, nada impede que este modelo seja extendido para outros tipos de aplicações como como comércio eletrônico, controle de acesso a áreas restritas, *home banking*, entre outros.

Finalmente, a integração do protótipo desenvolvido na validação deste modelo com rotinas de avaliação desenvolvidas em [HAC2000], gerou uma ferramenta de ensino a distância de fácil utilização, portável e de baixo custo que podem ser utilizados por professores na disponibilização de cursos a distância.

Abaixo seguem algumas sugestões para continuidade do trabalho:

- Extender o módulo de navegação dinâmica para que possa englobar todo o conjunto do HTML;
- No período em que este trabalho foi desenvolvido, não foram encontrados produtos biométricos a um custo que justificasse sua implementação. Porém, a cada dia são lançados novos programas e versões, a preços cada vez mais reduzidos. Assim, espera-se que em um breve período, possam surgir produtos biométricos que possam integrar-se neste sistemas;
- Desenvolvimento das rotinas de checagem randômica;
- Implantação do módulo SSL (*Secure Sockets Layer*) no servidor Apache, evitando o monitoramento de tráfego (*sniffing*);

- Implementação da restrição de acesso, possibilitando que apenas o sistema acesse determinados cursos, impedindo assim o acesso direto pelo usuário;
- Realizar o registro de tentativas de acesso mal sucedidas;
- Adicionar a característica de "personalizar *menus*", na qual podem ser adicionados componentes sem a necessidade de modificar o código *Java*.

Anexo 1 Especificação do Sistema em SDL

Este anexo contém a especificação formal do sistema proposto em SDL (*Specification and Description Language*). Segundo [TRI 92], o propósito desta linguagem é prover uma especificação e descrição dos sistemas de telecomunicações de forma não ambígua.

O SDL possui duas formas de representação dos sistemas: uma forma textual (SDL/PR) e outra gráfica (SDL/GR). A forma escolhida para representar este sistema foi a SDL/GR (*Graphical Representation*). Ambas formas são equivalentes.

A proposta da SDL é descrever o comportamento real do sistema independentemente da linguagem utilizada na implementação.

O sistema possui um grande bloco que comunica-se com o ambiente externo através de cinco canais bidirecionais. A figura A.1 apresenta a especificação do sistema Proxy.

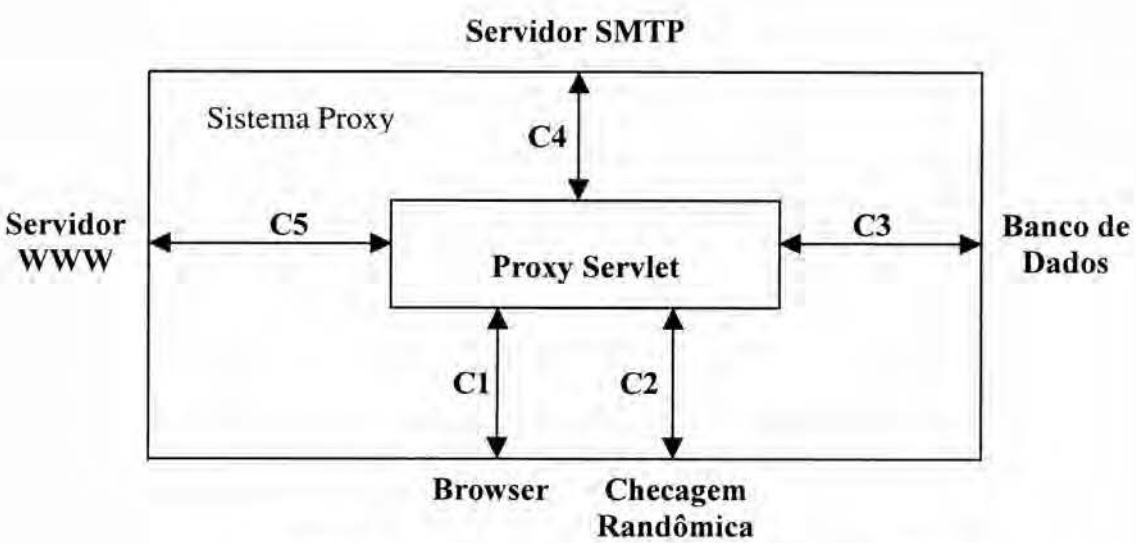

FIGURA A.1 - Especificação do sistema Proxy em SDL

A figura A.2 apresenta uma descrição geral da *Proxy Servlet*. Em sua inicialização, cria-se uma conexão com o banco de dados. A seguir, a *servlet* fica ociosa à espera de uma requisição. No momento em que chega uma requisição, a *servlet* verifica qual a operação envolvida e chama a função correspondente.

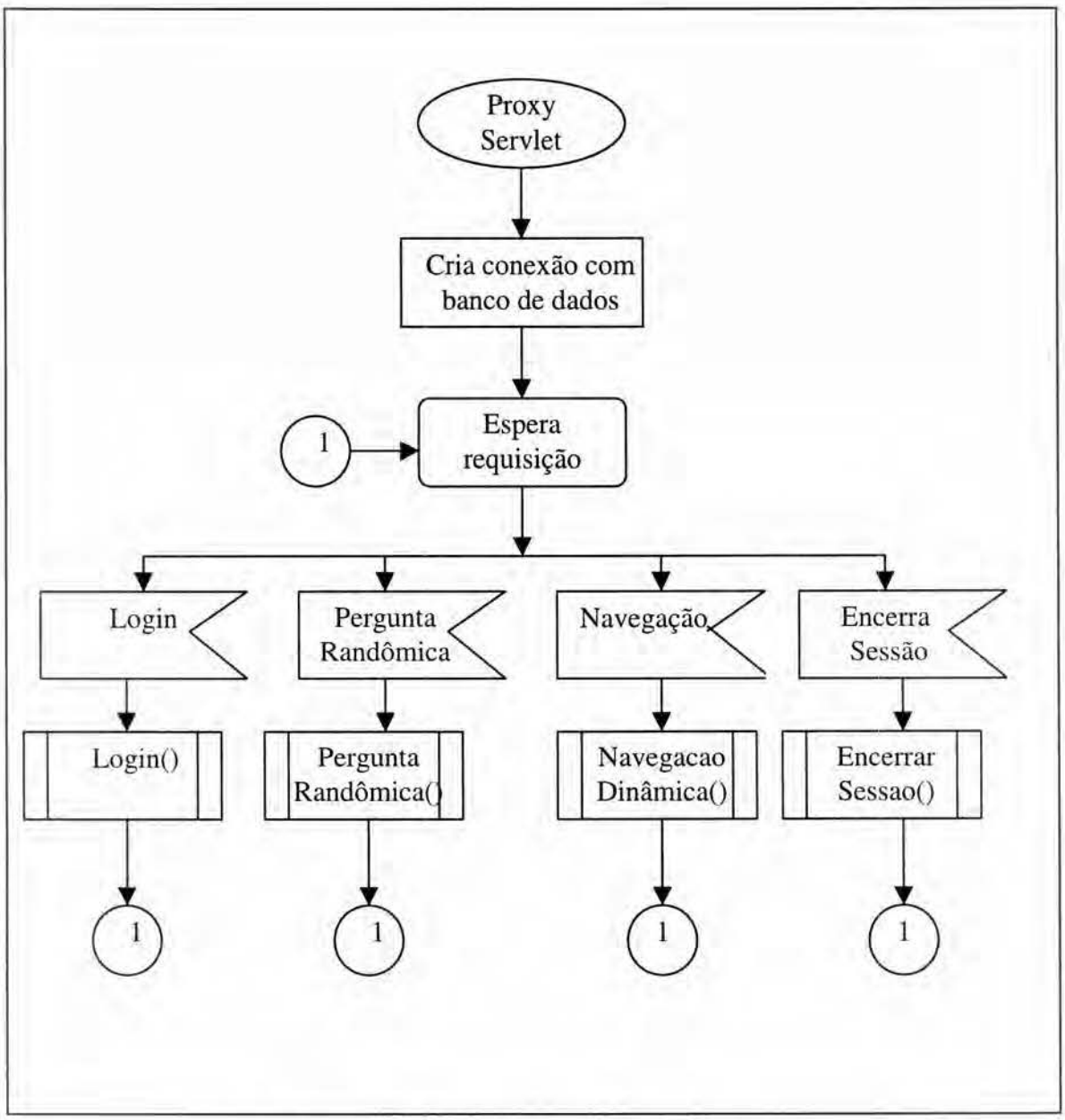

FIGURA A.2 - Descrição geral da Proxy Servlet

Se a operação selecionada for o *login()*, o sistema cria um *cookie* para usar no controle de sessões. A seguir, verifica se o programa de checagem randômica está ativo no computador do aluno. Este programa captura fotos em tempos aleatórios através de uma câmera digital e envia ao servidor remoto para posterior conferência. A seguir, verifica-se qual o tipo de autenticação que está sendo usada: biométrica ou através de senhas. Se a autenticação for válida, o sistema busca uma pergunta de forma aleatória no banco de dados e retorna uma página contendo este desafio. Em seguida, encerra a rotina e volta a esperar uma nova requisição. A figura A.3 apresenta a descrição do procedimento Login().

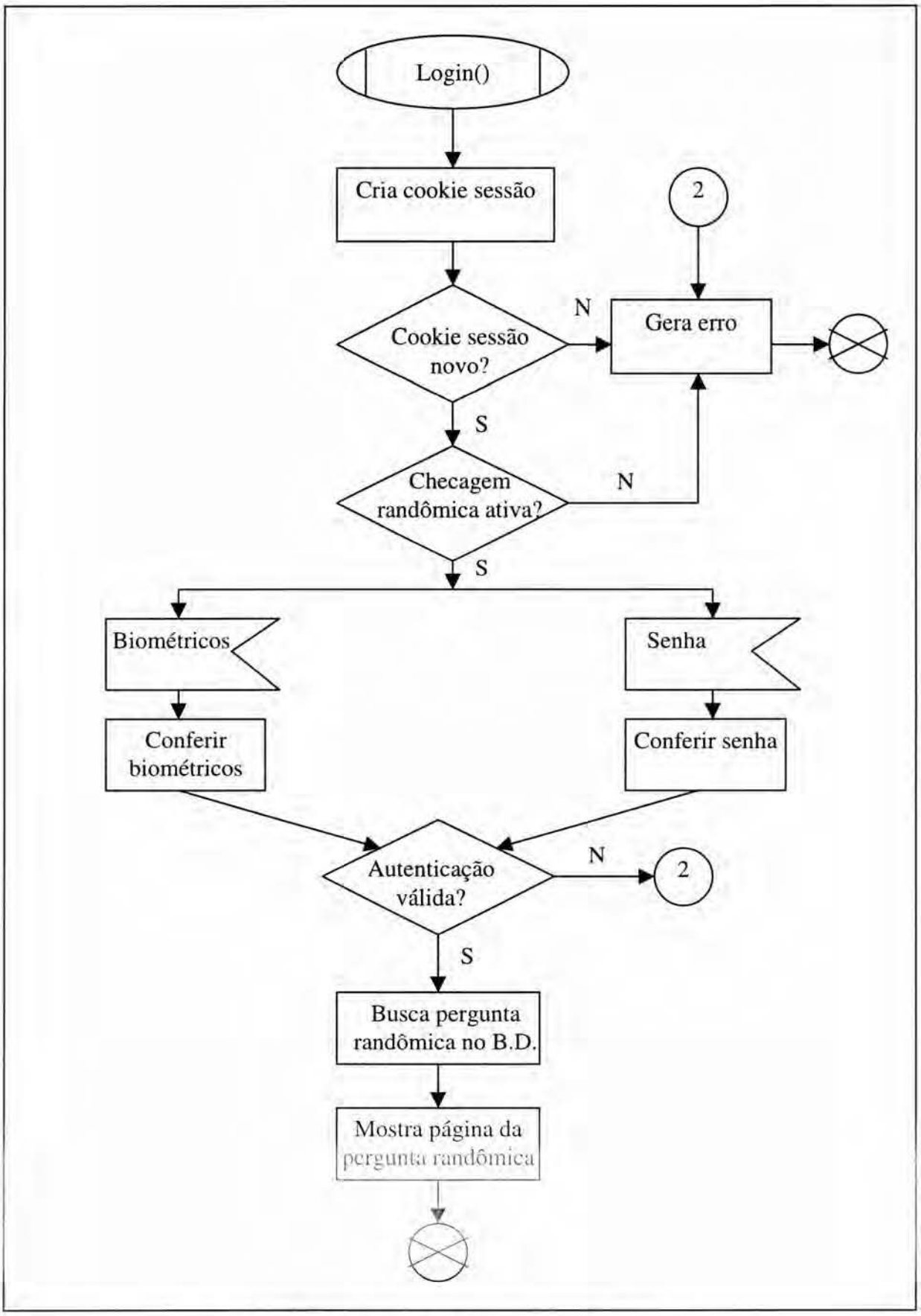

FIGURA A.3 - Descrição do procedimento Login()

Quando a operação for *pergunta randômica()*, o sistema verifica primeiramente se o *cookie* da sessão é novo. Se não for, ele recupera o *cookie* identificador da sessão e confere a resposta da pergunta randômica. Se ela for válida, o sistema seta um *flag* de autenticação completa e verifica o tipo de pessoa que está acessando o sistema, retornando a devida página inicial. A seguir, volta a esperar uma nova requisição. A figura A.4 apresenta a descrição do procedimento Pergunta Randômica().

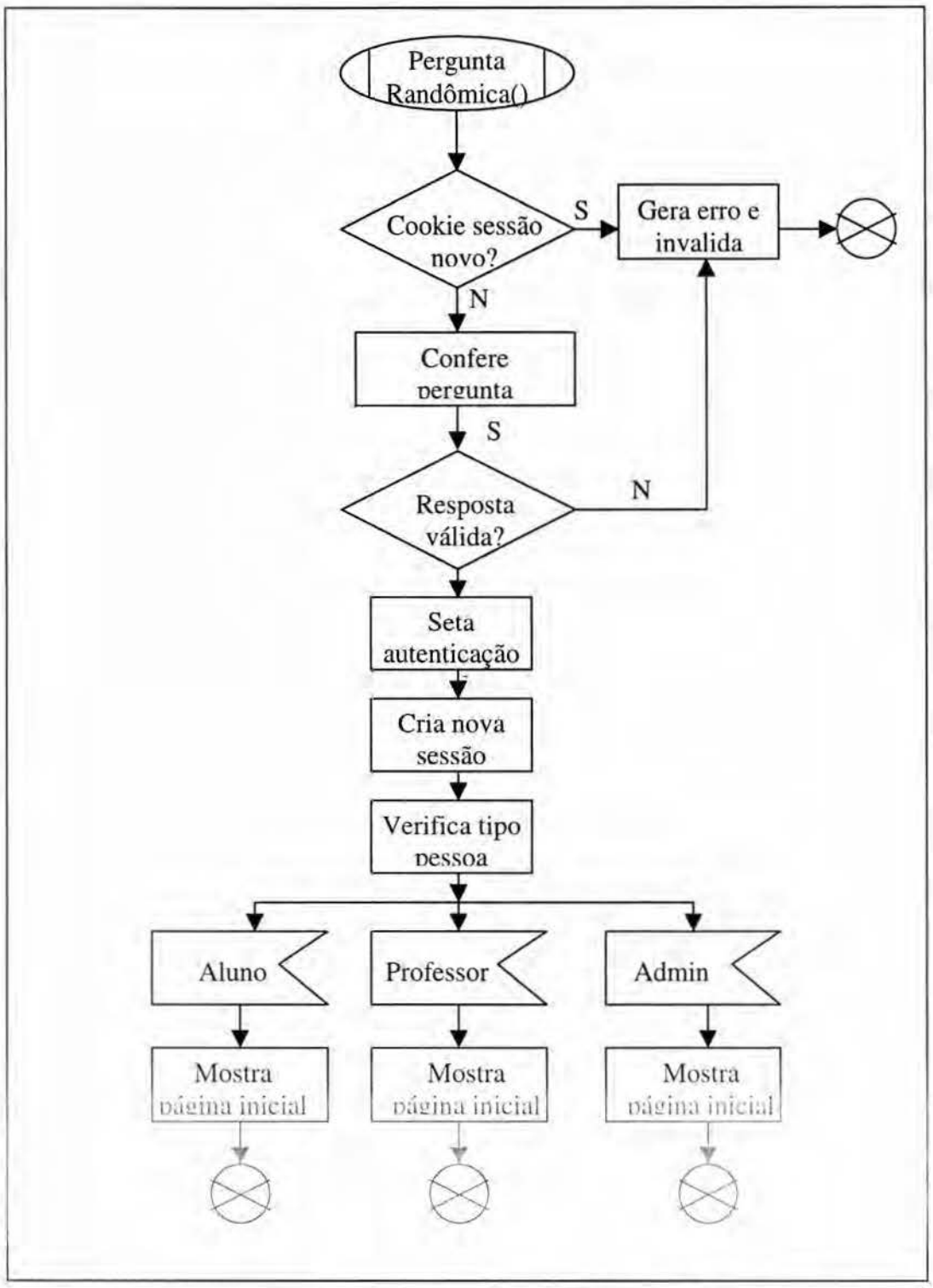

FIGURA A.4 - Descrição do procedimento Pergunta Randômica()

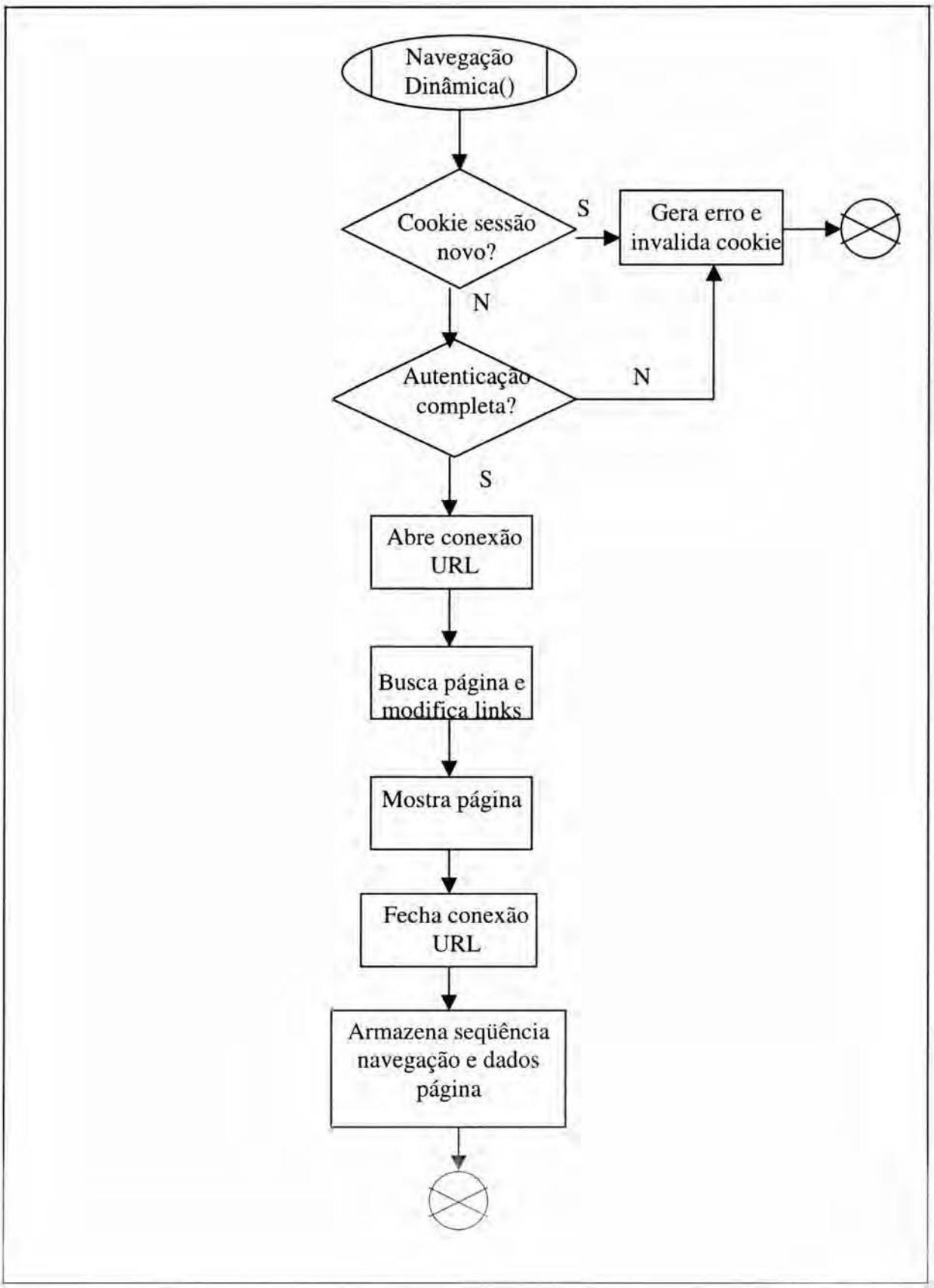

FIGURA A.5 - Descrição do procedimento Navegação Dinâmica()

No procedimento de *navegação dinâmica()*, o sistema testa se o *cookie* do controle de sessão é novo. Se não for, verifica o *flag* que indica se a autenticação está completa. Caso estiver, ele abre uma conexão URL com o servidor WWW destino, busca e modifica os *links* da página enviando-a ao usuário. A seguir, fecha a conexão URL e armazena informações sobre a seqüência de navegação que está sendo realizada pelo aluno e alguns dados adicionais da página utilizada. Após, volta a esperar uma nova requisição. A figura A.5 apresenta a descrição do procedimento Navegação Dinâmica().

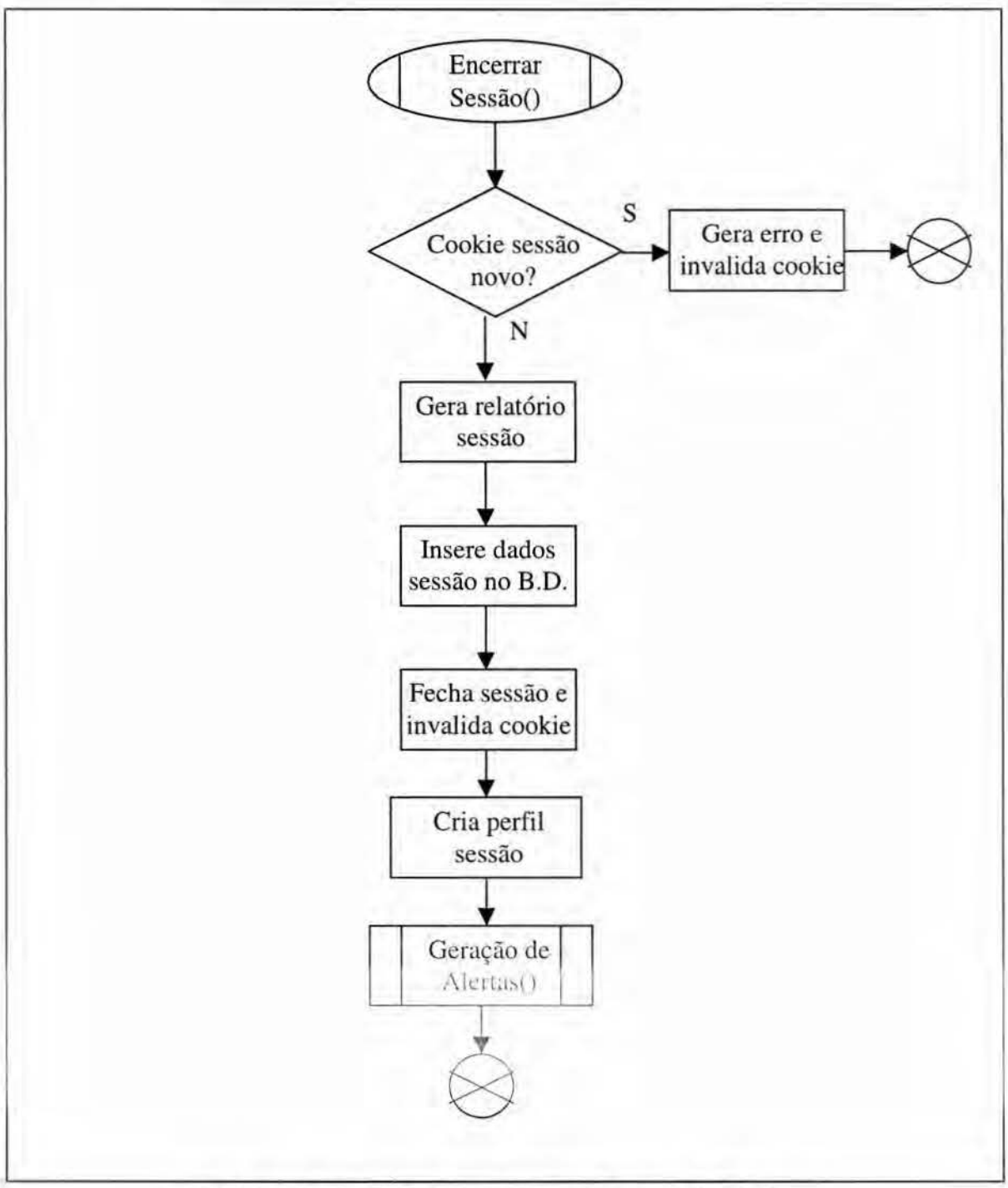

FIGURA A.6 - Descrição do procedimento Encerrar Sessão()

No procedimento de *encerrar sessão()*, o sistema testa se o *cookie* do controle de sessão é novo. Se não for, gera um relatório da sessão, apresentando dados do usuário, curso, tempo decorrido e seqüência de navegação da sessão corrente. Após, grava o *log* de informações da sessão no banco de dados. Em seguida, fecha a sessão corrente e invalida o *cookie* de controle de sessão. Por fim, cria o perfil do aluno nesta sessão e chama o procedimento de geração de alertas. A figura A.6 apresenta a descrição do procedimento Encerrar Sessão().

O procedimento *geração de alertas()* verifica se o perfil do aluno na sessão está de acordo com o perfil do aluno ao longo de todo o curso. Se não estiver, gera e envia uma mensagem alertando o professor. A figura A.7 apresenta a descrição do procedimento Geração de Alertas().

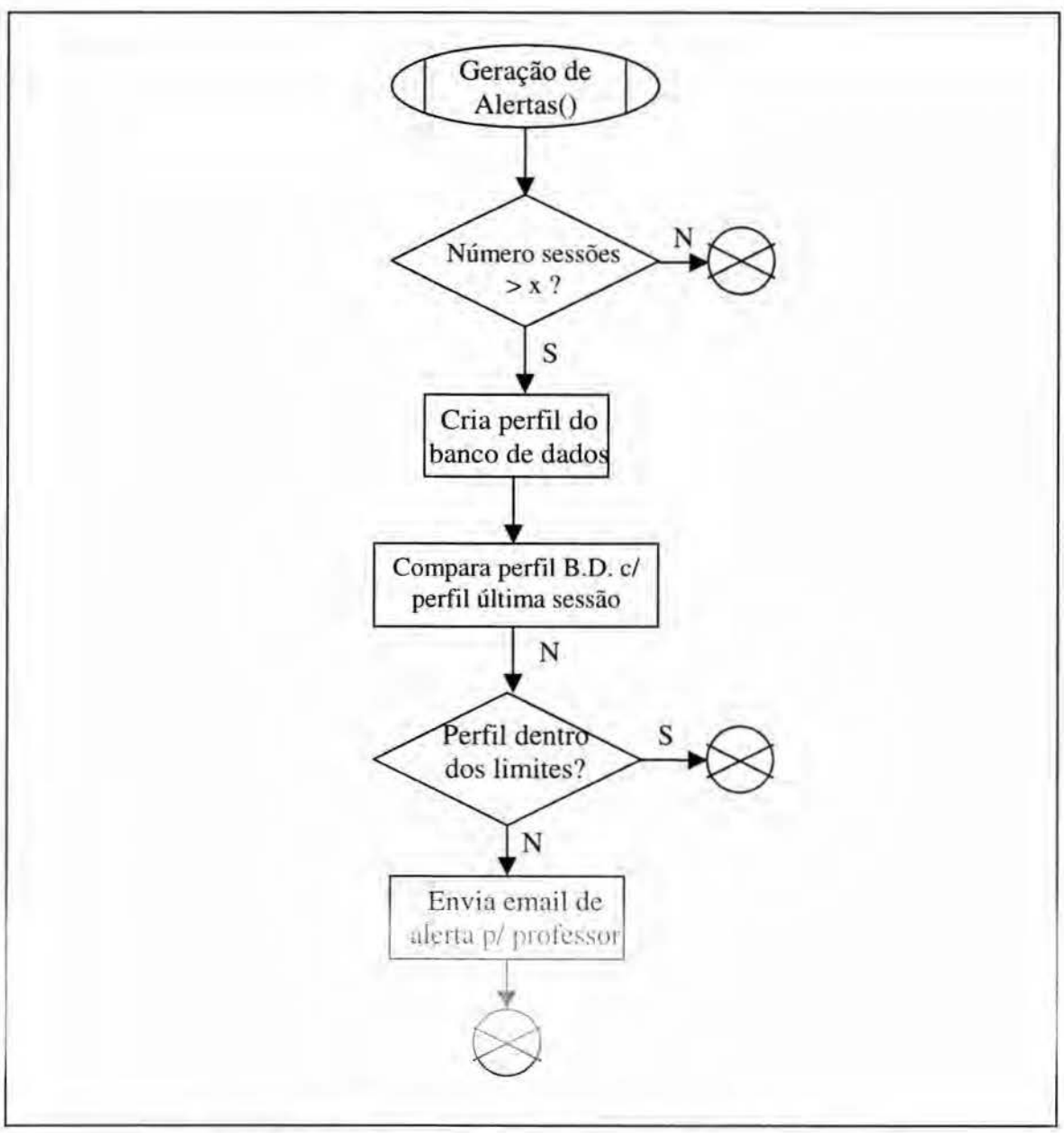

FIGURA A.7 - Descrição do procedimento Geração de Alertas()

Anexo 2 Modelo de Dados do Sistema

Este anexo contém o diagrama entidade-relacionamento assim como a descrição de todas as tabelas utilizadas pelo sistema.

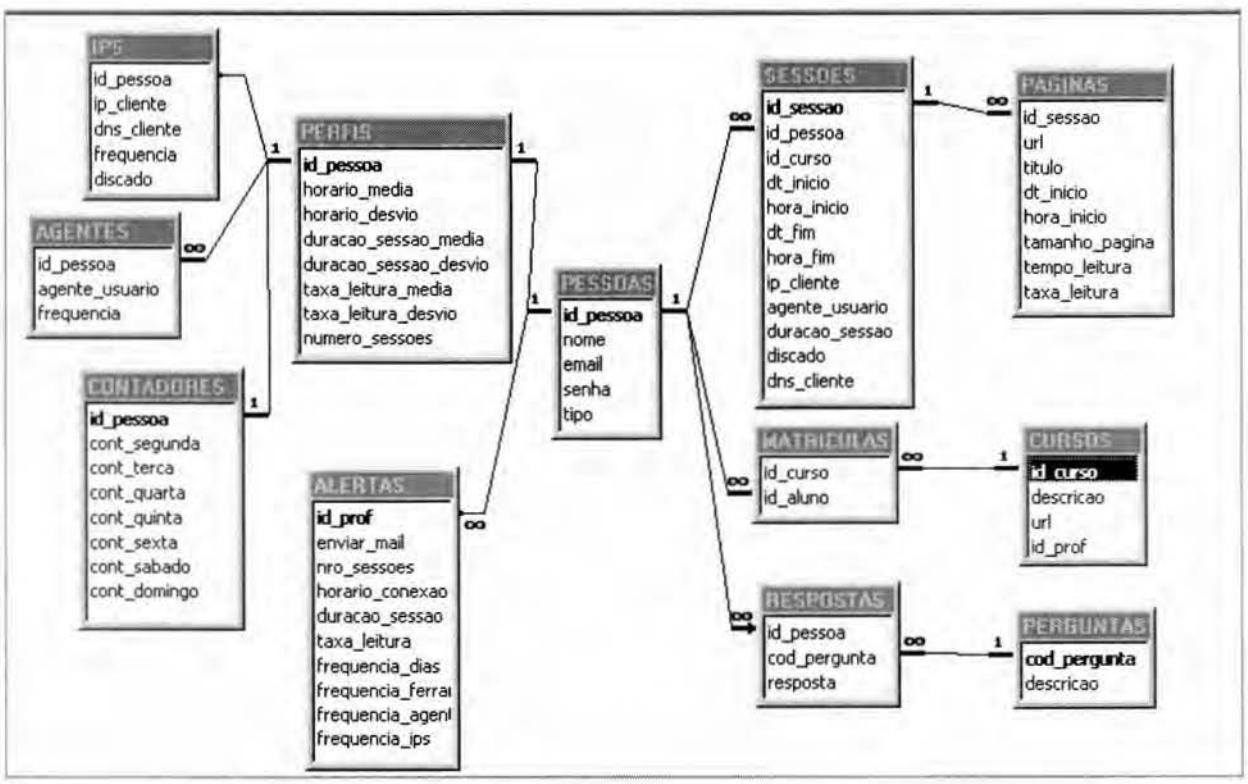

FIGURA B.1 - Diagrama de entidade-relacionamento

TABELA B.1 – Tabela PESSOAS

Tabela PESSOAS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_pessoa	VARCHAR(10)	Sim	X
nome	VARCHAR(30)	Sim	
email	VARCHAR(50)	Sim	
senha	VARCHAR(32)	Sim	
tipo	VARCHAR(10)	Sim	

TABELA B.2 – Tabela PERGUNTAS

Tabela PERGUNTAS			
Nome do Campo	Tipo	Requerido	Chave Primária
cod_pergunta	INTEGER	Sim	X
descricao	VARCHAR(80)	Sim	

TABELA B.3 – Tabela RESPOSTAS

Tabela RESPOSTAS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_pessoa	VARCHAR(10)	Sim	X
cod_pergunta	INTEGER	Sim	X
resposta	VARCHAR(50)	Sim	

TABELA B.4 – Tabela CURSOS

Tabela CURSOS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_curso	VARCHAR(10)	Sim	X
descricao	VARCHAR(150)	Sim	
url	VARCHAR(150)	Sim	
id_prof	VARCHAR(10)	Sim	

TABELA B.5 – Tabela MATRICULAS

Tabela MATRICULAS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_curso	VARCHAR(10)	Sim	X
id_aluno	VARCHAR(10)	Sim	X

TABELA B.6 – Tabela SESSOES

Tabela SESSOES			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_sessao	VARCHAR(50)	Sim	X
id_pessoa	VARCHAR(10)	Sim	
id_curso	VARCHAR(10)	Sim	
dt_inicio	VARCHAR(10)	Sim	
hora_inicio	INTEGER	Sim	
dt_fim	VARCHAR(10)	Sim	
hora_fim	INTEGER	Sim	
ip_cliente	VARCHAR(15)	Sim	
agente_usuario	VARCHAR(150)	Sim	
duracao_sessao	INTEGER	Sim	
discado	CHAR(1)	Sim	
dns_cliente	VARCHAR(50)	Sim	

TABELA B.7 – Tabela PAGINAS

Tabela PAGINAS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_sessao	VARCHAR(50)	Sim	
url	VARCHAR(150)	Sim	
titulo	VARCHAR(50)	Sim	
dt_inicio	VARCHAR(10)	Sim	
hora_inicio	INTEGER	Sim	
tamanho_pagina	INTEGER	Sim	
tempo_leitura	INTEGER	Sim	
taxa_leitura	FLOAT(10,2)	Sim	

TABELA B.8 – Tabela AUTENTICACOES

Tabela AUTENTICADORES			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_sessao	VARCHAR(50)	Sim	X
id_pessoa	VARCHAR(10)	Sim	X
id_curso	VARCHAR(10)	Sim	X

TABELA B.9 – Tabela PERFIS

Tabela PERFIS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_pessoa	VARCHAR(10)	Sim	X
horario_media	FLOAT(10,2)	Sim	
horario_desvio	FLOAT(10,2)	Sim	
duracao_sessao_media	FLOAT(10,2)	Sim	
duracao_sessao_desvio	FLOAT(10,2)	Sim	
taxa_leitura_media	FLOAT(10,2)	Sim	
taxa_leitura_desvio	FLOAT(10,2)	Sim	
numero_sessoes	INTEGER	Sim	

TABELA B.10 – Tabela CONTADORES

Tabela CONTADORES			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_pessoa	VARCHAR(10)	Sim	X
cont_segunda	INTEGER	Sim	
cont_terca	INTEGER	Sim	
cont_quarta	INTEGER	Sim	
cont_quinta	INTEGER	Sim	
cont_sexta	INTEGER	Sim	
cont_sabado	INTEGER	Sim	
cont_domingo	INTEGER	Sim	

TABELA B.11 – Tabela AGENTES

Tabela AGENTES			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_pessoa	VARCHAR(10)	Sim	X
agente_usuario	VARCHAR(150)	Sim	X
frequencia	INTEGER	Sim	

TABELA B.12 – Tabela IPS

Tabela IPS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_pessoa	VARCHAR(10)	Sim	X
ip_cliente	VARCHAR(15)	Sim	X
dns_cliente	VARCHAR(50)	Sim	
frequencia	INTEGER	Sim	
discado	CHAR(1)	Sim	

TABELA B.13 – Tabela ALERTAS

Tabela ALERTAS			
Nome do Campo	**Tipo**	**Requerido**	**Chave Primária**
id_prof	VARCHAR(15)	Sim	X
enviar_email	CHAR(1)	Sim	
nro_sessoes_inicial	INTEGER	Sim	
horario_conexao	CHAR(1)	Sim	
duracao_sessao	CHAR(1)	Sim	
taxa_leitura	CHAR(1)	Sim	
frequencia_dias	INTEGER	Sim	
frequencia_ferramentas	INTEGER	Sim	
frequencia_agentes	INTEGER	Sim	
frequencia_ips	INTEGER	Sim	

Anexo 3 Diagrama de Classes do Sistema

Este anexo apresenta o diagrama de classes do sistema, desenvolvido com a ferramenta *Rational Rose,* utilizando a notação UML (*Unified Modeling Language).* Também são apresentadas as classes utilizadas no sistema.

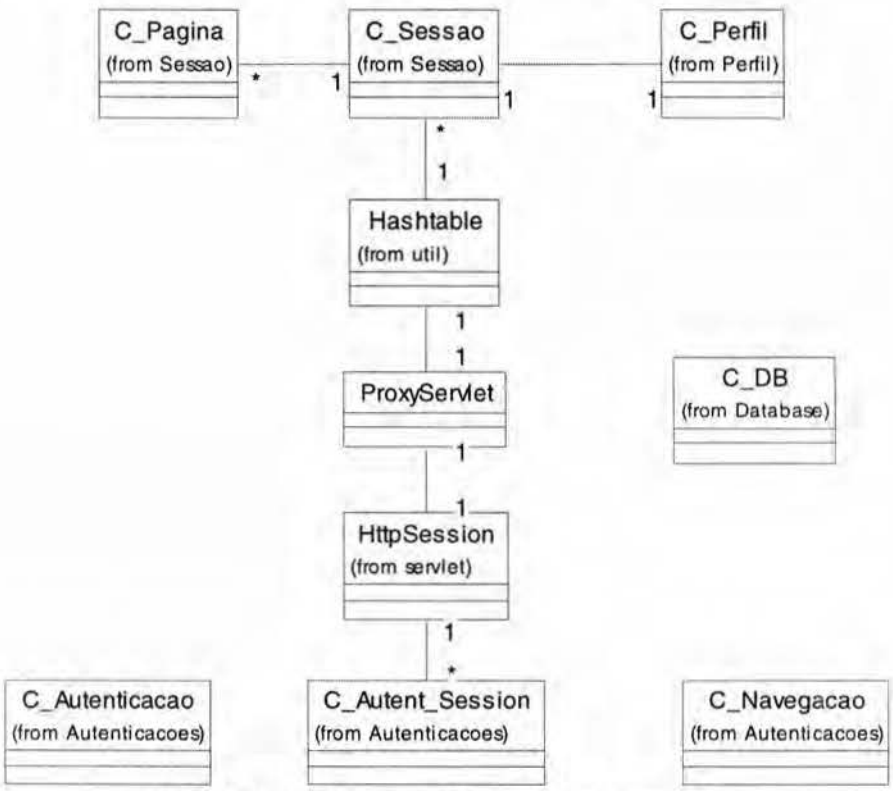

FIGURA C.1 - Diagrama de Classes do sistema

As classes acima estruturam-se em quatro pacotes: Proxy.Autenticacão, Proxy.Database, Proxy.Sessão e Proxy.Perfil. A figura C.2 apresenta a estrutura das classes.

FIGURA C.2 - Estrutura dos pacotes e classes

O pacote Proxy.Autenticação contém três classes: C_Autenticacao, C_Navegacao e C_Autent_Session, as quais são apresentadas respectivamente nas figuras C.3, C.4 e C.5. Estas classes são responsáveis pelas funções de autenticação e navegação dinâmica.

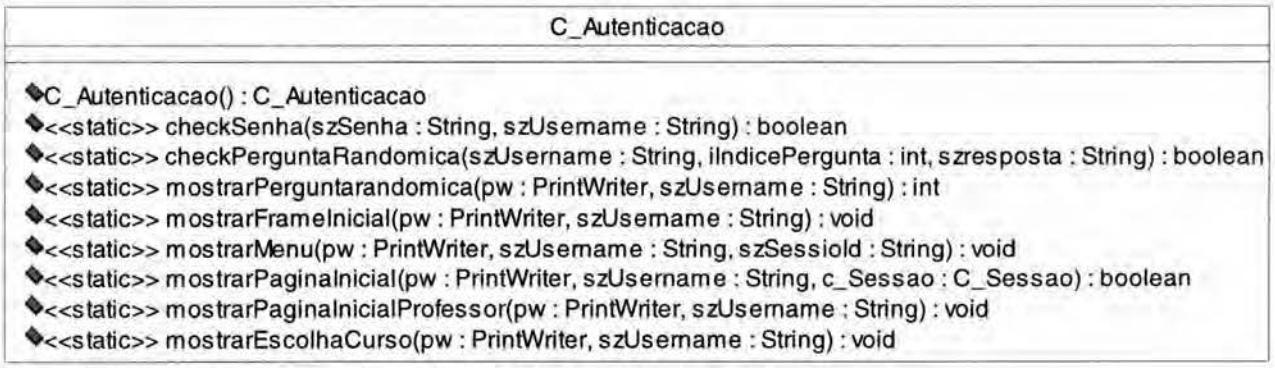

FIGURA C.3 - Classe C_Autenticacao

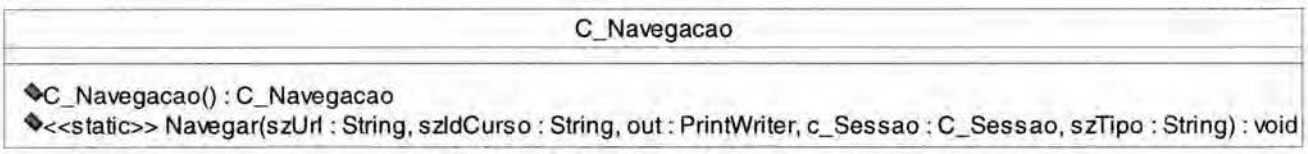

FIGURA C.4 - Classe C_Navegacao

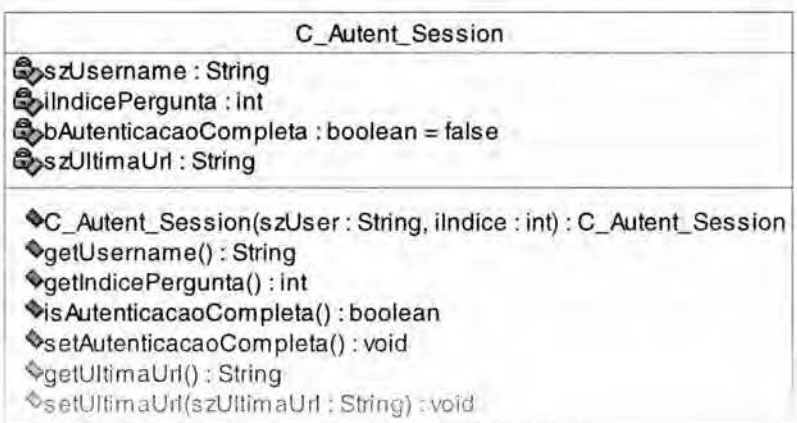

FIGURA C.5 - Classe C_AutentSession

O pacote Proxy.Database contém a classe C_DB e é apresentada na figuras C.6. Esta classe é responsável pela conexão e operações no banco de dados.

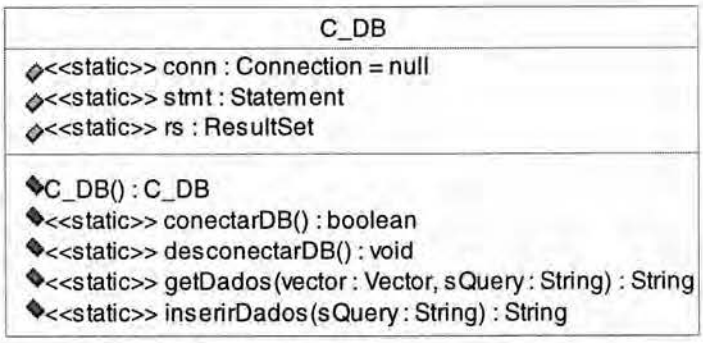

FIGURA C.6 - Classe C_DB

O pacote Proxy.Perfil contém a classe C_Perfil e é apresentada na figuras C.7. Esta classe é responsável pela geração do perfil do usuário e pelo envio de alertas.

FIGURA C.7 - Classe C_Perfil

O pacote Proxy.Sessão contém duas classes: C_Sessao e C_Pagina, as quais são apresentadas respectivamente nas figuras C.8 e C.9. Estas classes são responsáveis pelas funções de controle de sessão e pelos *logs* do sistema.

FIGURA C.8 - Classe C_Sessao

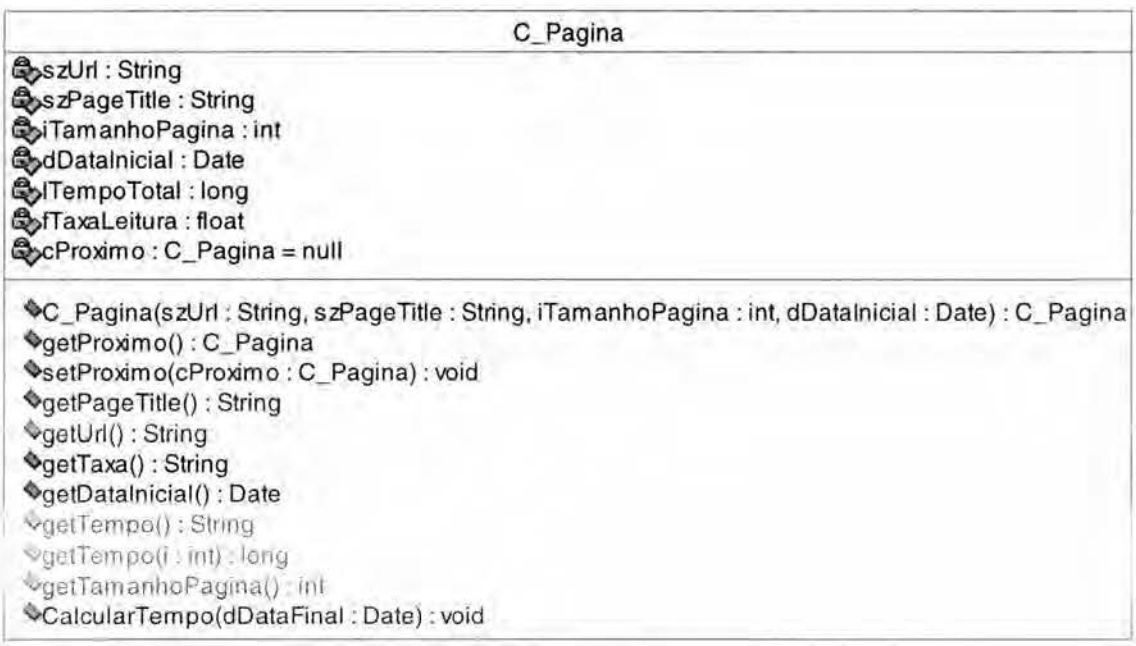

FIGURA C.9 - Classe C_Pagina

A classe ProxyServlet é a principal classe do sistema, responsável pelo recebimento das requisições através dos métodos doGet() e doPost() e pela realização das devidas operações. Além disso, a função init() cria a conexão com o banco de dados. A classe ProxyServlet é apresentada na figura C.10.

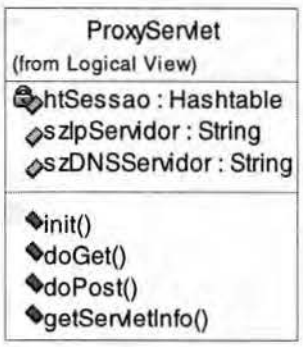

FIGURA C.10 - Classe ProxyServlet

Bibliografia

[AND99] AND INTERNATIONAL PUBLISHERS. **Comparison of Biometric Identification Methods.** Disponível por WWW em http://www.and.com/id/products/biometri/biometri.html (02 jul. 1999).

[BIC99] BIOMETRIC CONSORTIUM. **Biometric Testing Factors.** Disponível por www em http://www.biometrics.org/BioTesting.html (04 jun. 1999).

[BII99] BIOMETRIC IDENTIFICATION, INC. **Biometric ID & Gemplus Team to Deliver First Standalone Contactless Samrt Card System Enable with Secure Fingerprint Verification.** Disponível por www em http://www.gemplus.com/about/pressroom/press/access/1999/bioid_uk.htm (04 jun. 1999).

[BIO98] THE BIOMETRIC CONSULTING GROUP. **Comparation of Biometric Techniques.** Disponível por WWW em http://www.biometric-consulting.com/bio.htm (04 out. 1998).

[BIO99] INTERNATIONAL BIOMETRIC GROUP. **Miros.** Disponível por www em http://www.biometricstore.com/a_bio1/vendor/miros.htm (07 maio 1999).

[BIO99a] INTERNATIONAL BIOMETRIC GROUP. **Biometric Technology Offerings.** Disponível por www em http://www.biometricstore.com/a_biometrics_42/biometric_technology_offerings.asp (04 jun. 1999).

[BIO99b] INTERNATIONAL BIOMETRIC GROUP. **Finger Scan.** Disponível por www em http://www.biometricstore.com/a_bio1/technology/cat_finger_scan.htm (04 jun. 1999).

[BIS95] BISHOP, Matt; KLEIN, Daniel. Improving system security via proactive password checking. **Computers & Security**, Oxford, v.14, n.3, p. 233-249, 1995.

[BMP99] BIOMET PARTNERS, INC. **FingerFoto.** Disponível por www em http://www.biomet.ch/ff.htm (07 jul. 1999).

[BRO99] BROWN, Bruce. Anatomically Correct. **PC Magazine**. Disponível por www em http://www.zdnet.com/filters/printerfriendly/0,6061,295037-3,00.html (05 maio 1999).

[CAR97] CARISSIMI, Leonardo S. **Segurança em Transações Comerciais Eletrônicas.** Porto Alegre: CPGCC da UFRGS, 1997. 55p. (T.I.-665).

[FID99] FIDLER, Ross. **Information about IriScan.** Disponível por E-mail em rfidler@iriscan.com (24 jun. 1999).

[FIO98] FIORESE, Mauricio. **Mecanismos de Autenticação de Usuários.** Porto Alegre: CPGCC da UFRGS, 1997. 67p. (T.I.-765).

[FLE99] FLEURY, André M. **Facilitando o Acesso Seguro à Informação.** Palestra apresentada no II Peta Fórum, Porto Alegre, (15 jun. 1999).

[GUN99] GUNNERSON, Gary; PLAIN, Stephen W. Pronto para a biometria? **PC Magazine Brasil**, São Paulo, p.82-94, mar. 1999.

[HAC2000] HACK, Luciano E. **Mecanismos Complementares para a Avaliação do Aluno na Educação a Distância .** [S.l.: s.n.], 2000. Dissertação de mestrado em andamento.

[HON98] HONG, L. JAIN, A.K. Integrating Faces and Fingerprint for Personal Identification. **IEEE Transactions PAMI**, New York, v.20, n.12, p. 1295-1307, 1998.

[HUN98] HUNTER, J. ; CRAWFORD, W. **Java Servlet Programming.** Sebastopol, USA: O'Reilly, 1998. 510p.

[IDE99] IDENTIX INCORPORATED. **TouchSafe Personal.** Disponível por www em http://www.identix.com/products/tsp.htm (05 jul. 1999).

[ICS99] ICSA. **Biometric Survey.** Disponível por www em http://www.icsa.net/services/consortia/cbdc/survey/survey.ZIP (04 jun. 1999).

[JAI97] JAIN, A.K.et al. An Identity-Authentication System Using Fingerprints. **Proceedings of the IEEE,** New York, v.85, n.9, p.1365-1388, 1997.

[JAI98] JAIN, A.K.; PRABHAKAR, S.; ROSS, A. **Biometrics-Based Web Access.** Disponível por www em http://web.cps.msu.edu/TR/MSUCPS:TR98-33 (08 maio 1999). (MSU Technical Report, TR98-33).

[JAI99] JAIN, A.K.; KULKARNI, Yatin. A Multimodal Biometric System Using Fingerprint, Face, and Speech. In: INTERNATIONAL CONFERENCE ON AUDIO- AND VIDEO-BASED BIOMETRIC PERSON AUTHENTICATION, 2., 1999, Washington, D.C. **Proceedings ...** Disponível por www em http://web.cps.msu.edu/TR/MSUCPS:TR98-32 (08 maio 1999).

[KES99] KESSLER, Gary C. **Passwords - Strengths and Weaknesses.** Disponível por www em http://www.hill.com/library/staffpubs/password.html (08 maio 1999).

[KIM95] KIM, Hyun-Jung. Biometrics, is it a viable proposition for identity authentication and access control ? **Computers & Security**, Oxford, v. 14, n.3, p. 205-214, 1995.

[LOP99] LOPES, Antônio J. **Produtos de Ensino a Distância.** Disponível por www em http://www.medialab.fe.up.pt/disciplinas/ensdis/ajlopes/ensino.htm (03 abr. 1999).

[MAC99] MACHADO, Júlio H. A. P. **Sistemas de Gerenciamento para Ensino a Distância.** Porto Alegre: PPGC-UFRGS, 1999. (T.I.-784)

[MAN96] MANBER, Udi. A simple scheme to make passwords based on one-way functions much harder to crack. **Computers & Security**, Oxford, v.15, n.2, p.171-176, 1996.

[MCD99] MCDOWELL, Bob. **Information about TrueFace.** Disponível por Email em rmcdowell@miros.com (28 jun. 1999).

[NAT94] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guideline for Use of Advanced Authentication Technology Alternatives.** Disponível por www em http://www.itl.nist.gov/fipspubs/fip190.htm (18 set. 1998). (Federal Information Processing Standards Publication 190).

[OSW97] OWSTON, Ronald D. The World Wide Web: A Technology to Enhance Teaching and Learning? **Educacional Researcher,** [S.l.], v.26, n.2, p. 27-33, 1997.

[PFL97] PFLEEGER, Charles P. **Security in Computing.** 2.ed. New Jersey, USA: Prentice Hall, 1997. 574p.

[RIT97] RITZEL, Marcelo I. **Análise dos Aspectos Básicos para se Implementar Ensino a Distância Utilizando Sistemas Multimídia.** Porto Alegre: CPGCC-UFRGS, 1997. (T.I.-681).

[ROE98] ROETHENBAUGH, Gary. **Biometrics Explained.** Disponível por www em http://www.ncsa.com/services/consortia/cbdc/explained.htm (04 out. 1998).

[RU97] RU, Willem G.; ELOFF, Jan H. P. Enhanced Password Authentication through Fuzzy Logic. **IEEE Expert/Intelligent Systems & Their Applications,** New York, v.12, n.6, nov./dec. 1997.

[RUT99] RUTHSCHILLNG, E. E. et al. **A evolução dos ambientes de aprendizagem construtivistas.** Disponível por WWW em http://penta.ufrgs.br/~luis/Ativ1/AmbApC.html (05 jun. 1999).

[SEC99] SECURITY DYNAMICS, INC. **The SecurID Software Token Solution.** Disponível por www em http://www.securitydynamics.com/products/datasheets/securidst-ds.html (05 maio 1999).

[SIG99] SIGULEN, Daniel. **Educação a Distância.** Palestra apresentada na UFRGS, maio 1999.

[SPI79] SPIEGEL, Murray R. **Estatística**. São Paulo, Brasil: McGraw-Hill, 1979. 580 p.

[TRI92] TRINDADE, R. S. **Um Estudo da Linguagem SDL para Especificação e Teste de Protocolos.** Porto Alegre: CPGCC-UFRGS, 1992. (T.I.-258).

[TUC99] TUCKER, R. **Assessing the Virtual Classrooms:** A Progress Report. Disponível por www em http://www.intered.com/edv5n2.htm (22 maio 1999).

[VER99] VERIVOICE, INC. **VeriVoice Data Sheet.** Disponível por www em http://www.verivoice.com/datasheet.html (06 jun. 1999).

[VIS99] VISIONICS CORPORATION. **FaceIt Technology.** Disponível por www em http://www.faceit.com/live/markets/infosecurity/index.html (03 maio 1999).

[VIS99a] VISIONICS CORPORATION. **Technical Specifications.** Disponível por www em http://www.faceit.com/live/visionics/corpprof3.html (03 maio 1999).

[WEL99] WELCHER, Michele. **Information about American Biometric Biomouse Plus.** Disponível por E-mail em mwelcher@abio.com (29 jun. 1999).

[WU96] WU, Tzong-Chen; SUNG, Hung-Sung.Authenticating passwords over na insecure channel. **Computers & Security**, Oxford, v.15, n.5, p. 431-439, 1996.