Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Curso de Ciência da Computação

Higo Felipe Silva Pires

Federação de Identidades em Ambiente de Computação em Nuvem usando o Middleware Shibboleth

São Luís
2014

Higo Felipe Silva Pires

Federação de Identidades em Ambiente de Computação em Nuvem usando o Middleware Shibboleth

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal do Maranhão como parte dos requisitos para a obtenção do grau de BACHAREL em Ciência da Computação.

Orientador: Zair Abdelouahab

Doutor em Computer Studies – University of Leeds

São Luís

2014

Pires, Higo Felipe Silva.

Federação de identidades em ambiente de computação em nuvem usando o Middleware Shibboleth/ Higo Felipe Silva Pires. – São Luís, 2014.

32 f.

Impresso por computador (fotocópia).

Orientador: Zair Abdelouahab.

Monografia (Graduação) – Universidade Federal do Maranhão, Curso de Ciência da Computação, 2014.

1. . Computação em nuvem. 2. Gerenciamento de identidades. 3. Shibboleth. I. Título.

CDU 004.056

Higo Felipe Silva Pires

Federação de Identidades em Ambiente de Computação em Nuvem usando o Middleware Shibboleth

Este exemplar corresponde à redação final da monografia devidamente corrigida e defendida por Higo Felipe Silva Pires e aprovada pela comissão examinadora.

Aprovada em 21 de Julho de 2014

BANCA EXAMINADORA

Zair Abdelouahab (orientador)

Doutor em Computer Studies – University of Leeds

Vicente Leonardo Paucar Casas

Doutor em Engenharia Elétrica – Universidade Estadual de Campinas – UNICAMP

Samyr Béliche Vale

Doutor em Informatique – Université d'Angers

A Jesus por Maria.

Resumo

Usuários de computação em nuvem têm grande preocupação com os riscos de segurança implícitos à incorporação de seus recursos dentro deste ambiente. Mecanismos de gerenciamento de identidades e acesso são fundamentais para garantir a privacidade dos dados dos usuários inseridos no ambiente de computação em nuvem. Entre estes mecanismos inclui-se a o gerenciamento de identidades federadas. Uma federação é uma forma de associação de entidades consideradas confiáveis entre si que torna possível a cooperação entre os membros da federação. O objetivo deste trabalho é apresentar um estudo de caso referente à implementação de uma federação de identidades em ambiente de computação em nuvem usando o middleware Shibboleth. O cenário proposto é implementado para verificar a aplicabilidade. Os testes geraram os resultados esperados.

Palavras-chave: Gerenciamento de Identidades, Computação em Nuvem, Federação, *Single Sign-On*, *Shibboleth*.

Abstract

Users of cloud computing have great concern about the implicit security risks to the incorporation of their resources in this environment. Mechanisms for identity management and access are essential to ensure the privacy of user data inserted in the cloud computing environment. Among these mechanisms are included the federated identity management. A federation is a form of association of entities deemed reliable relative to each other which makes the cooperation between the members of the federation possible. The objective of this work is to present a case study regarding the implementation of an identity federation in cloud computing environment using Shibboleth middleware. The proposed scenario is implemented to verify applicability. The tests generated the expected results.

Keywords: Identity Management, Cloud Computing, Federation, Single Sign-On, Shibboleth.

Agradecimentos

A Deus, meu Criador e Redentor, Princípio e Fim deste trabalho.

A meu orientador Prof. Ph.D. Zair Abdelouahab pela oportunidade concedida, pelo apoio de verdadeiro educador e pelos conselhos e sugestões enriquecedores ao longo do trabalho. A ele, minha imorredoura gratidão.

Aos Professores membros da Banca Examinadora, Prof. Dr. Vicente Leonardo Paucar Casas e Prof. Dr. Samyr Béliche Vale, pela pronta disposição de avaliar este trabalho.

À minha família, pela excelente criação, amor e carinho sempre presentes. Muito obrigado, mãe (Rosa Amélia), pai (Simião), irmão (Arthur), primos, tios, avós, que nesta caminhada foram tão importantes. Deus abençoe a todos!

À minha amada namorada Aline Cabral, pelo amor, apoio e paciência nestes 11 meses, que foram os mais especiais da minha vida.

Aos diletíssimos confrades do Laboratório de Sistemas em Arquiteturas Computacionais (LABSAC) da UFMA, pela indispensável ajuda a este trabalho e e pela valorosa amizade. Meus mais sinceros agradecimentos a todos: Luiz Aurélio, Cláudio Aroucha, Willian Ribeiro, Dhully Andrade, Jonathan Santos, Mário Henrique, Leonardo Melo, Jean Pablo, Marcos Sá, Renato Ubaldo e Bruno Nogueira.

Ao Curso de Ciência da Computação, pela oportunidade da realização do curso; a todos os professores, pela atenção e esmero no ensino, e a todos os funcionários do Departamento de Informática – DEINF.

À FAPEMA (Fundação de Amparo à Pesquisa e ao Desenvolvimento Científico e Tecnológico do Maranhão), pelo financiamento da bolsa de estudo. A esta Fundação, meu agradecimento pelo investimento.

A todos os amigos da Associação Católica *Ad Maiorem Dei Gloriam*, pela perene amizade e valorosíssimas orações. E a todos aqueles que direta ou indiretamente contribuíram para a realização deste trabalho.

"Dai-me a penetração da inteligência, a faculdade de lembrar-me, o método e a facilidade do estudo, a profundidade na interpretação e uma graça abundante de expressão.

Fortificai o meu estudo, dirigi o seu curso, aperfeiçoai o seu fim, Vós que sois verdadeiro Deus e verdadeiro homem, e que viveis nos séculos dos séculos."

São Tomás de Aquino (1225-1274)

Lista de Figuras

Sumário

1 Introdução

Neste capítulo é apresentada uma descrição deste trabalho, com o objetivo de fornecer uma visão geral dos problemas tratados e dos objetivos principais do trabalho de pesquisa realizado. Em seguida, é apresentada a estrutura do documento, com uma descrição resumida do conteúdo abordado em cada capítulo.

1.1 Contexto

A computação em nuvem é considerada elemento primário no atual cenário da Tecnologia da Informação. De acordo com o *International Data Corporation* (IDC) [13], investimentos com serviços de computação em nuvem atingiriam a cifra de US$ 47,4 bilhões em 2013 e estima-se que atinjam os US$ 107 bilhões em 2017.

Uma das mais notaveis características da computação em nuvem é a possibilidade de pagamento somente pelos recursos contratados pelo usuário.

Autores como [22, 35, 47] definem a computação em nuvem como um paradigma computacional onde os usuários tem acesso sob demanda a um determinado conjunto de recursos computacionais compartilhados como redes, espaço em disco para armazenamento, serviços providos a um baixíssimo custo computacional, utilizando a Web através de vários dispositivos.

Existem hoje vários provedores que hospedam e fornecem serviços de computação em nuvem para usuários: *Amazon Web Services*, *Microsoft Azure*, *Google Apps*, entre outros.

No contexto dos serviços de computação em nuvem, uma vez que os dados trafegam fora do domínio do cliente, são necessárias funcionalidades que implementem a gerência dos usuários (autenticação e autorização) para controlar o acesso de usuários aos serviços providos pelo ambiente. Assim sendo, a prática do gerenciamento de identidades é da maior importância.

Com isto em mente, tendo por objetivo controlar o acesso dos usuários à nuvem, o gerenciamento de identidades federadas é considerado por especialistas como um importante fornecedor de segurança da informação, já que desempenha um papel essencial na implantação bem sucedida dos ambientes em nuvem. O seu uso em vários *Webservices* e arquiteturas computacionais, como a Computação em Grade, e o interesse de várias entidades (*CSA, ENISA, NIST*) de padronização envolvidos na computação em nuvem, mostra-se como forte indício da relevância do gerenciamento de identidades federadas [32].

O gerenciamento de identidades federadas (FIM) apresenta uma proposta para o intercâmbio de recursos entre diferentes partes confiáveis entre si, havendo a possibilidade de serem compartilhados recursos através informações do usuário. Uma propriedade importante neste possibilidade é o *Single Sign-On (SSO)* ou "Autenticação única", no qual o usuário é capaz de acessar vários recursos, autenticando-se apenas uma vez.

Os principais atores em um cenário de FIM são (1) o provedor de identidade (IdP), que efetua a autenticação das informações sobre clientes, (2) o provedor de serviços (SP), que contém as aplicações, as quais é permitido o acesso para o usuário final após a verificação da identidade efetuada pelo IdP, e (3) o cliente, que fornece uma credencial para se autenticar no IdP e acessar a aplicação que deseja, contida pelo SP, com o qual interage geralmente através de um *browser*.

Para explicarmos o termo "federação", valendo-nos inclusive do que nos diz o Dicionário Michaelis [10], podemos dizer que se trata do ato de estabelecer uma relação de mútua confiança entre os provedores. Posto isso, a arquitetura computacional proposta neste trabalho pode ser entendida.

1.2 Motivação

Uma das maiores preocupações das empresas que implementam ambientes de computação em nuvem são os riscos de segurança implícitos à incorporação de seus recursos dentro deste ambiente. Há vários trabalhos recentes, oriundos de várias áreas do conhecimento, tais como [17, 30, 43–45], que mostram a ênfase dada à segurança no contexto da computação em nuvem.

É quase consenso que a computação em nuvem começou em 2008, com o crescimento exponencial do uso de *Webservices* e serviços de armazenamento da Amazon. A partir daí, estudos são feitos de maneira contínua, com objetivo de estudar a computação em nuvem, em busca de soluções a problemas levantados. Uma pesquisa do *International Data Corporation (IDC)* [14], na qual foram entrevistados 244 executivos de TI, concluiu que 87,5% dos entrevistados preocupam-se com a segurança, dita como um dos principais entraves à implementação de sistemas baseados em computação em nuvem. A Figura 1.1 traz os resultados dessa pesquisa.

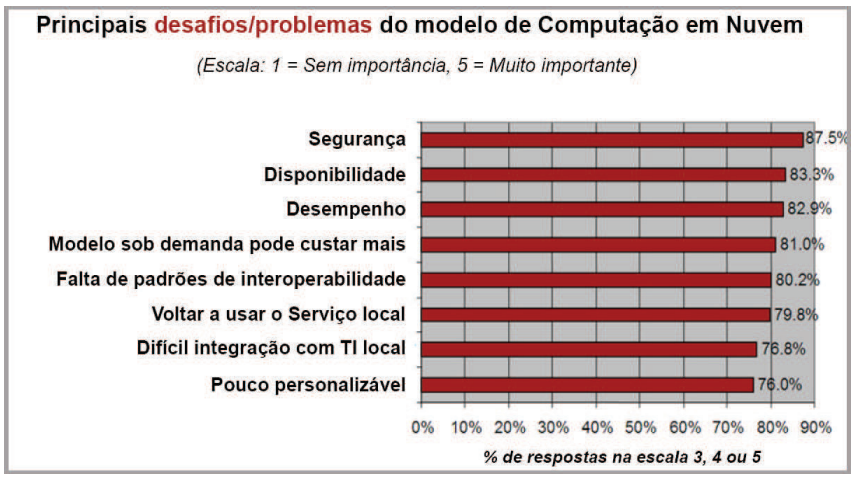

Figura 1.1: Preocupações inerentes à computação em nuvem. Adaptado de [14].

Os principais elementos para segurança da computação em nuvem são mostrados [19] (Identidades, Infraestrutura e Informação) a seguir na Figura 1.2.

Figura 1.2: Principais elementos para segurança em computação em nuvem. Adaptado de [19].

O primeiro elemento da Figura 1.2 é a Segurança, que é o propósito deste trabalho, focado no gerenciamento de identidades federadas, como tópico de estudo da segurança em computação em nuvem. Segundo [37] [12], a Segurança Computacional é requisito funcional para que haja garantia de sucesso em ambientes de Computação em Nuvem, e [28] destaca meios de manutenção da privacidade, para que dados de suma importância não sejam interceptados por agentes maliciosos. Assim sendo, a segurança cresce em importância conforme aumenta o número de serviços que utilizam autenticação e autorização para controlar o acesso de usuários [1] [3].

1.3 Objetivos

1.3.1 Objetivo geral

O objetivo geral deste trabalho é apresentar um estudo de caso envolvendo um sistema de gerenciamento de identidades usando o middleware Shibboleth e verificar a sua aplicabilidade em ambientes de computação em nuvem.

1.3.2 Objetivos Específicos

No sentido de alcançar o objetivo geral pretendido, buscar-se-ão atingir os seguintes objetivos específicos:

- Levantar os conceitos fundamentais de gerenciamento de identidades;
- Analisar os mecanismos de autenticação e autorização em ambientes distribuídos;
- Comparar as abordagens de gerenciamento de identidades;
- Identificar as principais tecnologias usadas para a implementação de sistemas de gerenciamento de identidades;
- Analisar os principais sistemas de gerenciamento de identidades, suas arquiteturas e seu funcionamento;
- Levantar os conceitos fundamentais da computação em nuvem e suas tecnologias;

- Verificar as estratégias de gerenciamento de identidades no ambiente de computação em nuvem;
- Aplicar um estudo de caso de um sistema de gerenciamento de identidade em um ambiente de computação em nuvem.

1.4 Organização do Trabalho

Este trabalho está divido em quatro capítulos. O capítulo 1 apresentou a Introdução, contemplando o contexto do cenário da Gestão de Identidades, bem como a motivação e os objetivos, gerais e específicos, do trabalho. No capítulo 2 serão apresentados os conhecimentos teóricos com os quais este trabalho está relacionado, portanto indispensáveis para o seu perfeito entendimento: Segurança da Informação, Computação em Nuvem, Gerenciamento de Identidades, além de uma abordagem sobre a especificação *SAML* e o *middleware Shibboleth*, usados no ambiente testado. No capítulo 3 será apresentado o estudo de caso proposto no objetivo geral deste trabalho, expondo os detalhes inerentes ao ambiente, bem como os resultados finais da implantação e dos testes. Finalmente, no capítulo 4 será apresentada a conclusão deste trabalho, onde é apresentada uma avaliação acerca da implementação do ambiente proposto, bem como alguns trabalhos futuros.

2 Revisão Bibliográfica

2.1 Segurança da Informação

Nesta seção, são apresentados conceitos inerentes à segurança da informação. Os tópicos versam sobre propriedades da segurança, termos importantes, conceitos sobre criptografia, e esclarece outros pontos como políticas e modelos. Esta seção faz, igualmente, uma descrição de diversos tópicos que serão abordados posteriormente.

2.1.1 Definição e Classificação

Com o crescimento de ambientes distribuídos, entre os quais o mais conhecido, a *Internet*, igualmente cresce a preocupação com a segurança da informação, por parte dos mais diversificados campos da sociedade: instituições públicas, empresas, e até mesmo os próprios cidadãos, isolada ou coletivamente. Em qualquer onde é minimamente necessária, a segurança da informação é um ponto crucial para a sobrevivência de várias entidades.

No atual cenário, dispositivos ao redor do globo têm acesso às informações via *Internet*, o que aumenta a complexidade e importância de proteção das informações. O nome genérico para as ferramentas e técnicas desenvolvidas para proteger dados e impedir atacantes é "segurança da informação" [38].

A segurança da informação geralmente é definida pelas suas propriedades: confidencialidade, integridade e disponibilidade. Tais propriedades são definidas mais adiante no texto. A segurança da informação pode ser definida nos seguintes termos:

- A prática de assegurar que os recursos importantes para as informações sejam protegidos contra violações de confidencialidade, comprometimento da integridade e contra a indisponibilidade a estes recursos [46];

- A proteção da informação contra vários tipos de ameaças, de modo que seja garantida a continuidade do negócio, minimizados ou eliminados os riscos ao negócio, maximizado o retorno sobre investimentos e oportunidades de negócio [2].

Alguns pesquisadores, como [23, 24, 41] classificam a segurança da informação em:

- **Segurança física:** Referente a equipamento, instalações e ao pessoal; estão as situações em que a parte humana, bem como a infraestrutura,exercem papel primário;
- **Segurança lógica:** Referente à implementação lógica: técnicas, metodologias e boas práticas; No mais das vezes pouco aparente, deve estar em permanente atualização e manutenção, de forma a acompanhar também a evolução dos riscos e das possíveis ameaças.

2.1.2 Terminologias

Outros termos, como os mencionados por [2, 18, 20, 21] aplicam-se também à segurança da informação, e são apresentados a seguir:

- **Ativo:** Qualquer patrimônio que tenha valor para a organização. Exemplos: dados, informações e equipamentos;
- **Usuários:** Funcionários, clientes, fornecedores;
- **Vulnerabilidades:** Fragilidades de um ativo ou grupo de ativos que pode ser atacada por uma ou mais ameaças. Exemplos: falhas em sistemas operacionais, contas com senhas fracas;
- **Risco:** Custo medido de ocorrência da exploração de uma vulnerabilidade. A análise qualitativa destes riscos é linha de base para criação das políticas de segurança;
- **Incidente:** Um simples ou uma série de eventos indesejados ou inesperados, com capacidade de comprometer as operações do negócio e ameaçar a segurança da informação;

- **Controle:** Forma de gerenciar o risco, através do uso de políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais;

2.1.3 Propriedades

A segurança da informação tem o objetivo de proteger os dados de usuários e organizações e estimular comportamentos seguros por meio do estabelecimento de políticas de segurança, e se baseia em um conjunto de propriedades [20], as quais são discutidas e referidas como "CID", conforme ilustra a Figura 2.1.

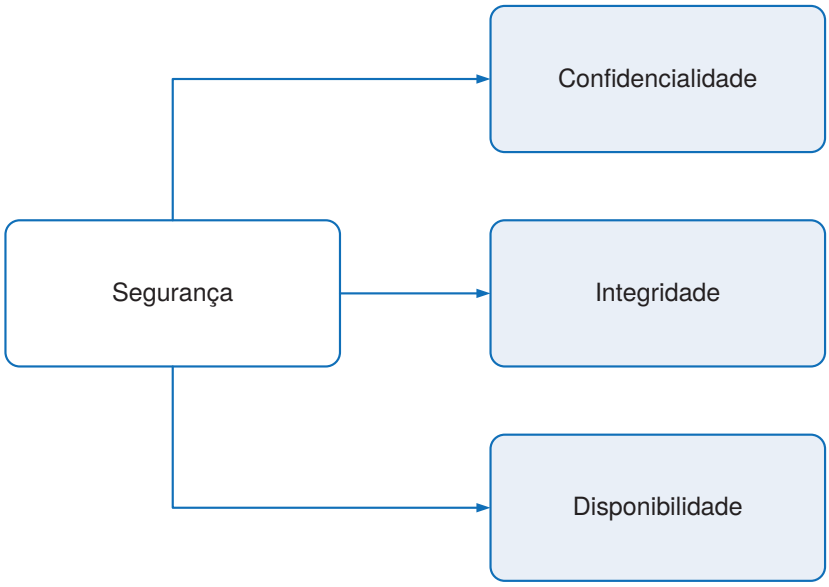

Figura 2.1: Propriedades da segurança. Adaptado de [41].

Cada uma das propriedades é definida conforme abaixo [21] [23]:

- **Confidencialidade:** Propriedade que garante que a informação só será acessada por quem está autorizado a acessá-la;
- **Integridade:** Propriedade que garante que haverá inteireza dos dados quando acessados, em relação ao momento em que foram enviados ao destinatário.
- **Disponibilidade:** Propriedade que garante que os usuários autorizados poderão acessar a informação sempre que possível.

Além dos conceitos "CID", existem outros conceitos aplicáveis à segurança da informação, descritos a seguir:

- **Confiabilidade:** Propriedade que se refere à confiança propriamente dita nos sistemas de computação. Envolve o grau de confiança em pessoas e/ou sistemas, no que se refere ao seu comportamento em determinado sistema computacional;

- **Autenticidade:** Propriedade responsável por checar a identidade do cliente que requer os dados, além de determinar a veracidade dos fatos que ocorrem no sistema;

  - **Irretratabilidade ou não-repúdio:** Propriedade responsável por garantir que afirmações autênticas emitidas por alguma pessoa ou sistema não podem ter sua autoria negada;

2.1.4 Ameaças e Ataques

Tendo sido expostas as propriedades da segurança da informação, serão citadas algumas das ameaças que podem comprometer essas propriedades.

Os atacantes, que são a força motriz dos ataques, são classificados como internos ou externos. Atacantes internos são aqueles que conseguem despistar os elementos de defesa da rede, e se passar por membros genuínos da rede, enquanto que os externos são os que mesmo fora da rede, mantém atividades maliciosas dentro dela.

A Figura 2.2 mostra as modalidades de ataques, segundo [36]. É considerado o fluxo normal de informação fluindo de um nó de rede A para um nó de rede B, como se observa na Figura 2.2;

- **Interrupção:** Ocorre quando um componente do sistema tem sua ou sua integridade ou sua disponibilidade violados, através de dano, físico ou lógico, aos dados;

- **Interceptação:** Occore quando uma entidade que não possui privilégios suficientes ganha acessos aos componentes, permitindo a captura de informações sigilosas, violando assim a confidencialidade;

- **Modificação:** Ocorre quando uma entidade falsifica componentes, além de ter acesso a eles sem a devida permissão. É uma ataque à integridade;

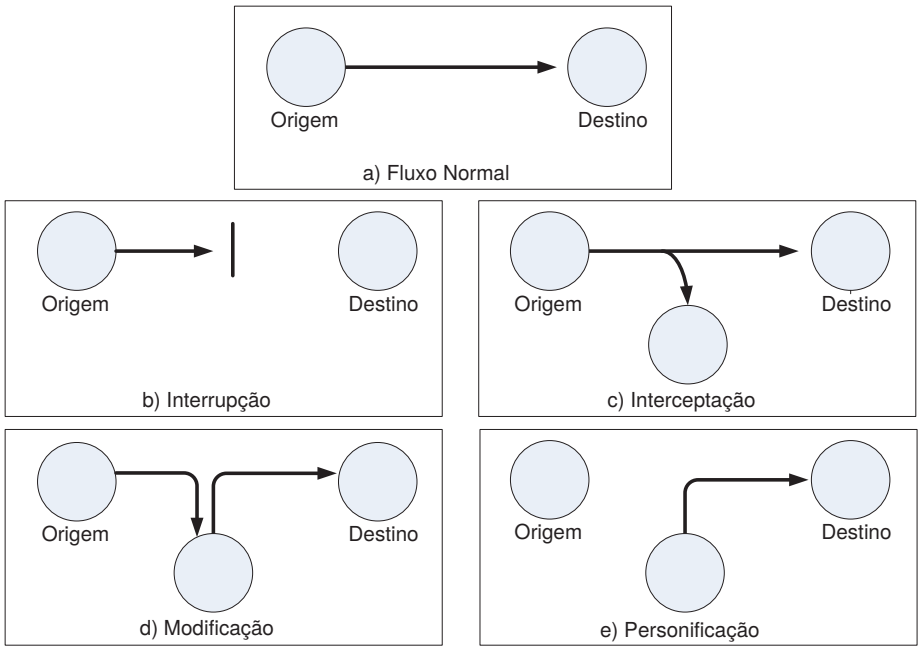

Figura 2.2: Categorias de Ataques [36].

- **Personificação:** Ocorre quando uma entidade maliciosa interpõe-se entre entidades comunicantes, e falseia os dados enviados a uma ou mais delas. Viola o princípio da autenticidade;

2.1.5 Políticas de Segurança

Segundo a norma *ABNT NBR ISO/IEC* 27002:2013 [2], "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software e hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."

Existem três tipos de políticas de segurança, segundo [26]: políticas de segurança física, políticas de segurança administrativa e políticas de segurança lógica.

As políticas de segurança física se ocupam com o que diz respeito à parte física do sistema. Aqui são definidas as medidas contra quebras de segurança física provocadas por incêndio, inundações, desastres naturais, etc.

Já as políticas administrativa tratam da segurança sob o ponto de vista organizacional, operacional e estratégico dentro da unidade organizacional.

Finalmente, as políticas de segurança lógica versam sobre alguns tópicos como permissões e autorizações inerentes ao sistema.

2.1.6 Sistemas Criptográficos

A criptografia é uma estudo de essencial importância para segurança da informação, e serve como ponto de partida de diversas facilidades, tais como a infraestrutura de chaves públicas (*Public Key Infraestruture - PKI*). As já citadas propriedades da segurança da informação - confidencialidade, integridade, autenticação e irretratabilidade - garantem as milhares de comunicações criptográficas executadas diariamente [25].

Criptografia (Do grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo de técnicas que, quando usadas, provêm a proteção de dados sensíveis, através do escondimento de sua verdadeira grafia. A cifragem é o processo de dissimular o texto da mensagem original, fazendo que permaneça oculta em um texto cifrado, até o momento que seja decriptada [33].

Tais processos de encriptação e decriptação são implementados por algoritmos que alteram textos claros em textos encriptados. Estes algoritmos se dividem em dois tipos:

- **Simétricos:** Utilização de uma chave apenas, tanto para cifragem quanto para decifragem. Têm melhor desempenho computacional, porém são menos complexos. Exemplos: *IDEA, TwoFish, Blowfish, Serpent, DES, AES, RC5, RC6, RC4* e *OTP*.
- **Assimétricos:** Utilização de duas chaves, uma pública e uma privada, uma para cifragem e outra, diferente, para decifragem. Exemplos são *RSA, Diffie-Helman, El Gamal* e Curvas Elípticas.

2.1.7 Princípios de Controle de Acesso

Num sistema de computação em nuvem, os serviços são providos para os mais diversos tipos de usuários, portanto é necessário definir normas que estipulem controles de acesso e permissões necessárias para acessar os serviços. Estas normas são definidas por três conceitos elementares: a autorização, autenticação e cumprimento [31,39], conforme a Figura 2.3.

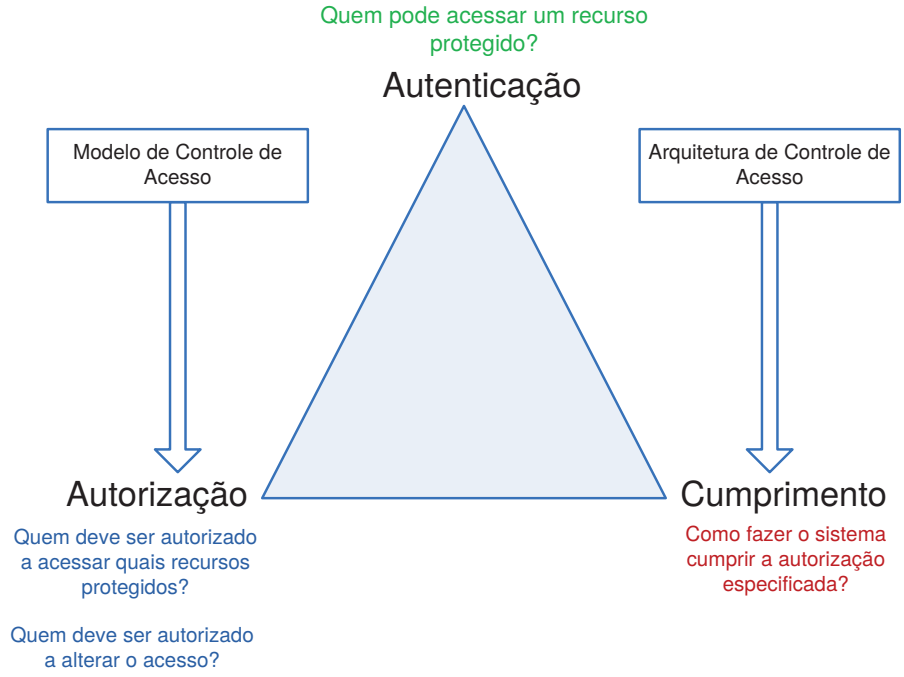

Figura 2.3: Conceitos de Controle de Acesso. Adaptado de [29]

- **Autorização:** Se refere aos recursos que serão protegidos, quais operações os clientes poderão efetuar neles e quais tipos de acesso serão permitidos a e esses recursos.

- **Autenticação:** Se refere ao processo de legitimação da identidade do cliente do sistema, ou seja, a confirmação de que o cliente é de fato quem diz ser. Geralmente esta confirmação é feita através do recebimento de um atributo único para cada cliente, como uma combinação de usuário e senha ou uma impressão digital;

- **Cumprimento:** Se refere à confirmação da permissão do acesso ao recurso pelo cliente quando satisfeitas as condições de acesso, obtendo assim, disponibilidade em relação ao sistema;

2.2 Computação em Nuvem

Nesta seção serão apresentados os conceitos elementares de computação em nuvem e as classificações dos modelos de serviço oferecidos.

2.2.1 Definições e Características

A expressão "nuvem" ou *cloud* é uma representação que remete ao elemento gráfico usado nas topologias lógicas de rede para representar a *Internet*. Já a Computação em Nuvem refere-se a uma combinação de recursos que podem ser administrados pelo cliente com um mínimo de conhecimentos. [7].

Em [22], Mell e Grance do *NIST* (*National Institute of Standards and Technology*) definem a Computação em Nuvem como um modelo que permite acesso sob demanda a um *pool* de recursos que podem ser contratados com um mínimo custo computacional e de solicitações ao provedor. Ainda em [22] enumeram-se cinco características comuns aos serviços de computação em nuvem:

1. **Autoatendimento sob demanda:** Um consumidor pode prover recursos de computação sob demanda, sem que haja necessidade de interação humana no processo;

2. **Acesso amplo à rede:** Os recursos disponíveis podem ser requeridos através de mecanismos que provém acesso para plataformas não necessariamente homogêneas, como *tablets*, *smartphones*, *notebooks*, etc.

3. ***Pool* de recursos:** Os recursos são reunidos para serem dispostos para vários clientes com diferentes níveis de *hardware* e *software*;

4. **Elasticidade Rápida:** Os recursos podem ser providos de maneira flexível(elástica), de acordo com a necessidade, a qualquer instante.

5. **Serviço Medido:** Os sistemas de computação em nuvem controlam e melhoram, sem intervenção humana, a distribuição dos recursos, de modo que um serviço seja fornecido de uma maneira proporcional aos seus requisitos de *hardware* e *software*;

2.2.2 Modelos de Serviços

Serviços de Computação em Nuvem possuem três modelos arquiteturais, a saber: Infraestrutura como Serviço (*IaaS*), Plataforma como Serviço (*PaaS*) e Software como Serviço (*SaaS*). Este modelo é conhecido como "SPI", em referência às iniciais de cada modelo. A Figura 2.4 apresenta as camadas dos modelos arquiteturais e, em seguida, é apresentada a descrição de cada um deles:

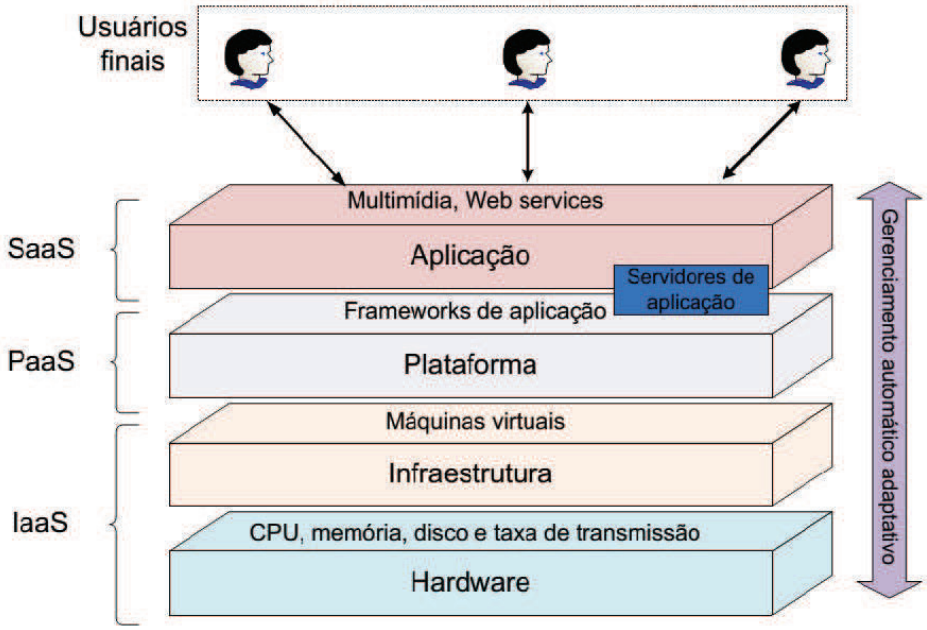

Figura 2.4: Serviços de Computação em Nuvem. Adaptado de Zhang et al. em [47]

- ***SaaS - Software as a Service*:** É oferecido ao cliente consumidor a utilização do serviço contido na nuvem. Neste modelo o consumidor não tem acesso à infraestrutura da nuvem, podendo, no máximo, passar alguns parâmetros para o funcionamento da aplicação. Um famoso exemplo é o Skype;

- ***PaaS - Platform as a Service*:** É oferecida ao consumidor uma plataforma com um conjunto de ferramentas. Assim como no *SaaS*, o consumidor não tem acesso à infraestrutura da nuvem;

- ***IaaS - Infrastructure as a Service*:** A infraestrutura – servidores, dispositivos de armazenamento, entre outros – é contratada como serviço, sendo o contratante apto a executar os serviços que tiver direito, de acordo com o contrato. Assim como no *SaaS* e no *PaaS*, o consumidor não tem acesso à infraestrutura da nuvem;

2.3 Gerenciamento de Identidades

Nesta seção serão apresentados os conceitos gerais de Gerenciamento de Identidades, seus tipos de modelos e sistemas, além das abordagens de implantação de *Single Sign On (SSO)*, que serão de fundamental importância para o entendimento deste trabalho.

2.3.1 Conceitos gerais

Chama-se gerenciamento de identidades um conjunto de funções, como gerência e trânsito de informações, que visam garantir a identidade de uma entidade e as informações nela contidas, permitindo que relações possam ocorrer de forma segura. Ao passo que uma pessoa escolhe quais informações suas serão reveladas ao mundo real, no mundo virtual esta operação é realizada por um sistema de gerenciamento de identidades [6]. A identidade é uma composição de partes menores, chamadas de identidades parciais. Algumas identidades parciais podem identificar uma entidade de maneira unívoca (um RG, por exemplo), outras não (a idade, por exemplo).

2.3.2 Sistemas de Gerenciamento de Identidades

Um sistema de gerenciamento de identidades é aquele responsável pela gerência das identidades parciais, e se baseia nas políticas e processos do ambiente no qual está inserido, tendo como resultado um subsistema de autenticação que trabalha de modo conjunto com um subsistema de gerenciamento de atributos. Em [4], o sistema de gerenciamento de identidades são elencadas as seguintes características que identificam um sistema de gerenciamento de identidades:

- **Usuário:** Interessado em acessar o recurso;
- **Identidade:** Valores que identificam o usuário;
- **Provedor de Identidades (*Identity Provider – IdP*):** Servidor responsável por emitir e validar a identidade de um usuário;

- **Provedor de Serviços (*Service Provider – SP*):** Servidor responsável por prover serviços a um usuário devidamente autenticado por um Provedor de Identidades;

2.3.3 Modelos de Gerenciamento de Identidades

Em [4, 15], os sistemas de gerenciamento de identidades são divididos em quatro categorias: tradicional, centralizado, federado e centrado no usuário. A Figura 2.5 ilustra cada modelo e estes serão descritos em detalhes a seguir.

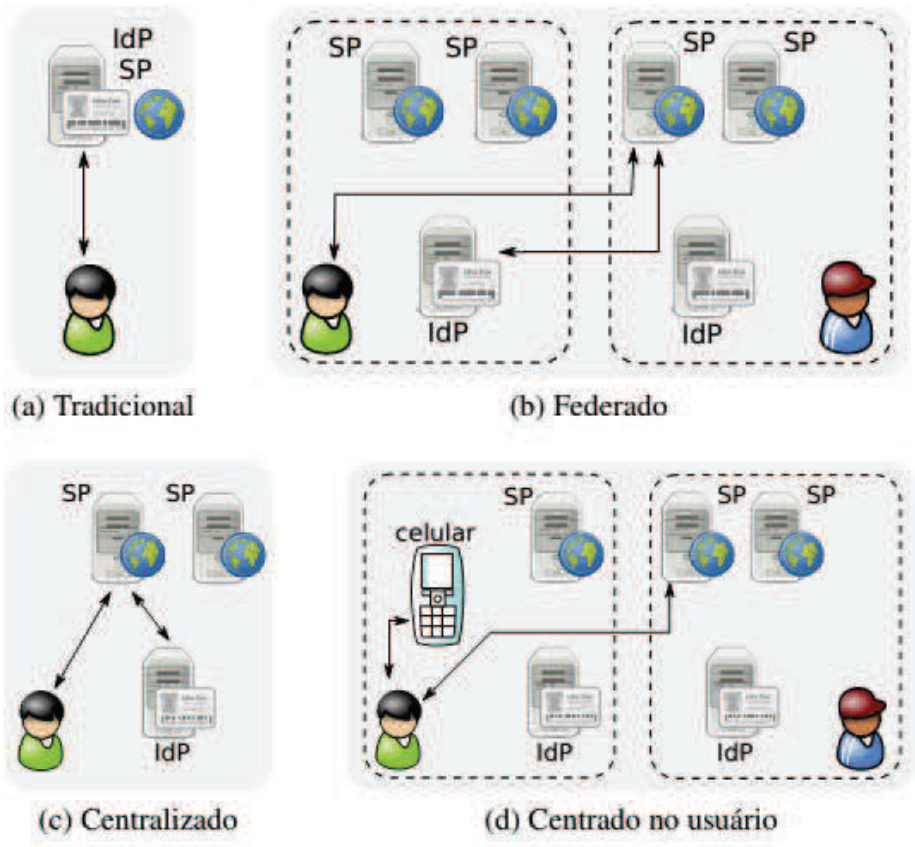

Figura 2.5: Modelos de Gerenciamento de Identidades. [42]

O ***modelo tradicional*** é o modelo mais usado atualmente na Internet: Nesse modelo, a identidade do cliente é tratada isoladamente por cada Provedor de Identidades (o qual atua também como Provedor de Serviços, como é possível ver na Figura 2.5a). Além disso, o cliente deve possuir uma identidade para cada Provedor de Serviços que queira acesssar. O uso do modelo tradicional tende a ter alto custo, tanto para os usuários, quanto para os mantenedores dos servidores: cada um dos Provedores de Serviços pode exigir um conjunto próprio de atributos para compor

a identidade digital do usuário, mas o grande problema deste modelo é que outros provedores podem fazer o mesmo, obrigando o cliente a manter várias contas, o que pode inviabilizar o seu uso. [8].

O ***modelo centralizado*** foi implementado para trazer a flexibilidade que o modelo tradicional não consegue prover, baseando-se em dois conceitos: compartilhamento das identidades entre SP's e autenticação única (*Single Sign-on – SSO*) [4]. No modelo centralizado, só existe um Provedor de Identidades responsável pela autenticação dos clientes, fornecendo aos Provedores de Serviços informações que todos os SP's devem confiar (ver Figura 2.5c). Já na autenticação única (*SSO*) há uma vantagem aos clientes: eles só precisam efetuar o *login* uma vez e, daí em diante, usufruir das credenciais emitidas pelos Provedores de Serviço. Finalmente, de acordo com [40], este modelo tem uma desvantagem: é dado ao Provedor de Identidades um controle altíssimo sobre as informações do usuário, podendo usá-las de maneira inapropriada.

O ***modelo federado*** visa melhorar a maneira na qual são feitas as troca de informações relativas às identidades através de relações de confiabilidade estabelecidas nas federações [5]. Nesse modelo, identidades emitidas em um domínio são consideradas aceitáveis por Provedores de Serviços de outros domínios e o conceito de autenticação única é assegurado. Dessa forma, o modelo federado evita que os clientes tenham que lidar com várias identidades diferentes e autenticar-se várias vezes, desnecessariamente.

O ***modelo centrado no usuário*** visa permitir que o cliente tenha total controle sobre suas credenciais. Além disso, o que torna esse modelo ainda mais diferenciado é que ele implementa partes dos outros modelos já anteriormente citados. Um exemplo: na proposta de [15], as identidades, destinadas a diferentes Provedores de Serviços, são armazenadas em um dispositivo de armazenamento, que fica em posse do próprio cliente. (ver Figura 2.5d).

2.4 *SAML*

Security Assertion Markup Language (*SAML*) é uma especificação baseada em XML que define uma infraestrutura para troca de credenciais e informações de

usuário, permissões e atributos na federação. A entidade responsável pelo *SAML* é o *Security Services Technical Committee* (*SSTC*), membro integrante da *Organization for the Advancement of Structured Information Standard* (*OASIS*). *SAML* apresenta informações em forma de ***asserções***, estruturadas em arquivos do tipo *XML*.

2.4.1 Componentes *SAML*

A especificação *SAML* é formada por diversos componentes, protocolos e categorias de ligações para estabelecimento de ligações entre entidades da federação [27].

SAML elenca alguns tipos de declarações possíveis para uma entidade *SAML* qualquer. Estes tipos serão definidos a seguir.

Originada de uma entidade declarante (*asserting party*), uma **asserção** baseia-se em uma requisição feita por uma entidade confiável (*relying party*). Ela é composta basicamente por informações como a entidade remetente da asserção, informações sobre validação da asserção, entre outros. Uma asserção em geral tem contidas em si três tipos de informações:

- **Autenticação:** Geradas pela autoridade autenticadora. Possui informações acerca de data, hora e método da autenticação;
- **Atributos:** Contém informações específicas do usuário;
- **Decisão de autorização:** Especifica as permissões do usuário dentro da federação;

Os **protocolos** são conjuntos de solicitações e respostas geralmente usadas pelos Provedores de Serviços. As **ligações** *SAML* são usadas pelos protocolos para transporte de mensagens entre as entidades da federação usando padrões de comunicação pré-definidos pelo sistema.

Os **perfis** *SAML* permitem que as asserções e protocolos trabalhem em um fluxo de informações. Isto é útil para promover o gerenciamento de identidades e o *Single Sign-On*. Há um subtipo de perfil, chamado **perfil de atributos**, que define como serão feitas as transmissões dos atributos nas asserções.

2.5 *Shibboleth*

O *Shibboleth* é um *middleware* que visa estabelecer uma estrutura que torne o gerenciamento de identidades de um certo grupo de usuários cadastrados mais simples. O projeto Shibboleth [34] foi uma iniciativa do consórcio *Internet2*, tendo como principal objetivo lançar uma implementação *opensource* para tratar situações que envolvam o gerenciamento de identidades e o controle de acesso em instituições acadêmicas. Hoje, o *Shibboleth* está em sua segunda versão, liberada no ano de 2008: O Provedor de Serviços encontra-se na versão 2.5.3, e o Provedor de Identidades na versão 2.4.0;

O *Shibboleth* foi obra de uma iniciativa do *Internet2* e do *MACE* (*Middleware Architecture Committee for Education*), em conjunto com 200 universidades americanas e européias, e indústrias e governo para desenvolver e distribuir aplicações de rede. O *Shibboleth* está fundamentado sobre padrões abertos como a *XML* e a *SAML* (*Security Assertion Markup Language*) e facilita que aplicações *web* usufruam das facilidades providas pelo modelo federado, sobretudo o conceito de autenticação única e a troca segura de atributos de usuários.

Dentro de um domínio *Shibboleth* são encontrados dois componentes principais, que são os já citados Provedor de identidades (*IdP*) e Provedor de Serviços (*SP*). Ambos os componentes implementam o *heap* de software fornecido *Shibboleth*, permitindo que haja o transporte das credenciais dos clientes do IdP ao SP [34]. No *Shibboleth*, a autenticação é executada na **instituição de origem do usuário**, através do *IdP*, fazendo uso dos mecanismos de autenticação preconizados pela instituição. Essa autenticação pode ser feita por vários métodos: nome de usuário e senha, *LDAP*, *X.509*, entre outros [6].

Quando é feita uma tentativa de acesso a um recurso abrigado por um SP, o cliente é redirecionado para o *WAYF* (*Where Are You From*, também chamado de **Servidor de Descoberta**), que é um servidor distinto do *SP* e do *IdP*, responsável por perguntar ao usuário qual instituição ele deseja acessar(em termos de federação de identidades, ele pergunta para o cliente em qual *IdP* ele deseja efetuar *login*). Depois de permitir a autenticação, o *IdP* irá gerar uma referência à autenticação e irá enviá-la para o *SP*.

A Figura 2.6 abaixo apresenta o fluxo de mensagens efetuado entre o Provedor de Serviços, de Identidades e o Servidor de Descoberta quando um cliente solicita um serviço ao Provedor de Serviços [11]:

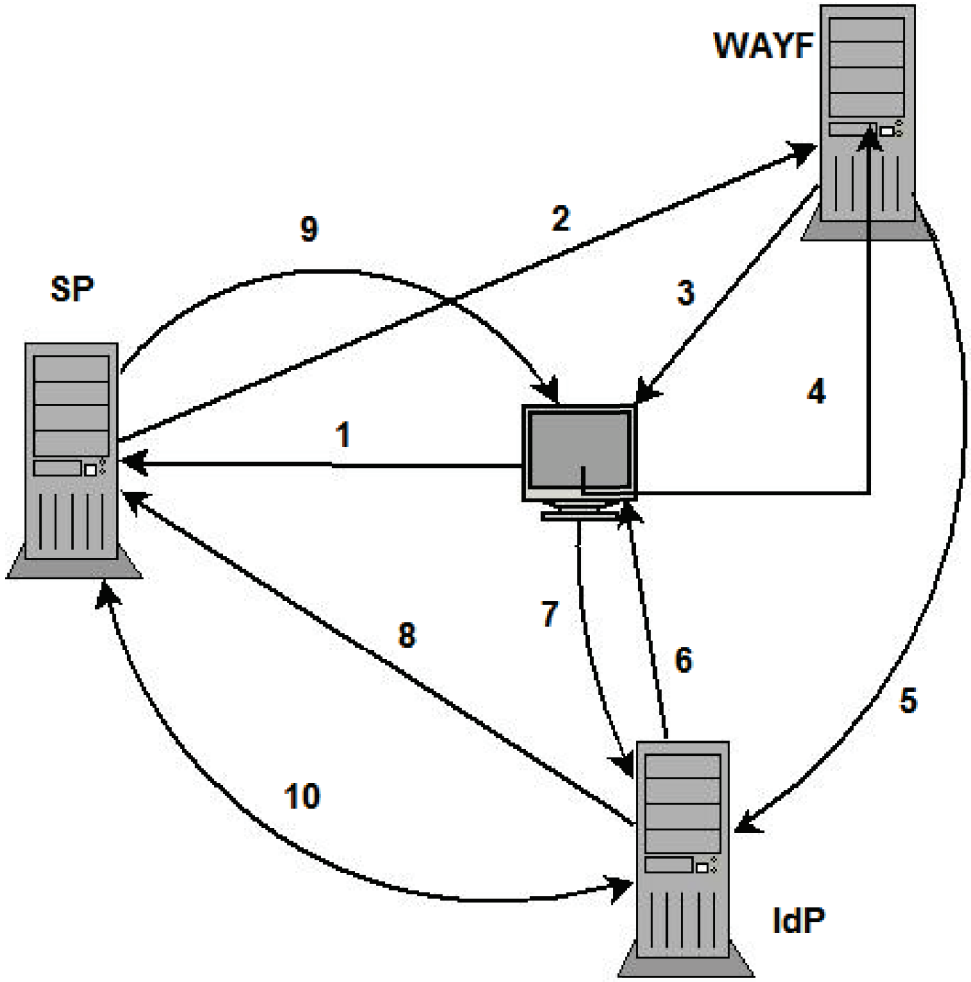

Figura 2.6: Fluxo de mensagens no *Shibboleth*. Adaptado de [9]

- **Passo 1:** O cliente através do seu *browser* solicita um serviço hospedado no Provedor de Serviços;
- **Passo 2:** O *SP* recebe a requisição e redireciona o *browser* para a tela inicial do Servidor de Descoberta;
- **Passo 3:** Nesta tela inicial, o *DS* apresenta ao cliente a lista de *IdP*'s disponíveis na federação;
- **Passo 4:** O usuário seleciona o *IdP* desejado;

- **Passo 5:** O Servidor de Descoberta atualiza os *cookies* responsáveis pela autenticação e redireciona o *browser* do usuário para a tela de login do *IdP* selecionado;

- **Passo 6:** O serviço de *Single Sign-On* é requisitado no *IdP* e ele adquire uma asserção *SAML* da Autoridade Autenticadora, e a gera para o *browser* do cliente;

- **Passo 7:** As credenciais do cliente (nome e senha, por exemplo), são fornecidas para o IdP de origem através de um método de requisição *HTTP POST*;

- **Passo 8:** Ocorre a autenticação de fato do cliente no *IdP*. Após isso, é retornada para o *browser* uma asserção, e o módulo consumidor de asserções do Provedor de Serviços processa o recebimento da resposta do pedido de *login*;

- **Passo 9:** Opcionalmente, o *SP* pede os atributos do *IdP*;

- **Passo 10:** O IdP retorna os atributos solicitados no passo anterior;

3 Estudo de Caso

Este capítulo descreve os experimentos realizados para implementação da Federação *Shibboleth*, em um ambiente de Computação em Nuvem.

3.1 Ambiente e Implementação

O ambiente usado para a realização do experimento é composto por um *SP Shibboleth*, um *IdP Shibboleth* e um Serviço de Descoberta *Switch AAI*.

Todos os componentes da Federação: o *SP Shibboleth*, o *IdP Shibboleth* e o *Discovery Service* são compostos, cada um, por uma máquina virtual com 1GB de RAM, processador Intel® Core™ i5 de 2,67 GHz e sistema Linux Ubuntu Server 12.04 LTS, sendo executadas no software *Eucalyptus*, responsável pela gerência do ambiente de nuvem. O computador hospedeiro está instalado no Laboratório de Sistemas de Arquiteturas Computacionais (*LABSAC*), do Departamento de Engenharia Elétrica da Universidade Federal do Maranhão.

3.1.1 Implementação do Provedor de Serviços

Para a realização de testes e demonstrações, primeiramente foi implantado um Provedor de Serviços em nuvem. O resultado foi a implantação de um servidor *Apache* sobre uma máquina virtual com o *software Eucalyptus*. Neste servidor, além da instalação do *SP Shibboleth*, uma pequena página HTML foi escolhida para servir de exemplo de recurso a ser oferecido como serviço. Um teste inicial do processo autenticação foi realizado com o uso da ferramenta *TestShib*, que fornece um *IdP* próprio para se testar instalações do *Shibboleth*. A seguir uma página *HTML* foi instalada e configurada para ser hospedada pelo *Shibboleth*. Finalmente, o SP foi configurado para ter uma relação de confiança com o Provedor de Identidades criado para o trabalho. Como resultado, a página hospedada pelo *SP* na nuvem é acessada pelo usuário quando ele acessa sua *URL* e o *Shibboleth* redireciona o acesso para o

Provedor de Identidades, onde ocorre a autenticação e o retorno uma asserção *SAML* com o resultado.

3.1.2 Implementação do Provedor de Identidade

O *IdP* deste trabalho visa obter a privacidade dos usuários da nuvem. Em um contexto mais amplo, o trabalho descrito tem como intuito a utilização de um recurso qualquer que englobe um provedor de identidades com uma camada de proteção à privacidade.

No cenário proposto, o usuário interessado no serviço hospedado e protegido acessa primeiramente o Provedor de Serviços. O Provedor de Serviços então o redireciona para seu respectivo Provedor de Identidades. O *IdP* está executando em um ambiente de nuvem, de maneira transparente ao usuário; ele, então, pede a autenticação do usuário e acessa seus atributos em sua base de dados de usuários. A instalação da aplicação do Provedor de Identidades começou com a infraestrutura que seria utilizada e foi necessário primeiramente definir o serviço de nuvem em que ele estaria disponível. A página *HTML* de teste deveria utilizar uma Infraestrutura como um Serviço (*IaaS*). Depois foram instalados aplicativos, serviços e módulos cuja presença no sistema é imperativa para o correto funcionamento do *IdP Shibboleth*, enumerados a seguir:

- ***OpenJDK Runtime Enviroment***, versão 1.6.0.27;
- Servidor de aplicações ***Apache Tomcat 6.0.22***, no qual deveriam ser executadas os recursos de autenticação;
- ***OpenLDAP***, o responsável por armazenar as informações do usuário. O IdP *Shibboleth* consulta ele através das suas configurações;
- ***uApprove***, que é um *plugin* de privacidade para o *Shibboleth* desenvolvido pela rede de universidades suíças *SWITCH*, para uso em sua federação acadêmica, a *SWITCHaai*. A versão 2.2.1 foi utilizada neste trabalho;
- ***Banco de dados MySQL***, exigido para o funcionamento do *uApprove*. A versão usada foi a 5.5;

3.1.3 Implementação do *WAYF*

Implementado na linguagem *PHP* e desenvolvido pela rede de universidades suíças *SWITCH*, o objetivo principal do *Where Are You From* (*WAYF*) deste trabalho é enviar um usuário qualquer para o *IdP* da sua organização. O *WAYF* também é chamado de *Discovery Service*, que é a especificação *SAML* que implementa o protocolo do *Discovery Service*. Em suma, o WAYF/DS apresentar ao usuário a uma lista de organizações e redirecionar o browser do usuário para o IdP, ou mesmo voltar para o SP acessado.

3.2 Resultados finais

O resultado da implantação dos Provedores de Identidades e Serviço, juntamente com o Servidor de Descoberta, todos sendo executados em ambiente de nuvem, é representado pela Figura 3.1.

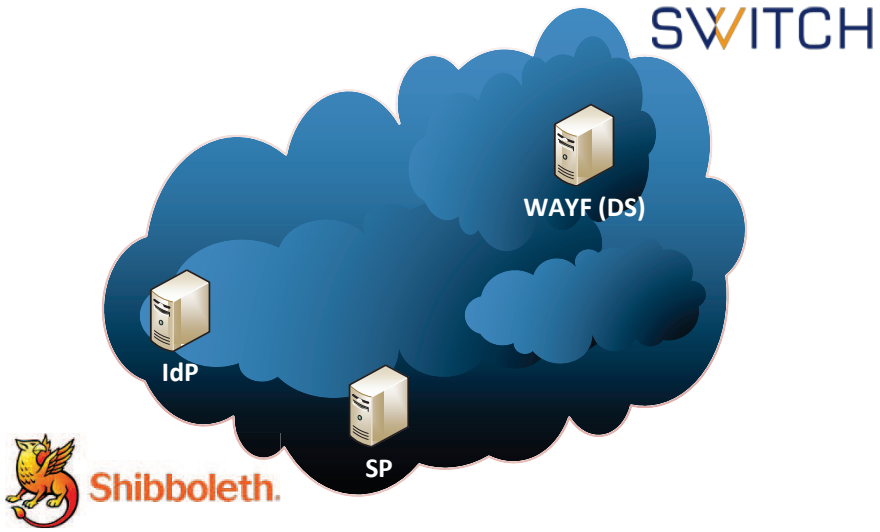

Figura 3.1: Cenário da Federação Shibboleth em Ambiente de Nuvem

Abaixo se encontram capturas de tela que demonstram o sistema em funcionamento:

Figura 3.2: Tela de login do *IdP Shibboleth*

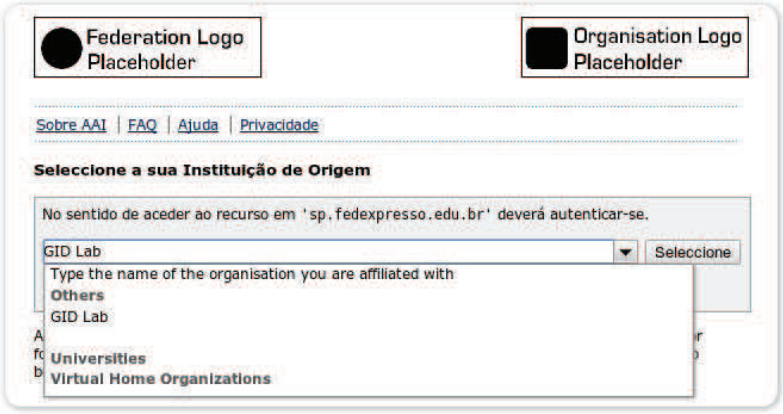

Figura 3.3: Tela inicial do *WAYF*

Figura 3.4: Tela com a homologação de atributos do cliente

Uma vez o cenário implantado, obteve-se o resultado descrito a seguir.

3.2.1 Acesso de serviços hospedados

Não há a possibilidade de acesso somente leitura, ou seja, através de usuário anônimo(o que comprometeria a segurança da nuvem). Para realizar este tipo de acesso, basta que o usuário digite o *URL* do serviço desejado em seu navegador web. Neste caso, o serviço só estará disponível para usuário internos à federação. O processo *mod_shib* verifica que o usuário não está logado e o encaminha para o Serviço de Descoberta (*WAYF*) da federação da qual é membro, onde o usuário escolhe a sua respectiva e é encaminhado para a *URL* do Provedor de Identidades (*IdP*), da instituição, sendo efetuado após isso um redirecionamento HTTP. Na *homepage* do Provedor de Identidade, o cliente insere suas credenciais (nome e senha) e caso bem-sucedido, *cookies* são emitidos e um *handle* – uma asserção *SAML* com as informações relativas à autenticação – é criado, sendo ligada de maneira unívoca ao cliente logado.

4 Conclusão

A expansão da Internet, como ambiente de transações entre entidades, que envolvem os mais diversificados tipos de conteúdo, trouxe à tona a óbvia necessidade da identificação das entidades em rede. A noção da importância da Gestão de Identidades Federadas tem aumentado consideravelmente nos últimos anos, e diz respeito às tecnologias e recursos que permitem que um cliente interaja e tenha acesso a múltiplos serviços com uma simples conta, um par de valores: usuário e senha. O principal recurso dessa gestão é a autenticação única, ou *Single Sign-On*, que possibilita ao cliente uma autenticação para vários serviços protegidos em domínios diferentes. [16].

Neste trabalho foi abordado o modelo federado, através de implementação no *middleware Shibboleth*. Este modelo permite a descentralização dos Provedores de Identidade em relação aos Provedores de Serviço, o que torna mais fácil o gerenciamento da infraestrutura dos provedores, para os administradores do sistema, e provê o uso de uma conta apenas, para diversos domínios, facilitando assim para os usuários. Neste modelo federado, a especificação mais abordada é o *SAML*, que define como serão feitas as relações entre cliente e servidores. Além ser exposta no trabalho a especificação mais usada, é também abordado o *middleware* de maior uso comercial e educacional, o *Shibboleth*.

Conclui-se, portanto, que a Gestão de Identidades é uma área do conhecimento com bastantes atualizações e mudanças, por isso bastante complexa. Por este motivo, nota-se que pesquisas que envolvam Gestão de Identidades, Identidades Federadas e Computação em Nuvem demandam um considerável conhecimento teórico e técnico do pesquisador.

4.1 Avaliação do trabalho

O objetivo deste trabalho era implantar um federação *Shibboleth*, um ambiente virtual que implemente a Gestão de Identidades em uma organização. Do

proposto entre os objetivos do trabalho, todas as atividades foram realizadas de maneira bem-sucedida. De maneira geral, a implantação da federação foi considerada realizada em sua plenitude: o ambiente, composto por um Provedor de Identidades, um Provedor de Serviços e um Serviço de Descoberta, além do usuário criado para os testes de autorização da liberação dos atributos solicitados pelo *SP* ao *IdP*, pela ferramenta *uApprove*. Ao final do processo, as máquinas foram disponibilizadas em um servidor local, para disposição de eventuais futuros pesquisadores do assunto.

4.2 Trabalhos futuros

Para trabalhos futuros, há algumas sugestões: a implantação *IdP+*, que nada mais é que um *IdP* que efetua a tradução das credenciais de segurança, permitindo a geração de certificados do tipo *X.509* e e que aplicações que não sejam desenvolvidas para interfaces *Web* sejam hospedadas em um Provedor de Serviços *Shibboleth*.

Outra sugestão refere-se ao **Serviço Gerador de Certificados** (***SGC***) que permite que credenciais *Shibboleth* sejam traduzidas para certificados digitais, que podem ser utilizados em operações que demandem o uso desses certificados. Outra abordagem futura refere-se à interoperabilidade entre o *Shibboleth* e outras tecnologias e *middlewares* de Gestão de Identidades, como *OpenID*, *SimpleSAMLphp*, *OpenAM*, entre outros que podem ou não implementar o padrão SAML usado pelo *Shibboleth*.

Referências Bibliográficas

[1] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. Ben Othmane, and L. Lilien. An entity-centric approach for privacy and identity management in cloud computing. In *Reliable Distributed Systems, 2010 29th IEEE Symposium on*, pages 177–183. IEEE, 2010.

[2] Associação Brasileira de Normas Técnicas (ABNT). *NBR ISO/IEC 27002:2013. Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação*.

[3] E. Bertino and K. Takahashi. *Identity Management: Concepts, Technologies, and Systems*. Artech House, 2010.

[4] A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer. User centricity: a taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527, 2007.

[5] J. Camenisch and B. Pfitzmann. Federated identity management. In *Security, Privacy, and Trust in Modern Data Management*, pages 213–238. Springer, 2007.

[6] D. W. Chadwick. Federated identity management. In *Foundations of Security Analysis and Design V*, pages 96–120. Springer, 2009.

[7] S. A. de Chaves, R. B. Uriarte, and C. B. Westphall. Implantando e monitorando uma nuvem privada. In *VIII Workshop em Clouds, Grids e Aplicaç oes*, 2010.

[8] E. R. de Mello. *Um modelo para confiança dinâmica em ambientes orientados a serviço*. PhD thesis, Universidade Federal de Santa Catarina, 2009.

[9] M. C. de Souza. *Implantação de uma Comunidade Acadêmica Federada para Experimentação usando Framework Shibboleth*, jul 2014.

[10] DICIONÁRIO MICHAELIS. Disponível em http://michaelis.uol.com.br, Acesso em 12-12-2013.

[11] G. Feliciano, L. Agostinho, E. Guimarães, and E. Cardozo. Gerência de identidades federadas em nuvens: Enfoque na utilização de soluções abertas. *Short course, XI SBSeg, Brazil*, 2011.

[12] B. Grobauer, T. Walloschek, and E. Stocker. Understanding cloud computing vulnerabilities. *Security & Privacy, IEEE*, 9(2):50–57, 2011.

[13] International Data Corporation (IDC). Disponível em http://www.idc.com/, Acesso em 12-12-2013.

[14] International Data Corporation (IDC). *New IDC IT Cloud Services Survey: Top Benefits and Challenges*. Disponível em http://blogs.idc.com/ie/?p=730, Acesso em 12-12-2013.

[15] A. Jøsang and S. Pope. User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference*, page 77. Citeseer, 2005.

[16] J. Kallela. Federated identity management solutions. Technical report, Technical report, Helsinki University of Techn ology. http://www. cse. tkk. fi/en/publications/B/1/papers/Kallela_final. pdf, 2008.

[17] U. Lampe, O. Wenge, A. Müller, and R. Schaarschmidt. On the relevance of security risks for cloud adoption in the financial industry. 2013.

[18] C. E. Landwehr. Computer security. *International Journal of Information Security*, 1, 2003.

[19] A. M. Lonea, H. Tianfield, and D. E. Popescu. Identity management for cloud computing. In *New Concepts and Applications in Soft Computing*, pages 175–199. Springer, 2013.

[20] F. P. Marzullo. *SOA na Prática: inovando seu negócio por meio de soluções orientadas a serviços*. NOVATEC, 2009.

[21] U. Maurer. Information security (part i). 2013. Disponível em http://people.ee.ethz.ch/ lamy/pdfs/infsec2013-lecture-notes.pdf, Acesso em 22-12-2013.

[22] P. M. Mell and T. Grance. Sp 800-145. the nist definition of cloud computing. Technical report, Gaithersburg, MD, United States, 2011.

[23] R. T. Michael T. Goodrich. *Introdução à Segurança de Computadores*. Bookman, 2013.

[24] M. A. E. Nagano and R. K. Yokoo. Gestão de segurança: proteção da informação e do patrimônio empresarial. 2013.

[25] E. T. NAKAMURA. Geus, paulo lício de. *Segurança de redes em ambientes cooperativos*, 2007.

[26] V. Nicomette. *La protection dans les systèmes à objets répartis*. PhD thesis, Institut National Polytechnique de Toulouse-INPT, 1996.

[27] OASIS. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, 2008. Disponível em https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf, Acesso em 07-07-2014.

[28] S. Pearson and G. Yee. *Privacy and security for cloud computing*. Springer, 2013.

[29] I. Ray and I. Ray. Trust-based access control for secure cloud computing. In *High Performance Cloud Auditing and Applications*, pages 189–213. Springer, 2014.

[30] C. Rong, S. T. Nguyen, and M. G. Jaatun. Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, 39(1):47–54, 2013.

[31] S. Ruj, M. Stojmenovic, and A. Nayak. Privacy preserving access control with authentication for securing data in clouds. In *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*, pages 556–563. IEEE, 2012.

[32] A. Saldhana, A. Nadalin, and M. Rutkowski. Identity in the cloud use cases version 1.0, 2012.

[33] B. Schneir. Applied cryptography. *John Wiley & Sons*, 1996.

[34] Shibboleth Architeture. Disponível em https://open-systems.ufl.edu/files/draft-mace-shibboleth-tech-overview-latest.pdf, Acesso em 07-07-2014.

[35] B. Sosinsky. *Cloud Computing Bible*. Wiley Publishing, 1st edition, 2011.

[36] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2013.

[37] H. Takabi, J. B. Joshi, and G.-J. Ahn. Security and privacy challenges in cloud computing environments. *Security & Privacy, IEEE*, 8(6):24–31, 2010.

[38] A. S. Tanenbaum. *Sistemas operacionais modernos*. Prentice- Hall, São Paulo, 3 edition, 2010.

[39] A. Tassanaviboon and G. Gong. Oauth and abe based authorization in semi-trusted cloud computing: aauth. In *Proceedings of the second international workshop on Data intensive computing in the clouds*, pages 41–50. ACM, 2011.

[40] J.-M. S. Tewfiq El Maliki. A survey of user-centric identity management technologies. *SECUREWARE'07: Proceedings of the The International Conference on Emerging Security Information, Systems, and Technologies*, pages 12–17, 2007.

[41] M. Veras. *Arquitetura de Nuvem - Amazon Web Services (AWS)*, volume 1293.6. 1 edition, 2013.

[42] M. S. Wangham, E. R. de Mello, D. da Silva Böger, M. Guerios, and J. da Silva Fraga. Gerenciamento de identidades federadas. *Minicurso-SBSeg 2010-Fortaleza-CE*, 2010.

[43] P. Yadav, P. Mishra, T. Sharma, and V. Sharma. Security issues in cloud computing and associated mitigation techniques. *International Journal of Innovative Research and Development*, 2013.

[44] R. Yogamangalam and V. S. Sriram. A review on security issues in cloud computing. *Journal of Artificial Intelligence*, 6, 2012.

[45] M. Y. A. Younis and K. Kifayat. Secure cloud computing for critical infrastructure: A survey. *Liverpool John Moores University, United Kingdom, Tech. Rep*, 2013.

[46] D. M. Yuri Diogenes. *Certificação Security+ — Da Prática Para o Exame SY0-301*. Number 9788561893194. 2 edition, 2013.

[47] Q. Zhang, L. Cheng, and R. Boutaba. Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1):7–18, 2010.