UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

Jonathan Iury Araújo dos Santos

Federação de Identidades em Ambiente de Computação em Nuvem com Simple-SAML

São Luís - MA
2014

Jonathan Iury Araújo dos Santos

Federação de Identidades em Ambiente de Computação em Nuvem com Simple-SAML

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

Orientador: Prof. Zair Abdelouahab

Ph.D em Ciência da Computação

São Luís - MA

2014

Santos, Jonathan Iury Araujo dos

Federação de Identidades em Ambiente de Computação em Nuvem com Simple-SAML / Jonathan Santos. – São Luís – MA, 2015.

12 f.

Orientador: Zair Abdelouahab

Monografia (Graduação) – Universidade Federal do Maranhão, Curso de Ciência da Computação, 2015.

1. Autenticação - Segurança. 2. Computação em Nuvem. 3. Computação Móvel I. Abdelouahab, Zair, orient. II. Título.

CDU 004-773.3

Jonathan Iury Araújo dos Santos

Federação de Identidades em Ambiente de Computação em Nuvem com Simple-SAML

Aprovada em 24 de julho de 2015

ASSINATURAS

Prof. Zair Abdelouahab (orientador)

Ph.D em Ciência da Computação

Jonathan Iury Araújo dos Santos

Aluno

Vicente Leonardo Paucar Casas

Ph.D em Engenharia Elétrica

Wagner Elvio de Loiola Costa

Mestrado em Ciência da Computação

Glossário

CSA Cloud Security Alliance. 21, 23, 24

ENISA European Network and Information Security Agency. 23

IaaS Infraestrutura como Serviço. 18

IDC International Data Corporation. 21

NIST National Institute of Standards and Technology. 23

PaaS Platforma como Serviço. 18

SaaS Software como Serviço. 18, 25

SAML Security Assertion Markup Language. 20

SSO Single Sign On. 19, 26

Lista de Figuras

Sumário

RESUMO

Aplicações de Computação em Nuvem estão vulneráveis a ameaças de segurança oriundas da Internet, por conta do compartilhamento de recursos com outros usuários e gerenciados por terceiros. As identidades de usuários fornecidas para as aplicações podem ser do tipo usuário/senha, certificados digitais, *tokens*, biometria, cartões, entre outros. Visando ao tratamento e manipulação de identidades de usuários, foram desenvolvidas sistemas de gerenciamento de identidades (SGI), e como exemplo de soluções que proveem o gerenciamento de identidades, tem-se o *Simple-SAML*, os *frameworks* do *Liberty Alliance, OpenID e o Microsoft CardSpace*. A implantação de um SGI geralmente envolve a instalação de um *middleware* que ficará responsável pelos serviços de identidade autenticação, autorização, entre outros) [4]. A diversidade de serviços e tecnologias se apresenta ainda como desafio para integração de identidades e dados de usuários no contexto distribuído. Para lidar com essas questões, técnicas de gerenciamento de identidades, especialmente as que utilizam a abordagem federada, se mostram fundamentais para proteger as informações de acessos não autorizados e permitir o intercâmbio de recursos entre as diferentes partes confiáveis entre si. O intuito proposto deste trabalho é desenvolver um modelo que permita a integração entre o SGI SimpleSAML por meio do protocolo Security Assertion Markup Language (SAML), com a finalidade de prover o acesso a aplicações na Computação em Nuvem.

Palavras-chave

Segurança da Informação;
Computação em Nuvem;
Sistemas de Gerenciamento de Identidades;

ABSTRACT

Computer Applications in Cloud are vulnerable to threats security arising from the Internet, sharing resources account with other users and management by third parties. The identities of users provided for applications can be of *user/password, digital certificates, tokens, biometrics, cards, among others*. Aiming to treatment and handling of user identities,have been developed, and as an example of solutions that provide identity management, there is the *Simple-SAML*, the *frameworks of Liberty Alliance, OpenID and Microsoft CardSpace*. The implementation of an SGI usually involves the installation of a *middleware* that will be responsible for identity services, authorization, etc.) [4]. The diversity of services and technologies also presents a challenge for integration of identities and user data in context. To address these issues, management techniques, especially those that utilize the federated approach, show essential to protect the information from unauthorized access and allow the exchange of resources among different trusted parties together. The purpose of this proposed work is to develop a model that allows the integration between SGI SimpleSAML through the Security Assertion Markup Language protocol (SAML), with the purpose of providing access to applications in cloud computing.

Keywords

Information security;
Cloud Computing;
of Identity Management Systems;

Agradecimentos

Gostaria de manifestar minha gratidão ao meu orientador e mentor Prof. Ph.D. Zair Abdelouahab pela oportunidade e chance de me acolher como aluno fornecendo-me condições para superar os desafios encontrados durante minha trajetória de vida acadêmica e me permitindo alcançar mais superar desafiar e este sonho de me formar e crescer em conhecimento tanto na minha profissão como pessoa. Um grande educador que pela oportunidade a mim concedida, me enriqueceu e conselhou-me ao longo deste trabalho. A este, exprimo a viva e humilde gratidão, pois sem este nada disso seria possível. A minha esposa querida e ao meu filho que foram de estimulo crucial para esta vitória em minha vida. Aos meus pais que sempre me motivaram para terminar este curso e a minha irmã Berthiê que sempre me considerou um "hacker"nos computadores. Aos meus queridos colegas e amigos do Laboratório de Sistemas em Arquiteturas Computacionais (LABSAC) da UFMA, pelo essencial apoio a esta pesquisa e pelas alegrias partilhadas. Obrigado Willian “Cloudman”, Higo Felipe, Mário Henrique, Bruno, Cláudio, Renato e Wagner.

1 Introdução

Pesquisadores como [13, 19, 24] definem a computação em nuvem como um modelo onde os usuários tem acesso sob demanda a um conjunto de recursos computacionais compartilhados e configuráveis, tais como redes, armazenamento, serviços ou aplicações que podem ser rapidamente provisionados e liberados com um mínimo de esforço de gerenciamento, utilizando a Web por meio de qualquer dispositivo (celulares, *tablets, notebooks*, etc).

Um provedor de computação em nuvem pode utilizar um ou mais modelos para a oferta de serviços tais como Infraestrutura como Serviço (*IaaS*), Plataforma como Serviço (*PaaS*) ou Software como Serviço (*SaaS*). No *IaaS*, o consumidor contrata uma infraestrutura de hardware podendo escolher a capacidade de configuração (ex.CPU, memória, discos), sistema operacional (ex.*Linux, Windows*) e quaisquer softwares - tipo de serviço oferecido, por exemplo, pela *Amazon* [1]. No *PaaS*, o consumidor contrata uma plataforma com um conjunto de ferramentas específicas para sua necessidade, como por exemplo linguagens de programação como um tipo de serviço oferecido pela *Google Apps*. E no *SaaS*, o consumidor contrata a utilização de uma aplicação hospedada em um ambiente de computação em nuvem, como o *Gmail*.

De acordo com [7, 20], a segurança é importante para garantir o sucesso também em ambientes de nuvem, e [15] destaca a proteção à privacidade, já que dados sensíveis passam a ficar sob a custódia de terceiros. Nesse contexto, o gerenciamento de identidades cresce em importância conforme crescem os serviços que precisam utilizar autenticação e controle de acesso de usuários [2,4]. Esta situação não é singular e corre em muitos serviços que são operados em ambientes de nuvem e precisam estabelecer a identidade de seus usuários ao mesmo tempo em que devem proteger sua privacidade.

As identidades de usuários fornecidas para as aplicações podem ser do tipo usuário/senha, certificados digitais, *tokens*, biometria, cartões, entre outros.

Visando ao tratamento e manipulação de identidades de usuários, foram desenvolvidas sistemas de gerenciamento de identidades (SGI), e como exemplo de

soluções que proveem o gerenciamento de identidades, tem-se o *Simple-SAML*, os *frameworks* do *Liberty Alliance, OpenID e o Microsoft CardSpace*. A implantação de um SGI geralmente envolve a instalação de um *middleware* que ficará responsável pelos serviços de identidade autenticação, autorização, entre outros) [4].

1.1 Motivação

Empresas tem interesse em mudar sua infraestrutura para modelos de computação em nuvem (*IaaS, PaaS, SaaS*). Entretanto, há um receio de adotar estes modelos devido aos riscos de segurança dentro do ambiente de computação em nuvem.

Em 2009, uma pesquisa do *International Data Corporation (IDC)* [8] com 244 executivos de TI investigou qual o aspecto mais preocupante quanto ao uso de serviços de computação em nuvens. Os resultados mostraram que 87,5% das pessoas entrevistadas preocupam-se com a segurança, apontando esta como uma das principais barreiras para adoção da computação em nuvem. A Figura 1.1 a seguir demonstra esses resultados.

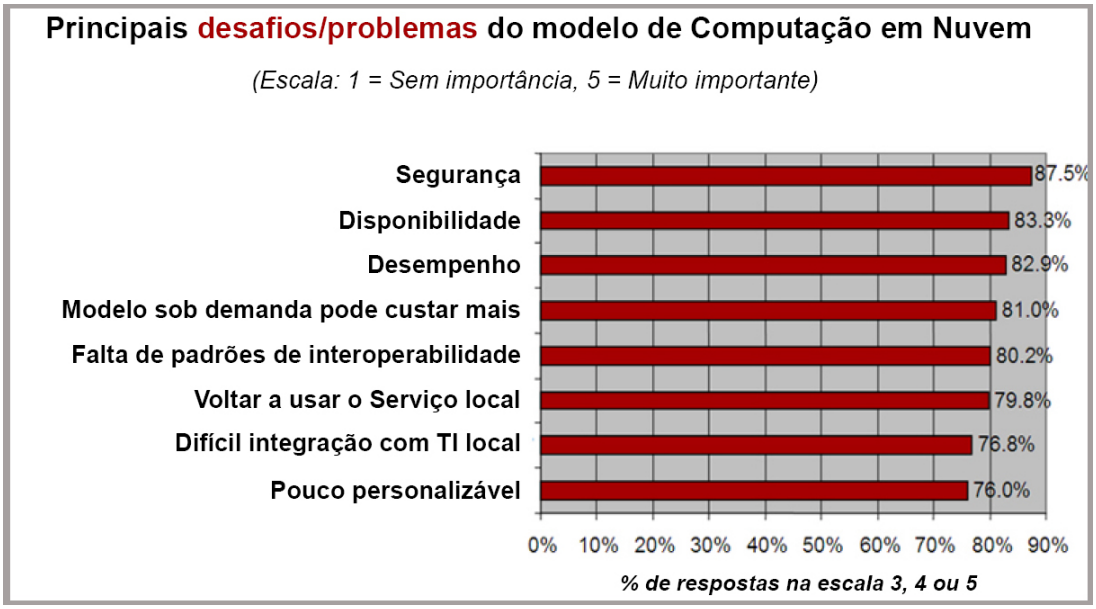

Figura 1.1: Preocupações inerentes à computação em nuvem. Adaptado de [8].

Mecanismos de segurança incluem sistemas de gerenciamento de identidades, que especialmente possuem funcionalidades necessárias para gerenciar o fluxo de identidade do usuário (ou seja, autenticação e autorização) para controlar

o acesso de usuários aos serviços consumidos dentro do ambiente de computação em nuvem. Por esta razão, o gerenciamento de identidades deve ser posto em prática para implantação do eucalyptus, cuja interação ocorra de forma transparente e segura. Este trabalho foca no gerenciamento de identidades, como categoria do campo de estudo da segurança em computação em nuvem eucalyptus e na praticidade oferecida pelo *SimpleSAML* a fim de complementar a segurança e atuar como gerenciador de identidades. O eucalyptus também apresenta menos complicações de configuração com a federação SimpleSAML por este utilizar recursos já ofertados pelas *VirtualMachines* a nível de serviço web. Ao contrário do Shibboleth que requer a configuração de seu ambiente das VirtualMachines(VMs) com o uso de plugins extras a serem configurados com o propósito de adaptação comunicativa entre o IDP, SP e SSO as Virtual Machines.

1.2 Objetivos

O objetivo geral desta pesquisa é estudar os sistemas de gerenciamento de identidades e verificar a sua aplicabilidade em ambientes de computação em nuvem.

1.2.1 Objetivos específicos

Inerente ao Objetivo Principal, deseja-se alcançar concomitantemente os seguintes objetivos específicos visados:

- Levantar os conceitos fundamentais de gerenciamento de identidades;
- Estudar os mecanismos de autenticação e autorização em ambientes distribuídos;
- Comparar as abordagens de gerenciamento de identidades com o Simple-SAML;
- 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 incluindo o Simple-SAML no Eucalyptus e seu tempo de resposta;
- Aplicar um estudo de caso de um sistema de gerenciamento de identidade no Eucalyptus.

1.3 Metodologia

A metodologia de pesquisa consiste na realização ordenada de várias atividades, listadas a seguir:

1. Pesquisa de acervos, para levantamento de informações de livros, teses, artigos, monografias, dissertações, periódicos, anais de congressos e *websites*;
2. Estudo dos mecanismos de autenticação e autorização dos sistemas de gerenciamento de identidades;
3. Levantamento dos requisitos tecnológicos de sistemas de gerenciamento de identidades e de computação em nuvem;
4. Implementação de um sistema de gerenciamento de identidade no Eucalyptus;
5. Testes e avaliação do estudo de caso do sistema de gerenciamento de identidade em funcionamento no Eucalyptus;
6. Elaboração da monografia;
7. Apresentação da monografia;

1.4 Apresentação dos Capítulos

Este trabalho de conclusão está dividido em 3 capítulos da seguinte forma: O primeiro capítulo apresenta e introduz o contexto atual do tema do trabalho, assim como sua área de atuação. Explica-se sobre a escolha do assunto, a problemática e metodologia empregada no desenvolvimento do trabalho. O segundo capítulo trada da fundamentação teórica, mostrando os conceitos necessários para o desenvolvimento e o entendimento desse trabalho. Nele são explicadas tecnologias como: Sistemas federados, segurança da informação, Computação em nuvem, protocolo SAML e em específico: *SimpleSAML* e *Eucalyptus*. No fim do capítulo, a computação em nuvem e suas seguranças para com seu ambiente incluindo seus serviços para o sistema federado para esta pesquisa, que são abordados em detalhes. No terceiro capítulo é ilustrado em detalhes a pesquisa implementada da federação *SimpleSAML* e seus resultados obtidos com os testes e avaliações propostas dentro do ambiente de nuvem *Eucalyptus*. No quarto e último capítulo, as conclusões, os objetivos atingidos, as limitações e os trabalhos futuros são apresentados e analisados.

2 Fundamentação Teórica

2.1 Segurança da Informação

Segundo [14] e [17] a garantia da segurança da informação em ambientes distribuídos, como a Internet constitui cada vez mais, uma preocupação mundial, englobando desde os organismos públicos, privados, universidades, empresas até os cidadãos. De forma individual ou coletiva, seja em bibliotecas ou arquivos digitais, na banca eletrônica, no *e-learning* (ensino à distância) ou em qualquer outra área, a segurança da informação é uma questão chave para a sobrevivência de muitas organizações. Para [17] nesse cenário, computadores e dispositivos portáteis em diversos lugares do mundo têm acesso às informações por meio de avançadas tecnologias e da Internet, aumentando a complexidade e importância de proteção das informações. O nome genérico para o conjunto de ferramentas projetadas para proteger dados e impedir hackers é a segurança da informação. Autores geralmente definem a segurança da informação baseada em suas propriedades (confidencialidade, integridade e disponibilidade) ou em defesa contra ameaças que impõem riscos aos negócios da organização . A seguir são apresentadas duas definições para o termo segurança da informação:

- É a prática de assegurar que os recursos que geram, armazenam ou proliferam as informações, sejam protegidos contra a quebra de confidencialidade, comprometimento da integridade e contra a indisponibilidade de acesso a tais recursos.
- É a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A IBM desenvolveu um framework que apresenta os níveis de segurança das arquiteturas de TI que devem ser estabelecidos, conforme ilustrados na Figura 2.1.

Figura 2.1: Gerenciamento de segurança de [14]

Segundo [16], [14] e [10], a segurança da informação pode ser classificada como segurança física e segurança lógica, cujas explicações são fornecidas a seguir:

- Segurança física: em geral, refere-se à gestão de pessoas, equipamentos e instalações. Em relação à gestão de pessoas, estão as situações em que a componente humana constitui a principal fonte de atenção e de risco em situações como o erro, a falha humana, a fraude ou o roubo. Quanto aos equipamentos, referem-se ao hardware computacional (por exemplo, computadores, servidores, infraestruturas de rede) e outros equipamentos, tais como o de fornecimento de energia, sistemas de controle de acessos físicos, sistemas de detecção e combate a incêndios. Por fim, referente às instalações, trata-se da perspectiva de engenharia e arquitetura, nomeadamente o local onde está fisicamente instalado o sistema que gere e armazena a informação digital. Refere-se ao nível infraestrutura física da Figura 2.1;

- Segurança lógica: semelhante à segurança física, também a segurança lógica é essencial para garantir a segurança da informação. Ainda que aparentemente menos visível, a segurança lógica deve estar em permanente atualização, de forma a acompanhar também a evolução dos riscos e das possíveis ameaças. Nesse aspecto, o princípio básico é que a segurança lógica deve ser implementada

em cada nível da arquitetura de TI. Refere-se aos demais níveis da Figura 2.1, que são descritos a seguir.

– Pessoas e identidades: as organizações precisam garantir que usuários autorizados por todas as empresas e cadeias de suprimentos tenham acesso aos dados e ferramentas necessárias, no momento que precisam, enquanto bloqueiam aqueles que não possuem autorização para acesso. O monitoramento de usuário com privilégios, que inclui as atividades de registro, se tornou uma importante necessidade. Ferramentas de gerenciamento de identidades são fundamentais para controlar a autenticação e autorização de acesso dos usuários.

– Dados e informações: a proteção de dados é questão de segurança mais importante para muitas organizações. As preocupações típicas incluem a maneira com que os dados são armazenados e acessados, os requisitos de conformidade e auditoria, as questões de negócios que envolvem o custo das violações de dados, os requisitos de notificação e os danos ao valor da marca.

– Aplicativos e processos: todos os requisitos de segurança (confidencialidade, integridade e disponibilidade) servem para aqueles aplicativos que se encontram em ambientes distribuídos como a rede. Isso inclui a garantia de que os serviços da Web publicados na Internet, por exemplo, sejam compatíveis com os níveis de segurança exigidos e atendam às políticas de negócios.

– Rede, Servidor e Terminal: em ambientes distribuídos e compartilhados, é imprescindível garantir que todos os domínios estejam devidamente isolados e que não exista a possibilidade de dados ou transações vazarem de um domínio para o outro. Conforme os dados saem do controle dos usuários, esses esperam que o ambiente possua recursos como detecção de invasão e sistemas de prevenção.

A segurança da informação, em geral, tem o objetivo de proteger os dados de usuários e organizações; tem o dever de estimular comportamentos seguros por meio do estabelecimento de regras e políticas de segurança; baseia-se na necessidade de se manter no sistema um conjunto de propriedades [52]. As três propriedades da segurança da informação são discutidas e referidas como “CID” (Confidencialidade, Integridade e Disponibilidade), conforme ilustra a Figura 2.2.

Cada propriedade tem sua função específica conforme as definições a seguir [14] e [18]:

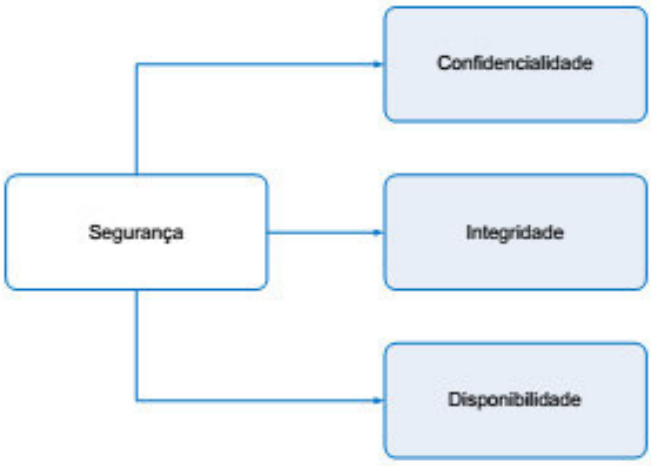

Figura 2.2: Propriedades da segurança de [14]

- Confidencialidade ou privacidade: propriedade necessária para garantir que a informação só será acessada por quem tem autorização. Um exemplo disto é quando um número de cartão de crédito vaza para outras fontes que não tinham autorização de ter aquele número. Ataques de espionagem para capturar dados da rede é um caso comum de violação da confidencialidade da informação. Ferramentas que usam Criptografia, por exemplo, dão suporte à confidencialidade, pois são capazes de embaralhar ou codificar dados para impedir que usuários não autorizados os leiam ou adulterem. Assim, somente pessoas com acesso a uma senha ou chave podem descriptografar e utilizar os dados.

- Integridade: propriedade necessária para garantir que haverá consistência e completude dos dados quando acessados. Um exemplo de integridade é quando se transmite uma mensagem para alguma pessoa e no meio do caminho essa mensagem é adulterada e o conteúdo é modificado. Nesse caso houve o comprometimento da integridade da mensagem por uma fonte não autorizada; Ataques de interceptação de mensagens podem culminar na modificação de dados e se configurar um caso de violação da integridade da informação. Ferramentas criptográficas anteriormente mencionadas ajudam a para proteger a confidencialidade da informação, negando acesso de usuários a dados sem que tenham os direitos de acesso adequados, colaborando para evitar, antes de tudo, que dados sejam modificados. Além disso, existem outras ferramentas especialmente projetadas para apoiar a integridade, incluindo as seguintes:

Cópias de segurança, somas de verificação (função que mapeia o conteúdo de um arquivo para um valor numérico) e códigos de correção (métodos para armazenar dados de modo que pequenas alterações podem ser facilmente detectadas e automaticamente corrigidas).

- Disponibilidade: propriedade necessária para garantir que os usuários que têm autorização poderão acessar a informação quando necessário. Um exemplo de comprometimento da disponibilidade é quando se tenta fazer uma transação bancária e o sistema falha ou encontra-se indisponível. Ataques de negação de Serviço ou Denial of Service (DoS) representam um caso comum de violação da disponibilidade do acesso à informação. Diversas ferramentas providenciam disponibilidade, incluindo as seguintes: proteções físicas (estruturas capazes de suportar tempestades, terremotos, explosões e enfrentar interrupções de energia) e redundâncias computacionais (computadores e dispositivos de armazenamento que servem como reserva no caso de falhas, por exemplo, arrays redundantes de discos (RAID)). Além dos conceitos de Confidencialidade, Integridade e Disponibilidade, discutidos anteriormente, existem diversos conceitos adicionais importantes nas aplicações modernas de segurança de computadores. De forma semelhante, esses conceitos podem ser caracterizados por um acrônimo de três letras, "GAA", que se referem a Garantia, Autenticidade e Anonimato.

- Garantia: propriedade necessária que se refere como a confiança fornecida é gerenciada em sistemas de computação. Reconhecidamente, a própria confiança é difícil de quantificar, mas sabemos que ela envolve o grau de confiança em pessoas ou sistemas, quando se comportam segundo a política de segurança, isto é, da forma prevista;

- Autenticidade: propriedade necessária para verificação da identidade do cliente que solicita o uso dos dados. É ainda a habilidade de determinar que afirmações, políticas e permissões oriundas de pessoas ou sistemas são genuínas. Formalmente, diz-se que um protocolo que consegue autenticidade demonstra não repúdio. – Não repúdio ou irretratabilidade: propriedade necessária para que afirmações autênticas emitidas por alguma pessoa ou sistema não podem ser negadas pela autoria. A principal forma de efetivar esta propriedade é por meio

do uso de assinaturas digitais (computações criptográficas que permitem a uma pessoa ou sistema se comprometer com a autenticidade de seus documentos de maneira única).

- Anonimato: propriedade necessária de que certos registros ou transações não sejam atribuíveis a qualquer indivíduo. Essa propriedade previne contra o perigo de espalhar identidades por meio de um hospedeiro de registros digitais, que associa a identidade a outros dados, como histórico médico, compras, registros legais, e-mail, etc. Se empresas precisam publicar dados sobre seus membros ou clientes, deve-se esperar que façam isso de modo a preservar a privacidade, usando uma das seguintes ferramentas:

  – Agregação: a combinação de dados de muitos indivíduos de modo que a divulgação dessas somas ou médias não possa ser vinculada a qualquer indivíduo. Exemplo: dados do IBGE não expõem detalhes sobre quaisquer indivíduos.

  – Mistura: o entrelaçamento de transações, informações ou comunicações de modo que não possam ser rastreadas a nenhum indivíduo. Exemplo: sistemas que podem misturar dados juntos de maneira quase aleatória, de forma que transações e pesquisas possam ser realizadas, mas sem a revelação de qualquer identidade individual.

  – Representantes (proxies): agentes de confiança que querem se engajar em ações para o indivíduo de maneira que não possam ser rastreados de volta para aquela pessoa. Exemplo: representantes de pesquisa na Internet são sites que fornecem a sua própria interface com o navegador, de modo que indivíduos podem visitar sites que poderiam estar bloqueados, por exemplo, devido aos países onde estão localizados.

  – Pseudônimos: identidades fictícias que podem servir como identidades reais em comunicações ou transações, mas que são conhecidas apenas por entidades de confiança. Por exemplo, muitos sites de redes sociais permitem que usuários interajam com os demais usando pseudônimos, de modo que eles podem se comunicar e criar um personagem online sem revelar sua verdadeira identidade.

2.2 Gerenciamento de Identidade

Nas relações comerciais, provedores de serviços (loja virtual, sistema acadêmico ou portal) necessitam de algum nível de confiança entre as partes pra realizar transações. Quando essa confiança não pode ser estabelecida diretamente, a interação ocorre por meio de um intermediário confiável para ambas as partes (também chamado de terceira parte), conforme ilustrado na Figura 2.3. Essa terceira parte é responsável por fornecer informações sobre o parceiro, dando origem ao conceito de identificação.

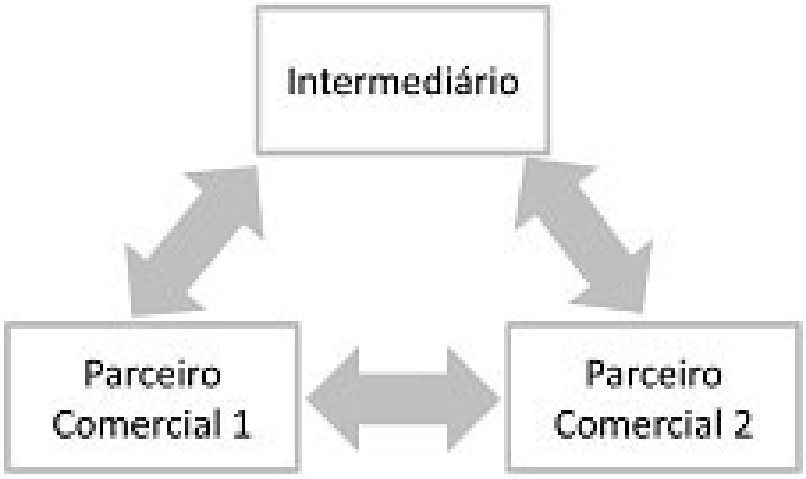

Figura 2.3: Relacionamento comercial de [14]

As identidades das partes envolvidas na transação são controladas e monitoradas por Sistemas de Gerenciamento de Identidades (SGI). Esses são programas ou frameworks que administram uma coleção de identidades, realizam sua autenticação, gerenciam seu uso e as informações vinculadas à identidade [10]. Sendo assim, o gerenciamento de identidades consiste de um sistema integrado de políticas, processos de negócios e tecnologias que permite às organizações o tratamento e a manipulação de identidades (atributos de identidade) de seus usuários [14] e [5]. O gerenciamento de identidades também envolve aspectos relacionados com a definição, certificação e gerenciamento do ciclo de vida das identidades digitais, infraestruturas para troca e validação dessas informações, juntamente com os aspectos legais [22].

O processo de identificação pode ser compreendido a partir dos seguintes componentes da identidade: sistema, entidade, identidade, identificador e credencial, conforme [21] e [23].

- Sistema: é um conjunto de software e hardware que armazena informações sobre entidades, credenciais, identidades, e processamento das operações de autenticação e autorização para proteger dados e serviços. Ex: Shibboleth, OpenAM, SimpleSAMLphp, OpenID etc;

- Entidade: pode ser um pessoa, um serviço de rede, um dispositivo computacional em rede ou um dispositivo de telefonia móvel. As entidades existem no mundo real. Elas usam credenciais e possuem um ciclo de vida independente.

- Identidade: é um conceito virtual utilizado por uma entidade para fornecer informações sobre si para o sistema. Uma identidade sempre está associada a uma entidade, geralmente constituída de um identificador único. O identificador é utilizado para provar a propriedade da identidade (por meio de credenciais) e fornecer informações (perfil) a um sistema. O sistema irá utilizar essas informações para tomar decisões sobre a entidade associada.

- Atributos: um conjunto de dados que descreve as características fundamentais de uma identidade. Como exemplo tem-se: nome completo, domicílio, data de nascimento e papéis [14] e [5].

- Identificador: é o índice único de uma identidade. Normalmente, um identificador é usado pelo sistema para referenciar uma identidade. Por exemplo, uma URL (Uniform Resource Locator) é única ao longo do tempo. Como exemplo de identificadores temos CPF, RG, número de matrícula e número de passaporte;

- Credencial: serve para provar uma identidade em um sistema. Podem existir vários tipos de credenciais, mas todas são utilizadas para provar a um sistema (com um nível aceitável de segurança). Exemplos de credenciais incluem certificados digitais X.509 assinados por uma autoridade certificadora (CA - Certificate Authority), senha, asserções SAML (Security Assertions Markup Language), dentre outros.

A ilustração do relacionamento entre os componentes da Identidade, é vista na Figura 2.11 em notação UML (Unified Modeling Language).

As principais operações no gerenciamento de identidades são [5, 14]:

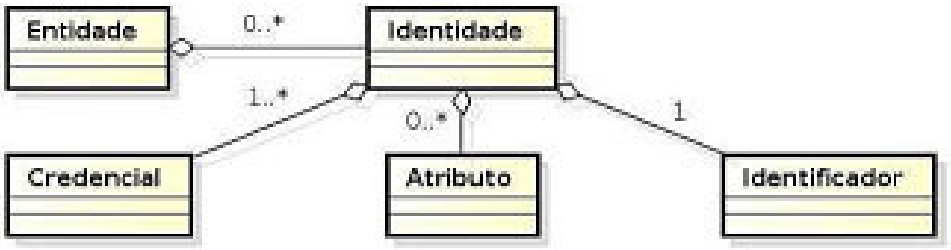

Figura 2.4: Componentes de Identidade de [14]

- Identificação: é a função de uma entidade fornecer uma identidade ao sistema por meio de um identificador;
- Autenticação: é a função do sistema verificar a legitimidade de uma identidade por meio da verificação de credenciais;
- Autorização: é a função do sistema conceder privilégios a uma entidade após a autenticação da sua identidade;
- Auditoria: é a função de registrar as ações realizadas por uma entidade em um sistema, gerando uma prova tanto para as partes envolvidas quanto para terceiros.

2.3 Controle de Acesso

Em sistemas distribuídos, os recursos são fornecidos para diversos usuários desconhecidos para suas aplicações. Portanto, é necessário definir o controle de acesso aos recursos, que inclui três conceitos fundamentais: autenticação, autorização e cumprimento [11] e [22], conforme ilustrado na Figura 2.3, e descritos a seguir.

- Autenticação: especificada em termos de protocolos, abordagens de determinação de quem pode acessar o recurso protegido. É o processo de verificar se a identidade do usuário é legítima, isto é, se o usuário é realmente quem diz ser. Exemplos: senha, cartão, impressão digital, etc;
- Autorização: expressa em termos de um modelo de controle de acesso, a autorização especifica os recursos que precisam ser protegidos, quais tipos de acesso (operações) são possíveis aos recursos, e que acesso é permitido a eles. Por

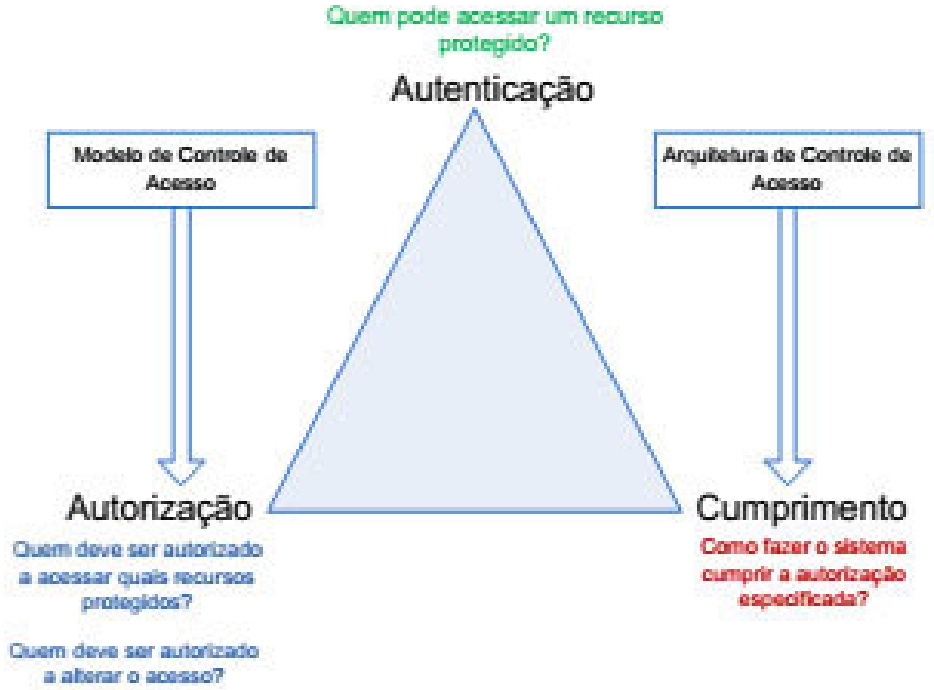

Figura 2.5: Conceitos de Controle de acesso adaptado de [14]

exemplo, um sistema de computador usa uma regra de controle de acesso para decidir se é permitido ou negado o acesso a um recurso baseado na identidade obtida durante a autenticação;

- Cumprimento: é definida por meio da validação dos requisitos para uma entidade ser autorizada a acessar determinado recurso. Ou seja, certificar a permissão do acesso ao recurso, por exemplo, quando satisfaz a condição de um cadastro; e, a obtenção do acesso por essa entidade aos recursos quando solicitado, verificando a disponibilidade do recurso quando solicitado ou negado caso o usuário não seja autorizado.

Diversas terminologias para a descrição dos modelos de controle de acesso têm sido desenvolvidas durante as últimas décadas. Qualquer mecanismo de controle de acesso pode ser descrito formalmente usando descrições de usuários, sujeitos, objetos, operações e permissões, e os relacionamentos entre estas entidades. Uma breve descrição desses termos será apresentada a seguir [9]:

- Usuários: referem-se tipicamente às pessoas que interagem com o sistema de computador, mas também podem representar outros agentes como algum dispositivo ou uma máquina;

- Sujeitos: são processos ou tarefas que agem em nome do usuário e executam uma operação ou uma série de operações sobre um ou mais objetos. Dois ou mais sujeitos podem corresponder a um mesmo usuário, mesmo que este tenha apenas um login e esteja na mesma sessão. Uma sessão é uma instância de diálogo do usuário com o sistema. Todos os sujeitos têm um identificador único;

- Objetos: são entidades do sistema sobre as quais as operações são executadas. No contexto de um Sistema Operacional, um objeto pode representar um arquivo. No contexto de um sistema gerenciador de banco de dados, um objeto pode ser uma tabela ou uma view. Outros exemplos de objetos são: buffers, diretórios de arquivos, páginas da web, programas, impressoras. A escolha de quais entidades que irão pertencer ao conjunto de objetos é determinada pelos requerimentos de proteção e objetivos de segurança do sistema;

- Operações: são processos ativos invocados pelo sujeito. Exemplos de operações no contexto de um sistema bancário podem ser: fazer depósito, saques, verificação do saldo, entre outros;

- Permissões (ou privilégios): são direitos dados a um individuo, ou ao sujeito agindo em nome do usuário, permitindo ao detentor do direito executar alguma ação no sistema. O termo permissão refere-se a uma relação entre o objeto, o sujeito, e a operação.

2.4 Computação em Nuvem

O termo nuvem ou *cloud* é uma metáfora em relação à forma como a Internet é usualmente mostrada nos diagramas de rede – como uma nuvem. Nesses diagramas, o ícone da nuvem representa todas as tecnologias que fazem a Internet funcionar, abstraindo a infraestrutura e a complexidade que esta engloba Gilbertson2011. Já a Computação em Nuvem, refere-se de modo geral a uma combinação de tecnologias (Virtualização, Computação Utilitária, Computação em

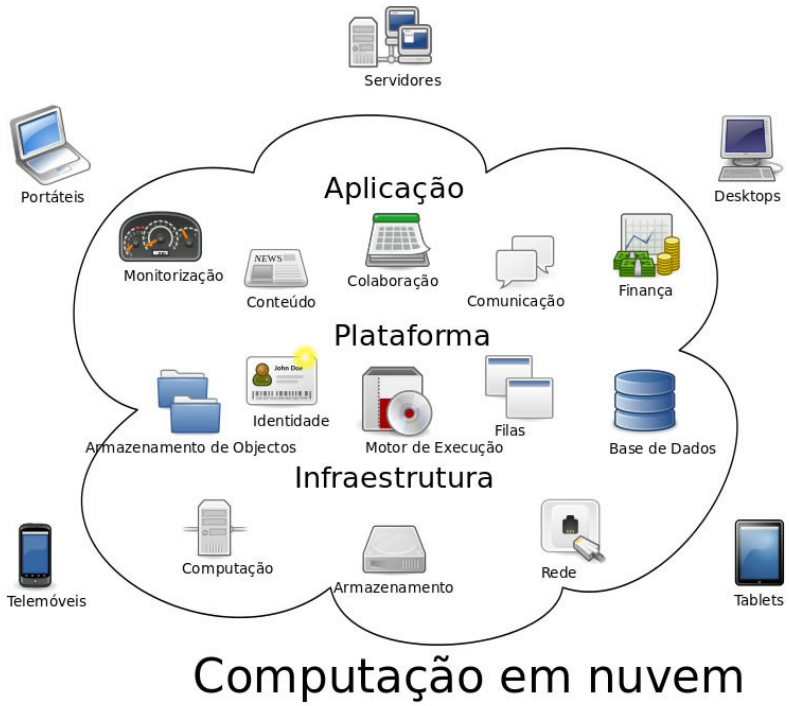

Figura 2.6: Figura ilustrativa da nuvem e suas camadas adaptado de [6]

Cluster e Arquitetura Orientada a Serviços), em que o usuário não precisa ter todo o conhecimento necessário para manter essa infraestrutura [14]. Em [14] e [12], Mell e Grance do NIST definem a Computação em Nuvem como um modelo para permitir acesso de rede ubíquo, conveniente, e sob demanda a um repositório compartilhado de recursos computacionais (redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com o provedor de serviços. Para os autores, os serviços de Computação em Nuvem baseiam-se em cinco características essenciais, que são:

1. **Autoatendimento sob demanda**: um consumidor pode provisionar recursos de computação, tais como processamento e armazenamento, sem a necessidade de interação humana com cada prestador de serviço;
2. **Acesso amplo à rede**: recursos são disponibilizados sobre a rede e acessados por meio de mecanismos padronizados que permitam utilizar quaisquer tipos de plataforma, como por exemplo, telefones celulares, tablet, notebooks e estações de trabalho;
3. **Agrupamento de recursos**: os recursos são agrupados para atender múltiplos consumidores com diferentes recursos físicos e virtuais atribuídos dinamicamente à medida que a demanda do consumidor é alterada;

4. **Elasticidade**: os recursos podem ser provisionados e liberados flexivelmente (em alguns casos automaticamente), para se ajustar à necessidade crescente ou decrescente. Para o consumidor, os recursos disponíveis para provisionamento parecem ser ilimitados e podem ser consumidos em qualquer quantidade e a qualquer momento;
5. **Monitoramento de serviço**: os provedores de Computação em Nuvem controlam e aperfeiçoam, automaticamente, o uso dos recursos, aproveitando uma capacidade de medição em algum nível de abstração apropriado para o tipo de serviço. O uso de recursos pode ser monitorado, controlado, criando-se relatórios que fornecem transparência, tanto para o provedor quanto para o consumidor.

Baseado em Acordos de Nível de Serviço (SLA), todos os modelos de serviços de Computação em Nuvem (ou seja, IaaS, PaaS, SaaS) podem ser provisionados através de quatro diferentes modelos de implantação de serviços de Computação em Nuvem: Privada, Comunitária, Pública, e Híbrida [1, 6], dependendo das necessidades do consumidor de serviços de Computação em Nuvem.

- Nuvem Privada: recursos computacionais são provisionados por uma organização particular (uma organização de negócio que envolve vários consumidores (várias unidades de negócios). Essencialmente, as interações são consideradas como B2B em que os recursos computacionais podem ser pertencidos, gerenciados e operados pela mesma organização, um terceiro, ou ambos.

- Nuvem Comunitária: recursos computacionais são provisionados por uma comunidade de organizações, para atingir um determinado objetivo (por exemplo, alto desempenho, requisitos de segurança, ou redução de custos). Basicamente, as interações são consideradas como B2B, onde os recursos de computação podem pertencer, ser gerenciados e operados pela mesma comunidade, um terceiro, ou ambos.

- Nuvem Pública: recursos computacionais são provisionados pelo público (por exemplo, um consumidor individual de serviços de nuvem, universidade, governo, organizações de empresas , ou uma combinação desses tipos de consumidores de serviços de nuvem). Essencialmente, as interações são consideradas como B2C em que os recursos computacionais podem pertencer,

ser gerenciados e operados por uma universidade, governo, ou organização de empresas, ou uma combinação de dois desses.

- Nuvem Híbrida: recursos computacionais são provisionados por dois ou mais modelos de implantação de nuvem (por exemplo, nuvens privadas e públicas podem ser implantadas em conjunto, utilizando um modelo de implantação híbrido). Basicamente, as interações incluem B2B e B2C, em que os recursos computacionais são interligados por diferentes nuvens utilizando técnicas de portabilidade (por exemplo, portabilidade de dados e aplicações, e em casos de nuvens cujos recursos estão saturados, necessitando de balanceamento de carga entre nuvens).

2.5 Modelos de Serviço

Serviços de Computação em Nuvem possuem três modelos diferentes, incluindo Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS) com base em diferentes Acordos de Nível de Serviço (SLAs) entre um provedor de serviços e um consumidor. A Figura 2.4 apresenta as camadas de serviços de Computação em Nuvem e, em seguida, a descrição de cada uma:

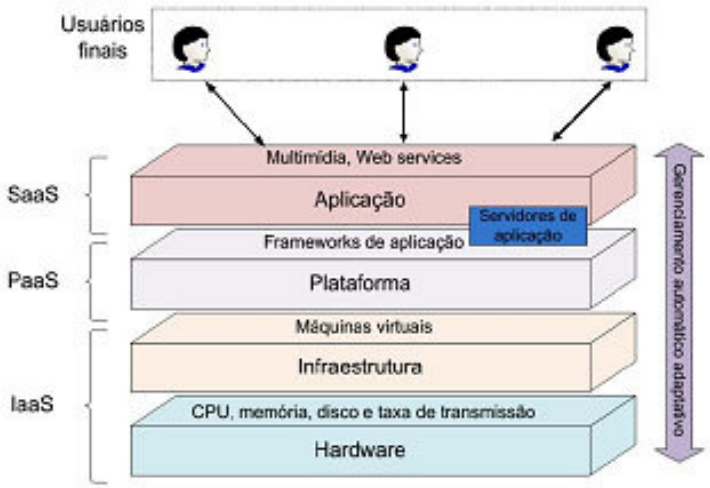

Figura 2.7: Camadas de Serviços adaptado de [24]

- IaaS: O consumidor contrata uma infraestrutura de hardware podendo escolher a capacidade da configuração (i. e. frequência de processamento, quantidade de

memória, quantidade de armazenamento, taxa de transferência e quantidade de dados transmitidos), qual sistema operacional será executado e softwares estarão disponíveis arbitrariamente. O consumidor tem controle total da infraestrutura virtual contratada, mas não tem controle sobre a localização ou os recursos físicos de fato. É, por exemplo, o tipo de serviço oferecido pela Amazon EC2;

- PaaS: Geralmente usada para desenvolvimento colaborativo, o consumidor contrata uma plataforma com um conjunto de ferramentas específicas (ex. controle de versões, ferramentas de comunicação e disponibilização de aplicações), usando as linguagens de programação suportadas pelo provedor, como é oferecido pela Google Apps, por exemplo. Nesse tipo de serviço o consumidor não tem acesso direto a configuração dos recursos físicos ou das camadas mais baixas de software;

- SaaS: O consumidor contrata a utilização de uma aplicação que está hospedada e em execução em uma nuvem, por exemplo, serviços oferecidos por um provedor de acesso a Internet. Esse é o tipo de serviço mais comum e, muitas vezes, o consumidor sequer tem ideia de que o serviço contratado faz parte de uma nuvem. Assim como em PaaS, nesse classe de serviço o consumidor também não tem acesso às camadas mais baixas da infraestrutura, por exemplo, o Google Docs e o Windows Live Mesh.

2.6 Segurança na Nuvem

Segundo os autores [6], [3], [1], [14] e [10]existem diversos aspectos críticos de segurança em nuvem. Os principais são:

- **Segurança de Identidades**: objetiva manter a integridade e confidencialidade dos dados e das aplicações, ao mesmo tempo que tornam o acesso disponível aos clientes autorizados. Os principais padrões e soluções utilizadas para a implantação de gerenciamento de identidades incluem o *SAML (Security Assertions Markup Language), OpenID, Shibboleth, Higgins, SimpleSAMLphp, OpenAM, XACML (Extensible Access Control Markup Language) e OAuth*.

- **Segurança da Informação**: nos tradicionais *data centers*, controles de acesso físico, de acesso ao hardware e software e de identidade combinam-se para proteger os dados. Na nuvem, a barreira de proteção da infraestrutura é difusa. Assim, a segurança da informação exigirá [14]:

  – **Isolamento dos dados**: na multi-alocação de recursos os dados do ambiente devem ser armazenados de forma segura, a fim de protegê-los quando vários clientes utilizam os recursos compartilhados. Virtualização, criptografia e controle de acesso são mecanismos que permitem vários graus de isolamento de dados entre empresas e clientes diferentes;

  – **Segurança dos dados**: os provedores de serviços devem fornecer mecanismos de segurança para proteger os dados de seus clientes. Isso envolve o uso de técnicas de criptografia e controle de acesso aos dados;

  – **Segurança de rede**: todo o fluxo de dados da rede deve estar seguro para evitar a perda e manipulação de informações. Para isso, podem-se utilizar técnicas de criptografia ou *firewall* e IDS que garantam a segurança e o monitoramento do tráfego de rede;

  – **Integridade dos dados**: qualquer tipo de transação deve seguir as propriedades ACID (Atomicidade, Consistência, Isolamento e Durabilidade) para garantir a integridade dos dados;

  – **Vulnerabilidade na virtualização**: uma máquina virtual oferece um ambiente completo similar a uma máquina física. Dessa forma, algumas vulnerabilidades encontradas em uma máquina física são também encontradas nos softwares de virtualização. Essas vulnerabilidades podem ser utilizadas por invasores para adquirirem determinados privilégios e violar outras restrições de segurança.

- **Segurança de Infraestrutura**: quando uma empresa contrata um serviço de IaaS e presta serviços a outros clientes, o provedor de IaaS é indiferente quanto às operações e ao gerenciamento de pedidos das empresas contratantes do seu serviço. Assim, é importante que o contratante assuma total responsabilidade por assegurar a sua infraestrutura, implantando, por exemplo, mecanismos de controle de acesso, de criptografia dos dados e/ou ferramentas de monitoramento da rede. Além disso, a segurança da infraestrutura física de um provedor deve ser garantida, como por exemplo pelo *SLA (Service Level Agreement)*.

3 Federação de Identidade usando SimpleSAML

3.1 Implementação e resultados

A arquitetura de um sistema federado se comporta e é representado de maneira didática e exemplificada conforme a figura 3.1 do site do próprio Google e Shibboleth para explicar o funcionamento e as etapas de um sistema federado.

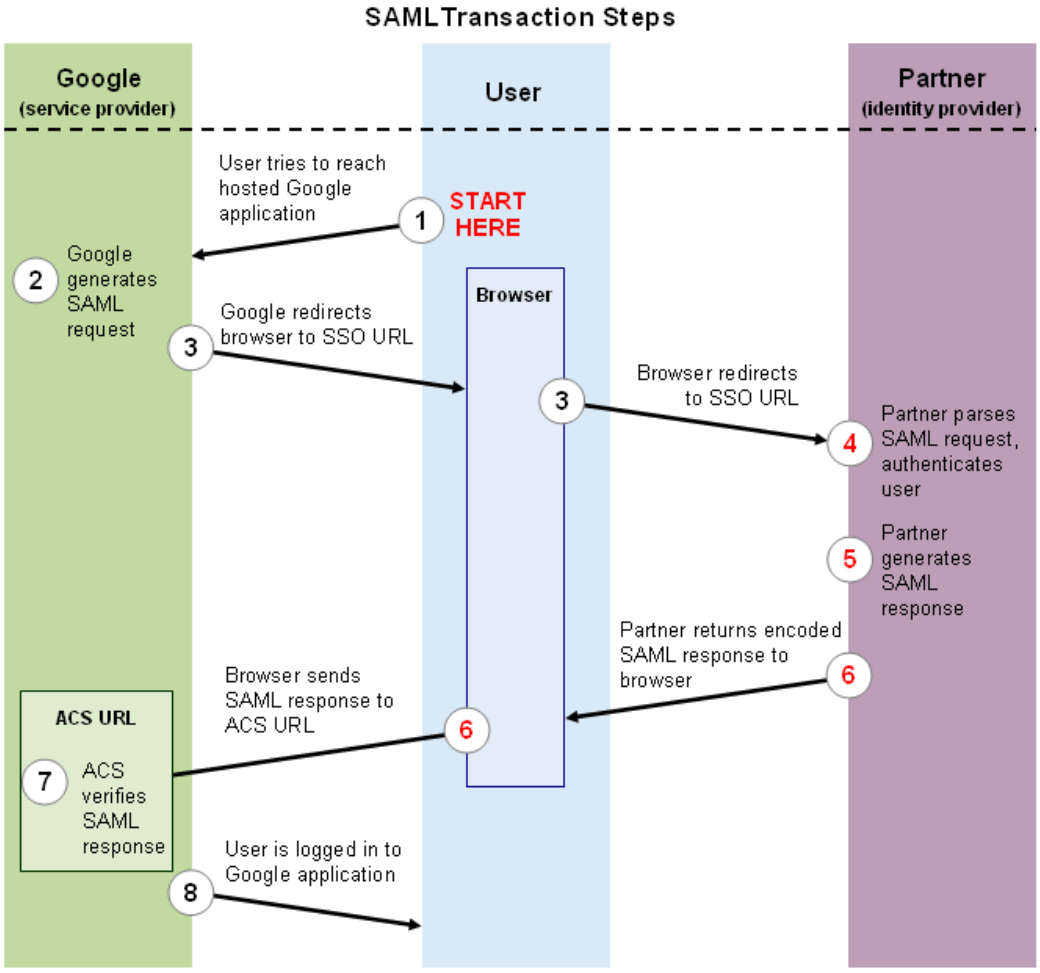

Figura 3.1: SistemaFederado de [6]

Explicando pelas numerações existentes na figura 2.2, o processo da federação começa com o *passo 1*, onde o usuário requisitando o serviço do SP (neste caso o Google) deseja utilizar. O google então realiza o *passo 2*, onde solicita as credenciais do usuário e gera sobre elas a solicitação do SAML correspondente para o

IDP valida-las, o que na figura 2.2 quem vai intermediar esse redirecionamento é o SSO pelo *passo 3*. No *passo 4*, o SSO entrega o SAML do usuário para o IDP e autentica-o(se estiver cadastrado e com permissão) para no *passo 5* gerar o SAML de autorização a ser retornado para o SP. Nos *passo 6 e 7* ocorre este retorno do SAML autenticado para o SP e o SP verifica e disponibiliza o serviço para o usuário. Deste modo, todo o processo para garantir a integridade, privacidade e disposição dos serviços fica relacionado por estas etapas, independente do tipo do *Sistema de Gerenciamento de Identidade*.

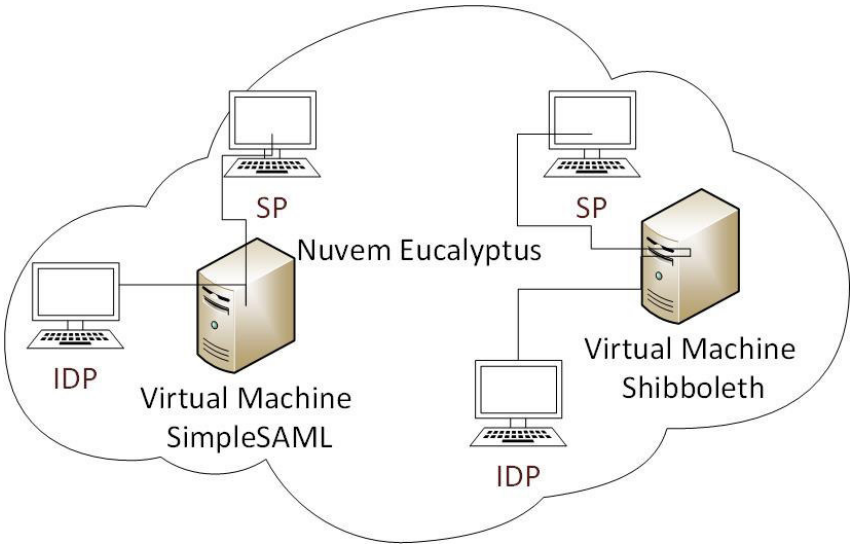

Figura 3.2: Arquitetura da Implementação

Como a figura 3.2 ilustra, na VM SimpleSAML da nuvem *Eucalyptus* temos o SimpleSAML com seu IDP e SP federados para realizar os testes e fazer uso do protocolo SAML. Enquanto que na VM Shibboleth da nuvem *Eucalyptus* temos o Shibboleth com seu IDP e SP respectivos para também realizar os testes e fazer uso do protocolo SAML. Ambos já tem configurados a atividade federativa de *Single-Sign-On*. Para realizar a configuração de cada federação o processo toma configurações parecidas, porém no Shibboleth as etapas de configuração são maiores por conta do módulo DS que deve ser configurado. Este Módulo DS é como um proxy, uma lista de IDPs confiáveis da federação na qual ele pode autorizar e se comunicar (caso haja mais de um(01) IDP). Nos testes e na implementação deste trabalho foi-se utilizado somente um(01) IDP. Para a configuração so SimpleSAML as etapas são mais simples por conta do processo de configuração do IDP ser similar ao SP, modificando somente a hierarquia de quem autoriza quem e quem fornece os serviços para quem.

Os hardwares utilizados para a execução tanto da nuvem quanto dos sistemas federativos são descritos e identificados da seguinte forma: Foi primeiramente utilizado 2 computadores, onde um*(nome teste)* foi utilizado exclusivamente para o desenvolvido das *VMs SimpleSAML e Shibboleth, tanto o SP como IDP* de cada federação respectiva. O outro*(nome cloud)* com a nuvem *Eucalyptus* instalada e configurada para efetuar os testes e resultados obtidos com a migração das VMs para o *eucalyptus*. A máquina *teste* possui um intel Core i5, 8GB RAM, HD de 500GB utilizando-se do software VirtualBox para a criação e configuração das VMs, enquanto que a máquina *cloud* possui intel core i7, 8GB RAM, HD de 1TB rodando o sistema de nuvem *Eucalyptus*.

O primeiro passo tomado para ambientar os experimentos foi criar duas(02) Virtual Machines na máquina *teste* para realizar as configurações do IDP e SP das respectivas federações SimpleSAML e Shibboleth. A Virtual Machine SimpleSAML instalou-se o sistema Lubuntu para prover cada módulo configurado do SimpleSAML. Pelo estudo da topologia federada, o SP e IDP normalmente se encontram em máquinas ou Virtual Machines Separadas, porém isso não interfere na comunicação ou performance da federação. Isso é apenas o ideal encontrado em implementações comerciais e de estudo teórico para melhor observação. Deste modo foi-se implementado em uma única Virtual Machine os dois(02) módulos IDP e SP do SimpleSAML, a fim de facilitar os estudos na coleta de resultados com módulos de teste como o JUnit e o BadBoy. A segunda Virtual Machine foi-se instalado e configurado a federação Shibboleth e seus módulos IDP e SP para avaliar seus desempenhos juntamente com o SimpleSAML e Compara-los.

Para a instalação e configuração do *SimpleSAML* baixa-se o pacote de instalação ".tar.gz"no site oficial do *SimpleSAML*, e segue o step-by-step da documentação configurando os arquivos .php e .conf citados para ascender o acesso a federação como ilustra a figura 3.3:

Como se observa, as credenciais utilizadas no *SimpleSAML* faz uso de um usuário e senha que devem estar cadastrados no IDP para acessa-los. Para a instalação e configuração do *Shibboleth*, os passos são um pouco diferentes, consistindo que baixe os pacotes específicos do *Shibboleth* para atuar como SP ou IDP, executando via terminal os comandos para a instalação do IDP e SP. Em seguida deve-se gerar o certificado para validar o endereço do IDP e HOST:

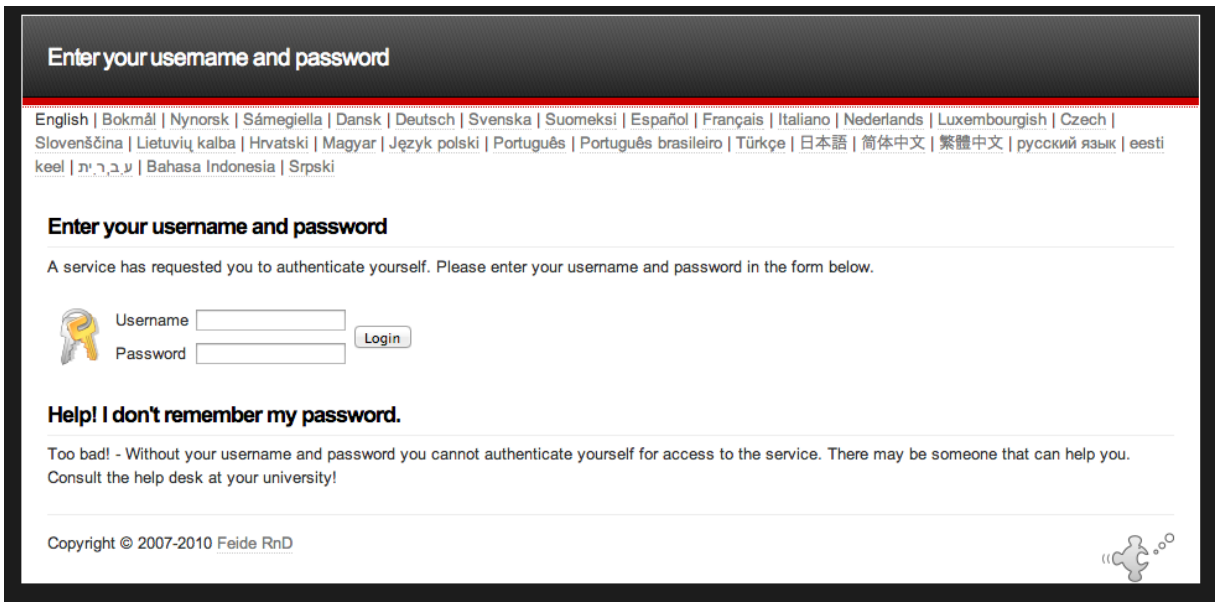

Figura 3.3: Home Screen SimpleSAML

cd /etc/shibboleth e sudo shib-keygen -h aaf.dev.labsacshib.com

Para finalmente começar a comunicação federativa, habilitando-se os serviços do proxy e do shibboleth. Com todos os serviços habilitados, ao acessar um serviço web pelo endereço da federação, uma página de boas vindas é carregada para o usuário como ilustra a figura 3.4:

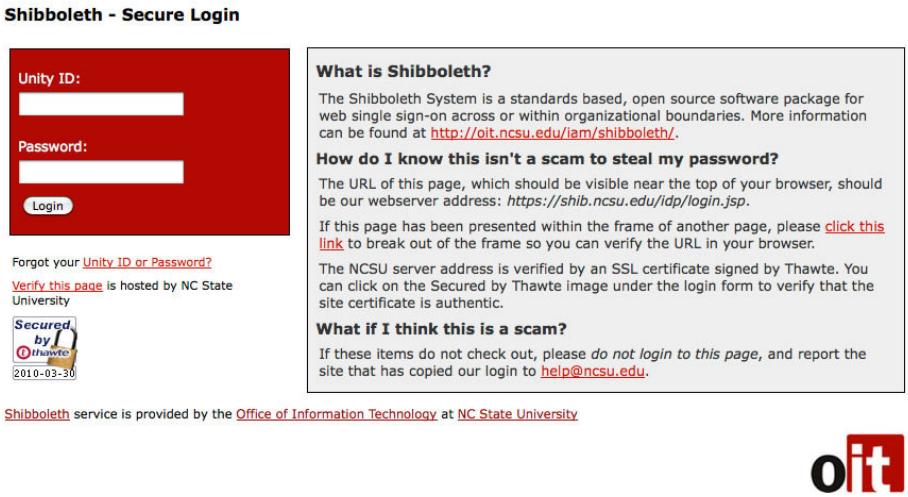

Figura 3.4: Home Screen Shibboleth

Em seguida exportou-se as VMs de cada federação para a máquina *cloud*, onde a nuvem *Eucalyptus* se encontra para iniciar os testes de federação e Single-Sign-On na nuvem. Para a instalação e configuração do *Eucalyptus*, foi feito o "How-TO"descrito no próprio manual do site da *Eucalyptus* adequando as configurações de

rede para o ambiente local do LABSAC e seus acessos. A nuvem apresenta o serviço de nuvem privada, pois são provisionados para uma pesquisa de organização particular [14]. Também é necessário configurar as especificações das VMs da nuvem para suas específicas instâncias. Nos testes e implementações foi adequando um padrão de 1GB de memória RAM e 1GHZ de processamento para cada VM federativa. Deste modo o resultado final é um linux CentOS com os serviços de nuvem instanciando VMs para sua execução.

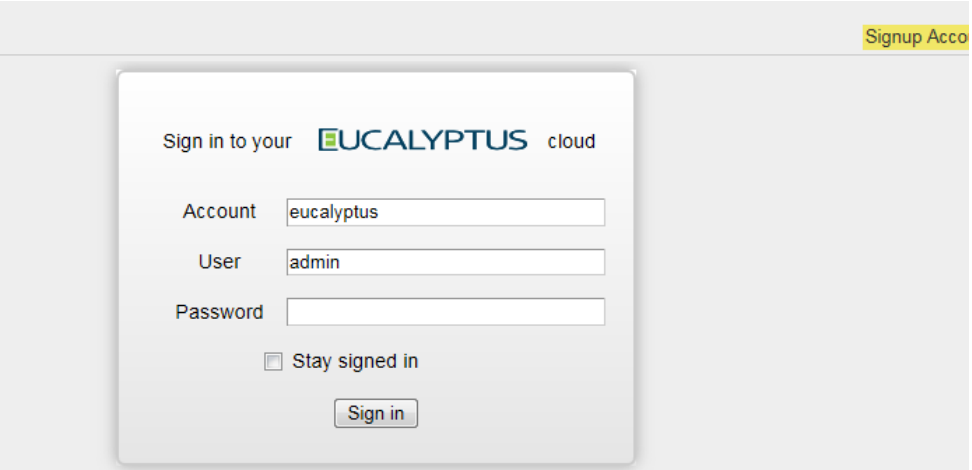

Figura 3.5: Login Eucalyptus

Os testes envolveram o tempo de autenticação com a liberação de serviço com base na segurança e topologia de cada federação na nuvem. Isto pelo programa Badboy é chamado de "round". O gráfico da figura 2.4 ilustra os resultados obtidos na federação Shibboleth na nuvem.

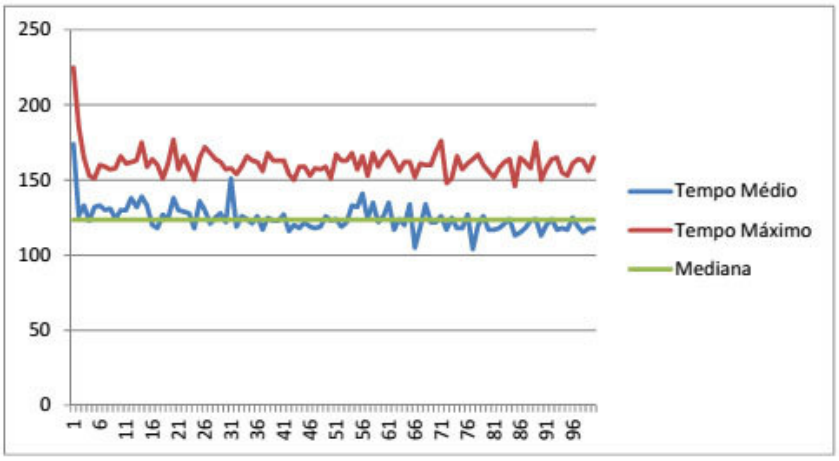

Figura 3.6: Resultado de acesso Shibboleth

No eixo Y a esquerda temos o tempo em milisegundos para autenticar, enquanto que no eixo X representa o numero X de usuários para autenticar na

federação. Cada cor no gráfico, consiste na representação do tempo médio, mínimo e máximo de autenticações na federação Shibboleth. Para a pesquisa, o tempo utilizado para destaque é o tempo médio, já que este remete a performance da federação. Partindo-se deste ponto, os resultados comparados com a federação SimpleSAML tem uma diferença evidentemente maior pelo motivo de não ter o módulo DS(Proxy) e diminuir o tempo de comunicação entre o IDP e SP. O gráfico da figura 2.5 ilustra os resultados de tempo médio do SimpleSAML juntamente comparado ao Sibboleth.

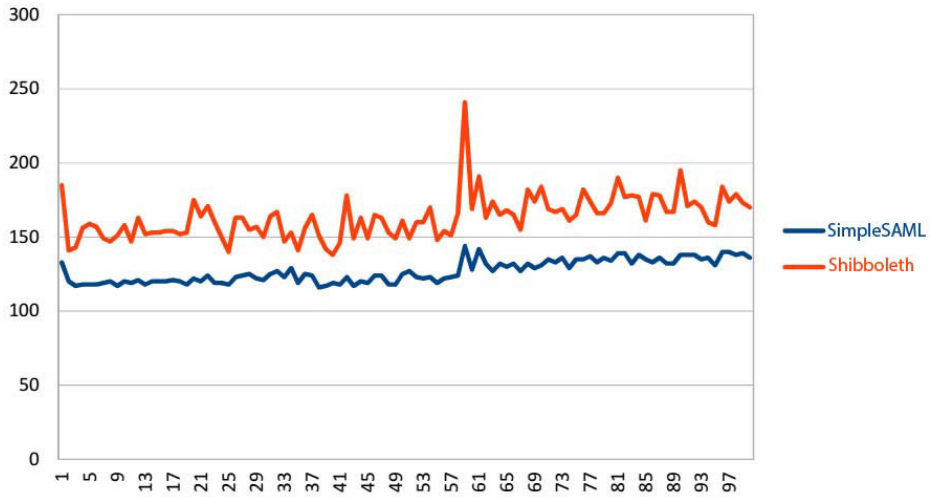

Figura 3.7: Resultado de acesso SimpleSAML

Pelo gráfico da figura 2.5 é perceptível a mudança de tempo de resposta entre o *SimpleSAML* e *Shibboleth*. Nesta comparação das federações nota-se que o tempo médio de autenticações de cada federação, o *SimpleSAML* apresenta um tempo médio melhor se comparado com o *Shibboleth*. Porém pelo JUnit, verificou-se que o número de rotinas no *Shibboleth* para garantir a identidade do usuário é vinte vezes mais demorada que o *SimpleSAML*, isto deveu-se ao módulo DS do *Shibboleth* que apesar de prejudicar o tempo médio de autenticações, também aumenta a segurança e confiabilidade da federação se comparado ao *SimpleSAML*. Sobre o *Eucalyptus*, a nuvem respondeu muito bem a integridade de se levar o funcionamento de um sistema federado para o ambiente de nuvem em ambos os *SGIs*, o que leva a concluir que a aplicabilidade da nuvem para serviços desta categoria pode ser explorado e em aspectos de escalabilidade consegue trazer resultados positivos para o SGI, seja ele qual for. A segurança é outro ponto que se aprimora nos seus serviços, pois além da segurança do próprio sistema de gerenciamento de identidade, também se tem a

segurança do próprio *Eucalyptus* para com os serviços nas VMs, o que garante uma segurança a mais para ataques externos aos *SGIs*.

4 Conclusão

Concluindo os resultados obtidos nos testes da implementação dos dois sistemas federados, em um ambiente de nuvem, é visível que o SimpleSAML apresentou uma performance mais rápida para realizar suas autenticações na federação se comparado ao Shibboleth. Também foi possível notar que o nível de confiabilidade e segurança, em compensação, é menor, se comparado a federação Shibboleth que incorpora uma confiabilidade e identidade maior pelo uso do módulo DS(proxy) para garantir que haja comunicação somente entre o IDP e SP autorizados, sem qualquer terceiro para burlar a integridade da federação.

4.1 Retrospectiva do trabalho

O trabalho apresentou resultados satisfatórios como ilustrados nas figuras 2.4 e 2.5, as fundamentações teóricas realmente deram peso para melhorar a compreensão e entendimento na implementação das federações e da nuvem, o que resultou no relacionamento mútuo do teórico e prático.

4.2 Avaliação do trabalho

O trabalho expandiu muito a compreensão de toda a arquitetura e topologia das federações e da computação em nuvem, além de ter alcançado o nível de confiabilidade e segurança esperados no devido ambiente controlado e nas medidas de comparação entre abas as federações se desempenhando na nuvem. Todos os objetivos foram alcançados com sucesso, tendo em vista a utilização da topologia de nuvem e de federação para integrar os testes. O *eucalyptus* também aumentou a segurança de ambas as federações. Ambas fazem usos de recursos da nuvem e estes estão amarrados a uma segurança de criptografia que impede invasões de fora da topologia pela camada de *Plataforma*. Valendo significativamente pelos resultados obtidos, incluindo

muitas outras possibilidades de implementação de ambas as arquiteturas para futuros projetos e avaliações.

4.3 Trabalhos futuros

Integrar outras topologias de nuvem e federação para testes, testar módulos individuais e cada federação e testar seus níveis de segurança para com a arquitetura. Incluir mais SPs para testes de latência e confiabilidade da rede, além da possibilidade de integrar uma manutenção remota da federação pela nuvem.

Referências Bibliográficas

[1] AMAZON. Disponível em http://aws.amazon.com/pt/, Acesso em 12-12-2013.

[2] 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.

[3] S. Balasubramaniam, G. A. Lewis, E. Morris, S. Simanta, and D. Smith. Identity management and its impact on federation in a system-of-systems context. In *Systems conference, 2009 3rd annual IEEE*, pages 179–182. IEEE, 2009.

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

[5] S. Gilbertson. *Lessons From a Cloud Failure: It's Not Amazon, It's You*. WIRED. Disponível em http://www.wired.com/business/2011/04/lessons-amazon-cloud-failure/, Acesso em 12-12-2013.

[6] GoogleApp. Disponível em http://www.google.com/intx/pt-br/enterprise/apps/business/, Acesso em 12-12-2013.

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

[8] 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.

[9] J. Jensen and A. A. Nyre. Federated identity management and usage control-obstacles to industry adoption. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pages 31–41. IEEE, 2013.

[10] M. Jose. Modelo de autenticação para sistemas de computação na nuvem. Master's thesis, Universidade Federal do Maranhão, 2013.

[11] M. Kamal. Potential of cloud-based infrastructure for small business development. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 4860–4867. IEEE, 2012.

[12] 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.

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

[14] L. A. B. Neto. Uma arquitetura para transposição de identidades federadas para computação em nuvem. Master's thesis, Universidade Federal do Maranhão, 2013.

[15] S. Pearson. Taking account of privacy when designing cloud computing services. In *Software Engineering Challenges of Cloud Computing, 2009. CLOUD'09. ICSE Workshop on*, pages 44–52. IEEE, 2009.

[16] M. G. Rita de Castro, Luiza Domingos. Gestão de vulnerabilidades em cloud computing: Um cenário da nuvem pública. 2012. Disponível em http://www.infobrasil.inf.br/userfiles/16-S1-2-97170-GestAcesso em12-12-2013.

[17] 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.

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

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

[20] 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.

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

[22] 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.

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

[24] 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.