GUILHERME PUPOLIN DOS SANTOS

PROPOSTA DE ARQUITETURA DE MONITORAMENTO DE POLÍTICAS ORGANIZACIONAIS DE PROTEÇÃO EM AMBIENTES DE *CLOUD COMPUTING*

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia de *Software*.

São Paulo
2012

GUILHERME PUPOLIN DOS SANTOS

PROPOSTA DE ARQUITETURA DE MONITORAMENTO DE POLÍTICAS ORGANIZACIONAIS DE PROTEÇÃO EM AMBIENTES DE *CLOUD COMPUTING*

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia de *Software*.

Área de Concentração: Tecnologia de Software

Orientador: Prof. Dr. Kechi Hirama

São Paulo
2012

[verso da folha de rosto]

FICHA CATALOGRÁFICA

[Colocar na versão final do trabalho em capa dura. Verificar como fazer em Diretrizes para Apresentação de Dissertações e Teses. Escola Politécnica da USP]

DEDICATÓRIA

À minha mãe, pai, avós e amigos pela importância que possuem em minha jornada. À Bruna Martin, a mulher que escolhi para construir uma próspera família.

AGRADECIMENTOS

À Universidade de São Paulo – USP que investiu em um curso de tamanha qualidade que impulsionou a minha carreira.

À Escola Politécnica da Universidade de São Paulo – EPUSP que disponibilizou excelentes doutores e mestres para a realização desse curso.

Ao PECE – Programa de Educação Continuada em Engenharia por nos trazer os conteúdos necessários para nosso aperfeiçoamento técnico-empírico

A minha família, por serem o alicerce para minha formação pessoal e profissional.

Á Bruna Martin, minha inspiração e força para completar esta jornada.

Um agradecimento para o Rafael Prado e família que me apoiaram nos momentos que mais precisei, em especial um agradecimento para seu Zé que sempre trará força para continuar e enfrentar todas as barreiras.

RESUMO

O paradigma *Cloud Computing* tem se tornado cada vez mais popular para as organizações mundo afora. Consequentemente, diversos desafios surgem para a garantia de proteção, confiabilidade e disponibilidade das robustas infraestruturas dos Provedores de Serviço em Nuvem (*Cloud Service Provider* - CSP), sobretudo, quando se trata de Nuvens Públicas. Neste sentido, este trabalho desenvolve uma análise sobre as principais ameaças que aflingem as Nuvens Públicas e, a partir do estudo comparativo entre *frameworks* e arquiteturas especializadas em proteção e monitoramento de políticas, extrai-se um conjunto de critérios que possam pautar o desenvolvimento de novos *frameworks* e arquiteturas que buscam centralização de políticas, proteção e combate à ameaças e vulnerabilidades em Nuvens Públicas. Por fim, este trabalho propõe um *framework* com base nos critérios levantados, com o intuito de apresentar um modelo com as seguintes características: (i) Funcionamento em ambientes SaaS, IaaS e PaaS; (ii) Interoperabilidade entre diferentes CPSs; (iii) Monitoramento Proativo de Políticas; (iv) Gerenciamento de políticas de proteção como serviço; (v) Proteção às sete principais ameaças da *Cloud Alliance Security*; (vi) Escrita de politica de proteção em linguagem natural; (vii) Implantação realizada dentro da empresa.

ABSTRACT

Cloud computing paradigm has become increasingly popular for worldwide organizations. Consequently, several challenges arise for protection guarantee, reliability and availability of robust infrastructure of cloud service providers - CSPs, especially when it comes to Public Clouds. Thus, this work developed an analysis on the major threats that afflict and Public Clouds, from the comparative study of frameworks and architectures specializing in monitoring and protection policies, extracted a set of criteria that can be guided to develop new frameworks and architectures that seek to policy centralization, protection and fight against threats and vulnerabilities in Public Clouds. Finally, this paper proposes a framework based on the criteria raised in order to provide a model, with the following characteristics: (i) operating environments SaaS, PaaS and IaaS (ii) interoperability between different CPSs; (iii) Proactive Monitoring Policy, (iv) Protection Policy Management as a service, (v) Protection againt seven major threats presented by Cloud Security Alliance (vi) Written protection policy in natural language, (vii) Deploy On-premise.

LISTA DE ILUSTRAÇÕES

Pág.

LISTA DE TABELAS

Pág.

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
BaaS	*Bandwidth as a Service*
CaaS	*Communication as a Service*
CAIQ	*Consensus Assessments Initiative Questionnaire*
CCM	*Cloud Controls Matrix*
CCSK	*Cloud Security Knowledge*
CSA	*Cloud Security Alliance*
CTP	*Cloud Trust Protocol*
DaaS	*Design as a Service*
EaaS	*Entertainment as a Service*
EC	*Elastic Cloud*
EfaaS	*Efficiency as a Service*
EvaaS	*Event as a Service*
GRC	*Achieving Governance, Risk Management and Compliance*
IaaS	*Infrastructure as a Service*
InaaS	*Information as a Service*
NIST	*National Institute of Standards and Technology*
PaaS	*Plataform as a Service*
PAP	Ponto de Política de Administração
PIP	Ponto de Informação Política
PMSP	*Policy Management Service Provider*
PraaS	*Protection as a Service*
ProaaS	*Product as a Service*
QoS	*Quality of Service*
RaaS	*Reward as a Service*
RDF	*Resource Descripition Framework*
SaaS	*Software as a Service*
SeaaS	*Security as a Service*
SLA	*Service Level Agreemen*
SraaS	*Service as a Service*
TaaS	*Time Management as a Service*
TI	Tecnologia da Informação
XML	*eXtensible Markup Language*

SUMÁRIO

Pág.

1. INTRODUÇÃO

As organizações estão cada vez mais olhando para o novo paradigma *Cloud Computing* como uma grande promessa de diminuição de custos e aumento de agilidade nas operações de TI (SRIVASTAVA et. al, 2011, p. 661).

Segundo o NIST (*National Institute of Standards and Technology*), *Cloud Computing* é um modelo que permite acesso de forma conveniente, sob demanda, de qualquer local a um conjunto de recursos computacionais configuráveis. *Cloud Computing* é um híbrido de tecnologia e modelos de negócio (MELL E GRANCE, 2011, p. 2). Consequentemente, diversos aspectos acerca deste paradigma passam a ganhar espaço com o intuito de permitir seu desenvolvimento dentro das organizações.

Neste sentido, este trabalho direciona seus estudos acerca de um tema em especial que corresponde à proteção em Nuvens Públicas e formas de monitoramento deste ambiente. Para tanto, este capítulo apresenta os principais aspectos que norteiam este trabalho apresentando suas motivações, justificativas e objetivos frente suas especificidades.

1.1. Motivações

O crescimento na adoção de *Cloud Computing* aumenta a cada ano. De acordo com a empresa de pesquisas Reston, estima que os gastos com *Cloud Computing* por parte de governos estaduais e municipais nos Estados Unidos crescerão 22% ao ano entre 2009 e 2014, saltando de 230 milhões de dólares para 620 milhões de dólares. Atualmente, os recursos destinados por esses governos a TI são da ordem de 56,6 bilhões de dólares (COMPUTERWORLD, 2009)

Como todos novos paradigmas possuem diversas preocupações até alcançar um grau de estabilidade, de acordo com a pesquisa do DCUG Sprint 2010, 60% dos que responderam a pesquisa dizem que o principal conceito a ser trabalhado para adoção do *Cloud Computing* é a proteção. (SRIVASTAVA et al., 2011, p.661)

Além dos desafios usuais de desenvolvimento seguro dos sistemas de TI, *Cloud Computing* apresenta um nível adicional de risco, pois os serviços são na maioria dos casos hospedados em provedores terceirizados (ZHANG et al., 2010, p.1328).

Existem organizações que estabelecem melhores práticas para a adoção e disponibilização de *Cloud Computing* de forma segura. A *Cloud Security Alliance*, organização sem fins lucrativos, formada por um grupo de profissionais, empresas, associações e outras partes interessadas tem como missão promover a utilização das melhores práticas para a garantia de proteção dentro do *Cloud Computing*, e para fornecer treinamento sobre os usos do *Cloud Computing*. (CSA, 2012a)

A *Cloud Security Alliance* possui diversas pesquisas relacionadas à proteção de *Cloud Computing,* sendo um dos estudos, o levantamento das sete principais ameaças envolvendo *Cloud Computing* desenvolvido com a empresa americana HP em 2010, para ajudar empresas a compreenderem as ameaças atuais e futuras e oferecer contramedidas para garantir que os processos de negócios, bem como de dados permanecem protegidos na nuvem (CSA, 2010).

As sete principais ameaças levantadas foram (CSA, 2010, p.6-7):

- Abusos e mal uso de *Cloud Computing*
- Interfaces e APIs inseguras
- Atacantes
- Compartilhamento tecnológico
- Perda ou vazamento dos dados
- Sequestros de conta/serviço
- Riscos desconhecidos

Como estas ameaças estão presentes principalmente nas Nuvens Públicas (ambientes em nuvem compartilhada por diversas organizações) onde há ganhos, por exemplo, na redução de custos em relação a Nuvens Privadas (ambientes em nuvem construida exclusivamente para determinada organização), cria-se dependência com um terceiro onde normalmente os clientes têm que apostar toda

sua confiança na segurança do Provedor de Serviços em Nuvem (CSP – *Cloud Service Provider*). O *Service Level Agreement* (SLA) é o único instrumento contratual de monitoramento entre o CSP e o cliente. Esta técnica de monitoramento, é classificada como monitoramento reativo, ou seja, quando há algum tipo de rompimento de SLA, é primeiramente identificado pelo CSP que então reporta (ou pelo menos deveria reportar) as insconsistências para seus clientes, consequentemente, desacelera a tomada de decisão pelo contratante dos serviços, uma vez que o monitoramento não é bilateral. (SRIVASTAVA et al., 2011, p.663)

Contudo, foi desenvolvida uma arquitetura que possibilita o Cliente de Serviços monitorar o cumprimento dos SLAs por parte dos provedores de serviço na existência de inconsistências. Este monitoramento é classificado como Monitoramento Proativo e avalia se as políticas adotadas pela empresa estão sendo respeitadas pelo Provedor de Serviço. Este tipo de monitoramento é fundamental para Nuvens Públicas no combate às ameaças identificadas pela CSA (2010), pois garante maior transparência na relação Cliente x CSP e utiliza uma arquittura híbrida em que o Cliente mantém a implantação interna à organização em comunicação monitorada com o ambiente externo. (SRIVASTAVA et al., 2011, p.663)

Uma politica que pode ser aplicada em uma arquitetura proativa é o controle do acesso aos recursos disponibilizados nos provedores de serviço evidenciado pela obra de Takabi e Joshi (2012, p.5501), contando a grande diversidade de plataformas de *Cloud Computing* e seus respectivos acessos, não permitindo o uso de apenas uma forma, mecanismo, linguagem ou ferramenta de autorização para monitoramento das políticas de proteção empresariais

1.2. Objetivo

O objetivo do trabalho é identificar fatores essenciais para a construção de novas arquiteturas ou frameworks com foco na proteção de Nuvens Públicas e propor um *framework* experimental a partir da centralização de politicas, monitoramento proativo, acesso a recursos em plataformas heterogêneas e proteção às ameaças identificadas pelo CSA (2010).

1.3. Justificativas

O monitoramento de políticas e proteção de ambientes *Cloud* tem sido amplamente discutido na comunidade científica, de forma que diversos trabalhos foram publicados acerca deste tema, justificando sua relevância para a continuidade destes estudos.

O *Cloud Security Aliance* apresenta as principais ameaças em ambientes *Cloud* levantadas a partir de diversas pesquisas, congressos e estudos com o intuito de nortear as organizações a construir ambientes *Cloud* melhor protegidos. Este trabalho se tornou referência para a concepção de novos estudos, destacando-se Srivastava, et al. (2011), que sugere a utilização de *Cloud Policies* em ambientes de monitoramento, ou seja, políticas que levam em consideração as especificidades dos ambientes *Cloud* para proteção às ameaças levantadas pela CSP (2010).

Por outro lado, Takabi e Joshi (2012) sugerem um *framework* com foco no controle de acesso, integração, gerenciamento e proteção de políticas entre nuvens heterogêneas. Wang e Luo (2011, p.114), acrescentam que os trabalhos relacionados a SLA e tratamento de políticas em ambientes *Cloud*, tendem a se concentrar principalmente na (i) alocação dinâmica de recursos para alcançar escalabilidade e disponibilidade do QoS; (ii) na provisão e gerenciamento automático de recursos; e (iii), estudo de perpectivas de mercado para provisão de serviços.

Os objetivos deste trabalho vão ao encontro das perspectivas apresentadas e, para pautar os conceitos trabalhados a respeito de arquitetura e *framework*, se baseia – primeiramente – na observação do clássico Zachman (1987, p.291) "*There is not an information systems architecture, but a set of them! Architecture is relative. What you think architecture is depends on what you are doing*", e entende "arquitetura" dentro da esfera de *Cloud Computing* como um padrão tecnicamente detalhado com fluxo e organização de seus elementos (físicos e/ou lógicos) capazes de definir uma estrutura base para a criação de um ambiente. Por outro lado, ao tratar de *framework* este trabalho remete a ideia de um arcabouço de conceitos, ferramentas e soluções tecnológicas combinadas e estruturadas servindo de base para um *rol* de soluções derivadas. (ZACHMAN, 1987)

1.4. Estrutura do Trabalho

O Capítulo 1 INTRODUÇÃO, apresenta as motivações, o objetivo, as justificativas e a estrutura do trabalho.

O Capítulo 2 *CLOUD COMPUTING*, apresenta a conceituação de *Cloud Computing*, suas caracteristicas, modelo de serviços e modelos de implantação de acordo com Mell e Grance (2011).

O Capítulo 3 RISCOS, AMEAÇAS E VULNERABILIDADES apresenta uma breve descrição da CSA – *Cloud Security Alliance*, introdução aos conceitos de ameaças, riscos e vulnerabilidades, apresentação das sete principais ameaças aos ambientes *Cloud* identificadas pela CSA e a proposição de sete principais critérios para uma arquitetura/framework integrado.

O Capítulo 4 ANÁLISE DE FRAMEWORKS E ARQUITETURAS DE MONITORAMENTO DE POLÍTICAS, apresenta a análise de cinco arquiteturas/*frameworks* e realiza uma comparação para identificar arquiteturas/*frameworks* compatíveis entre sí e aderentes aos critérios definidos no Capítulo 3 para a proposição de uma arquitetura/*framework* integrada.

O Capítulo 5 PROPOSTA DE ARQUITETURA/FRAMEWORK DE MONITORAMENTO, apresenta a proposição de uma nova arquitetura/framework integrada com base nos sete critérios apresentados no Capítulo 3, integrando as duas arquiteturas/*frameworks* mais aderentes aos critérios apresentadas no Capítulo 4.

O Capítulo 6 CONSIDERAÇÕES FINAIS, realiza o fechamento deste trabalho, concluindo aspectos relevantes sobre o trabalho além de propor estudos futuros acerca dos temas aqui levantados.

2. CLOUD COMPUTING

A *Cloud Computing* é um dos principais paradigmas da computação contemporânea, evidenciado principalmente pela perspectiva de orientação a serviços cuja dinâmica possibilita recursos computacionais (outrora mantidos pelas empresas como ativos e/ou produtos por consumidores em geral) serem acessados a partir de um provedor externo, sem a necessidade de manter uma infraestrutura computacional própria. Como o próprio Gartner (2012a) cita “A *Cloud Computing* vai modificar a TI como nunca fez antes”, pois modifica a tradicional perspectiva de que as empresas devem possuir infraestrutura de TI robusta mesmo que não seja o *core business* da empresa.

Este capítulo, então, apresenta uma visão geral sobre os conceitos que envolvem a *Cloud Computing* apresentando uma visão bastante ampla de forma a contextualizar o macrotema que este trabalho está envolvido.

2.1. Definição

Este trabalho tomará como referência primária para *Cloud Computing* a definição apresentada pelo *National Institute of Standards and Technology* – NIST como se vê a seguir:

> *Cloud Computing* é um modelo que permite acesso ubiquo, conveniente e on-demand à rede para um pool de recursos computacionais configuráveis compartilhados (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente fornecidos e liberados com o mínimo esforço de gerenciamento ou interação com o provedor de serviços. Este modelo de computação é composto de cinco características essenciais, três modelos de serviço e quatro modelos de implantação. (MELL e GRANCE, 2011, p.2)

A partir desta definição é possível compreender que a *Cloud Computing* é um modelo computacional que permite acesso a um conjunto de recursos compartilhados (armazenamento, aplicações, *softwares*, etc.) com o mínimo esforço ou interação com o provedor de serviços.

Gong, et al (2010, p.275) abordam que a *Cloud Computing* é baseada em TCP/IP integrada com tecnologias computacionais (rápido processamento, rede de

alta velocidade, grande quantidade de memória, arquitetura de sistema confiável). Já Sousa, Moreira e Machado (2009, p.3), com sua perspectiva orientada ao consumidor, mostra que o *Cloud Computing* permite que aos usuários o acesso aos serviços sem a necessidade de conhecimento sobre a tecnologia utilizada, fazendo com que os consumidores em geral possam acessá-los sob demanda independente de localização e conhecimento técnico.

Mesmo frente a estas discussões, é importante ressaltar que, existem diversas conceituações científicas para *Cloud Computing*, tornando evidente que este ainda é um termo em construção, sendo resultado – inclusive – de uma nova perspectiva para a computação paralela como aborda Gong et al. (2010, p.276) a *Cloud Computing*, *Grid Computing*, Computação de Alta Performance ou supercomputação e *Data Center Computing* pertencem todas à Computação Paralela. Mas, ainda sim, existem mais de 20 definições para *Cloud Computing* e cada uma delas possui foco em determinadas características desta tecnologia bem como seu surgimento. (GONG et al., 2010, p.275)

Desta forma, para um melhor entendimento da *Cloud Computing*, os próximos tópicos apresentam suas principais características, modelos de serviço e modelos de implantação sempre tendo como referência primária o Mell e Grance (2011).

2.2. Principais Características

Muitas das definições de *Cloud Computing* estão intimamente baseadas em suas características ímpares, responsáveis pelo surgimento deste novo conceito. Em linhas gerais, a *Cloud Computing* é gestada sob a convergência de tecnologias e serviços que, de acordo com Mell e Grance (2011, p.2) são responsáveis por compor cinco principais características dispostas na Tabela 1.

Tabela 1 – Características da *Cloud Computing* adaptado do Mell e Grance (2011, p.2)

Características	**Conceito central**
Self-service sob demanda (*On-demand self-service*)	Possibilidade de administrar os recursos sem necessidade de auxílio humano dos provedores de serviço.
Acesso à rede (*Broad network access*)	Garantia de acesso à administração dos recursos a partir de plataformas heterogêneas
Pooling de recursos (*Resource pooling*)	Capacidade de configuração de uso de acordo com especificidades geográficas, público alvo, entre outras necessidades personalizadas de serviço.
Elasticidade (*Rapid elasticity*)	Capacidade dos recursos de infraestrutura se adaptarem às demandas de uso, aumentando ou diminuindo capacidade.
Serviço medido (*Measured service*)	Capacidade de medir, controlar e monitorar o uso dos recursos contratados.

As características de *self-service* sob demanda do *Cloud Computing*, vão ao encontro à necessidade do consumidor adquirir serviços de forma instantânea e sob demanda sem a necessidade de interação humana. Ou seja, o cliente pode utilizar, configurar, comprar serviços virtualmente, sem necessidade de entrar em contato com um atendente.

O acesso à rede, por sua vez, corresponde a capacidade de acesso aos serviços a partir de mútiplas plataformas, por exemplo, tecnologias móveis. Em linhas gerais, a concepção de *Cloud Computing* faz com que não haja impeditivos para acessar os serviços e/ou paineis de controles dos mesmos, tornando fundamental o acesso remoto. Se o usuário desejar acessar seu painel de controles, a partir de seu *smartphone*, existe uma interface que possibilita este acesso.

A idéia de realizar um *pooling* de recursos personalizado para os serviços, vai ao encontro da capacidade de configuração dos serviços de acordo com a expectativa de uso e/ou necessidade de seus clientes, por exemplo, para diferentes

localidades. Neste sentido, é possível diferenciar a largura de banda dos serviços da Europa, Brasil, Norte América dinamicamente, de acordo com as necessidades e estratégias.

A elasticidade corresponde ao rápido escalamento de infraestrutura quando a infraestrutura corrente deixa de suprir o tráfego de banda/demanda de armazenamento/consumo do serviço contratado. Em outras palavras, a elasticidade garante teoricamente recursos computacionais infinitos, o que é explicado pelo rápido oferecimento de capacidade de consumo extra caso a capacidade de consumo existente seja totalmente utilizada. É importante ressaltar que, na mesma medida, o responsável pela contratação do serviço deverá arcar financeiramente com o consumo extra.

Para tanto, o serviço medido, garante o total controle, medição e monitoramento do serviço que está sendo utilizado. Esta característica é fundamental, principalmente em serviços elásticos pois garante transparência entre o cliente e provedor de serviços fazendo com que os processos de cobrança ocorram automaticamente, mas com garantia do nível de serviço acordado, acompanhando todo o processo.

Em linhas gerais, estas são as cinco principais características responsáveis por compor um serviço de *Cloud Computing*. Algumas fontes na literatura detalham estas características de acordo com suas necessidades gerando subcaracterísticas. Como abordam Gong et al. (2010, p.276), existem diversos sistemas e serviços de *Cloud Computing* com suas próprias características, dentre eles: Amazon EC2, Google App Engine, Microsoft Azure. Porém, em síntese, eles se baseiam nas cinco características discutidas.

2.3. Modelos de Serviço

Os modelos de serviço correspoondem as formas de oferecimento da *Cloud Computing* para seus clientes, sejam estes internos ou externos à organização. O Mell e Grance (2011, p. 2-3) apresenta três modelos de serviço: (i) SaaS – *Software*

as a Service; (ii) PaaS – *Plataform as a Service*; e, (iii) IaaS – *Infrastructure as a Service*. Para o entendimento de cada um destes modelos, este trabalho irá se basear primariamente na abordagem de Mell e Grance (2011, p.275) seguida de complementações de outros centros de pesquisa e ou pesquisadores.

Tratando-se de SaaS - *Software as a Service* (ou Software como um Serviço), tem-se a seguinte proposição:

> A capacidade oferecida ao consumidor é usar aplicativos do provedor rodando em uma infraestrutura Cloud. As aplicações são acessíveis a partir de vários dispositivos do cliente como um navegador ou uma interface de programa. O consumidor não administra ou controla a infra-estrutura subjacente à nuvem, incluindo rede, servidores, sistemas operacionais, armazenamento, ou até mesmo recursos de aplicativos individuais, com exceção de limitadas configurações específicas de aplicativos do usuário. (MELL E GRANCE, 2011, p.2)

O exposto possibilita o entendimento de que no modelo de serviço SaaS – *Software as a Service*, o provedor do serviço (sistema) se responsabiliza pela infraestrutura base para que este possa ser acessado pelo cliente. Este acesso pode ocorrer via browser ou a partir da interface de um programa. Em linhas gerais, a partir destas definições, é possível entender que o SaaS possibilita que o cliente mantenha foco em seu negócio de forma que não há dispendio financeiro e/ou esforços para manter uma infraestrutura física de servidores, banco de dados, entre outros localmente na empresa. Neste sentido, Espadas et al (2008, p.98) ilustram este modelo de serviços a conforme a Figura 1.

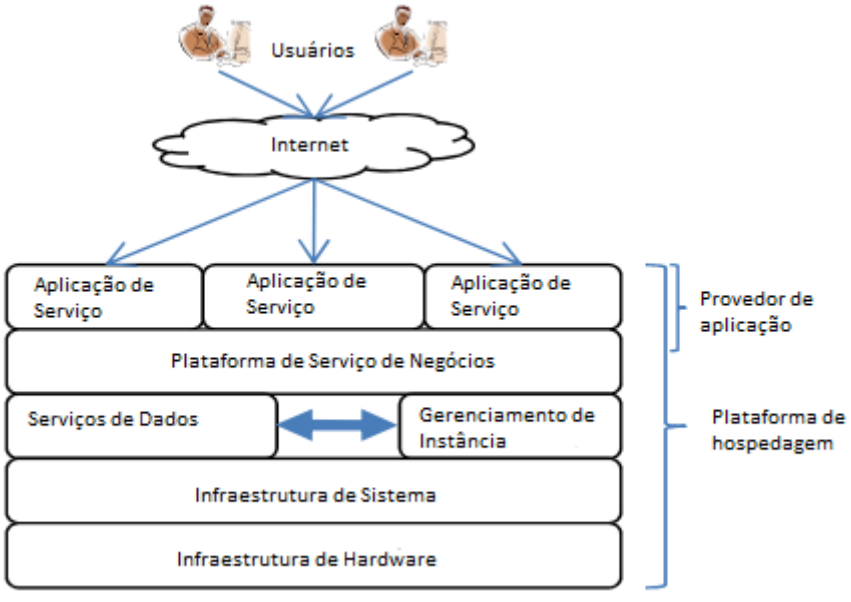

Figura 1 – Arquitetura SaaS (ESPADAS et al., 2008, p.98)

Este novo modelo de serviço possui grandes perspectivas de crescimento e retornos para o mercado de tecnologia. Como abordam Espadas et al., (2008, p.97) “Não é porque é uma “ideia legal”, mas porque fundamentalmente altera a economia dos softwares”. De acordo com o Gartner (2012b), os investimentos em SaaS em 2012 irão atingir 14.5 bilhões de dólares e, para 2015, estima-se 22.1 bilhões de dólares.

Por outro lado, quando se trata de PaaS – *Plataform as a Service* (ou Plataforma como um Serviço), Mell e Grance (2011, p.2-3) apresenta a seguinte definição:

> A capacidade oferecida ao consumidor é implantar uma infra-estrutura Cloud para para criação de aplicações usando linguagens de programação, bibliotecas, serviços e ferramentas de suporte do provedor. O consumidor não administra ou controla a infra-estrutura subjacente à nuvem, incluindo rede, servidores, sistemas operacionais, ou armazenamento, mas tem controle sobre os aplicativos implementados e configurações para o ambiente de hospedagem do aplicativo. (MELL E GRANCE, 2011, p.2-3)

Entende-se que o modelo de serviço PaaS – *Plataform as a Service* oferece uma plataforma de desenvolvimento de sistemas/aplicações a partir de um ambiente em nuvem. Novamente, o cliente não precisa se preocupar em manter uma infraestrutura própria de servidores, sistema operacional ou banco de dados, mas possui controle sobre o ambiente de desenvolvimento, o que possibilita, também configurar o ambiente do servidor. De acordo com publicação da Eweek (2012), o Gartner acrescenta:

> PaaS é uma referência comum para a camada de arquitetura Cloud que contém todos as aplicações de serviços de infra-estrutura, também conhecidas como "middleware". PaaS é a camada do meio da pilha de software "na nuvem". É a tecnologia intermediária entre a infra-estrutura subjacente do sistema (sistemas operacionais, redes, virtualização, armazenamento, etc) e aplicações de software. (EWEEK, 2012)

A partir desta visão, entende-se o PaaS como uma plataforma que se localiza entre a aplicação que está sendo desenvolvida e a infraestrutura mantida pelo provedor do serviço. O Gartner prevê que até 2015, a maioria das empresas terão parte de seus “*softwares* de negócio operando na nuvem, utilizando tecnologias ou serviços PaaS direta ou indiretamente. Ademais, estima que até 2016, a competição

entre os vendedores PaaS, irá impulsionar novos modelos de programação, padrões de desenvolvimento e líderes de mercado. (EWEEK, 2012)

Por fim, quando se trata de IaaS - *Infrastructure as a Service* (ou Infraestrutura como um Serviço) Mell e Grance (2011 p.3) apresentam a seguinte definição:

> A capacidade oferecida para o consumidor é a provisão de processamento, armazenamento, redes e outros recursos computacionais com capacidade de implantação e execução arbitrária, possibilitando incluir sistemas operacionais e aplicativos. O consumidor não administra ou controla a infra-estrutura cloud subjacente, mas tem controle sobre sistemas operacionais, armazenamento, aplicativos implementados e controle limitado dos componentes de rede selecionados (por exemplo, *firewalls* do *host*). (MELL E GRANCE, 2011, p.3)

O modelo de Serviços IaaS – *Infrastructure as a Service*, refere-se à capacidade de oferecimento de infraestrutura (processamento, armazenamento, componentes de rede, entre outros recursos) como um serviço, possibilitando que o consumidor possa incluir suas próprias aplicações, sistema operacional, configuração do servidor e dos componentes de rede, por exemplo, *firewall*. Neste modelo, o usuário pode comprar a infraestrutura que deseja, quatidade de processamento e armazenamento de forma que vá ao encontro de sua necessidade de negócios enquanto o provedor do serviço se responsabiliza pela infraestrutura física.

O Gartner (2011), por sua vez, entende que o IaaS – *Infrastructure as a Service* irá transformar toda a concepção de infraestrutura em TI nos próximos 10-20 anos. Em linhas gerais, de acordo com seus estudos o crescimento da IaaS de 2011 (previsto para de 3.7 bilhões de dólares) atingirá 10.5 bilhões de dólares em 2014.

Algumas literaturas, além de Mell e Grance (2011), ressaltam sobre a existência de novos modelos de serviço para a *Cloud Computing*, em que o mais comum é o StaaS – *Storage as a Service*, ou Armazenamento como Serviço. De acordo com Kundu, Banerjee e Saha (2010, p.146):

> Armazenamento como um serviço é um modelo de negócio em que uma grande empresa pode alugar o espaço de armazenamento para uma pequena empresa ou indivíduo através de sistemas de *Cloud Computing*. A principal vantagem de StaaS está na redução de custos - em pessoal, em *hardware* e em espaço de armazenamento físico. Por exemplo, um administrador de rede normalmente usa StaaS para *backup* de dados armazenados conforme o necessário, em vez de manter uma grande biblioteca de fitas e disposição de discos de armazenamento. (KUNDU, BANERJEE E SAHA, 2010, p.146)

A abordagem de StaaS corresponde a uma abordagem bastante específica em que a capacidade de armazenamento passa a ser oferecida como um serviço a partir de discos remotos de armazenamento que podem ser acessados em qualquer lugar. É bastante específico pois, como já foi abordado anteriormente, o modelo de serviço IaaS também oferece capacidade se armazenamento em seu portfólio de serviços, a questão é que, no StaaS, a especificidade garante que serviços como recuperação de desastres, *backup*, armazenamento de arquivos primário, secundário, terceário, etc. possam ser oferecidos com custo mais competitivo além maiores chances de personalização.

Apesar disso, Wu et al. (2010, p.381) chamam atenção ao fato de que, serviços de armazenamento possuem um conjunto de pré-requisitos para a garantia de integridade, confiabilidade, disponibilidade, etc., mas, devido à natureza conflitante destes requisitos ainda não há modelos que conseguem disponibilizar todos em um mesmo serviço.

É importante ressaltar que, estes modelos de serviço mais específicos correspondem a uma gama de novos serviços que vem sendo oferecidos dentro da *Cloud Computing* tangenciando necessidades mais pontuais. A partir da pesquisa de Kundu, Banerjee e Saha (2010, p.143), identificam-se os seguintes novos serviços: *Information as a Service* (InaaS), *Bandwidth as a Service* (BaaS), *Security as a Service* (SeaaS), *Design as a Service* (DaaS), *Product as a Service* (ProaaS), *Communication as a Service* (CaaS), *Entertainment as a Service* (EaaS), *Protection as a Service* (PraaS), *Efficiency as a Service* (EfaaS), *Time Management as a Service* (TaaS), *Reward as a Service* (RaaS), *Event as a Service* (EvaaS), *Service as a Service* (SraaS).

Isso mostra uma crescente demanda pelos modelos orietados à serviços e que, para além dos modelos tradicionais (IaaS, SaaS e PaaS) o *Cloud Computing* está imersa em um processo constante de atualização de sua estrutura bem como capacidade de geração de valor para seus consumidores.

2.4. Modelos de Implantação

Os modelos de implantação correspondem ao tipo de infraestrutura que comporta a nuvem de serviços. É importante entender que esta infraestrutura pode possuir diversos níveis de acesso, diferentes políticas de proteção e tecnologias que garantem maior ou menor segurança dos dados e informações que trafegam pelo serviço, exclusividade, desempenho, além de outros fatores que podem ser definidos caso a caso de acordo com o nível de serviços que o cliente está interessado.

Mell e Grance (2011, p.3) apresentam quatro modelos principais de implantação: (i) *Private Cloud* (Nuvens Privadas); (ii) *Community Cloud* (Nuvens Comunitárias); (iii) *Public Cloud* (Nuvens Públicas); e, (iv) *Hybrid Cloud* (Nuvens Híbridas);

As nuvem privadas, são construidas exclusivamente para determinada organização a partir de políticas próprias e liberdade de acesso delimitada pela organização. Como abordam Mell e Grance (2011):

> A infraestrutura de *Cloud* é provisionada para uso exclusivo de uma única organização compreendendo vários consumidores (por exemplo, unidades de negócios). Podem ser de propriedade, gerenciadas e operadas pela organização, um terceiro, ou alguma combinação entre eles, podendo existir dentro ou fora de suas instalações. (MELL E GRANCE, 2011, p.3)

Devido a suas caracteristicas exclusas, as nuvens privadas são conhecidas por possuir maior nível de segurança quando comparada às nuvens públicas, geralmente são estabelecidas em data centers privativos e com acordo de nível de serviços personalizado às necessidades do cliente.

Diferente das nuvens privadas, as nuvens públicas possibilitam o acesso público, ou seja, não restritivo. Em linhas gerais, as nuvens públicas contém

aplicações e sistemas de diversos usuários que coexistem. Para este modelo de nuvem, Mell e Grance (2011) apresentam a seguinte observação:

> A infraestrutura de *Cloud* é provisionada para uso aberto ao público em geral. de negócios). Podem ser de propriedade, gerenciadas e operadas por uma empresa, setor acadêmico ou organização governamental, ou alguma combinação entre eles. Ela existe nas instalações do provedor de serviços Cloud. (MELL E GRANCE, 2011, p.3)

As nuvens públicas são constantemente questionadas em relação a sua performance e segurança devido ao carater público, rol de serviços rodando simultaneamente, ambiente compartilhado, entre diversos outros fatores.

As nuvens comunitárias, por sua vez, suportam uma comunidade específica organizações que compartilhem de um mesmo SLA (*Service Level Agreement*), políticas de proteção, interesses em comum. De acordo com Mell e Grance (2011, p.276):

> A infraestrutura de *Cloud* é provisionada para uso exclusivo por uma comunidade específica de consumidores, de organizações que têm preocupações em comum (por exemplo, a missão, os requisitos de segurança, política e considerações de conformidade). Podem ser de propriedade, gerenciadas e operadas por uma ou mais das organizações da comunidade, um terceiro, ou alguma combinação entre eles, podendo existir dentro ou fora de suas instalações. (MELL E GRANCE, 2011, p.3)

Economicamente, as nuvens comunitárias costumam ser mais caras que as nuvens poúblicas, porém mais baratas que as nuvens privadas devido ao compartilhamento com outras organizações.

As nuvens híbridas, por fim, são compostas por nuvens privadas e nuvens públicas que interagem entre si. De acordo com Mell e Grance (2011, p.3):

> A infraestrutura em nuvem é uma composição de duas ou mais infra-estruturas de cloud distintas (comunidade, privado ou público) que permanecem como entidades únicas, mas estão unidas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicativos. (MELL E GRANCE, 2011,p.276)

Este tipo de nuvem permite a ampliação dos serviços de uma nuvem privada a partir da reserva de recursos em uma nuvem pública. Em linha gerais, esta ação estratégica permite que, em momentos de instabilidade dos serviços da nuvem

privada, seus serviços possam minimamente ser oferecidos a partir das nuvens públicas.

2.5. Considerações do Capítulo

As definições deste capítulo são fundamentais para entender a macroesfera que este trabalho está inserido e, principalmente, deixar claro sobre qual perspectiva conceitual este trabalho se baseia frente as diversas concepções de *Cloud Computing* presentes na comunidade científica.

Os capítulos seguintes desenvolvem uma abordagem com foco na garantia de maior proteção para Nuvens Públicas cujo Capítulo 3 apresenta os principais desafios enfrentados pela *Cloud Computing* no que se referem aos riscos, ameaças e vulnerabilidades da tecnologia.

3. RISCOS, AMEAÇAS E VULNERABILIDADES

O crescimento em escala mundial do paradigma *Cloud Computing* alavanca, sobremaneira, desafios relacionados à proteção de dados e informações principalmente no que se refere às nuvens públicas.

A partir das publicações "*Security Guidance for Critical Areas in Cloud Computing*" e "*Top Threats to Cloud Computing*" pela *Cloud Alliance Security* (CSA), têm-se uma visão profunda destes desafios que plotam à reflexão e a pesquisas ao redor do mundo com o intuito de garantir um maior nível de confiança no trato das nuvens públicas por ser diretamente afetada pelas ameaças tais como, uso nefasto e abusivo da *Cloud Computing*, interfaces e APIs inseguras, usuários maliciosos, problemas no compartilhamento tecnológico, perda e vazamento de dados, roubo de contas e serviços, riscos desconhecidos. (CSA, 2010)

A problemática se faz presente, pois, a utilização de nuvens públicas possibilita terceirizar toda a infraestrutura computacional da organização para um provedor de serviços, usufruindo apenas o necessário. Dentre os principais impactos para o negócio, destaca-se a diminuição dos custos operacionais, mas que, em contrapartida, se depara com riscos à proteção dos dados e informações da organização principalmente em serviços cujas políticas exigem alto nível de garantia, dificultando, inclusive, o estabelecimento de um SLA que atenda às necessidades do negócio .(CSA, 2010)

Frente a isso, este capítulo apresenta uma visão profunda sobre o papel da *Cloud Alliance Security* (CSA) no tratamento de ameaças em ambientes Cloud, refletindo sobre riscos, vulnerabilidades e definições propostas pela CSA e um conjunto de especialistas em proteção de dados e informações na nuvem.

3.1. Cloud Security Alliance (CSA)

O CSA – *Cloud Security Alliance* é uma organização sem fins lucrativos que promove investigações em melhores práticas de segurança nos ambientes *Cloud*. Dentre suas iniciativas, a CSA fornece capacitação e orientação para empresas do ramo além de auxiliar os CSPs a garantirem modelos de negócio seguros. (CSA, 2012a)

Além disso, possui um conjunto de programas, projetos e ações no campo da proteção da informação em ambientes *Cloud*, além de desenvolver pesquisas, eventos, conferências e publicar artigos e relatórios com o intuito de ajudar empresas e CSPs garantirem seus serviços de *Cloud Computing*.

Dentro do campo de ferramentas, pode-se destacar o GRC Stack que fornece um kit de ferramentas para avaliar nuvens privadas e públicas contra práticas que possam comprometer a proteção. Dentre as iniciativas do GRC (*Achieving Governance, Risk Management and Compliance*), pode-se citar como exemplo o *CloudAudit*, desenvolvido para simplificar processos de auditoria e coleta de dados, criando uma maneira padrão para os CSPs possam se comunicar de maneira segura e em conformidade com os niveis de serviço estabelecidos. As demais soluções relacionadas ao GRC são: *Cloud Controls Matrix* (CCM), *Consensus Assessments Initiative Questionnaire* (CAIQ), *Cloud Trust Protocol* (CTP). (CSA, 2012b)

O CSA também possui programas de certificação profissional, dentre as quais pode-se destacar o Cloud Security Knowledge (CCSK), projetado a partir de um rol de questões relaconadas à segurança em nuvem. O *syllabus* do exame é baseado em dois principais documentos: (i) "Orientação de Segurança para Áreas Críticas de foco em *Cloud Computing*"; e (ii) "*Cloud Computing*: Benefícios, Riscos e Recomendações para a Segurança da Informação", da Agência Europeia para a Segurança da Informação. (CSA, 2012c)

No que tece ao quadro de profissionais, a CSA é composta por pesquisadores e especialistas em segurança da informação, possui programa de afiliação e apoio de empresas que contribuem com capital tecnológico, financeiro e humano.

Esta estrutura possibilitou a publicação do documento "*Top Threats to Cloud Computing*" (CSA, 2010), cuja proposta visa auxiliar as organizações a tomarem decisões estatégicas a respeito de ameaças aos ambientes *Cloud*, melhor detalhadas nas próximas seções.

3.2. Riscos, Ameaças e Vulnerabilidades

Quando o assunto é proteção de dados e informações, muito se fala sobre ameaças, riscos e vulnerabiliades. Apesar disso, estes termos geram – muitas vezes – confusão e conflitos a respeito de seus significados dentro das discussões sobre segurança da informação.

De acordo com PMBOK (2008, p.226), o risco é um evento ou uma condição incerta que, se ocorrer, tem efeito em pelo menos um objetivo do projeto. Caso algum destes eventos se concretize, o mesmo pode influenciar positiva ou negativamente o projeto, sistema, ou contexto que esteja inserido. O ISO/IEC (2002, p.2) acrescenta que riscos correspondem a uma relação entre probabilidade de acontecimento x possíveis consequências. Na proposição do MoR (2012), o risco é definido como:

> Risco é um evento incerto ou conjunto de eventos que, se ocorrer, terá um efeito sobre a realização dos objetivos. Um risco é composto por uma combinação da probabilidade de ocorrência de uma ameaça ou oportunidade e a magnitude do seu impacto sobre os objetivos. (MoR, 2012)

Tratar riscos na esfera da proteção por sua vez, significa prever possíveis impactos para os clientes internos ou externos de determinados sistemas, serviços, produtos em relação a confiabilidade, integridade, disponibilidade e autenticidade dos dados e informações de uma organização. Como exemplificam Dahbur, Mohammad e Tarakji (2011, p.3):

> Por exemplo, se os usuários não são educados em processos e procedimentos, há uma probabilidade maior de que um empregado fará uma falta intencional ou não intencional que pode destruir dados. Risco amarra a vulnerabilidade, ameaça, e a probabilidade de exploração para o impacto nos negócios resultante. (DAHBUR, MOHAMMAD E TARAKJI, 2011, p. 3)

Neste sentido, a ISO/IEC (2002, p. 2), explicita que “cada vez mais, as organizações utilizam processos de gestão de risco, a fim de otimizar a gestão de oportunidades em potencial ". Tanto em organizações provedoras de serviços de *Cloud* (CSPs) quantas organizações clientes de serviços de *Cloud*, têm se mantido atentas aos riscos de determinadas tecnologias, sobretudo suas ameaças a partir avaliação e tomada de decisão devido a falhas que possam afetar produtos/serviços/informações das organizações.

Na visão de Dahbur, Mohammad e Tarakji (2011, p.3) uma ameaça corresponde a qualquer perigo em potencial para as informações ou sistemas de uma organização. A ameaça pode ser alguém ou alguma coisa que irá identificar uma vulnerabilidade específica e utilizá-la contra a empresa e/ou indivíduo. Estas vulnerabilidades, dizem respeito às fraquezas presentes em um *software*, *hardware* ou processo,que podem repercutir em uma uma porta de entrada para agentes maliciosos terem acesso a ambientes e/ou dados/informações restritos. Como abordam Dahbur, Mohammad e Tarakji (2011, p.3), vulnerabilidade caracteriza a ausência ou fraqueza de uma salvaguarda que poderia ser explorada.

3.3. Principais Ameaças

Como mencionado anteriormente, as principais ameaças aos ambientes *Cloud* são retratados pela CSA (2010) com a publicação do “*Top Threats to Cloud Computing*” sob a seguinte perspectiva:

> O objetivo deste documento, " *Top Threats to Cloud Computing",* é fornecer o contexto necessário para auxiliar as organizações na tomada de decisões referentes a gestão de risco em relação as estratégias de adoção de ambientes Cloud [...] Nosso objetivo é fornecer um produto de identificação de ameaças que possa ser rapidamente atualizado para refletir a dinâmica da Cloud Computing e evoluir rapidamente o ambiente de ameaça. (CSA, 2010, p.6)

Na atualidade, este artigo é uma das principais referências da área, sendo concebido a partir de uma série de debates, discussões e pesquisas que identificam sete principais ameaças à proteção dos ambientes *Cloud*. Como é abordado na pesquisa, o foco foi identificar características únicas e inerentes aos ambientes de *Cloud Computing*.

> Embora muitas questões, como a estabilidade financeira do provedor, criação de riscos significativos para os clientes, nós tentamos concentrar em questões que sentimos ser exclusivas ou muito ampliada pelas características-chave de Cloud Computing e seu compartilhamento, de natureza on-demand. (CSA, 2010, p.6)

Vale ressalta que a CSA visa dar continuidade à pesquisa para que esta possa ser periodicamente atualizada, para tanto, objetiva-se lançar uma segunda versão do documento em Julho de 2012.

De modo geral, a versão de 2010 foi responsável por identificar as seguintes ameaças:

1. Uso abusivo e transgressivo da computação em nuvem;
2. APIs inseguras;
3. Colaboradores internos mal intencionados;
4. Problemas relacionados ao compartilhamento tecnológico;
5. Perda e vazamento de dados;
6. Roubo de contas e serviços;
7. Perfil de riscos desconhecidos;

A Tabela 2 apresenta cada uma das ameaças listadas com maiores detalhes.

Tabela 2: Ameaças em ambientes *Cloud* (CSA, 2010, p.8-14)

Ameaça	**Descrição**	**Modelo Afetado**
Uso abusivo e transgressivo da computação em nuvem	Provedores IaaS oferecem aos seus clientes a ilusão de computação ilimitada, possibilitando aderir aos serviços com apenas um número de cartão de crédito válido, quando não oferecem a utilização de seus serviços com um periodo gratuito e sem maiores compromissos. A questão é que estes cadastros muitas vezes não verificam a validade do usuário cadastrado, e abusam desta anonimidade decorrente de um processo de cadastro frágil, spamers, desenvolvedores de aplicativos maliciosos e outros criminosos virtuais tem abusado destas brechas com certa impunidade,sobretudo,em ambientes PaaS. Consequentemente, os CSPs precisam de um processo de registro e validação mais rigoroso, inspeção rígida de tráfego de rede de usuários, e outras medidas de proteção.	IaaS e PaaS
APIs inseguras	Provedores de computação em nuvem (CSPs) disponibilizam uma série de interfaces de software ou APIs que usuários gerenciam e interagem com os servidores, porém, empresas e terceiros comumente realizam customizações e desenvolvimentos sobre essas APIs o que pode repercutir em aberturas para ataques e roubo de informações devido a falhas residuais. Para combater esta ameaça, são necessários processos que analisem o modelo de proteção das interfaces do CSP, além de autenticação forte com processos de controle encriptados.	Todos
Colaboradores internos mal intencionados	A ameaça de colaboradores internos mal intencionados é bem conhecida e resulta em espionagem industrial, roubo de informações, ataque a serviços. Em Cloud Computing, pela convergência entre serviços e clientes sob uma gestão única de domínio, combinado com a falta de transparência nos processos e procedimentos adotados pelos CSPs, este problema se torna ainda mais grave, sendo necessário processos que garantam a gerência e controle restritivo da cadeia de fornecimento conduzindo validação do CSP, transparência nas práticas de segurança como também dos relatórios de conformidade.	Todos
Problemas relacionados ao compartilhamento tecnológico	Fornecedores IaaS entregam serviços de forma escalável através da partilha infraestrutura. Muitas vezes, os componentes básicos que compõem esta infra-estrutura (por exemplo, caches de CPU, GPU, etc.) não foram projetados para oferecer propriedades de isolamento robustas para arquitetura multiusuários gerando níveis inapropriados de controle ou influência sobre plataformas subjacentes. È necessário uma forte compartimentalização para garantir que operações de um cliente não impactem negativamente em outros sistemas de outros clientes, uma vez que estes não devem ter acesso a nenhum dado, tráfego de rede, etc, atual ou residual de outrem.	IaaS
Perda e vazamento de dados	Existem vários modos de comprometer dados. Exclusão ou alteração de dados gravados sem a cópia de segurança do conteúdo é um exemplo. Perder a ligação entre um dado gravado e sua referência pode torná-lo irrecuperável assim como gravá-lo em uma mídia não confiável. Finalmente, partes não autorizadas devem ser impedidas de obterem acesso a dados sem autorização. A ameaça de comprometimento de dados aumenta no ambiente de computação na nuvem devido alto número de interações. Medidas como implementar forte controle de acesso em APIs, encriptar e proteger a integridade de dados em trânsito, analisar proteção de dados tanto em produção quanto em projeto, são necessárias contra esta ameaça.	Todos
Roubo de contas e serviços	Métodos de ataque, como phishing, fraude e exploração de vulnerabilidades de software são bastante comuns e o mesmo ocorre em ambientes Cloud. Se um invasor obtém acesso a credenciais de um Cloud User, eles podem espionar suas atividades e transações, manipular dados, retornar informações falsas, e redirecionar seus clientes a sites ilegítimos, utilizando a força da reputação da brand da empresa para replicar ataques na nuvem. Medidas como, proibir compartilhamento de credenciais de acesso entre usuários e serviços, utilizar técnicas de autenticação forte quando possível, empregar monitoramento proativo para detecção de atividades não autorizadas, são algumas das alternativas para combater esta ameaça.	Todos
Perfil de risco desconhecido	Um dos princípios do *Cloud Computing* é a redução da posse e responsabilidade de manutenção de hardware e software permitindo as empresas focarem em seu core business. Porém, pode resultar em exposições desconhecidas além de poder impossibilitar análises profundas em ambientes operacionais com alta necessidade de controle devido a pontos de obscuridade. Dentre as principais medidas para combater esta ameaça, destacam-se gerenciamento de logs de acesso, programação e monitoramento de alertas.	Todos

A definição destas ameaças é fundamental para o detalhamento da arquitetura/*framework* proposto por este trabalho, e são detalhas na seção a seguir.

3.4. Critérios para Elaboração de uma Arquitetura ou F*ramework* Integrado

Para a construção de uma arquitetura ou *framework* integrado com foco na proteção contra ameaças, ampla cobertura de modelos de serviço e garantia de melhor experiência para o usuário, as pesquisas realizadas por este trabalho propõem sete principais critérios para a composição de uma nova arquitetura ou *framework* integrado. Estes critérios têm como base arquiteturas e *frameworks* que os utilizam individualmente, mas que se utilizados em conjunto, a partir de uma arquitetura que comporte sua integração, podem proporcionar uma melhor experiência no trato das ameaças evidenciadas por este capítulo. Os critérios destacados são: (i) Funcionamento em ambientes SaaS, IaaS e PaaS; (ii) Interoperabilidade entre diferentes CPSs; (iii) Monitoramento Proativo de Políticas; (iv) Gerenciamento de políticas de proteção como serviço; (v) Proteção às sete principais ameaças da Cloud Alliance Security; (vi) Escrita de politica de proteção em linguagem natural; (vii) Implantação realizada dentro da empresa. (CSA, 2010; SRIVASTAVA et al., 2011; TAKABI E JOSHI, 2012)

A concepção de funcionamento em ambientes SaaS, IaaS e PaaS corresponde a proposição de uma arquitetura ou *framework* que possa ser aplicado a qualquer modelo de serviço (IaaS, SaaS e PaaS). Este critério se baseia no fato que das 7 (sete) ameaças definidas pela CSA (2010, p.8-14), 5 (cinco) tangenciam todos os modelos de serviço. Sob a perspectiva de ameaças futuras, a arquitetura ou framework deve levar em consideração o surgimento de novos modelos de serviço derivados do IaaS, SaaS e PaaS.

Em relação à interoperabilidade entre diferentes CPSs, a proposição deste critério corresponde à capacidade de comunicação das políticas definidas na arquitetura em CSPs heterogêneos. A definição deste critério se baseia na interpretação do artigo de Takabi e Joshi (2012) e visa que a arquitetura ou

framework possa tangenciar ameaças em diferentes ambientes, aumentando seu espectro de proteção.

Já em relação ao monitoramento proativo de políticas, explicita-se que sua responsabilidade é verificar se monitoramento do SLA definido entre cliente e CSP esta sendo cumprido ao longo de toda atividade do serviço. A definição deste critério está baseado em Srivastava et al. (2011, p.663), em que no monitoramento proativo os clientes de serviços possuem um mecanismo de controle que persiste em verificar se o SLA está sendo cumprindo pelos CSPs. Qualquer falha, ameaça, ou descumprimento das políticas é imediatamente reportado ao cliente dos serviços.

No que se refere ao gerenciamento de políticas de proteção como serviço, corresponde à capacidade de controle de recursos da arquitetura ou *framework* ante a gestão de politicas (ex. adição, remoção, edição de políticas), em geral, a partir de um *Policy Manager*. Este tipo de recurso permite intervenções imediatas no trato de políticas e possíveis vulnerabilidades.

Quanto à proteção às sete principais ameaças da *Cloud Alliance Security,* a arquitetura ou framework deve possuir estrutura de proteção nativa a todas as ameaças listadas pela CSA (2010, p.6-7), sendo estas ameaças exclusivas aos ambientes *Cloud* abstraídas a partir de pesquisas, fóruns, conferências na presença de especialistas do setor.

Escrever politicas de proteção em linguagem natural, diz respeito à arquitetura ou framework receber linguagem humana como *input* para a definição de políticas, como apresenta Takabi e Joshi (2012, p.5504) em sua proposta de *framework*. Este critério é fundamental, pois, algumas arquiteturas apenas conseguem processar políticas escritas diretamente em XML, ou outras linguagens de computador para que haja comunicação com os CSPs. Este critério visa tornar o ambiente *user friendly* na perspectiva de que, quanto mais simples for a arquitetura/framework para o usuário, mais aderente será ao gerenciamento das políticas e, consequentemente, das ameaças.

Por fim, a implantação realizada dentro da empresa, implica que o monitoramento deve ser realizado de dentro para fora da organização com o intuito de garantir maior controle e proteção aos dados, além de aumentar a sensação de maior proteção para os *stakeholders*. De acordo com a descrição das ameaças apresentadas pela CSA (2010, p. 8-14), de sete ameaças, apenas duas são aplicadas quando a implantação ocorre internamente na organização.

Com base nestas referências, os critérios apresentados são fundamentais para a construção de novas arquiteturas ou *frameworks*.

3.5. Considerações do Capítulo

A proposta de framework integrado presente no Capítulo 5 deste trabalho, além de servir como base para estudos futuros que busquem a garantia de proteção para *Clouds* Públicos aliados à comunicação entre plataformas heterogêneas, centralização de políticas e monitoramento proativo.

O Capítulo 4, por sua vez, apresenta a análise de um conjunto de arquiteturas e *frameworks* com o intuito de identificar as que mais se aproxima dos critérios levantados neste capítulo.

4. ANÁLISE DE *FRAMEWORKS* E ARQUITETURAS DE MONITORAMENTO DE POLÍTICAS

Após ser apresentada uma visão geral sobre *Cloud Computing* em relação a sua definição, características, modelos de serviços, modelo de deploy e os principais desafios e ameaças à segurança, vê-se, através de diversos estudos, um conjunto de propostas de *frameworks* e arquiteturas com o desafio de garantir maiores níveis de proteção, interoperabilidade entre outras questões que impulsionam o próprio desenvolvimento do campo do saber.

Na perspectiva de Wu et al (2010, p.381):

> Espera-se que Sistemas Cloud atendam vários requisitos rigorosos para a manutenção de dados e informações de usuários, incluindo alta disponibilidade, confiabilidade, performance, replicação e consistência dos dados, **mas devido à natureza conflituosa desses requisitos, nenhum sistema implementa todos eles juntos**. (WU et al, 2010, p.381, grifo nosso)

Ainda que Wu et al. (2010, p.380) direcionem sua observação para ambientes de armazenamento *Cloud*, sabe-se que o desafio de desenvolver plataformas mais robustas e capazes se superar suas limitações é inerente ao próprio crescimento da *Cloud Computing per se*. Frente a esta perspectiva, este capítulo faz o levantamento de artigos recentes da IEEE que propuseram *frameworks* e arquiteturas com foco na garantia de maiores níveis de proteção às ameaças, gerenciamento de políticas como serviço, interoperabilidade entre ambientes heterogêneos, com o intuito de identificar a possibilidade de propor uma arquitetura/framework integrado, com maior cobertura das questões levantadas.

4.1 Análise de *Frameworks* e Arquiteturas

Os artigos que foram selecionados possuem diversos pontos em comum, mas peculiaridades e espaços que podem ser complementados com uma abordagem intregrada, proposta do *framework* integrado deste trabalho. Foram então selecionados cinco principais artigos com temas convergentes a respeito dos critérios apresentados no Capítulo 3, descritos na Tabela 3.

Tabela 3: Artigos analisados

Artigo	Objetivo	Pontos centrais
Takabi e Joshi (2012) Policy Management as a Service	Propor um framework baseado em gerenciamento de politicas cujos recursos possam ser totalmente gerenciados por seus usuários além de garanti comunicação entre CSPs heterogêneos.	- Utilização de Linguagens Naturais - Comunicação entre CSPs heterogêneos - Compatível com qualquer modelo de implantação - Centralização de Políticas
Srivastava et al. (2011) An Architecture based on Proactive Model	Propor uma arquitetura de monitoramento proativo baseada na definição de Cloud para tratamento de ameaças.	- Monitoramento Proativo de Políticas - Definição de Cloud Policies - Centralização de Políticas na Security Cloud - Utiliza modelo de Implantação Hibrido
Wang e Luo (2011) Policy-Based SLA-Aware	Propor um framework baseado em gestão e monitoramento de SLAs hierárquico que garanta o mínimo de violação dos acordos de serviço.	- Monitoramento de violação dos SLAs - Serviço auto-adaptativo - Foco em arquiteturas IaaS - Trabalha tanto com Usuário quanto CSPs (ganha-ganha)
Basescu et al (2011) Managing Data Access	Propor um Framework de Gerenciamento Genérico de Proteção que permite provedores de Gestão de Dados em Cloud definir e aplicar politicas de proteção mais complexas.	- Foco em Data Storages - Interligação com ambientes heterogêneos - Politicas de Proteção - Busca linguagens de descrição expressivas de política
Bellessa et al (2011) NEtODESSA	Propor um sistema de monitoramento dinâmico de políticas garantindo segurança em nível de rede.	- Extensão do framework ODESSA - Trabalha com Politicas Dinâmicas - Trabalha com modelo baseado em inferência - Trabalha com tecnologias de descrição de recursos e openflow - Monitoramento em nível de rede

Em uma discussão mais profunda sobre os artigos estudados, Takabi e Joshi (2012, p.5505), propõem a utilização de linguagem natural na definição de políticas para que haja comunicação entre diferentes CSPs, em que, as políticas descritas a partir de linguagem humana são convertidas em linguagem de máquina – sendo este um dos fatores que possibilita a arquitetura se autorizar em ambientes *Cloud*

heterogêneos. É importante ressaltar que a proposta em questão privilegia controle total das politicas, podendo ser alteradas e inseridas com os recursos do serviço em modo de execução. No que se refere à capacidade de monitoramento, a proposta de Takabi e Joshi (2012, p.5506) suporta controle de acessos reativo, ou seja, os usuários não são obrigados a determinar todas as políticas de controle de acesso, a priori, mas podem atualizar politicas dinamicamente em tempo de execução como resposta aos pedidos de acesso que por ventura não tenham sucesso.

Srivastava et al. (2011, p.661-663), por sua vez, propõem uma arquitetura de monitoramento proativo cujas políticas, nomeadas "*Cloud Policies*", protegem o ambiente contra as sete ameaças levantadas pela CSA (2010). Em linhas gerais, a arquitetura é construída com base em um ambiente de Nuvem Privada que comporta uma *Security Cloud* que se comunica com o ambiente externo, configurando um modelo de implantação híbrido. Então, na *Security Cloud* são definidas as *Cloud Policies*, direcionadas para combater as ameaças leantadas pela CSA, além de outras ameaças definidas pelo cliente do serviço.

Ademais, a *Security Cloud* possui um mecanismo de monitoramento responsável por comparar se as *Cloud Policies* são compativeis com o ambiente externo, este monitoramento é continuo e persistente – característica da proatividade. Vale ressaltar que, a importância da proatividade reside no fato que os SLAs entre cliente e CSPs é o único aparato legal definido na contratação de serviços, porém, não há para o cliente formas de controlar se os SLAs estão sendo ou não cumpridos. O monitoramento proativo garante identificar se há possíveis violações no SLA definido entre as partes. A proposta de Srivastava et al. (2011, p.665), visa também centralizar as políticas em um único repositório amparado pela *Security Cloud*. Esta centralização possibilita maior facilidade de gerenciamento das políticas.

A arquitetura de Wang e Luo (2011, p. 114), por outro lado, apresenta um modelo de Gerenciamento de Recursos de Nuvem que satisfaz as necessidades do usuário e também dos CSPs. Em linhas gerais, Wang e Luo (2011, p.115-116) introduzem o conceito de SLA-*Aware* que, semelhante ao monitoramento proativo de Srivastava et al. (2011), monitora possíveis violações no SLA. É importante ressaltar

que, este modelo possui foco tanto no cliente quanto no provedor de serviço e, para tanto, desenvolve-se um mecanismo de provisão de serviços e políticas auto adaptativo responsável por garantir que os acordos definidos no SLA não sejam violados. A arquitetura é focada em um modelo de serviços IaaS e baseada em algoritimos de abstração. O provedor de serviços possui recursos que podem ser oferecidos aos clientes sob demanda e monitorados pelo Monitor de *Status* de Aplicação (ASM). Conforme Wang e Luo (2011, p.114) abordam, "O problema fundamental da *Cloud Computing* é o problema de *scheduling*, porque nos obriga fazer *trade-offs* entre os tipos de fatores, como consumo, custo de energia pena". Para tanto a arquitetura possui um Escalador responsável por programar e reprogramar os recursos de acordo com as políticas predefinidas.

A proposta de Basescu e Carpen-Amarie. (2011, p.459), por sua vez, propõe um *Framework* Genérico de Gerenciamento de Proteção que permite provedores de Gestão de Dados em Nuvem definir e aplicar políticas de proteção mais complexas. O *framework* em questão é designado a detectar e interceptar um conjunto de ataques através de uma linguagem de descrição de politicas expressiva, podendo ser facilmente interligado com vários sistemas gestores de dados. Este *framework* é focado em sistemas que gerenciam dados (*Data Storage*) e visa ser interligado com ambientes heterogêneos.

Para tanto, o *framework* define *Security Policies* descritas em XML. A arquitetura básica do *framework* contém: (i) um módulo *Policy Manager*, responsável por definir e assegurar que as *Security Policies* estão sendo aplicadas; (ii) um módulo que monitora Histórico de Atividades do Usuário disponibilizando as ações para o módulo de Gerenciamento de Políticas; (iii) um módulo de Gerenciamento de Confiança que atribui níveis diversos de confiança para cada usuário de acordo com seu histórico de ações. Dentre os pontos que devem ser destacados, ressalta-se que o *framework* possui monitoramento reativo, pois, a partir do histórico de ações dos usuários no sistema ele possibilita a tomada de decisão de acordo com as politicas definidas no *Policy Manager*. Além disso, as politicas são armazenadas internamente do *Cloud System*, não possuindo uma centralização das mesmas. (BASESCU E CARPEN-AMARIE, 2011, p.460-464)

Por outro lado, Bellessa et al. (2011, p.57) propõem um *framework* que possui um sistema de monitoramento dinâmico de políticas que garante segurança em nível de rede. Denominado de NetODESSA, o *framework* é uma extensão do ODESSA aplicado à camada de rede, permitindo a construção de redes dinâmicas cujos administradores podem escrever políticas de rede em tempo de execução. No que se refere às tecnologias utilizadas, destaca-se o RDF (*Resource Descripition Framework*), uma linguagem universal para descrição de recursos também utilizada por Takabi e Joshi (2012, p.5504), e o *OpenFlow*, protocolo que permite controlar o comportamento de um *switch* com a definição de ações para tipos específicos de conexões. Neste *framework*, introduz-se o conceito de *Dynamic Policy*, ou seja, uma politica de alto nível que não está presa a um *host* em específico, opera em nível de rede.

4.2. Comparativo entre Arquiteturas e F*rameworks*

Após a visão geral sobre as arquiteturas e *frameworks*, a Tabela 4 realiza questões-chave com base nos critérios levantados pelo capítulo 3 bem como outros fatores relevantes para comparar as arquiteturas/frameworks analisadas.

Tabela 4: Recursos das arquiteturas/*frameworks*

	Arquiteturas/*Frameworks*				
Questões	Takabi e Joshi (2012) *Policy Management as a Service*	Srivastava et al. (2011) *Architecture based on proactive model*	Wang e Luo (2011) *Policy-Based SLA-Aware*	Basescu et al. (2011) *Managing Data Access*	Bellessa et al (2011) NEtODESSA
Qual é o tipo de monitoramento?	**Reativo**	**Proativo**	**Proativo**	**Reativo**	**Proativo**
Consegue se autenticar em Clouds Heterogêneos?	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
Existe Gerenciamento de Políticas como serviço?	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
Existe proteção nativa às ameaças da CSA?	**Não**	**Sim**	**Não**	**Não**	**Não**
A recomendação de políticas é espontânea?	**Sim**	**Não**	**Não**	**Não**	**Não**
Qual é a linguagem de escrita da política?	**Linguagem Natural**	**Não especifica**	**XML**	**XML**	**XML**
Qual é o tipo de política utilizada?	***Access Policy***	***Cloud Policy***	***Policy***	***Security Policy***	***Dynamic Policy***
Existe centralização de políticas?	**Sim**	**Sim**	**Sim**	**Não**	**Sim**
Implantação é realizada dentro da empresa?	**Sim**	**Ambos**	**Ambos**	**Não**	**Sim**
Monitora qual ambiente Cloud?	**Todos**	**Todos**	**IaaS**	**StaaS**	**Todos**

Em relação à questão, “Qual é o tipo de monitoramento?” utilizado pelo *framework*, os artigos analisados levantam duas possibilidades: (i) monitoramento reativo, que após o SLA ser impactado com alguma inconsistência possui uma ação de controle; e, (ii) monitoramento proativo, que persiste em verificar se o SLA esta sendo cumprindo pelos CSPs. Neste critério, o *framework* proposto por Takabi e Joshi (2012, p.5506) e a arquitetura proposta por Basescu et al. (2011, p.462), possuem monitoramento reativo. Os demais artigos analisados são proativos.

A questão seguinte, “Consegue se autenticar em Clouds Heterogêneos?”, diz respeito à capacidade da arquietetura/*framework* possuir mecanismos de autenticação em diferentes CSPs, independente da tecnologia que utiliza. Para que isto seja possível, a arquitetura ou *framework* deve utilizar uma linguagem para comunicação interoperável, por exemplo, o XML, ou então possuir mecanismos de conversão da linguagem nativa de sua arquitetura ou *framework* para linguagens interoperáveis entre os CSPs. Todos os artigos analisados possuem minimamente formas de se comunicarem com diferentes CSPs, porém, alguns limitados a ambientes de serviços específicos, por exemplo, a proposta de Basescu e Carpen-Amarie (2011) especializada em comunicação StaaS. Nesta questão, destaca-se a proposição de Takabi e Joshi (2012, p.5501-5506) que possui mecanismos específicos para que não haja limitações, independente do modelo de serviços.

Já a questão, “Existe Gerenciamento de Políticas como serviço?”, verifica se as arquiteturas ou *frameworks* possuem um “*Policy Manager*” ou mecanismos semelhantes que permitem a adição, exclusão, edição de políticas como um serviço, acessadas a partir de uma interface comum em ambiente *Cloud*. Todos os ambientes comportam este critério, mas o *framework* de Takabi e Joshi (2012) possui abordagem especializada em *Policy as a Service*.

Por outro lado, em relação à questão “Existe proteção nativa às ameaças da CSA?”, corresponde à presença de políticas de proteção contra as sete ameaças identificadas pela CSA nativas a arquitetura ou *framework*. Apenas Srivastava et al. (2011, p.663-664) possuem esta preocupação a partir da definição de *Cloud Policies*.

Em relação à questão se “A recomendação de políticas é espontânea?” apenas Takabi e Joshi (2012, p.5503), propõem uma estrutura de *Policy Recomedations*, cujo *framework* auxilia na geração espontânea de políticas com base nas informações do *Cloud User*.

Quanto à questão “Qual é a linguagem de escrita da política?”, as arquiteturas/*frameworks* estudadas utilizam tanto XML quanto linguagem natural para definirem suas políticas. Em linhas gerais, o XML

(*eXtensible Markup Language*) é uma linguagem de marcação genérica que segue os padrões da W3C para comunicação via internet sendo amplamente utilizada pois cria uma infraestrutura única apra diversas linguagens, garantindo interoperabilidade na comunicação entre ambientes heterogêneos. Já as linguagens naturais, correspondem ao input de informações em linguagem humana, para tanto, a arquitetura ou *framework* possui mecanismos de conversão desta linguagem em linguagem de máquina. Dentre os artigos apresentados, apenas Takabi e Joshi (2012, p.5505) apresentam um mecanismo de conversão de linguagem natural de forma que esta possa ser dinamicamente interpretada e compatibilizada em diferentes CSPs, as demais arquiteturas ou *frameworks* utilizam XML.

A partir do estudo das arquiteturas ou *frameworks*, identificou-se que em relação à questão “Qual é o tipo de política utilizada?”, Takabi e Joshi (2012, p.5500-5506), utilizam Access Policies, ou seja, políticas de acesso que são definidas em linguagem natural cujo foco é garantir autenticação em ambientes heterogêneos. Em Srivastava et al. (2011, p.663-664), utilizam *Cloud Policies*, que são políticas com foco na proteção contra as sete ameaças da CSA além de outras ameaças que possam ser específicas de ambientes *Cloud*. Por outro lado, Wang e Luo (2011, p.115), utilizam apenas *Policy*, que são politicas genéricas sem nenhuma especificidade. Basescu e Carpen-Amarie (2011, p. 461), utilizam *Security Policies*, que são políticas de proteção com características próprias para proteção de *storages*. Por fim, Bellessa et al (2011, p.58), utilizam *Dynamic Policies*, que são categorizadas como políticas de rede.

Já a questão “Existe centralização de políticas?”, apenas Basescu e Carpen-Amarie (2011) não possuem um ambiente que mantém todas as políticas centralizadas. As demais arquiteturas ou *frameworks* possuem mecanismos que realizam a função de *Policy Database*, ou seja, um banco de dados de políticas. A centralização é fundamental para o gerenciamento das políticas, bem como mantê-las protegidas.

Quanto à questão “Implantação é realizada dentro da empresa?”, apenas Basescu et al. (2011, p.59) realizam a implantação externa à empresa. Por outro lado, Wang e Luo (2011, p.115) e Srivastava et al. (2011, p.665) podem realizar a

Implantação tanto fora quanto dentro da empresa devido ao modelo de arquitetura proposto.

Por fim, a questão “Monitora qual ambiente Cloud?“, mostra que as arquiteturas ou *frameworks* propostas por Takabi e Joshi (2012), Srivastava et al. (2011) e Bellessa et al. (2011) possuem monitoramento extensível para ambientes SaaS, PaaS e IaaS. Em linhas gerais, esta questão vai ao encontro do critério que visa à cobertura genérica dos modelos de serviço *Cloud*. Wang e Luo (2011) e Basescu et al. (2011) monitoram especificamente ambientes IaaS e StaaS respectivamente.

A Tabela 5 mostra um comparativo entre as aquiteturas ou *frameworks* analisadas com base nos critérios definidos no Capítulo 3.

Tabela 5: Comparativo de critérios presentes nas arquiteturas/*frameworks*

Criterio	Takabi e Joshi (2012) Policy Management as a Service	Srivastava et al. (2011) An architecture based on proactive model	Wang e Luo (2011) Policy-Based SLA-Aware	Basescu et al. (2011) Managing Data Access	Bellessa et al (2011) NEtODESSA
(i) Funcionamento em ambientes SaaS, IaaS e PaaS	**x**	**X**			**x**
(ii) Interoperabilidade entre diferentes CPSs	**x**	**X**	**x**	**x**	**x**
(iii) Monitoramento Proativo de Políticas		**X**		**x**	**x**
(iv) Gerenciamento de Políticas de proteção como Serviço	**x**	**X**	**x**	**x**	**x**
(v) Proteção às sete principais ameaças da CSA		**X**			
(vi) Escrita da politica de proteçãoem linguagem natural	**x**				
(vii) Implantação realizada dentro da empresa	**x**	**X**		**x**	**x**

A partir da análise e comparação de cada uma das aquiteturas ou *frameworks* apresentados, conclui-se que as arquiteturas que mais se aproximam dos objetivos

deste trabalho ante aos critérios apresentados no Capítulo 3, além de compatibilidade entre seus elementos de forma que uma complemente a outra em relação a carência de algum critério, corresponde a integração das arquitetura e *framework* de Takabi e Joshi (2012, p.5504) e Srivastava et al. (2011, p.665).

4.3. Considerações do Capítulo

O estudo em profundidade das arquiteturas e *frameworks* apresentadas foram fundamentais para realizar uma análise comparativa com base nos critérios identificados por esta pesquisa, identificando seus principais pontos fortes e frequezas em relação a proteção contra ameaças, vulnerabilidades e aderência às Nuvens Públicas. Desta forma, com base nas arquiteturas e *frameworks* que melhor se completam, o Capítulo 5 apresenta uma proposta de framework integrado aprofundando sobre os principais elementos presentes em Takabi e Joshi (2012) e Srivastava et al. (2011).

5. PROPOSTA DE FRAMEWORK DE MONITORAMENTO

Este capítulo tem como objetivo detalhar a proposta de arquitetura integrada introduzida no capítulo anterior. Para tanto, nas seções seguintes aprofundam-se nas definições da arquitetura e *framework* selecionados. E, é apresentada uma proposta de unificação destas arquiteturas com o intuito de aproveitar seus principais pontos fortes e equilibrar seus pontos fracos.

5.1. Arquitetura Proativa de Monitoramento de Políticas em Ambiente *Cloud*

Como ressaltado anteriormente, os ambientes públicos de *Cloud Computing* estão suscetíveis às principais ameaças definidas pela *Cloud Security Alliance*, o que pode ser um impeditivo para o pleno cumprimento das políticas e expectativas definidas no SLA dos serviços. É importante ressaltar que, uma política, como bem explicitada Bellessa et al. (2011), corresponde a um conjunto de regras responsáveis por garantir o comportamento dos serviços.

Porém, políticas de proteção tradicionais são funcionais para modelos de infraestruturas tradicionais, muitas vezes em um *Data Center* da própria empresa. A partir desta visão, Srivastava, et al. (2011) faz menção à *Cloud Policy* como um conjunto de regras pertinentes aos serviços de *Cloud Computing* de forma que haja preocupação em mapear os reais requisitos de segurança de uma organização que adota estes serviços, garantindo o cumprimento de suas especificidades, sobretudo nas questões apontadas pelo Gartner *Seven Security Risks of Cloud Computing*. (NETWORKWORLD, 2008)

> Adoção de Cloud Computing é uma mudança de paradigma no uso de TI por uma organização. Por isso defendemos que uma política Cloud separada faria jus ao caso. Entre outros, o benefício deve incluir esforço concentrado da gestão e compreensão de que é necessário para tal mudança. Esta política Cloud irá aumentar as políticas de segurança da organização. (SRIVASTAVA et al., 2011, p.663)

Para tanto, a proposição de uma arquitetura para monitoramento do cumprimento das *Cloud Policies* e sua especificação no contrato de serviço (SLA),

de acordo com Srivastava, et al. (2011, p.663), deve ser baseada nos seguintes pontos:

I. Garantia do aumento das políticas de proteção de uma empresa a partir de uma *Cloud Policy* estruturada.

II. Monitoramento proativo e reporte de violação das políticas definidas pela *Cloud Policy* a partir de um *Security Cloud* que opera como um subsistema dentro de uma Nuvem Privada.

A garantia do aumento das políticas de proteção a partir de uma *Cloud Policy* estruturada vai ao encontro das questões já levantadas por Srivastava, et al. (2011, p.663). Tecnicamente, o conjunto de politicas definidas na *Cloud Policy* irá definir o que será monitorado pela arquitetura, estando guardadas dentro de uma Security Cloud. Para tanto, a arquitetura é desenvolvida a partir de uma Nuvem Privada para que seja possível comportar a *Security Cloud*.

> A Security Cloud é inicialmente provisionada obrigatoriamente em uma nuvem privada. Em seguida, é permitido escalar dinamicamente e utilizar seus recursos extras disponíveis. O processo é estritamente dinâmico, de modo a não afetar a disponibilidade dos *Cloud Users*. A Security Cloud, libera, então, prontamente os recursos caso necessário. (SRIVASTAVA et al., 2011, p.665)

A arquitetura é desenvolvida a partir de uma Nuvem Privada para que seja possível comportar a *Security Cloud*.

Como deixam claro Srivastava, et al. (2011, p.666), a *Security Cloud* tem como principal objetivo monitorar os CSPs, além de:

1. Monitorar *blacklists* do próprio provedor de serviço.
2. Avaliar vulnerabilidade
3. Testes de invasão
4. Auditoria dos históricos das transações
5. Sistema de Prevenção de Intrusão baseada em Hosts.

Em linhas gerais, *a Security Cloud* alinhada as *Cloud Policies* consistem na principal estrutura de segurança da arquitetura proposta cujas funções da são fundamentais para a garantia do monitoramento proativo do ambiente de serviços *Cloud*.

> A Security Cloud desempenha a importante função de monitorar o Provedor de Serviços Cloud. Ao invés acompanhar passivamente as reivindicações do CSP sobre a capacidade de implementar segurança, **a abordagem pró-ativa garante que a organização não seja pega desprevinida quando acontece algum desastre.** (SRIVASTAVA, et al., 2011, p.665, grifo nosso)

A grosso modo, a proatividade de monitoramento é responsável por verificar se o CSP possui suporte às Politicas estabelecidas via SLA (*Service Level Agreement*), além de persistir o monitoramento destas políticas garantindo que não haja incidentes devido à continuidade de serviços fora do SLA contratado ou problemas que possam vir a afetar o ambiente dos serviços. A Figura 2 mostra uma visão mais detalhada da arquitetura.

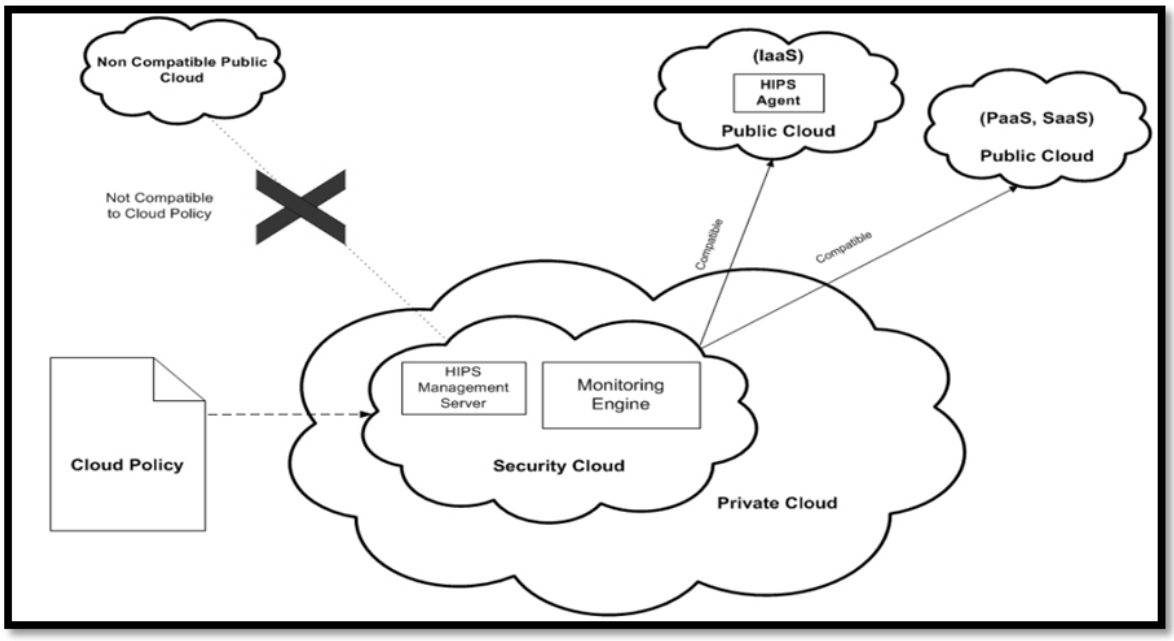

Figura 2 - Representação da Arquitetura de Monitoramento Proativo de *Cloud Policies* (Srivastava, et al., 2011, p.665)

Com base nas questões já definidas, a mecânica da arquitetura baseia-se no completo controle e monitoramento da Nuvem Privada e das Nuvens Públicas que fazem parte do ambiente de serviços *Cloud*. A partir da definição do conjunto de

Cloud Policies anexadas à *Security Cloud*, a máquina de monitoramento da *Security Cloud* mantém a comunicação com os CSPs das Nuvens Públicas pertencentes ao ambiente, além de verificar se novos serviços de Nuvens Públicas são ou não compatíveis com as políticas pré-existentes. Caso não haja compatibilidade, o serviço não será aceito. A arquitetura em si, faz uma comparação se os serviços externos à Nuvem Privada, sob monitoramento da *Security Cloud*, possuem o mesmo nível de serviço que os serviços Internos. Como abordam Srivastava et al. (2011), o monitoramento é contínuo e persistente, garantindo maior controle sobre a segurança das Nuvens Públicas .

5.2. Detalhamento do *Framework* de Gerenciamento de Politica como Serviço (PMaaS *Framework*)

A seção anterior se preocupou em descrever uma estrutura de monitoramento proativo para Nuvens Públicas, tendo como base a definição de *Cloud Policies*, as quais levam em consideração às especificidades da *Cloud Computing* ante suas principais ameaças – levantadas pelo Gartner (NETWORKWORLD, 2008) e pelo *Cloud Security Alliance*. (CSA, 2010)

Evocando o conceito de PMaaS – *Policy Management as a Service*, ou seja, entrega o gerenciamento de políticas de proteção como serviço, Takabi e Joshi (2012) reiteram sobre as capacidades do modelo garantir aos clientes total administração do das políticas de produtos ou serviços que estejam em execução em uma infraestrutura *Cloud* a partir de uma interface de serviços, mas cujos desafios residem no desenho de um controle de políticas integrado, que possa ser utilizado entre diferentes CSPs e em um ambiente de gerenciamento comum. Isso se dá, pois, os ambientes tradicionais de *Cloud Computing* empregam seus próprios modelos de autenticação, linguagem e solução de gerenciamento.

> O ambiente de Cloud Computing não permite o uso de um mecanismo de autorização única, linguagem única de políticas ou ferramenta de gestão para vários CSPs. Cada CSP utiliza sua própria solução de controle de acesso e mecanismo de autorização muitas vezes intimamente ligado a um CSP e tem pouca flexibilidade em termos de resposta às exigências de um determinado usuário de segurança. (TAKABI E JOSHI, 2012, p.5500)

> [...] Os usuários devem utilizar diferentes soluções de controle de acesso disponíveis para CSP para proteger seus dados e controlar a sua disseminação. Políticas de controle de acesso podem ser compostas em linguagens incompatíveis e mantidas separadamente em cada CSP. (TAKABI E JOSHI, 2012, p.5501)

Consequentemente, os usuários acabam por gerenciar individualmente diversos serviços, aplicando as políticas individualmente. Sob esta perspectiva, tem-se um custo de eficiência, uma vez que seus clientes podem utilizar múltiplos serviços sob um mesmo SLA, o que geraria uma mesma política, mas, tradicionalmente, têm que fazer o gerenciamento (inserção, deleção, modificação de uma política) caso-a-caso. Em geral, esta dificuldade de interoperabilidade se dá devido à existência de diferentes *Policy Languages* e falta de um ambiente e linguagem comum que centralize as políticas e serviços. (TAKABI E JOSHI, 2012)

Neste sentido, o *framework* proposto por Takabi e Joshi (2012, p.5504) - Figura 3 - permite centralizar as diferentes políticas de acesso aos recursos contratados pela empresa nos CSPs, garantindo sincronização das politicas e recursos entre diferentes serviços, independente de onde as informações são armazenadas ou distribuídas.

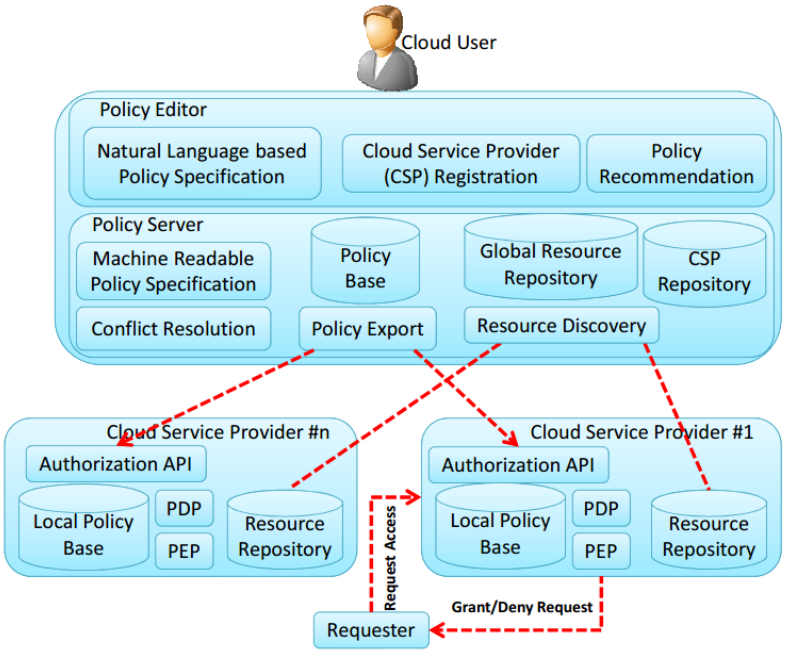

Figura 3 - Representação *Framework* de Gerenciamento de Politica como Serviço (PMaaS *Framework*) (Takabi e Joshi, 2012, p.5504)

Per se, é baseado em quatro componentes principais: (i) *Cloud User*; (ii) *Cloud Service Provider* (CSP); (iii) *Policy Management Service Provider* (PMSP); e, (iv) *Requester*. Cuja mecânica permite que o controle de acesso às politicas possam ser aplicados a um conjunto de recursos hospedados em vários CSPs. A descrição de cada componente e do funcionamento do *framework*, de acordo com as especificações de Takabi e Joshi (2012, p.5502-5503), segue a seguir:

(i) *Cloud User*: O responsável por gerenciar as politicas de acesso no PMSP, por adicionar os serviços de diversos CSPs e para adicionar os CSPs no PMSP. O *Cloud User* utiliza um gerenciador de políticas unificado isentando de aplicar a mesma política em CSPs diferentes. Para tanto, utilizam linguagem natural para especificar as políticas não necessitando conhecer diversas linguagens.

(ii) *Policy Management Service Provider* (PMSP): Responsável por permitir ao Cloud User gerenciar as políticas de acesso. O *Cloud User* específica as políticas de acesso em uma linguagem natural e o PMSP traduz para linguagem de máquina. O PMSP também é responsável pela resolução de conflitos entre as políticas e a exportação das políticas para os CSPs. O PMSP atua em duas frentes o *Policy* Editor e *Policy Server*.

- *Policy Editor*: O *Policy Editor* age como ponto de política de administração (PAP) e fornece interfaces para os *Cloud Users* gerenciar políticas de acesso em um único local. Ele facilita o processo de gestão das políticas, permitindo que os *Cloud Users* especifiquem as suas políticas em linguagem natural. Ele também lida com o processo de registro dos CSPs. Além disso, inclui uma unidade de recomendação de política que usa informações relacionadas com o *Cloud User* e seus recursos para recomendar algumas políticas.

- *Policy Server*: O *Policy Server* age como o ponto de informação política (PIP) e é responsável por interagir com o *Policy Editor* e os CSPs, bem como traduzir as políticas definidas pelo *Cloud User* em uma linguagem de máquina. Ele mantém um repositório de CSPs associadas a cada *Cloud User*. Também é responsável pelo processo de descoberta de recursos. Depois que o *Cloud User* registra seus CSPs para a PMSP, a PMSP se comunica com

cada CSP para encontrar recursos e os armazena em um repositório global de recursos que contém todos os recursos e sua associação com os *Cloud Users* e CSPs. Estes recursos são apresentados na interface do editor de política para o *Cloud User* para ajudá-lo na especificação políticas. Além disso, ele recebe as políticas especificadas pelo *Cloud User* no *Policy Editor*, analisa, e os transfere para linguagem de máquina armazenando em uma base de políticas.

(iii) *Cloud Service Provider* (CSP): CSP disponibiliza um ou mais serviços para utilização dos *Cloud Users*. Um CSP controla os acessos aos recursos de acordo com as políticas inseridas pelos *Cloud Users* e avalia as solicitações de acesso, sendo responsável pelas permissões de acesso.

(iv) Requester: Uma aplicação controlada por uma pessoa/organização que interage com um CSP a fim de ter acesso a algum recurso pertencente ao *Cloud User*.

Um dos principais pontos do *framework* na resolução dos problemas levantados anteriormente é a utilização de linguagens naturais que são convertidas em linguagem de máquina pelos PMSPs. Além disso, quando há transferência de políticas entre diferentes CSPs, não é necessário modificações na política, uma vez que os PMSPs também se responsabilizam pelas conversões em operações de transferência. Esta mecânica é o ponto central para a garantia de interoperabilidade entre diferentes "*Policy Languages*", possibilitando centralizar a comunicação de serviços heterogêneos em um ambiente comum.

> Facilita a capacidade dos usuários gerir as políticas de acesso usando um gerenciador de política centralizado que fornece interfaces utilizáveis para a especificação de políticas de acesso e exportá-los para os CSPs em nome do usuário. (TAKABI E JOSHI, 2012, p.5501)

> Um gerenciamento centralizado de políticas poderia ajudar o pessoal de segurança para **melhor gerenciar a segurança proporcionando uma melhor visão sobre as políticas de acesso** aplicadas aos recursos da organização em serviços diferentes. (TAKABI E JOSHI, 2012, p.5502, grifo nosso)

Por fim, devido à centralização das politicas proporcionada pelo *framework*, há ainda contribuição na manutenção de um mesmo nível de segurança para todos os ambientes de serviço.

5.3. Gerenciamento de Politicas como Serviço Proativamente Monitorado

A partir da análise dos modelos expostos nas seções anterioresé possível identificar o potencial de ambas as propostas quanto ao monitoramento proativo e interoperabilidade de políticas em ambientes *Cloud*, respectivamente. Além dos potenciais, ambos os modelos, per se, apresentam um conjunto de discussões acerca de questões referentes a possíveis melhorias, falhas e complementações. Sob esta perspectiva, e imersão em ambas as abordagens, este trabalho propõe a unificação entre os modelos por apresentarem características complementares, desenhando uma nova arquitetura de serviços: Gerenciamento de Politicas como Serviço Proativamente Monitoradas.

Em linhas gerais, esta nova arquitetura constrói um modelo de gerenciamento de políticas como serviço proativamente monitoradas, ou seja, com base no *framework* proposto por Takabi e Joshi (2012, p.5504), garante-se um ambiente de gerenciamento de políticas centralizado e interoperável. Por outro lado, com base na arquitetura de Srivastava et al. (2011, p.665), garante-se monitoramento proativo das ameaças às políticas definidas. A grosso modo, desenhar esta arquitetura visa garantir maior robustez para o ambiente de serviços sob duas principais perspectivas: (i) interoperabilidade; e, (ii) segurança.

No que se refere a (i) interoperabilidade, um *Cloud User*, a partir de linguagens naturais, define diferentes políticas que serão processadas pelos *Policy Management Service Providers* (PMSPs) e convertidas em linguagem de máquina possibilitando comunicação das políticas entre diferentes CSPs.

> *Cloud Users* utilizam um sistema unificado de gestão política para controlar o acesso a todos os seus recursos espalhados na nuvem. Eles não precisam lidar com diversos sistemas de gestão de políticas vinculados a cada CSP. [...] *Cloud Users* compõe as políticas de controle de acesso usando linguagem natural controlada e não precisam usar linguagens varias linguagens de politica especificas. (TAKABI E JOSHI, 2012, p.5506)

Em análise, o monitoramento da arquitetura de Srivastava, et al. (2011) cumpre com seus objetivos no que tece ao tratamento de ameaças, mas, em contrapartida, a dificuldade de manter o controle de acesso aos recursos de diferentes serviços *Cloud* para a exportação e importação das politicas desenvolvidas não é individualmente suportado pela arquitetura.

No que se refere a (ii) proteção, reitera-se que as *Cloud Policies* garantem as especificidades da *Cloud Computing* no tratamento das ameaças no ambiente de serviços. Como explicitado nas seções anteriores., as *Cloud Policies* estão contidas em uma *Security Cloud*, centralizando todas as politicas de acesso aos provedores de serviço externos que serão acionados seguindo as regras definidas no monitoramento. Por tal motivo, a *Security Cloud* se torna o local mais indicado para a implantação do *framework* (PMaaS), além do que, a mesma está obrigatoriamente contida em um ambiente de Nuvem Privada.

> Assumimos que não há nível suficiente de confiança entre Cloud User e provedor PMaaS para implantar o serviço. **No entanto, o PMaaS poderia ser implantado como nuvem privada dentro de uma organização** ou totalmente controlada por um usuário individual para evitar preocupações com a privacidade. (TAKABI E JOSHI, 2012, p.5507, grifo nosso)

Sob esta perspectiva, o novo framework passa a garantir tanto interoperabilidade entre as *Cloud Policies*, quanto maior nível de segurança para o framework PMaaS. Outra intervenção é que as *Cloud Policies* passam a fazer parte do *Policy Editor* do *framework* de Takabi e Joshi (2012, p.5504). A Figura 4 mostra uma visão integrada do *framework* proposto.

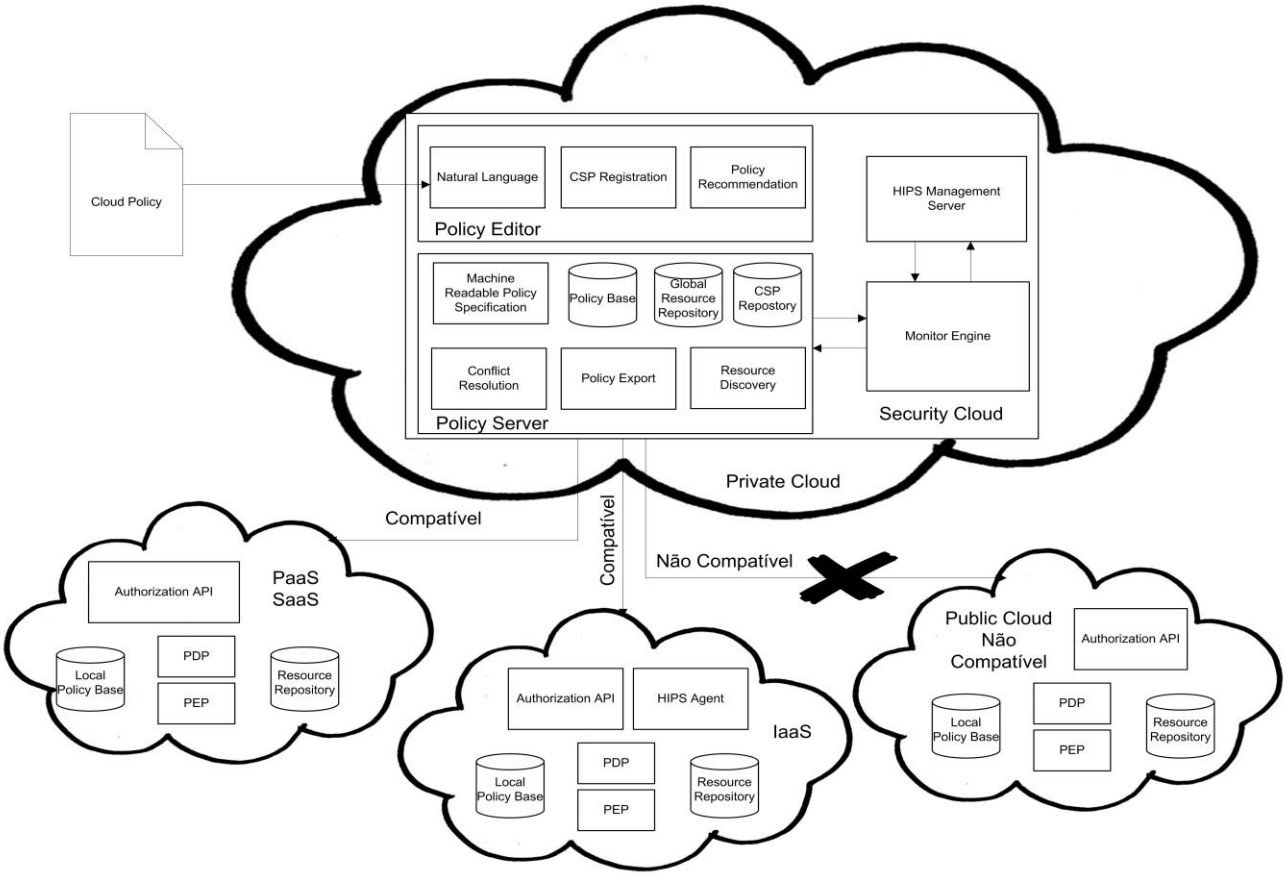

Figura 4: Proposta de integração baseada em Takabi e Joshi (2012, p.5504) e Sirivastava et al. (2011, p.665)

É importante ressaltar que as *Cloud Policies* serão escritas em linguagem natural dentro das interfaces de registros do *Policy Editor*, que irá transformar as *Cloud Policies* em linguagem de máquina e serão armazenadas em um banco de politicas (*Policy Base*).

Ainda referente ao *Policy Editor*, destaca-se que a interface CSP *Registration* deverá armazenar as informações pertinentes aos CSPs que serão utilizados pela organização, cujos registros ficarão no CSP *Repository* em que o *Monitor Engine* buscará detalhes e informações para conexão do CSP monitorado

A última interface de registro de políticas é o *Policy Recommendation* que, a partir de informações do usuário e dos seus recursos, recomenda politicas (TAKABI E JOSHI, 2012, p.5503). Este ponto é um dos principais diferenciais da arquitetura

integrada, pois, para além de aumentar o nível de proteção contra as ameaças e centralizar as políticas, quanto mais Políticas forem inseridas no sistema, maior será o número de recomendações – tornando a arquitetura escalável e melhor protegida conforme novos SLAs são definidos e novas políticas criadas.

Com as politicas e os CSPs devidamente cadastrados o *Monitor Engine* pode executar as funções de exportação das politicas, verificação de violação do SLA, descobrimento dos recursos, análise de compatibilidade do CSP com as políticas e autenticação nas diferentes APIs disponibilizadas.

O funcionamento do *Monitor Engine* se baseia na leitura das *Machine Redeable Policy Specifications* que estão contidos na *Policy Base*, então extrai as informações presentes no CSP *Repository* e, devido a integração com o *framework* de Takabi e Joshi (2012, p.5504), se comunica com a API de autorização dos CSPs para estabelecer com comunicação CSPs heterogeneos. Este processo ocorre com o apoio do *Policy Export*, responsável por exportar as politicas para os CSPs. Por fim, após a exportação das políticas, o *Monitor Engine* analisa todos os CSPs cadastrados verificando se suas politicas são condizentes com a empresa, e analisa também se houve ou não violação de SLA, e se o *Cloud* é compativel ou não com sua estrutura.

Quando os serviços disponibilizados pelos CSPs o *Monitor Engine* aciona o HIPS *Management Server*, que instala uma estrutura local para maior controle e proteção. É importante neste momento, traçar um paralelo com Wang e Luo (2011, 114), pois assim como sua arquitetura de SLA *Aware*, o HIPS *Management Server* tem como estratégia colocar um agente dentro do Cloud para monitoramento.

O *Resouce Discovery*, por sua vez, mapeia todos os recursos de cada *Cloud* para vizualizar as políticas de forma centralizada e auxiliar na resolução de conflitos. Os recursos são armazenados no *Global Resource Server*.

Por fim, em relação ao *Policy Decision Point* e *Policy Enforcement Point*, estas estruturas correspondem aos controles de politicas internos do CSP que a partir das politicas exportadas pela arquitetura proposta, permitem que o CSP faça a

comunicação com o requester, ou seja, a aplicação utilizada pela empresa, liberando ou negando acesso.

5.4. Considerações do Capítulo

O presente capítulo analizou em profundidade a proposta de arquitetura e *framework* de Takabi e Joshi (2012, p.5504) e Srivastava, et al. (2011, p.665) respectivamente, para então propor um *framework* integrado. Em linhas gerais, com a integração entre as ambas as propostas, estima-se alcançar maior proteção das Nuvens Públicas - sobretudo - contra as sete ameaças levantadas pela CSA (2010). Um dos principais elementos deste capítulo corresponde à possibilidade de garantia de escalabilidade de proteção devido a utilização de *Policy Recomendations*, uma vez que, quanto mais políticas existem no na base de dados, mais recomendações são realizadas com base no perfil do *Cloud User* tangenciando possíveis vulnerabilidades não identificadas.

O Capítulo 6 apresenta as considerações finais deste trabalho, bem como proposta de estudos futuros.

6. CONSIDERAÇÕES FINAIS

O presente trabalho trouxe a modelagem de um novo *framework* de monitoramento para ambientes *Cloud* com o intuito de garantir maior proteção e robustez para Nuvens Públicas.

Esta proposta foi possível a partir da análise de um conjunto de frameworks e arquiteturas em paralelo com estudos e pesquisas referentes a proteção de ambientes baseados em *Cloud Computing*.

A partir dos resultados encontrados neste trabalho, este capítulo faz o fechamento crítico da pesquisa, ressaltando as principais contribuições e possibilidade de trabalhos futuros derivados da continuidade das propostas deste trabalho.

6.1. Contribuições do Trabalho

Dentre as principais contribuições do trabalho, destaca-se o levantamento de sete critérios propostos na sessão 3.4. para construir uma arquitetura com foco na proteção das ameaças identificadas pela CSA (2010). Estes critérios podem servir de subsídio para a proposição de novas arquiteturas ou *frameworks*, de forma que a proposição deste trabalho é uma de suas derivações.

Além disso, destaca-se a proposição do novo modelo de "Gerenciamento de Politicas como Serviço Proativamente Monitorado" na sessão 5.3, que com a integração entre o *framework* de Takabi e Joshi (2012 p.5504) e a arquitetura de Srivastava, et al. (2011, p.665) para além de garantir o cumprimento dos sete critérios propostos por este trabalho e descritos no Capítulo 3, devido sua complementariedade, haja a minimização de suas fragilidades individuais e ganhos de produtividade na produção de politicas com auxílio das *Policy Recomendations*.

Além disso, as *Policy Recomendations*, garantem escalabilidade para o *ramework* na recomendação de políticas com base no perfil dos *Cloud Users*, de

forma que, quanto mais políticas compõem a arquitetura, maior será o número de recomendações ante possíveis riscos/vulnerabilidades que não tenham sido consideradas. Vale ressaltar que, isso é possível devido à centralização de todas as políticas em um repositório comum, que também garante maior facilidade de gerenciamento e proteção das políticas.

As principais limitações da proposta deste trabalho correspondem a necessidade de uma gama maior de ferramentas para que a nova arquitetura possa ser implementada, consequentemente, os custos envolvidos poderão ser maiores, sobretudodevido a necessidade de uma Nuvem Privada para compor o modelo de implantação hibrido.

Em questão de desempenho, apesar de não haver testes empíricos, espera-se que não haja impactos negativos decorrentes da integração uma vez que a proposta é apartada do sistema principal, porém, leva-se em consideração a possibilidade do aumento do número de transações de verificação de violação concorrer com as transações de uso comum da arquitetura em seu estado natural, inclusive, devido ao fluxo de recomendações decorrentes pelo *Policy Recomendation*.

Por fim, o trabalho identifica necessidade de alinhamento constante com as atualizações propostas pela CSA em relação às ameaças nos ambientes *Cloud*. Em linhas gerais, em julho de 2012 será lançado um novo relatório com atualizações referentes as ameaças recentes para os ambientes *Cloud*. É válido ressaltar que *Cloud Computing* ainda é um campo em constante expansão e, partindo da exploração (a exemplo de um conjunto de outros pesquisadores do setor) propôs uma arquitetura teórica para estudo e possível implementação para testes, pois acredita-se em seu valor operacional ante ganhos para a proteção da informação e produtividade na gestão de *Cloud Policies*.

6.2. Trabalhos Futuros

Para trabalhos futuros, realizar um teste empírico do *framework* proposto a partir de sua implementação em ambiente simulado, analizando seu potencial na proteção contra as ameaças identificadas pela CSA (2010), bem como suas limitações em relação a impactos em desempenho e custos de implementação para organizações de pequeno, médio e grande porte, com o intuito de verificar sua complexidade e viabilidade.

REFERÊNCIAS

BASESCU, C.; CARPEN-AMARIE, A. *Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies*. In: International Conference on Advanced Information Networking and Applications, p. 459-466, 2011.

BELLESSA, J.; KROSKE, E.; FARIVAR, R.; MONTANARI, M.; LARSON, K.; CAMPBELL, R. *NetODESSA: Dynamic Policy Enforcement in Cloud Networks*. In: 30th IEEE Symposium on Reliable Distributed Systems Workshops, p. 57-61, 2011.

COMPUTERWORLD. *Gastos dos EUA com cloud devem crescer 22% ao ano até 2014*. Disponível em: <http://cio.uol.com.br/tecnologia/2009/12/23/gastos-dos-eua-com-cloud-devem-crescer-22-ao-ano-ate-2014/>. Publicação, dezembro de 2009. Acessado em: 01/06/2012.

CSA. *Top Threats to Cloud Computing V1.0*. Cloud Security Alliance. Março, p. 1-14, 2010.

_____. *Cloud Security Alliance – ABOUT*. Disponível em <https://cloudsecurityalliance.org/about/>. 2012a – Acessado em: 05/06/2012.

_____. *Cloud Security Alliance – Research*. Disponível em <https://cloudsecurityalliance.org/research/>. 2012b – Acessado em: 05/06/2012.

_____. *Cloud Security Alliance – GRC*. Disponível em <https://cloudsecurityalliance.org/research/grc-stack/>. 2012c – Acessado em: 05/06/2012.

_____. *Cloud Security Alliance – Education*. Disponível em <https://cloudsecurityalliance.org/education/ccsk/faq/>. 2012d – Acessado em: 05/06/2012.

DAHBUR, K.; MOHAMMAD, B.; TARAKJI, A. B. *A Survey of Risks, Threats and Vulnerabilities in Cloud Computing*. New York Institute of Technology Amman,

Jordan School of Engineering and Computing Sciences New York Institute of Technology Amman, Jordan School of Engineering and Computing Sciences. 2011.

ESPADAS, J.; CONCHA, D.; MOLINA, A. *Application Development over Software-as-a-Service platforms*. In: The Third International Conference on Software Engineering Advances. P. 97-104. 2008.

EWEEK. *Platform as a Service Entering Pivotal Year: Gartner*. Disponível em: <http://www.eweek.com/c/a/IT-Infrastructure/Platform-as-a-Service-Entering-Pivotal-Year-Gartner-543626/>. Publicação, Março de 2012. Acessado em: 05/06/2012.

NETWORKWORLD. *Seven Cloud Computing Security Risks*. Disponível em: <http://www.networkworld.com/news/2008/070208-cloud.html>. Publicação, Janeiro de 2008. Acessado em: 05/06/2012.

GARTNER. Disponível em: <http://www.gartner.com/it/page.jsp?id=1622514>. Publicação, Abril de 2011. Acessado em: 05/06/2012.

_____. *The why of Cloud*. Disponível em: <http://www.gartner.com/technology/research/cloud-computing/>. 2012a. Acessado em: 05/06/2012.

_____. *Gartner Says Worldwide Software-as-a-Service Revenue to Reach $14.5 Billion in 2012*. Publicação, Março, 2012. Disponível em: <http://www.gartner.com/it/page.jsp?id=1963815>. 2012b. Acessado em: 05/06/2012.

GONG, C.; LIU, J.; ZHANG, Q.; CHEN, H.; GONG, Z. *The Characteristics of Cloud Computing*. In: 39th International Conference on Parallel Processing Workshops, p. 275-279. 2010.

ISO-IEC. *Risk Management Vocabulary – Guidelines for use in Standards*. Guide 73:2002. British Standards, 2002.

KUNDU, A.; BANERJEE, C.; SAHA, P. *Introducing New Services in Cloud Computing Environment*. International Journal of Digital Content Technology and its Applications, vol. 4, n. 5, August, 2010.

MoR. *What is MoR*. Disponível em <http://www.mor-officialsite.com/AboutM_o_R/WhatIsM_o_R.asp>. 2012 – Acessado em: 05/06/2012.

MELL, P. GRANCE, T. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology Recommendations of the National Institute of Standards and Technology*. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930. NIST Special Publication 800-145. P. 1-3. September, 2011.

PMBOK. *Guia PMBOK 4° Edição*. Project Management Institute – PMI, 337 páginas, 2008.

SOUSA, F. R. C.; MOREIRA, L. O.; MACHADO, J. C. *Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios*. ERACEMAPI - Escola Regional de Computação dos Estados do Ceará, Maranhão e Piauí, p.1-26, 2009.

SRIVASTAVA, P.; SINGH, S.; PINTO, A. A.; VERMA, S.; CHAURASIYA, V. K.; GUPTA, R. *An architecture based on proactive model for security in Cloud Computing*. In: IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011MIT, Anna University, Chennai. Junho, p. 661-666, 2011.

TAKABI, H.; JOSHI, B. D. *Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment*. In: 45th Hawaii International Conference on System Sciences, p. 5500-5508, 2012.

TAKABI, H.; JOSHI, J. B. D.; AHN, G. J. *Security and Privacy Challenges in Cloud Computing Environments*. IEEE Security and Privacy, Vol. 8, No. 6, pp. 25-31, 2010.

WANG, Z.; Luo, X. *Policy-Based SLA-Aware Cloud Service Provision Framework*. In: Seventh International Conference on Semantics, Knowledge and Grids, p.114-121, 2011.

WU, J.; PING, L.; GE, X.; WANG, Y.; FU, J. *Cloud Storage as the Infrastructure of Cloud Computing*. In: International Conference on Intelligent Computing and Cognitive Informatics, p, 380-383, 2010.

ZACHMAN, J. *A framework for information systems architecture.* IBM SYSTEMS JOURNAL, VOL 26. NO 3, p. 276-292, 1987.

ZHANG, XUAN; WUWONG, N.; LI, H.; ZHANG, X. *Information Security Risk Management Framework for the Cloud Computing Environments*. In: 10th IEEE International Conference on Computer and Information Technology (CIT 2010), p. 1328-1334, 2010.