Material Didático

ENGENHARIA DE REDES PARA CLOUD COMPUTING

FACULESTE
FACULDADE DO LESTE MINEIRO

31 99449-2833
31 4116-5404

CREDENCIADA JUNTO AO MEC PELA PORTARIA
Nº 3.455 DO DIA 19/11/2003
www.faculeste.com.br

SUMÁRIO

FACULESTE

A história do Instituto FACULESTE, inicia com a realização do sonho de um grupo de empresários, em atender a crescente demanda de alunos para cursos de Graduação e Pós-Graduação. Com isso foi criado a FACULESTE, como entidade oferecendo serviços educacionais em nível superior.

A FACULESTE tem por objetivo formar diplomados nas diferentes áreas de conhecimento, aptos para a inserção em setores profissionais e para a participação no desenvolvimento da sociedade brasileira, e colaborar na sua formação contínua. Além de promover a divulgação de conhecimentos culturais, científicos e técnicos que constituem patrimônio da humanidade e comunicar o saber através do ensino, de publicação ou outras normas de comunicação.

A nossa missão é oferecer qualidade em conhecimento e cultura de forma confiável e eficiente para que o aluno tenha oportunidade de construir uma base profissional e ética. Dessa forma, conquistando o espaço de uma das instituições modelo no país na oferta de cursos, primando sempre pela inovação tecnológica, excelência no atendimento e valor do serviço oferecid**o.**

A camada de Transporte

A função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores caso necessário, repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade. Além do mais, tudo isso deve ser feito com eficiência e de forma que as camadas superiores fiquem isoladas das inevitáveis mudanças na tecnologia de hardware. A camada de transporte também determina que tipo de serviço deve ser fornecido à camada de sessão e, em última análise, aos usuários da rede. O tipo de conexão de transporte mais popular é um canal ponto a ponto livre de erros que entrega mensagens ou bytes na ordem em que eles foram enviados. No entanto, outros tipos possíveis de serviço de transporte são as mensagens isoladas sem nenhuma garantia relativa à ordem de entrega e à difusão de mensagens para muitos destinos. O tipo de serviço é determinado quando a conexão é estabelecida.

TCP/IP

O TCP/IP (também chamado de pilha de protocolos TCP/IP) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou ainda, protocolo de interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas (Modelo OSI), onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração.

LDAP

Lightweight Directory Access Protocol, ou LDAP, é um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP. Um diretório LDAP geralmente segue o modelo X.500, que é uma árvore de nós, cada um consistindo de um conjunto de atributos com seus respectivos valores. O LDAP foi criado como uma alternativa ao muito mais incômodo Directory Access Protocol (DAP).

Um diretório LDAP tende a refletir vários limites políticos, geográficos e/ou organizacionais, dependendo do modelo adotado. A utilização do LDAP hoje em dia tende a se basear nos nomes já existentes do sistema Domain Name System (DNS), na estruturação dos níveis mais básicos de hierarquia. Mais profundamente, podem aparecer estruturas representando pessoas, unidades organizacionais, impressoras, documentos, grupos de pessoas ou qualquer outra coisa que represente um nó.

Camada de Aplicação

A camada de aplicação é a camada que a maioria dos programas de rede usa de forma a se comunicar através de uma rede com outros programas. Processos que rodam nessa camada são específicos da aplicação; o dado é passado do programa de rede, no formato usado internamente por essa aplicação, e é codificado dentro do padrão de um protocolo.

Alguns programas específicos são levados em conta nessa camada. Eles proveem serviços que suportam diretamente aplicações do usuário. Esses programas e seus correspondentes protocolos incluem o HTTP (navegação na World Wide Web), FTP (transporte de arquivos), SMTP (envio de email), SSH (login remoto seguro), DNS (pesquisas nome <-> IP) e muitos outros.

Existem diversos protocolos nesta camada. Como exemplo de alguns deles podemos citar:

· **SMTP (Simple Mail Transport Protocol**) é utilizado para a comunicação entre serviços de correio eletrônico na Internet.

· **POP (Post Office Protocol)** é utilizado para recuperação de mensagens de correio eletrônico via Internet.

· **IMAP (Internet Mail Access Protocol)** - também é utilizado para recuperação de mensagens de correio eletrônico via Internet, mas de forma mais avançada que o POP3.

· **HTTP (Hypertext Transport Protocol**) – utilizado para a publicação de sites WEB na Internet.

· **FTP (File Transfer Protocol)** – utilizado para publicação de arquivos na Internet.

· **DNS (Domain Name System)** - Utilizado para a distribuição de nomes de domínio

DNS

O DNS (Domain Name System - Sistema de Nomes de Domínios) é um sistema de gerenciamento de nomes hierárquico e distribuído visando resolver nomes de domínios em endereços de rede (IP).

O sistema de distribuição de nomes de domínio foi introduzido em 1984, e com ele, os nomes de hosts residentes em um banco de dados podem ser distribuídos entre servidores múltiplos, diminuindo assim a carga em qualquer servidor que provê administração no sistema de nomeação de domínios. Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP. Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. Este tipo de servidor usa como porta padrão a 53. A implementação do DNS-Berkeley, foi desenvolvido originalmente para o sistema operacional BSD UNIX 4.3.

HTTP

O Hypertext Transfer Protocol (HTTP), em português Protocolo de Transferência de Hipertexto, é um protocolo de comunicação (na camada de aplicação segundo o Modelo OSI) utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos.1 Ele é a base para a comunicação de dados da World Wide Web. Hipertexto é o texto estruturado que utiliza ligações lógicas (hiperlinks) entre nós contendo texto. O HTTP é o protocolo para a troca ou transferência de hipertexto.

SEGURANÇA DE REDES

VPN

Rede Privada Virtual é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

Deve ser notado que a escolha, implementação e uso destes protocolos não é algo trivial, e várias soluções de VPN inseguras são distribuídas no mercado. Advertem-se os usuários para que investiguem com cuidado os produtos que fornecem VPNs.

Criptografia

A Criptografia tem suas origens a muitos anos. Comenta-se que o imperador Romano Júlio César teria sido o primeiro a emprega-la quando enviava cartas criptografadas, pois não confiava no mensageiro e havia o risco dele ser capturado, no caso de uma guerra. O método utilizado por César era simples: ele rescrevia a carta somando 3 a posição da letra, ou seja, o "A"(1) passaria a ser "D"(4), o "B"(2) "E"(5) e assim sucessivamente, imaginado as letras dispostas em círculo, ou seja, a lista não termina no "Z"mas continua daí no "A"novamente.

Hoje a Criptografia utiliza técnicas muito mais complexas que as de César Augusto mais a sua ideia ainda é empregada. Uma ligeira modificação de sua ideia

original consiste, em vez de trocar cada caractere por ele + 3, troca-lo por ele + "n". Para descriptografar, portanto, o receptor deverá saber o valor de "n". Introduzimos ai o conceito de "chave". Já não basta o receptor conhecer apenas o método empregado, mas também deve conhecer a chave. Esta técnica, no entanto, é fácil de ser quebrada (manualmente, pois com o auxílio de computadores é muito fácil testar se um "A"foi substituído por algum dos outros 25 caracteres existentes) tendo-se em vista uma tabela de frequência para língua utilizada. Por exemplo, no inglês estudos comprovam que as letras mais usadas são e, t, o, a, n, i, etc. Precisaríamos apenas de uma tabela com suas frequências.

Firewall

Um firewall (em português: Parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, proxy de aplicações, etc. Os firewalls são geralmente associados a redes TCP/IP.1 ..

Este dispositivo de segurança existe na forma de software e de hardware, a combinação de ambos é chamado tecnicamente de "appliance". A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

CLOUD COMPUTING

Cloud Computing ou Computação em Nuvem começa a delinear como a tendência de desenho da infraestrutura de TI para as próximas décadas. Bastante discutido e comentado nos últimos 4 anos, este caminho agora parece mais natural, até em função de uma adoção de virtualização de servidores em larga escala pela grande maioria das empresas. No Brasil ainda existe um receio à nova tecnologia talvez pela falta de conhecimento dos profissionais de TI, pela Infraestrutura disponível e pelas incertezas e inseguranças da nova tecnologia. Em consequência disso o Brasil, no ano de 2012, fico em ultimo lugar na pesquisa realizada pela BSA

que levava em conta um plano de politicas de nuvens composta por sete itens que iremos falar mais adiante.

O conceito propõe que tudo o que precisarmos no que diz respeito à utilização de software e hardware será cobrado baseado no que usarmos, ou seja, você não gasta mais do que deveria gastar e não precisa se preocupar com versões de SO e Aplicativos, as Compras de Peças, Equipamentos, Cabos, configurações e etc., pois qualquer que seja a implementação necessária de qualquer um desses recursos terá de ser feito pelo seu provedor de Cloud Computing contratado restando assim como sua única preocupação é em pagar pelo tempo o que gastou. Tanto para empreendimentos, grandes ou pequenos, quanto para entidades governamentais em todo o mundo, um fato é claro: a Cloud Computing representa a próxima grande contribuição do software e das tecnologias de computação para maior produtividade e maior crescimento econômico.

Segundo Ruschel Cloud Computing é uma tendência recente de tecnologia que tem por objetivo proporcionar serviços de tecnologia da Informação sob-demanda com pagamento baseado no uso. Cloud Computing pretende ser global e prover serviços para todos, desde o usuário final que hospeda seus documentos pessoais na Internet até empresas que terceirizarão toda a parte de TI para outras empresas. Diante desse cenário, grandes empresas como Amazon, Google, Microsoft, HP, IBM, dentre outros, entraram nessa área oferecendo diversas modalidades de Cloud Computing.

A segurança da informação é de extrema importância seja para uma empresa ou para o próprio indivíduo, a todo o momento estamos sujeitos a ameaças, sejam suas causas naturais ou não, intencionais ou não. Informações privilegiadas em relação a terceiros nas mãos de pessoas mal intencionadas podem gerar perdas irreparáveis, conflitos, podem decidir o futuro de uma ou várias pessoas. Na Cloud Computing onde tudo está mantido na internet a preocupação com segurança precisa ser ainda maior, pois os riscos e ameaças existentes são ainda mais constantes. Carneiro reforça que apesar dos benefícios de captar a computação nas nuvens de alguém, existem armadilhas potenciais. As principais preocupações em relação à Cloud Computing residem em dois aspectos: Privacidade e Segurança. Você deve confiar em um estranho para proteger seus aplicativos e informações neles contidas?

Diversas pesquisas vêm sendo realizadas para solucionar este problema. Neste trabalho serão apresentadas algumas dessas propostas.

COMPUTAÇÃO EM NUVEM

Segundo Taurion uma definição simples de Cloud Computing pode ser um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na internet. Um ambiente de Nuvem não vai resolver todos os problemas de TI nas empresas. Algumas aplicações irão funcionar muito bem em nuvens e outras não irão.

Desta forma o NIST define Cloud Computing descrevendo cinco características essenciais, três modelos de serviço e quatro modelos de implementação. Eles estão sumarizados visualmente na figura 1 e Esclarecido em seguida.

Figura 1: Modelo Visual da Definição Corrente de Cloud Computing do NIST - CSA

Características Essenciais

Os serviços na nuvem apresentam cinco características essenciais, adaptadas NIST, que demonstram suas relações e diferenças das abordagens tradicionais de computação:

- **Autoatendimento sob-demanda:** O usuário pode adquirir unilateralmente recurso computacional na medida em que necessite e sem precisar de interação humana com os provedores de cada serviço. Um exemplo seria o processamento no servidor ou armazenamento na rede.

- **Amplo acesso a rede:** Os recursos são disponibilizados através da rede e acessados por meio das plataformas computacionais (thin clients), tais como celulares, laptops e PDAs.

- **Elasticidade Rápida:** Recursos podem ser rapidamente e elasticamente obtidos, em alguns casos automaticamente, caso haja a necessidade de escalar com o aumento da demanda, e liberados, na retração dessa demanda. Para os usuários, os recursos disponíveis para uso parecem ser ilimitados e podem ser adquiridos em qualquer quantidade e a qualquer momento. A virtualização auxilia muito na computação nuvem

- **Pool de Recursos:** Os provedores de serviços estão agrupados para servir a múltiplos clientes, usando um modelo de “múltiplos inquilinos”, com recursos físicos e virtuais diferentes, sendo dinamicamente alocados e realocados de acordo com a demanda. Estes clientes não precisam ter conhecimento da localização física dos recursos computacionais, podendo somente especificar a localização em um nível mais alto de abstração, tais como o país, estado ou Data Center. Exemplos de recursos: armazenamento, processamento, memória, largura de banda e máquinas virtuais.

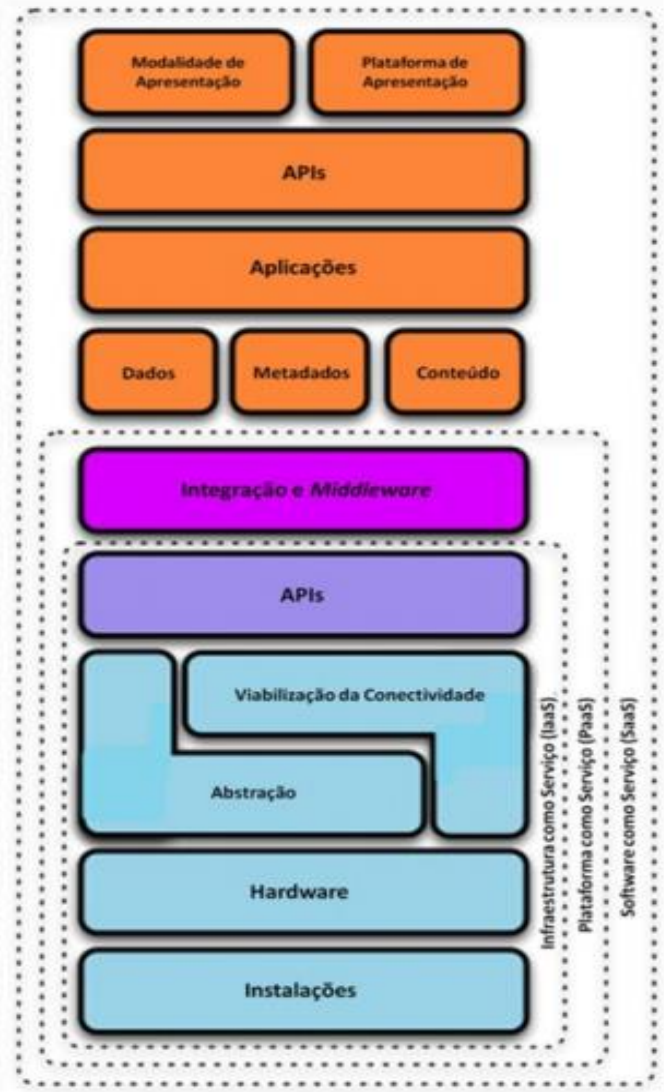
- **Serviços mensuráveis ou Medição de uso dos serviços**: Os sistemas em nuvem possuem recursos automaticamente controláveis e aperfeiçoáveis alavancando a capacidade de medição a um nível apropriado ao tipo de serviço. Tanto o provedor quanto o consumidor podem monitor e controlar a utilização dos recursos. Exemplos: armazenamento, processamento, largura de banda e número de contas ativas dos usuários.

Modelos de Serviços

De acordo com a NIST e CSA os tipos de serviço que podem ser utilizados pela nuvem são: SaaS, PaaS e IaaS. Estes modelos são importantes, pois eles definem um padrão arquitetural para soluções de computação em nuvem. Software as a Service ou Software como Serviço (SaaS): É definido como um software que você pode acessar via Internet. É implantado e mantido pelo provedor. Não há nenhum investimento prévio; em vez disso, você paga pelo uso conforme necessário - SYMANTEC. Como exemplos podemos destacar os serviços de Customer Relationship Management (CRM) da Sales-force e o Google Docs e Google Gmail – Ciurana e o Prezi Platform as a Service, ou Plataforma como Serviço (PaaS). Oferece uma plataforma para criar suas próprias aplicações na nuvem. Toda a infraestrutura é implantada e mantida pelo fornecedor. Além disso, é fornecido um conjunto de APIs para criação das aplicações. Não há nenhum investimento prévio. Em vez disso, você paga pelo uso conforme necessário - SYMANTEC. Um exemplo conhecido seria o Google Apps Engine – Ciurana e não muito conhecido Aneka – Vecchiola.

Infrastructure as a Service ou Infraestrutura como Serviço (IaaS). Oferece a infraestrutura básica, como servidores, switches, recursos de armazenamento, recursos de processamento em um modelo sob demanda. A infraestrutura é mantida pelo provedor. Não há nenhum investimento prévio; em vez disso, você paga pelo uso conforme necessário - SYMANTEC. Segundo Vaquero tudo isso se deve ao a virtualização, que possibilita dividir, atribuir e dinamicamente redimensionar os recursos para se constituir sistemas personalizados demandados pelos clientes. Segundo Marcon Considera a adoção de mais um serviço: Identificação para nuvem como um serviço (IDaas): o CSA considera o IDaas um serviço de gerenciamento de identidades para nuvem, sendo externo as aplicações e aos provedores que utilizam as identidades. O IDaaS é um serviço que fornece gerenciamento de identidade e do ciclo de vida dos usuários, funções de controle de acesso, Single Sign-On etc. Este serviço pode ser utilizado pelos modelos SaaS, PaaS IaaS.

Figura 2 – Modelo de Referência de Nuvem – CSA



Modelos de Implementação

De acordo com CSA independente do modelo de serviço utilizado existem quatro modelos de implantação de serviços de nuvem, com variações para atender a requisitos específicos.

- Nuvem Pública: Descreve um modelo usado pelo provedor para implantar serviços públicos em nuvem, para qualquer empresa utilizar (mediante uma taxa) - SYMANTEC. A infraestrutura de nuvem é disponibilizada ao público em geral ou a um grande grupo industrial e é controlada por uma organização que vende os serviços

de nuvem. Segundo Taurion uma nuvem publica é uma caixa preta aonde o eventual falta de transparência sobre a sua tecnologia, seus processos e organização torna difícil a avaliação do nível de segurança e privacidade que o provedor é capaz de oferecer.

- Nuvem Privada: Descreve um modelo usado pela organização para implantar serviços privados em nuvem; apenas para seus públicos de interesse - SYMANTEC. A infraestrutura da nuvem é operada exclusivamente por uma única organização. Ela pode ser gerida pela organização ou por terceiros, e pode existir no local ou fora do ambiente da empresa. De acordo com Taurion uma nuvem privada ou interna é uma nuvem computacional confinada à Data Center da empresa.

- Nuvem Comunitária. A infraestrutura da nuvem é compartilhada por diversas organizações e suporta uma determinada comunidade que partilha interesses (por exemplo: a missão, os requisitos de segurança, política ou considerações de conformidade). Também tem a opção de ser localizada nos domínios das organizações ou fora delas

- Nuvem Híbrida: A infraestrutura da nuvem é uma composição de duas ou mais nuvens (privada, comunitária ou pública) que permanecem como entidades únicas, mas estão unidas pela tecnologia padronizada que permite a portabilidade de dados e aplicativos (por exemplo, “cloud bursting” para balanceamento de carga entre as nuvens).

POLÍTICAS DE COMPUTAÇÃO NA NUVEM

Conforme a crescente adesão da Cloud Computing se pressupõe a adoção de políticas adequadas em cada uma das sete áreas usadas no índice da BSA:

1. Garantia da privacidade: O sucesso depende da confiança dos usuários na utilização e proteção devida de seus dados.

2. Promoção da segurança: Provedores de nuvem devem poder implementar segurança de última geração sem exigências de uso de tecnologias específicas

3. Combate ao crime digital: Sistemas legais devem oferecer mecanismos efetivos para o cumprimento da lei, e para que os próprios provedores possam combater o acesso indevido a dados armazenados na nuvem.

4. Proteção da propriedade intelectual: As leis de propriedade intelectual devem oferecer proteção clara e vigorosa contra apropriação indevida e infração de recursos da estrutura da nuvem.

5. Garantia da portabilidade de dados e harmonização de regras internacionais: Governos devem trabalhar em conjunto com a indústria para desenvolver padrões e minimizar obrigações legais conflitantes impostas sobre provedores de nuvem.

6. Promoção do livre comércio: A capacidade da nuvem de promover crescimento econômico depende de um mercado global que transcenda barreiras ao livre comércio.

7. Estabelecimento da infraestrutura de TI: Incentivo ao setor privado em estrutura de banda larga e de leis que promovam o acesso universal para a banda larga.

SEGURANÇA EM COMPUTAÇÃO EM NUVEM

Segundo Mourato, a segurança em um âmbito de sistemas de informação são os recursos e medidas necessários para proteger a informação de incidentes, como manipulação ou violação de dados, falhas e etc., a recuperação e minimização dos possíveis danos também fazem parte da segurança da informação. Na computação tradicional os usuários tem total controle sobre seus dados, processos e seu computador. Ao migrar para Cloud Computing todos os serviços e manutenção dos dados são fornecidos por um provedor de nuvem. O cliente desconhece quais processos estão em execução ou onde os dados estão armazenados. Sendo assim as organizações precisarem ser mais responsáveis pela confidencialidade e pela conformidade das práticas de computação na empresa.

A Symantec realizou uma pesquisa para avaliar a situação de Cloud Computing na América Latina, e seu estudo mostrou a Segurança como o principal objetivo e preocupação das organizações entrevistadas para migração para a nuvem. 86% dos entrevistados acreditam que a nuvem não causará impacto ou até mesmo vai melhorar a postura de segurança. De outro lado, eles classificam a segurança como a principal preocupação. Que são: Surto de malware; Roubo de dados por hacker; Compartilhamento inseguro de dados confidenciais via nuvem; Uso Irregular da Nuvem; Vazamento de Informação. Princípio da Segurança da Informação em um modelo de Nuvem Publica envolvem Integridade, Confidencialidade; Disponibilidade, Autenticidade, Não-repúdio. Lembrando que Nuvem Privada o nível de segurança é muito maior, pois esta dentro do firewall e ai existe um maior controle e estrita aderência às restrições regulatórias.

Para garantir o mínimo de segurança em Cloud Computing temos algumas soluções simples que podem auxiliar e muito. As soluções são propostas são: Utilização de Senhas Fortes, Token (Dispositivo eletrônico gerador de senhas – Utilizado em Sites de Banco), Cartão de segurança (Ao realizar alguma operação de acesso, um dos códigos do cartão será solicitado aleatoriamente) e biometria (Marca algum traço da pessoa). Lembrando esse são soluções simples que em alguns casos não irão funcionar corretamente, como por exemplo, o caso do Token que não funcionaria em celulares.

Observamos ainda que uma boa segurança exige modelos que reconcilie a capacidade de expansão e diversas alocações de empresas com uma necessidade de confiança. Ao deixar de lado às medidas de controle na computação tradicional as empresas devem ter o cuidado de terem a sua disposição a segurança de identidades, informação e infraestrutura. Mas para que isso possa vir acontecer primeiramente deverá existir uma confiança nos sistemas e nos provedores de Nuvem, podem assim verificar os processos e os eventos na nuvem. Alguns elementos da segurança é muito importante que são: controle de acesso, a segurança dos dados, a conformidade e o gerenciamento de eventos.

Segurança de identidades

A segurança da identidade preserva a integridade e a confidencialidade dos dados e dos aplicativos enquanto deixa o acesso prontamente disponível para os usuários apropriados. O gerenciamento completo de identidades, os serviços de autenticação de terceiros e a identidade federada se tornarão elementos fundamentais para a segurança da nuvem. O suporte a esses recursos de gerenciamento de identidade para usuários e componentes da infraestrutura será um dos principais requisitos da Cloud Computing e a identidade precisará ser gerenciada de maneira que gere confiança.

Ele exigirá:

- Autenticação sólida: Para oferecer suporte a empresas deve ir além da fraca autenticação com nome de usuário e senha. Isso significa adotar técnicas e tecnologias que já são padrão na TI corporativa, como autenticação sólida (autenticação de vários fatores com tecnologia de senha única), federação dentro de empresas e, entre elas, a autenticação com base em risco que mede o histórico de comportamento, o contexto atual e outros fatores para avaliar o nível de risco de uma solicitação de usuário.

- Autorização mais dispersas ou granular: a autorização pode ser especificada dentro de uma empresa ou até de uma nuvem privada, mas para manipular dados confidenciais e requisitos de conformidade, as nuvens públicas precisarão de recursos granulares de autorização que possam ser persistentes na infraestrutura da nuvem e ao longo de todo o ciclo de vida dos dados.

Ao criar um serviço de identidades nas Nuvens devem ter suportar a delegação de direitos administrativos, repassando assim o gerenciamento aos administradores individuais de cada ambiente (SaaS, PaaS, IaaS) e consequentemente pode gerenciar as contas dentro de seu próprio domínio [13] É necessário um mecanismo a fim de prover autenticação e autorização de usuários pertencentes ao mesmo domínio/empresa como usuário parceiros. Para que a cooperação seja realizada com êxito, as entidades parceiras devem definir politicas para o compartilhamento de recursos junto ao domínio federados.

Esse processo envolve mecanismo ou serviço de SSO (Single Sign-On) que pode ser terceirizado, instanciado a organização consumidora. Ele deve fornecer o suporte aos processos de criação e emissão das credenciais. Temos a Opção do OpenID.

Segurança das informações

Não existe mais as barreiras físicas nas nuvens, desta forma os dados deverão ter maior segurança que os acompanhe e os proteja. Segundo a RSA exige seis itens principais que são.

- **Isolamento de dados:** Todos os processos serão fortes para permitir níveis variáveis de separação entre corporações, comunidades de interesse e usuários.

- **Segurança de dados mais granular:** Os dados confidenciais demandarão segurança no nível do arquivo, do campo ou até do bloco para atender às demandas de garantia e conformidade.

- **Segurança consistente dos dados:** Precisará da criptografia (Assunto tratado logo em seguida) em trânsito e em repouso, além do gerenciamento em toda a nuvem e ao longo de todo o ciclo de vida dos dados.

- **Classificação eficiente de dados:** As empresas precisarão saber quais dados são importantes e onde eles estão localizados como pré-requisitos para tomar decisões sobre o custo/benefício do desempenho, além de garantir o foco nas áreas mais essenciais dos procedimentos de prevenção contra a perda de dados.

- **Gerenciamento dos direitos às informações**: Exige que as políticas e os mecanismos de controle no armazenamento e o uso das informações sejam diretamente associados às informações.

- **Controle e conformidade:** Criação de informações de gerenciamento e validação — monitorando e fazendo a auditoria do estado de segurança das informações com recursos de registro.

De acordo com Marcon poderá utilizar um serviço que cria as politicas de controle de acesso em um local, que pode ser dentro da organização, e ser executadas em outros. As atualizações são realizadas periodicamente ou através de batch de acordo como preferir. Existe alguns software gratuitos para isso como o XACML – eXtensible Access Control Markup Language e a WS-Policy.

PRIVACIDADE E COMPUTAÇÃO EM NUVEM

A privacidade é a limitação do acesso aos dados de determinado registro, assim como a garantia ao indivíduo de seu anonimato, e de liberação de acesso somente para pessoas com permissão. Na Informática a privacidade consiste nos direitos e obrigações dos indivíduos e organizações com relação à coleta, uso, conservação e divulgação de informações pessoais. Podemos relacionar a privacidade com a confidencialidade. Definindo desta forma que uma informação não deve estar disponível ou divulgada a indivíduos, entidades ou processos não autorizados pela política de acesso.

A integridade das informações é uma questão indispensável, seja em ambientes de Cloud Computing ou com recursos próprios. Os provedores devem adotar instrumentos e procedimentos os mais avançados disponíveis e esforçar-se para prover níveis de segurança e privacidade melhores dos que os alcançáveis com o emprego recursos computacionais próprios. Para este finalidade, a criptografia e o gerenciamento de chaves apresentam-se como um método eficiente e eficaz, fornecendo a proteção e acesso aos recursos protegidos. É um método não só recomendado, como também exigido por lei e regulamentos em determinados países.

A Cloud Security Alliance confeccionou o Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem. Neste guia envolve tópicos como Arquitetura da Nuvem, Governança na Nuvem e Operando na Nuvem. De acordo com esse guia tirei algumas informações relacionados a privacidade. Os clientes de nuvem querem que seus provedores cifrem seus dados para assegurar que os mesmos estejam protegidos não importando onde estejam localizados fisicamente. Da mesma forma, o provedor de nuvem precisa proteger os dados sensíveis de seus clientes.

Como forma de implementação, aconselha-se que se adote a criptografia não só para os dados em trânsito, aqueles trafegados entre o cliente e o provedor de nuvem, quanto para aqueles que estejam em repouso no ambiente do provedor, além das mídias de backup destes dados. Isto irá proteger os dados contra acessos indevidos de outros locatários dos serviços de nuvem, de provedores maliciosos, perda ou roubo de mídias dentre outros. Para garantir o acesso aos dados criptografados por usuários legítimos e de direito, é fundamental que um processo de gerenciamento de chaves seja definido, com a criação de repositórios seguros de chaves, o acesso limitado a estes repositórios, e a da adoção de soluções de backup e recuperação de chaves.

Neste processo o gerenciamento das chaves deve ser segregado do provedor onde os dados são hospedados, fornecendo maior garantia de confidencialidade. Existem vários padrões e diretrizes aplicáveis ao gerenciamento de chaves na nuvem. O Key Management Interoperability Protocol (KMIP), da OASIS, é um padrão emergente para um gerenciamento de chaves interoperável na nuvem. Os padrões IEEE 1619.3 cobrem criptografia de armazenamento e gerenciamento de chaves, especialmente no que diz respeito a armazenamento IaaS

COMPUTAÇÃO EM NUVEM EM REDES

A evolução do cenário tecnológico mundial acontece a taxas mais aceleradas. As instituições tentam acompanhar tal crecimento quanto à necessidade do uso intensivo dos recursos tecnológicos para acelerar os processos, serviços e organização da infraestrutura, tratados anteriormente de maneira rústica, mesmo tendo aplicação tecnológica adequada para o momento. Percebe-se tal busca tanto em ambientes restritos (intranet) quanto em ambientes abertos (extranet). Direcionando o foco para grandes empresas, quase não existem instituições realizando atividades que, antes, eram realizadas manualmente, e hoje, após a informatização dos processos, se tornou digital. O acúmulo de informação na infraestrutura é inevitável e cada vez maior, seja em computadores pessoais, bases de dados centralizadas ou servidores (Cabral, 2009).

A área de telecomunicações, por sua vez, acompanhou os grandes avanços tecnológicos, e, em um curto espaço de tempo, grandes porções dos recursos digitais, outrora apenas disponíveis nos equipamentos de maneira restrita e local, tornaram-se presentes em ambientes abertos em rede, num crescimento exponencial e contínuo, de acordo com a expansão da Web. Assim, acompanhando tal movimento, o aumento da largura de banda vem causando crescimento do tráfego de áudio e vídeo, mas por motivos diferentes. As empresas enxergam a oportunidade de transportar o tráfego de voz e vídeo usando a Internet visando a redução de custos nas contas telefônicas e aluguel de enlaces (links) dedicados para vídeo conferência (Tanenbaum e Wetherall, 2011).

Esse processo contínuo advém da simplificação da computação, além da diminuição dos preços dos equipamentos como um todo, o que retrata o aumento de tecnologia em uso por corporações de todos os continentes, gerando um aumento da infraestrutura instalada, consumo de energia, custos de manutenção, além do impacto ambiental pela utilização de silício da fabricação dos componentes. Nesse sentido, há uma corrente na computação que defende arduamente o conceito da utilização da computação como serviço, onde gera um impacto imediato na diminuição de recursos instalados e consumidos, além da corrente ecológica denominada TI verde (Muruguesan, 2008), que defende o aumento da virtualização de recursos em

detrimento ao aumento de infraestrutura física. Dessas ideias e conceitos inovadores surgem virtualizadores e servidores de virtualização, e neles criam-se estações, servidores e redes com máxima disponibilidade de recursos de hardware e software, completamente transparentes aos usuários.

Inovar é preciso! Surge o conceito de computação como serviço, que é definido como “informaticidade” (Meira, 2006). A informática tão simples quanto a eletricidade. Nesta analogia à da energia elétrica em sua implantação e expansão, inicialmente aos “trancos e barrancos”, até tornar-se estável e confiável. Este paralelo entre a eletricidade e a computação em nuvem é bastante adequado, pois a disponibilização da computação como serviço através da nuvem, no estágio atual está em processo de implantação como bem pervasivo, ou seja, uma facilidade assumida como disponível, cuja existência só é percebida quando da sua eventual ausência.

O advento da computação em nuvem é fruto da evolução e da união dos conceitos e fundamentos técnicos das áreas de virtualização de servidores, Computação em Grade (Grid Computing), Computação em Grupo (Cluster Computing), Software orientado a serviços, gestão centrais de dados (Data Centers), dentre outras. O modelo tem-se mostrado eficiente na utilização de softwares, no acesso, armazenamento e processamento dos dados por meio de diferentes dispositivos e tecnologias web, deste modo transformando os sistemas computacionais físicos em uma base virtual (Taurion, 2009).

Sob uma visão macro, a Computação em Nuvem advém do princípio de que todos os recursos de infraestrutura de TI (hardware, software, gestão de dados e informação), até então tratados como um ativo pelas corporações passam a ser acessados e administrados através da world wide web (nuvem), utilizando navegadores (browsers), fazendo com que qualquer tipo de equipamento (smartphones, notebooks, netbooks, desktops, etc) passe a ser ativo da empresa na gestão dos dados armazenados remotamente. As empresas não comprariam nem manteriam seus recursos tecnológicos, dados e sistemas. Tais ativos seriam providos por fornecedores, mesclando infraestrutura e serviços capacitados para atender a demanda correspondente. O paradigma da computação em nuvem revela-se como novidade na área, porém uma série de questões e problemas necessitam ser respondidos e solucionados, para que se possibilite a sua plena utilização e a adoção sem receios pelas empresas.

COMPUTAÇÃO PARALELA EM REDE LOCAL (CLUSTER)

Para falar de computação em grupo numa rede local ou cluster é necessário iniciar com uma definição de redes computacionais agrupadas, que segundo a referência (Asanovic et. al., 2009), a computação em rede local agrupada consiste em um aglomerado de computadores distintos, geralmente de configurações homogêneas, interconectados através de uma rede de interconexão (geralmente uma rede local Ethernet) e visíveis como sendo um único computador paralelo, trazendo benefícios como alta disponibilidade e redundância

Os avanços da tecnologia de computadores geralmente não acompanham a demanda solicitada e, às vezes, a utilização de supercomputadores é inviável financeiramente. Uma alternativa a ser adotada pode ser a soma dos recursos computacionais já existentes utilizando-os de forma mais apropriada e equilibrada, resultando em um ganho substancial de desempenho (speedup). Neste contexto, podem ser aplicados os paradigmas de grade (grid) computacional que melhor usufruem, respectivamente, dos recursos e serviços de maneira local e geograficamente distribuída (Colvero et al., 2005).

Em um ambiente de computação paralela de rede local, a alocação de recursos é efetuada por domínio administrativo centralizado, sendo desnecessária a segurança do processo e do recurso, caso a rede de interconexão (intracluster) seja desacoplada da rede de acesso externo. Este tipo de ambiente pode se beneficiar de protocolos de comunicação mais eficientes entre suas unidades de processamento (Colvero et al., 2005).

REFERENCIAS

BSA. **Pontuação Global de BSA, Computação em Nuvem da BSA** - Um Guia para Oportunidades Econômicas. Disponível em: < http://portal.bsa.org/cloudscorecard2012/assets/pdfs/GlobalCloudScorecard_pt.pdf > Acesso em: 5 jan. 2013.

CARNEIRO, Ricardo Jose Gouveia; RAMOS, Cleisson Christian Lima da Costa. **A Segurança na Preservação e Uso das Informações na Computação nas Nuvens.** Disponível em: < http://www.4learn.pro.br/guarino/sd/08-Cloud%20Computing.pdf> Ultimo acesso em: 4 de jan. de 2013

FRANCISCONI, Carlos Fernando; GOLDIM, Jose Roberto. **Aspectos Bioeticos da Confidencialidade e Privacidade.** Disponível em: < http://www.portalmedico.org.br/biblioteca_virtual/bioetica/ParteIVaspectosbio-eticos.htm> Ultimo acesso em 11 de Abril de 2012

RUSCHEL, Henrique; ZANOTTO, Mariana Susan; MOTA, **Welton da Cos-ta. Computação em Nuvem.** Disponível em: Ultimo acesso em: 7 de jan. de 2013
JOHNSON, B. Cloud computing is a trap, warns GNU founder Richard Stallman. setembro 2009.

TAURION, Cezar. Cloud Computing: Transformando o Mundo do TI. 1ª Ed., Editora Brasport, Rio de Janeiro, RJ - 2009. [7] **NIST (National Institute of Standards and Technology)- The NIST Definition of Cloud Computing, Version 15, September 2011, National Institute of Standards and Technology, I**nformation Technology Laboratory – Gaithersburg, Maryland – USA. Disponível em: . Acesso em 10 de dez. de 2012

CSA (Cloud Security Alliance). **Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem**, 2010. Disponível em: Acesso em: 15 dez. 2012>.
SALESFORCE 2013]. Salesforce. .

CIURANA, E. (2009). **Developing with Google App Engine**. Apress, Berkely, CA, USA.

VECCHIOLA, C., Chu, X., and Buyya, R. (2009). **Aneka:** A Software Plat-form for .NET-based Cloud Computing, pages 267–295. In: W. Gentzsch, L. Grandinetti, G. Joubert (Eds.). High Speed and Large Scale Scientific Computing. IOS Press, Amsterdam, Netherlands.

VAQUERO, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. (2009). **A break in the clouds:** towards a cloud definition. SIGCOMM Comput. Commun. Rev., 39(1):50–55.

MARCON, Arlindo; LAUREANO, Marcos; SANTIN, Altair; MAZIERO, Carlos. **Aspectos de Segurança e Privacidade em Ambientes de Computação em Nuvem**. Disponível em: Ultimo acesso em: 12 de novem. de 2012

MOURATO, Joao Carlos Gomes. **Segurança de Sistemas de Informação**. 2008. Artigo de Licenciatura em Engenharia Informática - Escola Superior de Tecnologia e Gestão – Instituto Politécnico de Portalegre, Porto Alegre - RS

BRODKIN, Jon (2008). **Gartner: Seven cloud-computing security risks.** Network World, disponível em:

SYMANTEC. **Pesquisa sobre Situação de Cloud Computing:** Resultados América Latina. Disponível em: < http://www.symantec.com/content/pt/br/enterprise/images/theme/state-ofcloud/State-of-Cloud-Report-LAM-PORT-FN.pdf>. Acesso em: 12 jan. 2013.

CASTRO, R. C. C., Pimentel de Sousa, V. L., **Segurança em Cloud Computing:** Governança e Gerenciamento de Riscos de Segurança, In: III Congresso Tecnológico de TI e Telecom InfoBrasil 2010, Anais Eletrônicos; Fortaleza, CE, 2010. Disponível em http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud.pdf

OpenID (2012). **OpenID Foundation** - OIDF. OpenID Foundation.

RSA**. Pontuação Global de BSA, Computação em Nuvem da BSA** - Um Guia para Oportunidades Econômicas. Disponível em: < http://portal.bsa.org/cloudscorecard2012/assets/pdfs/GlobalCloudScorecard_pt.pdf > Acesso em: 5 jan. 2013.

PREZI 2010. . [21] Mather, T., Kumaraswamy, S., e Latif, S. (2009). **Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance**. O'Reilly Media.

GUERRA , Fernando C. G. D. Marcelo de Alencar Veloso Rogério Luís Massensini **Cloud Computing:** Questões Críticas Para A Implementação Em Organizações Públicas Disponível em:.