Uma Arquitetura para Geração e Implantação de Tiquetes de Confiança

Implementação de sistema de tíquetes em ambiente de nuvem

Luis Gustavo Souza Silva
Faculdade do Gama – Universidade de Brasília Universidade de Brasília
Brasília - DF, Brazil
luisgustavodd@hotmail.com

Antonio Bezerra da Silva Júnior
Faculdade do Gama – Universidade de Brasília Universidade de Brasília
Brasília - DF, Brazil
antoniojunior.ti@gmail.com

Edna Dias Canedo
Faculdade do Gama – Universidade de Brasília Universidade de Brasília
Brasília - DF, Brazil
ednacanedo@unb.br

***Resumo*— Este artigo descreve a arquitetura e os componentes de um mecanismo de geração e implantação de Tíquetes de Confiança (TT, do inglês *Trust Tickets*) para o ambiente de Computação em Nuvem. Os Tíquetes de Confiança visam o aumento da confiança e segurança do ponto de vista do Dono dos Dados (DO) ao garantir que apenas os usuários registrados e autenticados pelo DO tenham acesso às informações.**

Palavras-chave—Tíquetes; confiança; segurança; computação em nuvem;

I. INTRODUÇÃO

A computação em nuvem é definida como um modelo com alta escalabilidade que funciona sob demanda [*apud* MELL e GRANCE 2009] ao tentar deslocar toda a infraestrutura computacional para a rede de forma a reduzir os custos de software e hardware [VAQUERO et al. 2009].

O Dono dos Dados (DO), o Usuário dos Dados (U) e o Provedor de Serviços da Nuvem (CSP) são partes importantes da computação em nuvem [AHMED e XIANG 2011]. Eles representam os papéis da arquitetura de uma nuvem e cada um representa interesses e responsabilidades específicas. Segundo [AHMED e XIANG 2011], um cenário típico de um Software como Serviço (SaaS) é ter o Dono dos Dados como o responsável por fornecer os dados, que serão disponibilizados ao Usuário dos Dados por meio de um Provedor de Serviços da Nuvem.

Toda a infraestrutura de Nuvem será desenvolvida usando-se a plataforma VMWare ESXi v5.1 e a ferramenta VMWare vSphere v5.1. A primeira, trata-se de uma plataforma, "instalada diretamente no hardware de servidor, inserindo uma camada robusta de virtualização entre o hardware e o sistema operacional" [VMWare 2009], a segunda, uma ferramenta para administração de Máquinas Virtuais (VMs) e recursos das mesmas (alocação dinâmica). A Figura 1 apresenta a esquematização do uso da alocação dinâmica.

O uso da ferramenta VMWare ESXi, bem como sua implantação em qualquer organização, garante os princípios básicos de computação em Nuvem: (i) gerenciamento avançado de recursos; (ii) desempenho e escalabilidade; (iii) alta disponibilidade; (iv) interoperabilidade; (v) segurança; e (vi) capacidade de gerenciamento [VMWare 2009].

Figura 1 – Esquema de Virtualização VMWare ESXi [VMWare 2009]

É importante ressaltar que se tratam de ferramentas pagas, ou seja, todos os trabalhos realizados foram feitos através de versões gratuitas, fornecidas por 60 (sessenta) dias para testes pela própria empresa.

Este trabelho pretende:

- Prover uma arquitetura prescritiva de um mecanismo de geração de Tíquetes de Confiança;
- Prover uma arquitetura prescritiva de um mecanismo de implantação de Tíquetes de Confiança.
- Prover uma estrutura de Nuvem que comporte a aplicação do mecanismo de Tíquetes, ou seja, uma estrutura que contenha três máquinas virtuais, representando: (i) o Usuário dos Dados; (ii) o Dono dos Dados; e (iii) o Provedor de Serviços da Nuvem.

Para facilitar o entendimento deste artigo sua organização é descrita a seguir. Na seção 2, serão apresentados os trabalhos relacionados e que basearam este artigo. Na seção 3, será descrito o mecanismo de Tíquetes de Confiança proposto por [AHMED e XIANG 2011]. Na seção 4, serão descritos os módulos e componentes da arquitetura. Finalmente na seção 5, é apresentada a conclusão, bem como as sugestões de trabalhos futuros.

II. TRABALHOS RELACIONADOS

Segundo [AHMED e XIANG 2011] a computação em nuvem possui problemas e desafios no que diz respeito a confiança [*apud* ZHANG, CHENG e BOUTUBA 2010] e segurança [*apud* CHANG e CHOI 2010]. Trabalhos sobre o fornecimento controlado e seguro de dados já foram feitos. Porém esses ou carecem de detalhes [*apud* ARMBRUST 2010], ou são muito complexos [*apud* YU. WANG, WEN, LOU 2010] ou não são transparentes [*apud* SANKA, HOTA, RAJRAJAN 2010]. Em [AHMED e XIANG 2011] são propostos mecanismos para a geração e implantação de Tíquetes de Confiança.

III. MECANISMOS DE TÍQUETES DE CONFIANÇA

O mecanismo proposto por [AHMED e XIANG 2011] utiliza a criptografia como mecanismo de confiança para atender a confidencialidade dos dados. Neste mecanismo, o Provedor de Serviços da Nuvem mantém a informação, que foi cifrada com a chave secreta K_O, e que somente poderá ser acessada após o Usuário dos Dados ter sido registrado pelo Dono dos Dados junto ao Provedor. O Usuário dos Dados recebe a chave secreta K_O para poder decifrar as informações.

O mecanismo de tíquetes de confiança pode ser divido em duas partes: Geração e Implantação. A geração das chaves inicia-se com uma mensagem do Usuário dos Dados para o Dono dos Dados. A partir dessa mensagem, o DO gera um Tíquete de Confiança, que é armazenado em uma tabela com as capacidades desse usuário. O DO então envia uma mensagem ao CSP e ao Usuário dos Dados com a lista de capacidade do usuário, com a chave pública do usuário e o Tíquete de Confiança. O CSP armazena os dados recebidos em uma tabela com as capacidades do usuário. Em seguida o CSP envia uma cópia assinada do Tíquete de Confiança para o Dono dos Dados e para o Usuário dos Dados, que também recebe a chave secreta K_O. Os casos de uso do mecanismo de geração são representados na Figura 2.

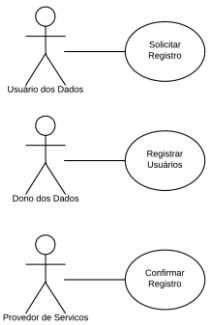

Figura 2. Geração do Tíquete de Confiança

A implantação do mecanismo começa quando o Usuário dos Dados tenta acessar os dados no CSP. Para isso, Usuário envia uma mensagem cifrada com o Tíquete de Confiança. O CSP decifra a mensagem e valida os atributos do Tíquete de Confiança e, caso sejam válidos, envia uma mensagem cifrada com os dados cifrados com a chave secreta K_O e o decifra. Caso contrário o CSP informa um erro ao Usuário dos Dados. Os casos de uso mecanismo de implantação do tíquete de confiança são representados na Figura 3.

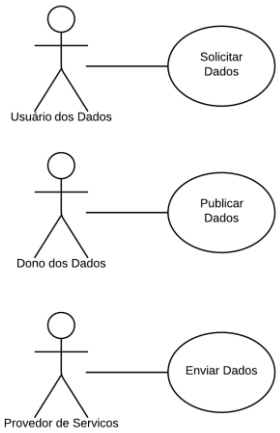

Figura 3. Implantação do Tíquete de Confiança

IV. PROJETO

Para implementar o mecanismo foi elaborada uma arquitetura prescritiva em linguagem orientada a objetos. A arquitetura atende as seguintes necessidades:

- O sistema deve ser capaz de criptografar a mensagem com criptografia de chave simétrica, de chave assimétrica e de assinar mensagens;
- O sistema deve ser distribuído.

Dessa forma, foram criados os módulos de Segurança, que atende a primeira necessidade, de Rede, que atende a segunda necessidade, e do Mecanismo, que implementa o mecanismo proposto. Esta arquitetura foi implementada usando a linguagem Java. Além disso, foi usada a plataforma VMWare ESXi para criar máquinas virtuais e simular o que aconteceria em uma nuvem, os aspectos de configuração e aplicação do sistema no ambiente de Nuvem são abordados na subseção 4.4, a seguir. Essa abordagem foi a mesma usada por [AHMED e XIANG 2011].

O módulo de Segurança é o responsável por prover mecanismos para cifrar, decifrar, assinar, verificar assinatura e geração de chaves de criptografia. Esse módulo é composto pela classe Segurança. A classe Segurança é a responsável por gerar as chaves e por cifrar, decifrar, assinar e verificar as assinaturas.

A figura 4 apresenta a classe de segurança desenvolvida no experimento prático.

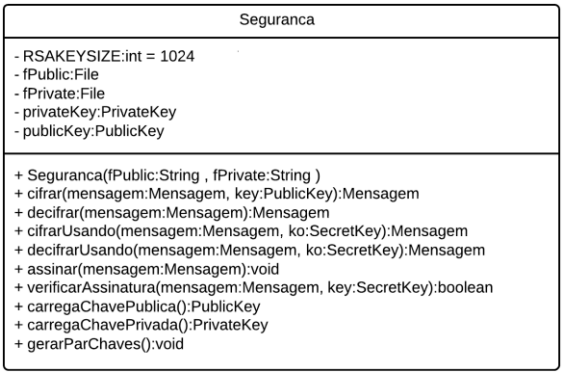

Figura 4. Classe Segurança

A. Rede

O módulo de Rede é o responsável por enviar as mensagens cifradas dos participantes do protocolo de Tíquete de Confiança pela rede. É composto pela classe Rede, pela classe Contato e pela classe Mensagem. A classe Rede é a responsável por enviar e receber mensagens. A classe Contato é a responsável por conhecer o IP e a porta do Usuário dos Dados, do Dono dos Dados e do Provedor de Serviços. Além disso, fornece método para distribuir as chaves públicas desses contatos. A classe Mensagem possui um corpo, onde pode ser inseridos os bytes de vários tipos de dados, um campo de assinatura, onde ficam os bytes de assinatura das mensagens assinadas e um campo para armazenar a chave simétrica para decifrar usada para cifrar a mensagem. A chave simétrica é cifrada com a chave pública do destino da mensagem. A figura 04 representa as classes de rede, de mensagem e de contato, que compõe o módulo de Rede. A figura 5 apresenta as classes Rede, Mensagem e Contato desenvolvidas.

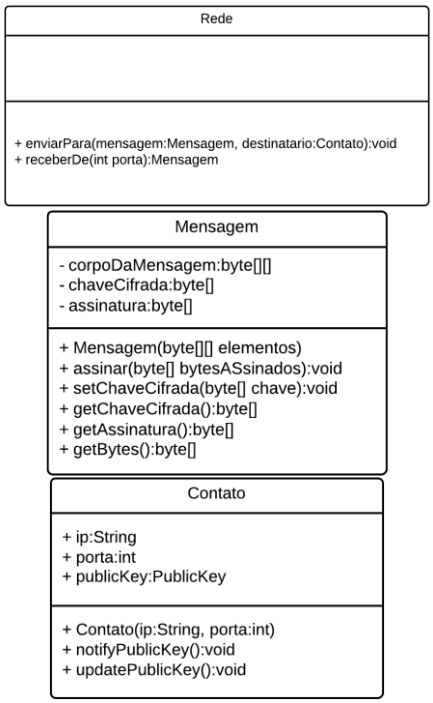

Figura 5. Classes Rede, Contato e Mensagem.

B. Mecanismo

O módulo do Mecanismo é composto por classes que representam o Dono dos Dados, o Usuário dos Dados e o Provedor de Serviços da Nuvem. Essas classes trocam mensagens usando os métodos disponibilizados pelos outros dois módulos. A figura 05 representa as classes que receberam as responsabilidades, atributos e métodos, para realizar este mecanismo, enquanto a figura 06 apresenta o fluxo de operações entre os atores do sistema.

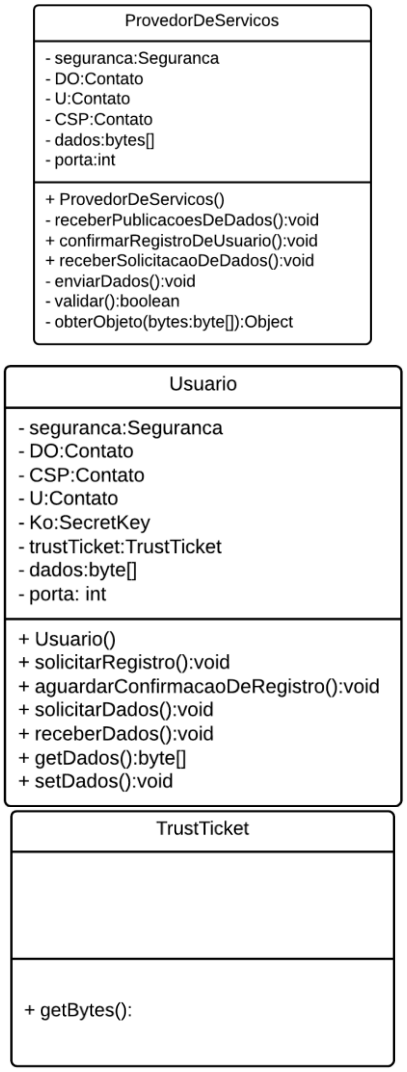

Figura 6. Classes DonoDosDados, Usuario, ProvedorDeServicos

A implementação do sistema de tíquetes foi feita usando a linguagem Java. A simulação da infraestrutura da nuvem será apresentada na seção 4.3 a seguir.

C. Implantação na Nuvem

Dentro do contexto da Nuvem, a implementação foi feita da seguinte maneira: foi instalado o *VMWare ESXi* v5.1 em uma máquina, e a administração das *VMs* foi feita através de

uma outra ferramenta, o *VMWare vSphere Client*, por onde as mesmas puderam ser instanciadas e seus recursos alocados (conforme apresentação das ferramentas na Seção 1 (Introdução).

Através do *VMWare vSphere Client* foram criadas duas *VMs*, uma delas simulando o ambiente do Provedor de Serviços e a outra o ambiente do Dono dos Dados. Não foi criada nenhuma máquina para usuário pelo fato de que o mesmo poderia se tratar de qualquer outro computador, como o caso de um dos notebooks usados para o desenvolvimento das atividades.

Ao se destinar uma VM para cada um dos "papéis" (Dono dos Dados e Provedor de Serviços), já era prevista a separação do Sistema de Tíquetes em módulos executáveis de maneira independente, desta maneira, seguindo o projeto apresentado na subseção 4.3 (Mecanismo). Importante destacar o grande papel das entidades "Rede" e "Contato", apresentadas na Figura 4 da subseção 4.2 (Rede). Estas entidades são as responsáveis por enviar as mensagens através da rede, seguindo o endereço de IP armazenado. Este IP será fixado de acordo com o endereço atribuído a cada VM instanciada e endereço do computador do Usuário.

V. CONCLUSÃO

A arquitetura proposta foi implementada de maneira satisfatória. Isto é, o mecanismo foi implementado atendendo as necessidades estipuladas. Entretanto, foi necessária um adaptação quando a cifragem das mensagens. No protocolo RSA, o tamanho da chave é proporcional ao tamanho da mensagem. Por isso, foi usada uma técnica que consiste em cifrar a mensagem com uma chave simétrica e cifrar essa chave com a chave pública do protocolo RSA.

Além disso, a implementação feita é a mínima necessária para observar o comportamento do mecanismo. Dessa forma, foi vislumbrada possibilidades de trabalhos futuros. Esses trabalhos podem seguir a linha de deixar a implementação e arquitetura atuais mais robustas e completas, como, por exemplo, o uso de threads. Outra sugestão de trabalho seria evoluir essa arquitetura para que pudesse ser aplicada em aplicações reais ao invés de apenas em simulações.

REFERÊNCIAS

[1] AHMED, M.; XIANG, Y. Trust ticket deployment: A notion of a data owner's trust in cloud computing. In: Proceedings of the 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. Washington, DC, USA: IEEE Computer Society, 2011. (TRUSTCOM '11), p. 111–117. ISBN 978-0-7695-4600-1.Disponível em: <http://dx.doi.org/10.1109/TrustCom.2011.17>

[2] P. Mell and T. Grance (2009), "The nist definition of cloud computing", National Institute of Standards and Technology.

[3] Vaquero, LM., L. Rodero-Merino, J. Caceres, and M. Lindner (2009). "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review 39, no. 1, pp. 50-55.

[4] H. Chang and E. Choi (2010), "Challenges and Security in Cloud Computing", Communication and Networking, pp. 214-217.

[5] Q. Zhang, L. Cheng, and R. Boutaba (2010), "Cloud computing: state-of-the-art and researchchallenges," Journal of Internet Services and Applications, vol. 1, pp. 7-18.

[6] S. Sanka, C. Hota, and M. Rajarajan (2010), "Secure data access in cloud computing", in IEEE 4th International conference on Internet Multimedia systems architectures and applications, IMSAA 2010 Bangalore, India, pp. 1-6.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, (2010) "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," IEEE INFOCOM 2010.

[8] VMWare. "VMware ESX e VMware ESXi: Os hypervisores líderes do mercado com produção comprovada". 2009. Disponível em <http://www.vmware.com/files/br/pdf/products/VMW_09Q1_BRO_ESX_ESXi_BR_A4_P6_R2.pd