

considerando um tempo de execução aceitável do processo, além de utilizar componentes acessíveis como a linguagem java que é largamente utilizada para o desenvolvimento de sistemas. Utilizou-se também uma infraestrutura de nuvem bem consolidada e acessível, que é o Microsoft Azure, que permite a criação e configuração de máquinas virtuais em poucos minutos.

A principal preocupação do trabalho foi o processo de emissão automático do certificado de atributo, pois sem esse requisito atendido o processo de autenticação e autorização para a nuvem não seria atendido plenamente de forma dinâmica, em razão pela qual a cada tentativa de acesso por parte do cliente seria necessária uma ação humana de execução para a emissão do certificado de atributo. Com o sistema de autorização criado essa ação não é necessária pois o processo de emissão é automatizado no provedor de autorização, viabilizando o modelo apresentado para a computação em nuvem.

Após a realização de todos os testes foi possível identificar que um trabalho futuro é a adaptação do modelo para possibilitar a utilização da infraestrutura criada por mais de um provedor de serviço. Essa alteração permitiria ao cliente a utilização do mesmo certificado digital para mais de um serviço. Sendo assim a emissão dos certificados de atributos ocorreria conforme a necessidade dos sistemas que o usuário necessitasse utilizar. Com a alteração sugerida o modelo poderá ser ainda mais apropriado para o cenário de nuvem, possibilitando a utilização do provedor de autorização para diversos provedores de serviço.

Referências

- Chapin, P. C., Skalka, C., and Wang, S. X. (2008). Authorization in trust management: Features and foundations. *ACM Comput. Surv.* 40, 3, Article 9, page 48.
- Farrell, S. and Housley (2002). An internet attribute certificate profile for authorization. RFC 3281.
- Fiorese, M. (2000). Uma proposta de autenticação de usuários para ensino a distância. Master's thesis, Programa de Pós-Graduação em Computação, Universidade Federal do Rio Grande do Sul.
- Housley, R., Polk, W., Ford, W., and Solo, D. (2002). Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. RFC 5280.
- Hwang, J.-J., Wu, K.-C., and Liu, D.-R. (2000). Access control with role attribute certificates. *Computer Standards and Interfaces*, 22:43–53.
- Junior, A. S. A. (2011). Gerenciamento de identidades como um serviço para ambiente de computação em nuvem. Master's thesis, Programa de Pós-Graduação em Ciência da Computação – Universidade Federal de Santa Catarina, Florianópolis.
- Kang, M.-H., Kim, K.-N., and Ryou, H.-B. (2003). An authorization mechanism for web services using an attribute certificate. *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on*, pages 144–150.
- Mell, P. and Grance, T. (2011). The nist definition of cloud computing.
- Nielsen, J. (1994). *Usability Engineering*. Academic Press.
- Thompson, M. R. and Essiari, A. (2003). Certificate-based authorization policy in a pki environment. *ACM Transactions on Information and System Security*, 6:566–588.