Cloud Computing/Cloud Storage Project Specification

1) List of team members.

   Krystal Carlton, Amir Koupaei, Cody Jenkins

2) The exact title of your project (it can be different than a corresponding project topic proposed by the instructor; it should take into account the exact scope of your project).

   Security Challenges in Cloud Computing

3) Introduction and motivation. Placement of the problem in the broader research area. Why is this project worth working on? Why is it original? Why is it practical?

   Why worth working on.

   - Increased interest for commercial and private enterprises
   - Attractive technology
   - There is a need to insure confidence in the security methods being used to secure data for a cloud's user community.

   Why it is original and practical.

   - As cloud computing evolves, encryption associated with it does as well leading to advances in the whole field
   - Understanding how cloud computing encryption works is fundamental to understanding how secure data is within the cloud
   - Knowing how encryption techniques are implemented within the various cloud computing platforms available separates theory from implementation

4) List of alternative solutions (protocols/algorithms/implementations) you are planning to explore.

   Propose to reverse engineer the process by investigating how the below vendors answer each of our proposed questions:

   Microsoft Azure
   NetApp
   IBM
   Google

5) Detailed description of problems/hypotheses you are planning to investigate.

Data stored within the cloud storage environment is no longer within the direct control of the user whose data it is. We plan to investigate how various vendors are currently providing cloud storage security, what schemes and implementations they are using and what vulnerabilities these implementations may have. To gather this information we will contact each vendor with a specific set of questions to gather technical information as needed to supplement research. Using this

information, we should be able to conclude what a user should require for confidence in a cloud storage system.

6) A tentative list of questions you will be seeking an answer to.
   a) Once data is moved to the cloud, how can a user be sure they are the only ones who can gain access?
      i) "Honest but curious" vendors
      ii) Intentional misuse by vendors
      iii) Attacks from hackers
   b) How are applications and services secure within the cloud, eg, when utilizing cloud computing to perform some function, whether it be editing a document or running a virtual server, how are these processes secured?
      i) During processing
      ii) During storage
      iii) During transportation
   c) What is the process to secure a user's data in cloud storage?
   d) How are cloud vendors handling key management for cloud customers?
   e) What is the standard for data at rest security?
      i) If there is no standard, what should a user require to have confidence in cloud storage security?
7) Procedure for verifying the results of your investigation.

   - Investigate what types of solutions companies offering cloud computing are utilizing and how
   - Investigate what vulnerabilities implemented solutions have and how, if at all, the vendor addresses it
   - Apply theory to practicality – ensure the vendor descriptions of security matches the theory and does not overstate
   - Develop a rating system for vendors for how well they implement confidentiality, integrity and authentication

8) Time schedule, including intermediate goals to be achieved by the dates of progress reports: Oct. 15-17, Nov. 5-7, Nov. 19-21.

   - By first progress report Oct 15-17
     - Should have a summary of security issues facing the cloud
     - Initial outline of security implementations by some vendors
   - By second progress report Nov 5-7
     - Comprehensive descriptions of security techniques/schemes implemented by vendors and how these work
     - Investigation of vulnerabilities these schemes may face
   - By third progress report Nov 19-21
     - Comparison of theoretical approaches with current cloud implementations
     - Beginning conclusions of what security standards users should look for

9) A list of possible areas, where the specification can change depending on the progress of the project.

- Access to vendor specific cloud information may not be publicly available and we may have to pare down the number of vendors we investigate
- Practical testing may be limited, which would require us to rely on academic publishing for our evaluation.

10) Tentative table of contents of your final report.

- Abstract
- Introduction
- What is a cloud
  - Software
  - Hardware
  - Services
- Security Issues Facing the cloud Environment
  - Intro
- Microsoft Azure
  - Access control
  - Data storage
  - Key Management
- IBM
  - Access control
  - Data storage
  - Key Management
- Google
  - Access control
  - Data storage
  - Key Management
- NetApp
  - Access control
  - Data storage
  - Key Management
- Proposed security standard
  - Vendor standards
  - Standards that provide user confidence
- Final Remarks

11)List of literature.

References

[1] H. Takabi, J. b. JosHi and G.-J. aHn, "Security and Privacy Chalenges in Cloud Computing Environments," *IEEE*

Security and Privacy Magazine, pp. 24 -31, 2010.

[2] D. Bender, "Privacy and Secuirty Issues in Cloud Computing," *The Computer & Internet Lawyer,* pp. 1-16, 2012.

[3] B. Weber, "www.infosecurity-magazine.com," 26 August 2013. [Online]. Available: http://www.infosecurity-magazine.com/view/12052/comment-securing-dataatrest-with-selfencrypting-drives/. [Accessed 24 09 2013].

[4] SecureAuth, "How to Use SAML SSO to Link Your Active Directory to the Cloud," SecureAuth Corporation, 2010.

[5] Cloud Security Alliance, "Security Guidance for Critical Areas of Cloud Computing v3," Cloud Security Alliance, 2011.

[6] S. K. S. L. Tim Mather, Cloud Security and Privacy, Sebastopol: O'Reilly Media, Inc., 2009.

[7] M. V. D. a. A. Juels, "On the impossibility of cryptography alone," in *USENIX conference on Hot topics in security*, 2010.

[8] S. Dara, "Cryptography Challenges for Computational Privacy," pp. 1-4, 2013.

[9] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing,* vol. 5, pp. 220-232, 2012.

[10] Y.-R. Chen, C.-K. Chu, W.-G. Tzeng and J. Zhou, "CloudHKA: A Cryptographic Approach for Hierarchical Access Control in Cloud Computing," in *11th International Conference on Applied Cryptography and Network Security*, 2013.

[11] K. Yang, Z. Liu, Z. Cao, X. Jia, D. S. Wong and K. Ren, "TAAC: Temporal Attribute-based Access Control," [Online]. Available: http://eprint.iacr.org/2012/651.pdf. [Accessed 28 September 2013].

[12] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," 02 July 2008. [Online]. Available: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853. [Accessed 5 October 2013].

[13] T. G. Peter Mell, "The NIST Definition of Cloud Computing," National Institue of Standards and Technology, Gaithersburg, 2011.

[14] National Institute of Standards and Technology, "Federal Information Processing Standards," U.S. Department of Commerce, [Online]. Available: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. [Accessed 5 October 2013].

[15] W. Ashford, "Six security issues to tackle before encrypting cloud data," 22 March 2013. [Online]. Available: http://www.computerweekly.com/news/2240180087/Six-security-issues-to-tackle-before-encrypting-cloud-data.

[16] J. Raghavi, "A Survey on Cloud Storage Systems and Encryption Schemes," *International Journal of Engineering and Technology,* vol. 5, no. 2, 2013.

[17] C. Evans, "Encryption techniques and products for hardware-based data storage security," September 2011. [Online]. Available: http://www.computerweekly.com/feature/Encryption-techniques-and-products-for-hardware-based-data-storage-security. [Accessed 24 September 2013].

[18] G. Parann-Nissany, "Securing Your 'Data at Rest' in the Cloud," 27 June 2012. [Online]. Available: http://www.porticor.com/2012/06/securing-cloud-data-ct/. [Accessed September 2013].

[19] V. Winkler, Securing the Cloud, Syngress, 2011.