Factors Influencing Adoption of Encryption to Secure Data in the Cloud

Kenneth E. Stavinoha

Cisco Systems, San Jose, California
kestavin@cisco.com

Abstract. This research measured factors that influence the adoption of encryption to secure data in the cloud and provided guidance on when encryption might be most appropriate. Additionally, the study investigated the important elements necessary to develop a framework for a secure cloud computing environment. The objective of this research was to provide normative guidance and empirical data that assists both cloud service providers and users of cloud technology in selecting the best mitigation, or suite of mitigations, that most effectively protect data in the cloud. This research helps to fill a gap by examining issues affecting cloud consumers, the elements that play a role in the decision to use a cloud service, and the influencing factors in the decision to use encryption to secure data in the cloud.

1 Introduction

As organizations contemplate the adoption of cloud computing, concerns regarding security and control over client data are being brought to the forefront, as are issues of responsibility between consumers and providers. An IDC (2008) survey and two Avanade (2009a, b) surveys found that while an increasing number of organizations are viewing cloud computing as a viable technology, the most prevalent factor inhibiting the adoption of cloud computing is security. A Ponemon (2011) survey of cloud service providers found that the vast majority did not view cloud security as their responsibility but instead pointed the finger at the cloud consumer. Furthermore, the providers did not perceive a competitive advantage over the competition in offering secure cloud solutions. Research performed by the Queen Mary University of London School of Law found that for a majority of off-the-shelf cloud services, the service contracts were typically written to absolve the cloud service provider of any responsibility for security failures, except where legislation dictated otherwise (Bradshaw, Millard, & Walden, 2011).

Three primary aspects covered in this study were concerns over the security of data in the cloud, the factors in the decision to adopt a new technology, and recommendations on the use of encryption to secure data. The literature has consistently shown that concerns over security, governance, and privacy rank highly in the minds of consumers when considering the use of cloud computing services (Avanade, 2009a; Avanade, 2009b; Blum & Krikken, 2009; CSA, 2009; Chichester, 2009; Chow et al.,

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 357–365, 2013.

2009; ENISA, 2009; Fischmann, 2008; Forsheit, 2009; Kaufman, 2009; Mowbray & Pearson, 2009). Research by Dynes, Brechbuhl, and Johnson (2005), Fichman (1992), and Johnson and Goetz (2007) and suggests that the decision to adopt a technology – particularly information security – is a complex process and that information technology (IT) and information assurance (IA) professionals were most often relied upon for their expertise when organizations considered adopting new IT tools and/or technologies. Finally, encryption is a frequently recommended solution for protecting data as found in standards, guidance, and legislation (21 CMR 17.00, 2010; CSA, 2010; ENISA, 2009; HIPAA HHS, 2006; ISO/IEC 27002, 2005; McCallister et al., 2010; NRS 603A, 2010; PCI DSS, 2009).

However, there are practical limits to encryption as a "cure-all" solution for securing data. As cited by CSA "encryption itself does not necessarily prevent data loss" (CSA, 2009, p.60) because there are vulnerabilities – such as weak authentication – and failures of process – such as poor key management – which can adversely affect the security which encryption is meant to provide. If the cloud service provider performs the encryption and key management (CSA, 2009; Blum & Krikken, 2010; ENISA, 2009), this may weaken protection of the data because a third party has control over, and potentially access to, the data (Couillard, 2010; Gellman, 2009). There is also the challenge of encrypting data at rest versus data in transit which are typically separate actions requiring different sets of encryption keys, additional key management, and separate processing. The largest gap in cryptography is the inability to effectively and efficiently maintain encryption on data in use. Homomorphic encryption – which could enable some processing of data while it remains encrypted - is being offered as a potential solution (Chow et. al, 2009; Fischmann, 2008; Lauter, Naehrig, & Vaikuntanathan, 2011; Naone, 2011), but it will require further research and testing, which may take many years, to bring homomorphic encryption into play as a realistic business solution (Blum & Krikken, 2009; ENISA, 2009; Schneier, 2009).

2 Experiments

Based on research by Dynes, Brechbuhl and Johnson, (2005), Fichman (1992), Johnson and Goetz (2007), and prior willingness to adopt technology research by Cole (2008), Comings (2008), Lease (2005), Ting (2008), and Turek, (2011), it was deemed relevant to solicit the perceptions of IT/IA professionals on their willingness to adopt encryption to secure data in the cloud. The four independent variables for this research - security effectiveness, organizational need, reliability, and cost-effectiveness – have been identified by a number of researchers as factors in the decision to adopt a technology (Ettlie, 2006; Lease, 2005; Roberts & Pick, 2004; Soliman & Janz, 2004; Tobin & Bidoli, 2006; VarShney et al., 2002) and yielded the four research questions posed in this study:

Question 1: Is an IT/IA professional's willingness to adopt encryption to secure data in the cloud dependent on his/her perception of its security effectiveness?

Question 2: Is an IT/IA professional's willingness to adopt encryption to secure data in the cloud dependent on his/her perceived need for security technologies?

Question 3: Is an IT/IA professional's willingness to adopt encryption to secure data in the cloud dependent on his/her perception of its reliability?

Question 4: Is an IT/IA professional's willingness to adopt encryption to secure data in the cloud dependent on his/her perception of its cost effectiveness?

To measure the dependent variable – willingness to adopt encryption to secure data in the cloud – participants were asked about their willingness to adopt encryption and if they believed that encryption uses proven technology. To measure security effectiveness, participants were asked if they would adopt encryption to secure data in the cloud and consider that the use of encryption is secure, if they considered encryption more secure than other data protection methods, whether they had concerns about the technology of encryption, and if they were willing to adopt encryption to secure data in the cloud. For the measurement of organizational need, participants were asked if they perceived that their organization needed to improve the security of its IT assets in the cloud, if they perceived that their organization needed encryption to secure its IT assets in the cloud, and if they perceived that encryption of data in the cloud provided significant benefit to their organization. To measure reliability, participants were asked if they perceived encryption to be reliable, and if they perceived it to be more reliable than other IT security methods. Cost effectiveness was measured by asking respondents if they perceived encryption to provide a good value for the cost, if they perceived that maintenance costs for encryption were lower than other IT security methods, and if they perceived that encryption offered cost savings as compared to other IT security methods.

3 Results

In the hypothesis testing, it was shown that all four of the hypotheses were supported via analysis of the Chi-Square Test for Independence. IT/IA professionals' willingness to adopt encryption to secure data in the cloud is dependent on their perception of its security effectiveness, reliability, cost effectiveness, and the needs of their organizations. The results in this study align with those of previous researchers and guidance in the literature in noting the influence of these four independent variables in the decision to adopt a security technology.

Once it was established that there was a relationship between the dependent variable and each of the independent variables, further statistical analysis was performed to evaluate the strength of those relationships. Pearson's Product Moment Correlation showed that the strongest relationships between dependent and independent variables were, in descending order, security effectiveness ($r = .563$), organizational need ($r = .453$), cost effectiveness ($r = .333$), and reliability ($r = .324$). All of these relationships were statistically significant ($n = 172$, $p = .001$).

Table 1. Pearson Correlation for Dependent and Independent Variables

		Dependent Variable	Need	Reliable	Cost	Security
DV	Pearson Correlation	1	.453**	.324**	.333**	.563**
	Sig (2 tailed)		.000	000	.000	.000
	N	172	172	172	172	.172
N	Pearson Correlation	.453**	1	.087	.356**	.236**
	Sig (2 tailed)	.000		.259	.000	.002
	N	172	172	172	172	172
R	Pearson Correlation	.324**	.087	1	.215**	.392**
	Sig (2 tailed)	.000	.259		.005	.000
	N	172	172	172	172	172
C	Pearson Correlation	.333**	.356**	.215**	1	.268**
	Sig (2 tailed)	.000	.000	.005		.000
	N	172	172	172	172	172
S	Pearson Correlation	.563**	.236	.392**	.268**	1
	Sig (2 tailed)	.000	.002	.000	000	
	N	172	172	172	172	172

** Correlation is significant at the 0.01 level (2-tailed).

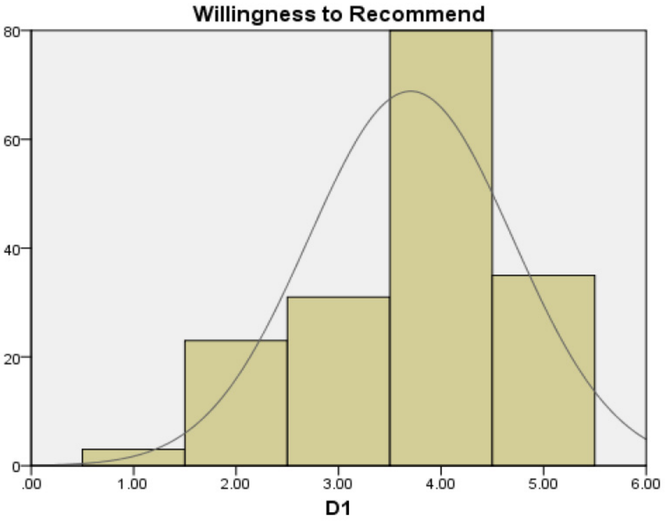

Fig. 1. Histogram: Willingness to Recommend Encryption

While the survey focused on IT/IA professionals, 31.4% of participants identified themselves as being in an IT/IA management role. The results of additional statistical analysis showed that the perceptions of the management respondents the adoption of encryption to secure data in the cloud were largely similar to those of the entire sample population. For this study, the alignment of perceptions for IT/IA management and IT/IA professionals reflects results in the research of Dynes, Brechbuhl, and Johnson (2005) in that IT/IA management often relies on the advice of IT/IA professionals when considering the adoption of security technology.

3.1 Alternatives to Encryption

One item in the survey asked respondents to choose a course of action if encryption was not available as an option to secure data in the cloud. The vast majority of respondents (56.4%) indicated that they would not use a cloud service for this data if encryption was not an option to protect it, while the next highest percentage of respondents (26.4%) replied that access controls would be relied upon if encryption were not available. Only 9.2% of respondents felt that anonymization of the data was a suitable choice if encryption were not available and the lowest number of respondents (8%) felt that relying on the contract with the cloud provider to protect the data was an acceptable option.

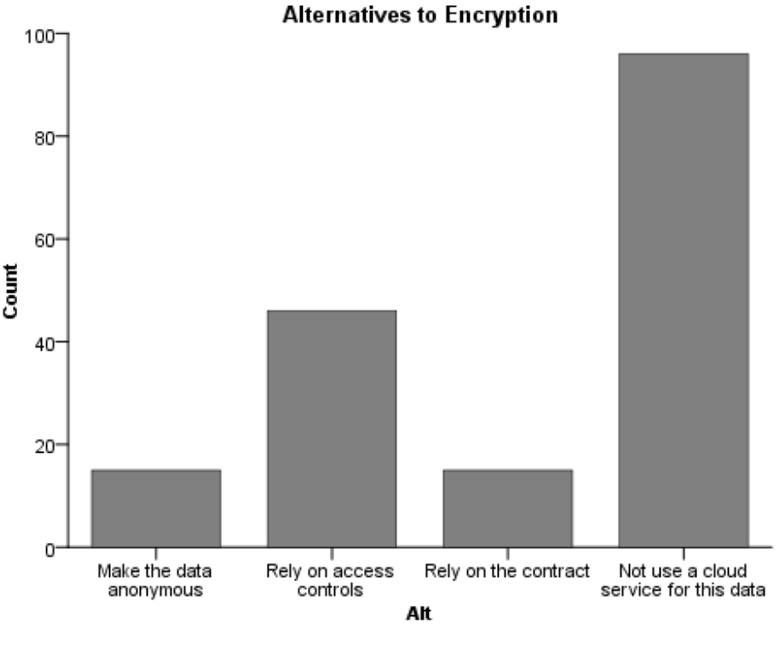

Fig. 2. Survey results for encryption alternatives query

The management subset was even more adamant: 62.96% chose not to use a cloud service for data if encryption was not an option. Only 3.7% of the management respondents chose to use anonymization as an option, and the percentages for the other two options were largely similar to those stated above.

4 Conclusions

The information provided in this research is valuable to both those considering using a cloud service as well as those developing and/or providing cloud services. The results of this research align with earlier studies cited heretofore in that, clearly, users of cloud services feel a strong need to protect their data. Encryption is an often-recommended solution which IT/IA professionals have years of experience in, and a large percentage of those professionals prefer not to use a cloud service if encryption is not an option to protect their data. This need becomes a critical factor in the decision to utilize one cloud offering versus another and it benefits both cloud consumer and provider if encryption is an option.

Implications for practitioners are clear – users of cloud services expect that there will be reasonable options for securing their data. Cloud service providers that feel security is not an important factor in the decision to use a cloud service, or believe that it is not beholden on the cloud service provider (CSP) to provide reasonable data security options, will discover that services lacking this desired feature are less attractive to consumers. While such providers may be able to enjoy some measure of success in these relatively early days of cloud computing with a "caveat emptor" mentality, the law of diminishing returns will likely come into play as more mature service offerings evolve along with an increased willingness by providers to share risks with cloud consumers.

Cloud consumers must educate themselves on the risks and rewards of various service offerings, and solicit the advice of subject matter experts on legal, regulatory, security, privacy, and governance issues prior to serious consideration of using a cloud service to create, store, process, or transfer data. While data owners can outsource some of the responsibility for protecting their data, they cannot effectively outsource the liability for any failure. The penalties of fines, sanctions, regulatory actions, and possible litigation, along with the negative financial impact of damaged reputation and brand, can easily render insignificant the proposed cost savings of a cloud service. The term service level agreement (SLA) has become a buzzword to the point that it seems to be the solution for everything cloud, and therefore consumers must understand well the intended purpose of such agreements and the limitations in scope and remedy provided by them.

In the most idealistic sense, a major premise of the cloud is that the consumer "pays no attention to that man behind the curtain" and signs a contract with a provider who appears to provide the entire solution as stated in the sales literature. However, the cloud service provider will likely have dependencies on other providers (storage, network, application, processing, etc.) – none of which are necessarily contractually obligated directly back to the consumer. Further, these dependencies may change frequently and suddenly without the knowledge of the consumer – especially when cloud service providers are trying to meet elasticity requirements - and it can become a challenge for the consumer to know where their data is and how/if it is being appropriately protected. This daisy chain of trust may well pose risks over which the cloud consumer has no direct legal remedy, and the contract with the provider may not afford such. Increased levels of due diligence and due care are required by policy makers to ensure that cloud service agreements sufficiently identify and address all pertinent risks to the organization, that responsibilities are clearly delineated among all parties, and that remedies are explicitly understood in the case of performance failure and/or breach of contract.

Any organization contemplating using a cloud service should perform thorough due diligence around sensitivity of their data, vulnerabilities of the environment, reputation of the cloud service provider(s), and terms of the contract. While benefits of cloud computing in terms of efficiencies, flexibility, productivity, and cost savings have been shown both in empirical research and more frequently in white papers and case studies, not all of these benefits can be generalized across the vast spectrum of cloud services, infrastructures, and platforms to provide useful data for comparison and study. Hopefully, in the longer term, cloud standards, taxonomies, and ontologies will provide the foundation for a clear understanding of the risks and rewards of cloud computing which transcend current boundaries. In the current environment and for the near future, cloud consumers should entrust their data only to those providers whose platforms and services clearly meet the needs of their organization and do not introduce unacceptable levels of risk.

References

1. Avanade (January 2009a) global survey of cloud computing. Retrieved from the Avanade website:
   `http://avanade.dk/_uploaded/pdf/avanadethoughtleadershipcloudsurveyexecutivesummary833173.pdf`
2. Avanade (September 2009b) global survey of cloud computing. Retrieved from the Avanade website:
   `http://www.avanade.com/Documents/Research%20and%20Insights/fy10cloudcomputingexecutivesummaryfinal314006.pdf`
3. Blum, D., Krikken, R.: Using encryption to protect sensitive data in cloud computing environments (2010), Retrieved from The Burton Group website:
   `http://www.burtongroup.com/Client/Research/Document.aspx?cid=1904&contentView=FullContent`
4. Bradshaw, S., Millard, C., Walden, I.: Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. Information Journal of Law and Information Technology 19, 187–223 (2011), doi:10.1093/ijlit
5. Cloud Security Alliance (CSA), Security guidance for critical areas of focus in cloud computing v2.1. (2009) Retrieved from Cloud Security Alliance website:
   `http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf`

6. Chichester, R.: Litigating on the clouds. Retrieved from the Texas Bar CLE Online Library (2009), http://www.texasbarcle.com/CLE/OLSearchResults.asp?ViewProgram=25231&searchtype=VA&sCalledFrom=OLSEARCH.ASP&FreeOnly=
7. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling data in the cloud: Outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009), pp. 85–90. ACM, Chicago (November 13, 2009), doi:10.1145/1655008.1655020
8. Cole, S.: Adopting Biometrics: factors that influence decision-making managers (unpublished doctoral dissertation). University of Fairfax, Vienna, Virginia (2008)
9. Comings, D.: Factors influencing the development of COTS information security products that meet federal requirements for national security systems (unpublished doctoral dissertation). University of Fairfax, Vienna, Virginia (2008)
10. Couillard, D.: Defogging the cloud: Applying fourth amendment principles to evolving privacy expectations in cloud computing. Minnesota Law Review 93, 2205–2239 (2010), http://ssrn.com/abstract=1832982 (retrieved)
11. Dynes, S., Brechbuhl, H., Johnson, M.E.: Information security in the extended enterprise: Some initial results from a field study of an industrial firm (Working Paper Series 05-1). Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth. (2005), http://www.tuck.dartmouth.edu/cds-uploads/publications/pdf/Paper_InfoSecurityExtended.pdf (retrieved)
12. Ettlie, J.: Managing innovation. Elsevier Butterworth-Heinemann, Burlington (2006)
13. European Network and Information Security Agency (ENISA), Cloud computing: Benefits, risks and recommendations for information security. Retrieved ENISA website (2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
14. Fichman, R.: Information technology diffusion: A review of empirical research. In: DeGross, J.I., Becker, J.D., Elam, J.J. (eds.) Proceedings of the Thirteenth International Conference on Information Systems, ICIS 1992, pp. 195–206 (1992)
15. Fischmann, M.: Data confidentiality and reputation schemes in distributed information systems, Humboldt University, Berlin, Germany. Doctoral thesis (2008), http://edoc.hu-berlin.de/dissertationen/fischmann-matthias-2008-05-23/PDF/fischmann.pdf (retrieved)
16. Forsheit, T.: Legal implications of cloud computing – part four (2009), Retrieved from the Information Law Group web site: http://www.infolawgroup.com/2009/11/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-four-ediscovery-and-digital-evidence/
17. Department of Health and Human Services (HHS), Health insurance portability and accountability act (HIPAA) administration simplification. Regulation Text 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through February 16 2006, Retrieved from the HHS website (2006), http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
18. International Standards Organization/International Electrotechnical Commission (ISO/IEC), Information technology - Security techniques - Code of practice for information security management. ISO/IEC, Geneva (2005)

19. Johnson, M., Goetz, E.: Embedding information security into the organization. IEEE Security and Privacy 5(3), 16–24 (2007), doi:10.1109/MSP.2007.59
20. Kaufman, L.: Data security in the world of cloud computing. IEEE Security and Privacy 7(4), 61–64 (2009), doi:10.1109/MSP.2009.87
21. Lauter, K., Naehrig, M., Vaikuntanathan, V.: Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, CCSW 2011. ACM, New York (2011), http://dx.doi.org/10.1145/2046660.2046682
22. Lease, D.: Factors influencing the adoption of biometric security technologies by decision making information technology and security managers (2005), http://drdavidlease.com/uploads/David_Lease_UMI_Dissertation.pdf (retrieved)
23. Mass. Gen. Laws § 17 Standards for the Protection of Personal Information. 201 CMR 17.00
24. McCallister, E., Grance, T., Scarfone, A.: Guide to protecting the confidentiality of personally identifiable information. Retrieved from the National Institute of Standards and Technology (NIST) website (2010), http://www.nist.gov/manuscript-publication-search.cfm?pub_id=904990
25. Mowbray, M., Pearson, S.: A client-based privacy manager for cloud computing. In: Proceedings of the Fourth International ICST Conference on Communication System Software and Middleware, pp. 1–8. ACM, New York (2009), doi:10.1145/1621890.1621897
26. Naone, E.: Homomorphic encryption. Technology Review (May/June 2011), http://www.technologyreview.com/computing/37197/ (retrieved)
27. Nevada Gen. Laws NRS 603A: Security of Personal Information (2010)
28. Payment Card Industry, PCI, Data security standard requirements and assessment procedures v1.2.1. (2009) Retrieved from the PCI website: https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html
29. Ponemon Institute, Security of cloud computing providers study (2011), Retrieved from the Computer Associates website: http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf
30. Roberts, G., Pick, J.: Technology factors in corporate adoption of mobile cell phones: A case study analysis. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS 2004 - Track 9) (2004), doi:10.1109/HICSS.2004.1265678
31. Soliman, K., Janz, B.: Interorganizational information systems: Exploring an internet-based approach. Information and Management 41, 697–706 (2004), http://dx.doi.org/10.1016/j.im.2003.06.001
32. Ting, W.: Factors influencing the adoption of enterprise wide information security metrics by decision making managers (unpublished doctoral dissertation), University of Fairfax, Vienna, Virginia (2008)
33. Tobin, P.K.J., Bidoli, M.: Factors Affecting the Adoption of Voice over Internet Protocol (VoIP) and other Converged IP services in South Africa. South African Journal of Business Management 37(1), 31–40 (2006)
34. Turek, J.: Factors That Influence Security Executives to Recommend Unified Threat Management (unpublished doctoral dissertation), University of Fairfax, Vienna, Virginia (2011)
35. VarShney, U., Snow, A., McGivern, M., Howard, C.: Voice Over IP. Communications of the ACM 45(1), 89–95 (2002), doi:10.1145/502269.502271