iJET EXPLORE International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 5, May, 2012

Maintaining Payment Card Industry (PCI) Compliance in the Cloud

Nigel McKelvey, Kevin Curran[1]
Computing Department, Letterkenny Institute of Technology, Port Road, Letterkenny, Co Donegal, Ireland.
[1]School of Computing and Intelligent Systems, University of Ulster, Derry, Northern Ireland

ABSTRACT

Protecting privacy is a major concern of people using the internet. Purchasing items online inevitably builds up profiles within databases. Ensuring that this data remains protected is vital if society is to continue to trust electronic avenues of purchasing. Having credit card information leaked or hacked is of serious concern. PCI Compliance attempts to protect individual users from such situations. With Cloud architectures still relatively new, can customers still be guaranteed protection? This paper will endeavour to research this area and determine if procedures exist in the Cloud that can adhere to and implement PCI Compliance adequately. The PCI standard is primarily concerned with protecting the details of a credit card, which while perfectly acceptable, it does not take into consideration any other factors. Therefore, if the compliance is to be maintained in a Cloud environment where other vulnerabilities exist, can it still be successful? This essay will explore these questions and provide some insights.

Keywords: *PCI-Compliance, SecaaS, Cloud, Security*

1. INTRODUCTION

In order to be PCI-compliant, attempting to structure the Cloud so that credit card payments are made external to the Cloud might go some way to alleviating the potential risks involved. According to the PCI standard, compromised data could negatively affect consumers as well as merchants. It argues that just a single incident regarding a credit card could be very damaging to the reputation of the company involved. It also stipulates that account data breaches could potentially lead to loss of sales, lawsuits, insurance claims, cancelled accounts, payment card issuer fines and Government fines (PCI SSC). The purpose of the PCI standard is to protect cardholder data and the environment or network that the data itself is stored (PCI-CCRA, 2011). The primary problem with this approach is that technologies are constantly evolving. The cloud architecture for example is a prime example of how a relatively modern approach to networking could have significant impact on how PCI Compliance is administered.

A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualised computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumer (Buyya et al., 2008).

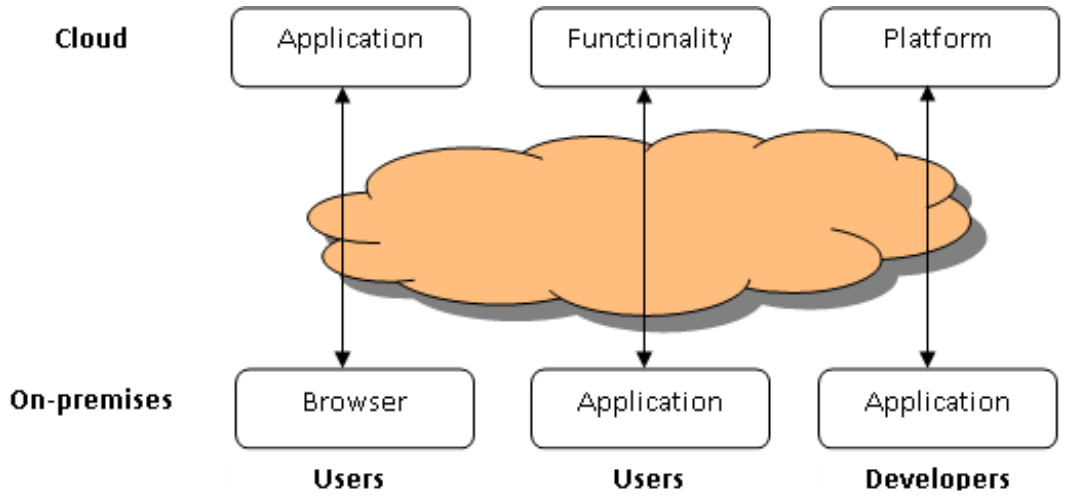

Figure 1: Cloud separated into three general areas (Chappell, 2008)

Cloud computing has been around since the eighties, yet it has recently become a topic of great debate in the market. The last number of years has seen a steady rise in the number of companies adopting the service. Cloud offers various advantages to companies, in particular to small and medium enterprises (SMEs) who are attracted to the cost saving and flexibility that Cloud has to offer. On the other hand, many companies have raised concerns about the security issues that cloud also presents and are apprehensive about moving their data to the Cloud.

2. THE CLOUD

"*Computing may someday be organized as a public utility just as the telephone system is a public utility*" (Garfinkel, 2011). In 1961, John McCarthy made that remark during a speech at the MIT centennial celebration. The idea has been around for some time now, but has only been embraced by industry in the last number of years. Cloud computing has generated a lot of attention and the number of enterprises adopting the cloud is steadily growing. The definition of cloud computing is unclear due to its current evolutionary state. Currently, the National Institute of Standards and Technology (NIST) are widely believed to have the correct definition of cloud computing. They define the cloud as "a model for convenient access to a shared pool of computer resources that can be easily released when needed" (Mell, 2011).

Cloud computing is an on demand service that provides resources, software and information through the internet (Engle, 2011). It allows the client to use the providers' servers and databases when they need it. Cloud computing inherits the security risks that the internet presents. The very nature of what the cloud is, computing over the internet, is one of its biggest vulnerabilities (Rosenbaum, 2011). Cloud security is essentially the same as security in any other IT environment. Yet the various technologies used to provide the service, coupled with the architecture, presents new security issues to the enterprises that are difficult to resolve (CSA, 2011). It is easy for any company to paper over the risks with the cost saving benefits that cloud has to offer, as well as the flexibility of the on demand service. For some, in particular those who handle sensitive consumer data, the vulnerability of the cloud overshadows it capabilities. The security issues in cloud computing can be traced back to two main areas; the internet and the cloud provider.

The client has no control once their data leaves the house. They can not control the cloud provider, unless of course it is their own private cloud or perhaps a community cloud that offers some control or access. Nevertheless, regardless of who governs the cloud, it is certain that neither the client nor the provider can control the internet. The internet is a playground full of hackers waiting to expose any security flaws that they encounter. The vulnerabilities of the cloud should not deter from the capabilities. The cloud can provide so much storage and processing power company; more so, it is provided easily and affordable. Cloud computing comes in three main forms, known as service models. Each model offers a suitable service that can be very beneficial depending on what the company requires.

- Infrastructure as a Service (IaaS): Provide the consumer with computer resources such as storage and processing.

- Platform as a Service (PaaS): Provide the consumer with a platform that they can deploy onto using programming languages provided by the cloud supplier.

- Software as a Service (SaaS): Provides the consumer with software they can use without the need of installing it on their machines.

3. CLOUD IMPLEMENTATIONS

In a private cloud, the provider and consumer are within the one enterprise. It is deployed and controlled from a private enterprise. Deploying a private cloud offers the reassurance of control, leaving the security and compliance in the hands of the company. It also relaxes any concern over privacy, as the cloud is in house and does not leave the company. It can be argued that the creation of a private cloud defeats the purpose of using the cloud. Surely the purpose of cloud computing is to offer flexible computing as a cost saving service. If the company needs more space, then they will require more servers. If they get more servers as backup, how much will it cost the company to have so many servers sitting in stand by? Creating a private cloud would also cost the company time and money to set up the servers and implement the cloud, before they install and maintain industry standard security to protect it (Claybrook, 2010). There is often a common misconception that private clouds are more secure, purely because it is on a private network. This is not entire true, as nearly all private networks are connected with a public network (Till, 2011). This is not to dismiss the use of private clouds. It also offers advantages as well. Private clouds avoid the dangers that cloud providers present and the cost of renting on a pay as you use service. For a large company that is dispersed, a private cloud would offer advantages. The United States government have started using a private cloud as a cost saving method to information sharing and application processing (Paquette S et al., 2010). If a company can create a private cloud with that can match the security of any leading cloud provider, then certainly a

private cloud can work. If not, then a public cloud may be the solution.

Public clouds provide multiple customers with computer resources. Customers use this service as a pay as you go, only spending what they use. This can save a company a lot of money, which is probably the main reason why many businesses are considering the move to the cloud. The software artefact for this thesis will be hosted on a public cloud. The public cloud offers the most flexible and cost saving service, along with other essential characteristics. Public clouds are the most common cloud that is used by enterprises and the software artefact aims to use this type of cloud to present security issues to any enterprise using or considering adopting a cloud from a public provider. The PCI Standard requires that a process and a mechanism are provided to allow for "timely forensic investigation in the event of a compromise to any other client or the provider itself" (Cox, 2010). Are cloud providers currently in a position to meet this requirement? There is no option with PCI-Compliance for risk acceptance and 100% compliance is required, therefore it could be argued that compliance with certain cloud deployments (such as a public cloud) are not possible. (Cox, 2010)

4. SECURITY IN THE CLOUD

Security as a Service (SecaaS) is an emerging service that many leading anti virus companies are developing. SecaaS is simply providing security management as a service. This is done by providing security applications such as anti virus as a service over the internet. Companies such as McAfee and Symantec have started to provide SecaaS (Sec, 2011). What these companies have done is a true example of what the cloud can do. They have turned the clouds main vulnerability into a capability. The adoption of SecaaS has also been met with uncertainty by consumers. The CSA have released a white paper that identifies what SecaaS is and the various different categories that fall under SecaaS, such as email security and web security (Sec, 2011). The idea of providing security through the cloud is new, but certainly it could potentially become synonymous with cloud. Companies adopt the cloud to save on storage costs. When you consider security is another cost that companies would look at reducing the cost in. If SecaaS can establish itself as a secure service, then it would obviously become a leading service model.

5. PCI-COMPLIANCE AND SECURITY

82% of IT professionals believe the need for cloud-specific security standards is an urgent requirement. Cloud provider Terremark advises that customers can locate PCI-compliant systems on its hosting service, though it does not promise that explicitly with its Enterprise Cloud. That does not imply that security is not present, merely that an undefined specification is impossible to satisfy (Fogarty, 2010). PCI neglects many aspects of the cloud which makes the mandatory adhering to PCI standards (the case for many businesses) a risky business. The PCI standard is updated every two to three years which is a mini-lifetime in computing terms (Greene, 2010). The evolution of technology in recent years has been exponential and businesses may find themselves faced with increased costs in dealing with modern security vulnerabilities while still being bound to adhering to the PCI standard which might have found itself behind schedule in technological terms at least. The following is a list which details some of the rules that an organisation must abide by in order to maintain their PCI-compliance:

- Build and maintain a secure network: This includes firewall installation and a secure password policy.
- Protect the cardholder's personal data: This entails implementing data encryption across any public network.
- Maintain a network vulnerability management program: This includes regular updates to anti-virus software and other security software applications.
- Implement strong access control measures: This requires a unique ID assignment for each employee with network access.
- Regularly monitor and test networks: This means monitoring and keeping track of all access to cardholder data.
- Maintain an Information Security policy: Basically, this means adhering to all of the above, and documenting the policy as part of IT standard operating procedures. (PCCD, 2007)

If implementing the PCI standard completely, adhering to it and maintaining it are working well for an organisation – then what happens if that organisation is using services in a cloud that gets hacked? Who takes the financial burden of the attack? The organisation themselves? The cloud providers? The service providers? Technically, if an organisation is adhering to the PCI-Standard and an attack takes place, then they are not financially responsible (PCIC, 2011). A scenario such as this can give some indication as to the potential issues that exist with PCI-Compliance and a Cloud environment. Visa fined non-compliant merchants $4.6 million in 2006 and $3.4 million in 2005 (Harman, 2008). With such fines in place, the pressure to conform to the standard is increased.

The premise of PCI is certainly valid, but its approach has not changed with the emergence of the cloud – which is the primary cause for concern.

There is no direct contractual relationship between merchants and payment card companies, therefore, merchants cannot be directly required to legally adhere to Security Programs or the PCI Standard by payment card companies. Similarly there is no direct duty for service providers to comply with PCI or Security Programs and finally, a merchant compliance with PCI is directly dependent on contractual obligations imposed on its Service Providers (Navetta, 2008). This begs the question of what happens when you have two merchants sharing cloud resources, one adhering to the PCI standard and one not? This is assuming that PCI-Compliance is not considered to be a legal requirement. Cloud paradigms also assume that organisations/individuals accessing the cloud could be from anywhere in the world. Laws differ from country to country, therefore prosecuting someone under PCI regulations could prove problematic.

6. CONCLUSION

The issue of security is a major part of the cloud. Any company considering the cloud must understand the various risks involved and the issues surrounding its protection. The companies are handing over their data without the responsibility associated. As a result clients are given little protection and until a standardisation enforces better protection, it is up to the client to cover themselves. If PCI-Compliance is something that an organisation must adhere to, then cloud providers will need to re-adapt accordingly or perhaps PCI Standards need to adapt to the cloud.

REFERENCES

[1] Baker, S. (2007). Google and the wisdom of the clouds. http://www.msnbc.msn.com/id/22261846/

[2] Chappell, D. (2008). A Short Introduction to Cloud Platforms. An enterprise-Oriented View. http://www.davidchappell.com/CloudPlatforms--Chappell.pdf

[3] Claybrook, B. (2010). The Bumpy Road to Private Clouds. Computer World, pages 18–23.

[4] Cox, P. (2010). Is PCI compliance attainable in a public cloud? http://searchcloudcomputing.techtarget.com/tip/Is-PCI-compliance-attainable-in-a-public-cloud

[5] CSA, (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Technical report, Cloud Security Alliance.

[6] Engle, P. (2011). An Improving Cloud. Industrial Engineer: IE, page 20. ISSN: 1542894X.

[7] Greene, T. (2010). What's Wrong with the PCI Security Standard. http://www.cio.com/article/592279/What_s_Wrong_with_the_PCI_Security_Standard?page=2&taxonomyId=3089

[8] Fogarty, K. (2010). Cloud Computing: Would PCI Compliance Help or Hurt Security? http://www.networkworld.com/news/2010/061010-cloud-computing-would-pci-compliance.html

[9] Garfinkel, S L, (2011). The Cloud Imperative. MIT. http://m.technologyreview.com/business/38710/

[10] Harman, B. (2008). PCI Compliance Can Make Your Organization Stronger and Fitter. NETPRO. http://isacahouston.org/documents/NetPro_ISACA-HOU_PCI_Aug08_vFinal.pdf

[11] Mell, P. (2011). The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. ISSN:10476210. (Accessed online 19th February 2012).

[12] Navetta, D. (2008). The Legal Implications, Risks and Problems of the PCI Data Security Standard. InfoSec Compliance.www.secureretailpayments.com/resources/The_Legal_Implications_of_PCI(FINAL).doc

[13] Paquette, S. (2010). Paul T. Jaeger, and Susan C. Wilson. Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly, pages 245–253.

[14] PCCD (2007). Protecting Credit Card Data: How to Achieve PCI Compliance. White Paper. http://www.motorola.com/web/Business/_Documents/static%20files/PCI_New.pdf

[15] PCIC (2011). PCI Compliance. What Changes are there to the PCI Standards in 2010? http://www.pcicompliancesaq.com/What_Changes_are_there_to_the_PCI_Standards_in_2010

[16] PCI-CCRA (2011). PCI-Compliant Cloud Reference Architecture.http://img.en25.com/Web/SAVVIS/CORP- Whitepaper PCICompliantCloudArchitecture2.PDF

[17] PCI SSC. PCI Security Standards Council. *Why Comply with PCI Security Standards?* https://www.pcisecuritystandards.org/security_standards/why_comply.php

[18] Buyya, R. (2008). Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. *10th IEEE Int. Conference on High Performance Computing and Communications*.http://arxiv.org/ftp/arxiv/papers/0808 /0808.3558.pdf

[19] Rosenbaum, D. (2011). Cloud Control. CFO, pages 31–34.

[20] SEC (2011). Defined Categories Of Service. White paper, Cloud Security Alliance. https://cloudsecurityalliance.org/wp-content/uploads /2011/09/SecaaS_V1_0.pdf

[21] Till, S. (2011). The Cloud: Secure Enough for Security. SDM: Security Distributing & Marketing, pages 107–110.