# PCI DSS Compliance Validation of Different Levels of Merchants in a Multi-tenant Private Cloud

Peter Olajide, Pavol Zavarsky, Ron Ruhl, Dale Lindskog
Information Systems Security Department
Concordia University College of Alberta, Edmonton, Canada
polajide@student.concordia.ab.ca, {pavol.zavarsky,ron.ruhl,dale.lindskog}@concordia.ab.ca

Abstract — **Payment Card Industry Data Security Standard (PCI DSS) compliance validation is an integral part of a security program used by credit card brands to enhance payment security through assessment of compliance to the PCI DSS. On the other hand, the introduction of virtualization technology as part of cardholder data environment (CDE) system components allows merchants to maximize their return on investment through deployment of Virtual Machines (VMs) as part of their CDE. At the same time, different levels (1-4) of merchants can now share same private cloud for the deployment of their CDEs. This paper will examine the assessment method applicable to the varying levels of merchants using the private cloud for compliance validation to PCI DSS. Using Visa card as a case study, we will show that the use of a mix of Self-Assessment Questionnaire (SAQ) methods by level 2-4 merchants (i.e. small merchants) and Qualified Security Assessment (QSA) by level 1 merchants (i.e. big merchants) for assessment can introduce vulnerabilities that may impact the security of cardholder data stored in the private cloud. We will explore the risk assessment process in [3] to describe the impact of using the two different assessment methods by merchants sharing the same infrastructure.**

***Keywords: PCI DSS, Validation, Private Cloud, In-scope, CDE, Isolation, Multi-tenancy***

## I. INTRODUCTION

The new PCI DSS V2.0 has included virtualization and the use of cloud computing as part of system components that can be used in the deployment of CDEs. In this new dispensation where merchants can now share environments, there is a high possibility of propagation of vulnerabilities from VM to VM of merchants sharing the same private cloud as compared to the traditional standalone CDE. Therefore, the need to review the existing assessment methods applicable to merchants for their PCI DSS compliance validation cannot be overemphasized. PCI DSS compliance validation is one important requirement of the card brands in enforcing merchants to implement security controls in their CDEs. Merchants processing, storing and transmitting cardholder data are required to use one of the two assessment methods for their PCI DSS compliance validation. The new version 2.0 of PCI DSS now permits merchants to co-exist in a private cloud. In PCI DSS V2.0, SAQ can be used by one Merchant and QSA by another merchant for the assessment of PCI DSS compliance in the private cloud depending on the level of the merchants.

The risks of shared hosting and virtualized environment are well known and have been reported extensively in different papers. The previous PCI DSS version1.2 introduced shared hosting as a service that can be used for the deployment of CDE. Current version of PCI DSS v2.0 then included virtualized environments in the deployment of CDE. Both services allow a single server to provide services for multiple customers and merchants. Hosting (shared or virtualized) in the private cloud, provides economical alternatives to dedicated hosting (standalone). Virtualized environment is often considered a step up to shared hosting in terms of security. In shared hosting, operating system and installed services are determined by the service providers, whereas in virtualized environment customers are given the option to choose their operating system and install services they need. Shared hosting is difficult to secure, as multiple customers share the same operating system. Virtualized environments have independent administrators that are empowered to implement secure system configurations and to maintain up to date patches of the operating system in their own virtual machines.

As our goal is to assess the potential impact of using a mixed assessment method in a private cloud, we report an estimated number of transactions that can be exposed by two merchants using the private cloud. We show that the use of a mix of SAQ method by level 2 – 4 merchants (i.e. small merchants) and QSA method by level 1 merchants (i.e. big merchants) for validation of compliance with PCI DSS is a security risk to the cardholder data of customers deployed by merchants using the private cloud. Since one of the criteria used by Visa for qualifying merchants to use SAQ or QSA is the total number of annual transactions processed by merchants and the potential risk exposure if the cardholder data is compromised [1] [2] [6], the potential impact of using SAQ by merchants in the private cloud is higher than the impact that will be experienced by the same merchants when using traditional standalone hosts. Our paper recommends QSA for merchants using the private cloud because of the higher risks in the numbers of cardholder data that can be exposed when compared to the standalone environment.

We use risk assessment methodology described in PCI SSC virtualization guidelines [3] to assess the impact of using the mix of SAQ and QSA methods in the private cloud. In section I, we briefly define some important components of this paper like; private cloud, PCI DSS compliance validation and assessment method. We begin the risk assessment process in section II by defining the environment used for our analysis and identifying all the system components of merchants using the private cloud. In section III, we identify vulnerabilities, threats and analyze risks of using the mixed assessment methods in a private cloud. Section IV describes the impact of SAQ method on the other merchants using the multi-tenant private cloud. We present the outcome of the risk assessment process by estimating the total number of transactions that can be compromised as a way to show the impact of using SAQ method as against using QSA in the multi-tenant private cloud. Our analysis is theoretical as we have made no attempt to survey organizations using the mix of assessment methods in their private cloud environment. However, survey of organizations using this arrangement is a potential area for future research. In section V we review related research and conclude the paper in section VI.

### *A. Private Cloud*

Private cloud is a cloud computing deployment with limited service access and with system components that are controlled/owned by the customer[3][23][24]. Private cloud can be hosted in the premise of a customer (called on-premise) or out-sourced to a third party provider. Private cloud also possess the five defining attributes of cloud computing in that it uses Internet technology for access, is scalable, service-based, metered by use, shared and elastic[24]. The system devices in a private cloud are dedicated to a specific set of people, enterprise or enterprises. Customer using the private cloud gained control and ownership of services through involvement in implementation and limiting hardware and software sharing. One assumption of this paper is that our reference private cloud is owned by a group of companies, and contains their subsidiaries as tenants. A typical example is the government agencies using a private cloud.

Depending on the business objective of the companies using the private cloud, different cloud service models can provide different levels of access to cloud services. We use infrastructure as a Service (IaaS) as it provides exclusive control to computing resources which allows tenants to run their own application and operating systems in a virtual machine [23]. This level of access reduces the challenges of defining scope and assigning responsibilities that may affect the achievement of PCI DSS compliance in a private cloud. Therefore, merchants sharing the private cloud are responsible for ensuring their PCI DSS compliance validation.

In this paper, we refer to our reference private cloud as a multi-tenancy private cloud because it consists of more than one merchant sharing the same private cloud. In IaaS, different VMs of merchants may reside on the same host that are controlled by the service provider's policies and management software (Hypervisor) [23]. Security of multi-tenancy private cloud can be impacted by a flaw in the hypervisor or policies exposing the VMs of one tenant to the VMs of another.

### *B. PCI DSS Compliance Validation*

Validation in simple term, means to show evidence that you are doing the right things. Validation in the context of PCI DSS is to show to the card brands that a merchant has implemented all the PCI DSS requirements. PCI DSS compliance validation is done annually and helps card brands ensure through assessments that merchants comply with the PCI DSS requirements. Compliance validation is expected to help identify vulnerabilities (if any) and ensure that appropriate levels of cardholder information security are maintained [1]. The 2011 and 2010 compliance report [15] [21] by Verizon showed that about 22% of Level 1 merchants were compliance validated at the initial report of compliance (IROC). IROC - is the first compliance validation action done by the QSA before the final ROC that will be submitted to the card brand. IROC is like a preliminary assessment to evaluate the state of compliance of merchants and to expose PCI DSS requirements that are not implemented by merchants. This gives the merchants the opportunity to quickly remediate requirements that are not in place before the assessment is completed. QSA is mainly done by a third party security company and has a higher chance of detecting PCI DSS requirements that were not implemented or were overlooked by merchants being assessed for remediation. The main components of compliance validation are: annual assessment and quarterly vulnerability network scan.

### *C. Assessment Methods: QSA and SAQ*

The two assessment methods being used by Visa for validation of compliance are: QSA (by third party security companies) and SAQ. The assessment method applicable to a merchant is based on the validation levels of the merchant. Validation levels are currently based on annual volume of transactions of individual merchant. Visa transaction volume is based on the annual number of Visa transactions (inclusive of credit, debit and prepaid). There are four compliance levels (Level 1 - 4) which are based on the Visa annual volume of transactions. Service providers are divided into two levels (Level 1 -2), also based on annual volume of Visa transactions. Level 1 comprises of merchants processing over 6 million Visa transactions annually; level 2 merchants process 1 million to 6 million transactions (Point Of Sale terminal (POS) and e-commerce); level 3 merchants 20,000 to 1 million e-commerce transactions and level 4 processes up to 1 million Visa transaction or less than 20,000 e-commerce Visa transactions annually. Level 1 service providers transmit over 300,000 Visa transactions annually and level 2 service providers transmit less than 300,000 transactions annually. Level 1 merchant and service provider also undergo QSA for their annual validation of compliance with PCI DSS. Level 2 - 4 merchants and level 2 service providers are validated using self-assessment questionnaire (SAQ Type A-D).

In QSA method, Report of Compliance (ROC) is prepared at the end of the annual QSA and submitted by the security company to Visa for review. This shows that Visa enforcement on Level 1 members to PCI DSS compliance is higher than the other levels of merchants. As the name SAQ suggests, it is a self-evaluating assessment of PCI DSS requirements and can only be used by level 2, 3 and maybe level 4 merchants. Merchants are not mandated in SAQ to engage a third party like the qualified security assessors for their validation.

**Table 1: The Characteristics of the different methods of assessment used for compliance validation to PCI DSS**

| | SAQ | QSA |
|---|---|---|
| Volume of transactions | < 6 million | Over 6million |
| Assessor | Merchant (self) | Third party qualified security company |
| Type | Yes/No questionnaire | On-site security assessment |
| Output | Completed questionnaire | Report of compliance |
| Who submits report | Merchant | Third party qualified security company |
| Report Review by | Acquirer | Visa (Card Brand) |

## II. DEFINITION OF A MULTI-TENANT CDE

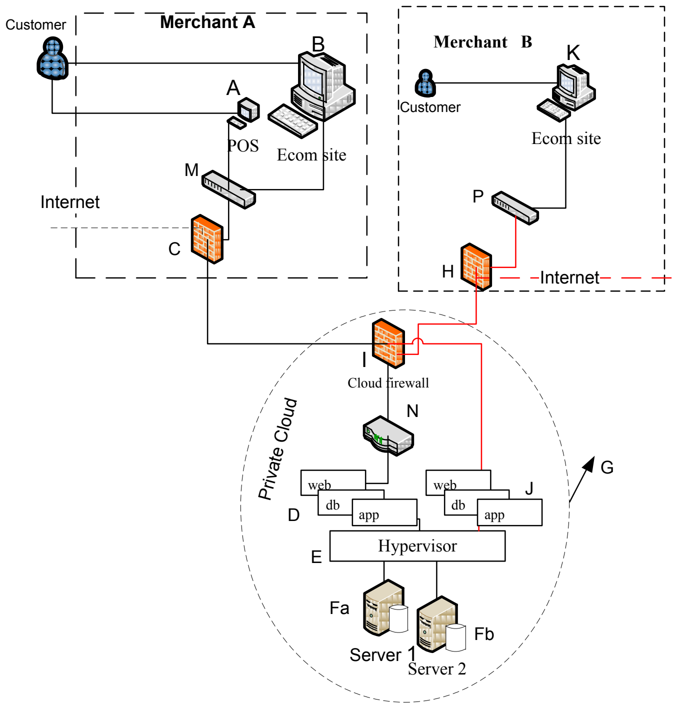
Multi-tenant CDEs consist of two or more merchants deploying parts of their CDE in the same infrastructure. The environment being considered in this paper is a private cloud using virtualization technology to consolidate computing resources on the physical hosts. VM is one of the CDE system components that can be deployed by merchants in the private cloud. The use of VMs by merchants as part of their CDEs presents more complexity than the traditional CDE deployment on a standalone physical host. Another system component that is now introduced in this environment is the hypervisor. Hypervisor is a specialized and optimized operating system (OS) that manages and maps traffic from the VMs to the underlying VM host's physical hardware.

Some of the activities for defining the environment of our risk assessment process are described as follow:

### *A. Physical Site Details For Each Component*

We describe a multi-tenant private cloud as an environment where member companies belonging to a group of companies are sharing the same private cloud. A typical example is the government agencies using a private cloud. These government agencies are independent credit card merchants registered by the same or different acquirers. The Private cloud being referenced in this paper uses virtualization to decouple the underlying physical devices into logical units, to enhance provisioning and resource utilization [16]. Figure 1 shows reference architecture for a multi-tenant private cloud with two different levels of merchants sharing computer resources. The traditional CDE deployment is an environment using standalone physical servers and is divided into; customer area and back office [20]. Customer area represents system components used by merchant's customers for inputting or accepting cardholder data into the CDE. It includes mainly; point of sales terminals (POS) used for card-present transactions or website of merchant used for card-not-present transactions. Back office area comprises servers, firewall and network devices that connect to the inputted cardholder data from the customer area. Unlike the back office in a traditional CDE deployment, system components in a multi-tenant CDE deployment of a private cloud are shared by the merchants using the private cloud as described in the next sub-section B.

**Figure 1: Example of CDE of Multi-Tenant Merchants using private cloud (IaaS)**



## B. *Identification of System Components In A CDE Of Multi-tenant Private Cloud*

The first step of PCI DSS assessment is the discovery process which is critical to compliance validation as it identifies the in-scope system components that must be validated by individual merchants for PCI DSS compliance. In-scope system components refer to the system components that directly interact with the cardholder data; hence they will be validated for PCI DSS compliance. In a mixed mode environment in which the in-scope and out-of scope virtual components are running on the same hypervisor, both may be considered to be in-scope. The reason for this is to reduce the numbers of avenue for attacks like VM side channels and cross VM information leakages due to sharing of physical resources.

In Figure 1, the illustrated CDEs of merchants in a multi-tenant private cloud are derived from the PCI SSC definition of a traditional CDE [20]. There are two CDEs shown in the diagram above; one for Merchant A and the other for Merchant B. System components of the reference architecture are listed below and the description of the letters are shown in table 2:

- CDE of Merchant A contains the following system components: A-B-M-C-I-N-D-E-F(a & b)-G
- CDE of Merchant B contains : K-P-H-I-N-J-E-F(a & b)-G
- Service providers - I-N-D-J-E-F(a & b)-G

The Service provider is responsible for the compliance and compliance validation of system components that are shared by the merchants using the private cloud (i.e. the hypervisor, physical hardware hosts etc.). The private cloud system components are located in the datacenter (G) of the service provider. The service provider is responsible for the physical access control of the datacenter(G).

## C. *Visibility Between Components*

Private cloud presents a unique scenario where physical hosts are shared between cloud tenants, for instance; system components I-N-E-F-G are shared by all the CDEs. VMs - D are virtual machines of Merchant A and VMs -J are used by Merchant B; both are connected to the hypervisor "E". Each VM of merchants is dedicated to a primary function as recommended by 2.2.1 of PCI DSS[7]. For example, web, application and database servers of merchant A and B are implemented on separate VMs. In an Infrastructure as a Service (IaaS) cloud service model, Merchant A has exclusive control of their VMs -D, but should not have access to VMs-J of Merchant B. The same applies to Merchant B, having control over its own VMs -J. This is achieved through the hypervisor running on top of the VMs physical host to segment VMs of merchants sharing the same physical hosts. Merchants (A and B) will be responsible for the PCI DSS compliance validation of their system components such as; applications, operating systems and databases running inside their VMs (D and J respectively).

## D. *Primary Function And Assignment of Owners For Each Component*

One of the reasons why the merchants and not the service providers will be responsible for the assessment of their virtual machine's system components is to ensure privacy of the critical cardholder data in the VMs. PCI DSS also recommends that system components in the cloud environment must be assigned to responsible entities [3]. However, PCI DSS compliance of system components is a joint responsibility of members in the cloud – merchants and cloud service provider. Service providers must ensure that system components assigned to them comply with PCI DSS while merchants are responsible for the PCI DSS compliance of the remaining system components in their CDEs. Areas of responsibility assigned to entities (merchants and services providers) must be properly documented. Sharing responsibility between entities will simplify the scope and cost of PCI DSS compliance, allowing entities to know their in-scope system components and to implement appropriate PCI DSS controls. Having system components properly assigned to entities will also increase the success rate of validation and lower the cost of PCI DSS compliance validation.

For the purpose of this research; assignment of responsible entities to system components of CDEs described in the reference Multi-tenant CDE in figure 1 can be shared as shown in table 2. System components (I-E-F-G) that are shared by all the cloud merchants will be assigned to the cloud service providers. Merchants will be responsible for compliance validation of system components that are directly used by their CDEs.

### *E. Identification Of Traffic And Data Flow Between Components*

Traffic coming from the customer area represents an un-trusted traffic from the ecommerce site of merchants (B and K) or POS (A). The traffic coming from the customer area of merchants is first filtered by the merchant's firewalls. Traffic coming from merchants A's customer is filtered by firewall C and traffic originated by merchant B's customer is filtered by firewall H. Firewall rules on the firewall C and H permit traffic that conforms with the set rules or disallow traffic that does not meet the set rules. Permitted customer's traffic are either sent to the payment processor's gateway via the internet or routed to the back office area (VMs). Traffic going to the back office area enters the private cloud via the shared cloud firewall (I). The in-bound traffic from both merchant's networks pass through the same cloud firewall (I). At the same time out-bound traffic from the merchants virtual machines (D and J) located in private cloud also pass through I. Firewall I which is shared by both merchants, identifies traffic of each merchants and route them to the appropriate VMs of merchants. Traffic in the VMs is internal and are handled by the hypervisor (E). Data from VMs of merchant A is stored on host storage volume Fa and that of merchant B is stored on the storage volume Fb.

**Table 2: CDE system components with members responsible for PCI DSS compliance [3]**

| S/N | In-scope system Components | Responsible member |
|---|---|---|
| 1 | Point of sales Terminal (POS) - A | Merchant A |
| | Ecommerce Site - B | |
| | Network switch - M | |
| | Firewall/Router - C | |
| | VMs (application, Database, Operating system, patching) - D | |
| 2 | Ecommerce Site - K | Merchant B |
| | Switch and Firewall/Router – P,H | |
| | VMs ( application, Database, Operating system, patching) - J | |
| 3 | Firewall/Router - I, N | Service Provider |
| | VMs (D and J) logical isolations | |
| | Hypervisor - E | |
| | Physical Host - F (a & b) | |
| | Datacenter -G | |

### *F. Other Activities In Defining Virtual Environments*

The virtual components as shown in figure 1 are: VMs-D, VMs-J and hypervisor E. The physical components in the private cloud are firewall I, router N, server 1 and server 2. Virtual machines of merchants (D and J) are placed on the two hosts being managed by the hypervisor E. The VMs are segmented through the hypervisor running on top of the VMs physical host to segment VMs of merchants sharing the same physical hosts. The hypervisor is used as the management interface and is controlled by the system administrator of the private cloud provider.

## III. RISK IN THE DEPLOYMENT OF CDE IN A MULTI- TENANT PRIVATE CLOUD

In the previous section we described the first element of the risk assessment process - define environment. In this section, we continue with the other three important elements of the risk assessment process; identify threats, identify vulnerabilities and analyze risk.

### *A. Identify Threats*

Most threats that exist in traditional physical environments are also possible in a virtual environment like the private cloud with some additional ones specific to virtual environments[3][17]. Some of the known traditional threats that can also be used in a private cloud are: social engineering, hacking, spear phishing, botnets, malware to mention a few. These threats have multiplier effects when used by an attacker in a private cloud as more than one merchant are sharing the environment. Insider threat is one of the top 7 cloud threats listed by Cloud Security Alliance[16]. This threat can be amplified by the malicious behavior of the cloud's or merchant's administrator to violate system configuration of VMs or hypervisor.

Hacking has become so popular that most of the recent payment data breaches are partially or wholly linked to it in one way or the other[15][21]. Some of the threat actions that are used in hacking are: password cracking to gain unauthorized access through brute force attack or password dictionary; SQL injection - use of unverified user's input to deceive applications to run SQL code that was not intended; command and control attack used when a backdoor has been established; exploitation of guessable administrator's credentials or default configurations.

Malware is malicious code that is injected and executed on computer system. Malware can be injected into the systems in different ways; by clicking on unsolicited internet links, downloading from untrusted web sites, email attachment and social media. Malwares can create a backdoor that allows remote access and control. A typical example is PoisonIvy, a common backdoor Trojan developed by a Chinese speaker. This malware was used in the recent Nitro attacks for stealing intellectual property from the chemical industry [17]. Another threat action of malware is the key logger, used by attackers to capture user's activity data. RAM scraper is a threat action of malware used for capturing data from the memory of the system.

Physical tampering of the hardware hosting the VMs is also a threat in a private cloud setting. Can someone sneak into the datacenter of a private cloud and install malicious code to probe the memory of the server? We may believe this is unlikely, going by the physical security provided to secure the facilities; but it is possible with an insider attack.

### B. Identify Vulnerabilities

A lot of research have been done on the vulnerabilities in the cloud and virtualization. Vulnerabilities in a virtualized environment include hypervisor as a single point of failure, increased complexity of virtual components, lack of separation of duties, dormant VMs, Virtual migration attack, VM Snapshots, information leakage and system misconfiguration.

Virtual escape is a threat characterized by the exploitation of the virtualization infrastructure or weak isolation between VMs. Virtual escape is any action that may result in a user or administrator of one VM gaining unauthorized access to another VM or the underlying physical host. One action is to run an arbitrary code from a VM in the context of the physical host. Upon success, an attacker gains access to unauthorized data of other VMs or access to the memory of the host. An attacker might penetrate the isolation between VMs via virtual escape. Studies have shown that it is possible to determine if VMs are co-located on the same physical hardware, therefore making it easier for an attacker to target the memory of the host storing sensitive data - increasing the chances of a successful attack [22]. Memory is a key asset as it stores sensitive data and can be a potential target for attack. Hypervisor can be a single target for an attacker to take over control of the host, memory, VM guest operating system and the application running in the VMs.

Mix of VMs using different assessment methods, a focus of this research, is also considered a vulnerability. VMs using weak assessment method will typically have lesser security controls than the VMs using a third party comprehensive assessment that may result to additional vulnerabilities. VMs using SAQ may be categorized as lower-trust level VM and the VM of QSA merchants, a high-trust level. Hosting VMs of different trust levels on the same host could reduce the overall security of the other VMs or the virtual host to the least-protected component (SAQ VM)[3]. This is one of the general principles of security, "security is only as strong as the weakest link".

### C. Analyze Risks

Analyzing the risk, we use a private cloud consisting of two different levels of merchants to analyze the risk of using the mix of SAQ and QSA assessment method for the validation of PCI DSS compliance. We will assign hypothetical numbers of transactions to merchants for the purpose of our analysis. It is assumed that merchant A is a level 1 and merchant B is a level 3 merchant. Merchant A processes 6.5 million annual visa transactions and is qualified for a QSA method of assessment. Merchant B on the other hand, processes 700,000 Visa transactions annually and thus qualifies for SAQ assessment. The total annual Visa transactions stored, processed or transmitted by the two merchants using the private cloud will therefore be the summation of annual transactions of both merchants (A+B), which is 7.2million as illustrated in the example given in table 3 below.

Visa requires level 1 merchant to undergo on-site QSA, which involves a comprehensive on-site QSA assessment by a qualified security assessor. Merchant B is a Level 3 merchant and is required to undergo a SAQ method for validation of compliance to PCI DSS. merchant B is required to use SAQ type D, if for instance merchant B has payment application that is connected to the internet and stores card holder data. SAQ type D is a type of SAQ that has the most self-evaluation questions. SAQ-D contains over 208 yes/no questions to be completed by merchants.

The mix of QSA and SAQ methods used by merchants A and B respectively may result in a weak validation of compliance in the private cloud. This may increase the number of cardholder data that can be potentially exposed if any of the VMs of merchants in the private cloud is compromised. Merchant B may be considered a weak link in the process because the SAQ assessment method being used to validate compliance with PCI DSS is not as comprehensive as that of merchant A. One of the findings of the Verizon security assessors was that most of the merchants validated by Verizon considered themselves compliant when assessing their own PCI DSS compliance. With the third party assessment done by Verizon, 78% of the merchants were found not implementing some of the PCI DSS requirements [15][21]. Suffice to say that SAQ merchants (Merchant B) may likely not be compliant. As a result, vulnerabilities from merchant “B's” CDE may allow an attacker gain an initial entry into the private cloud. After the initial entry, a determined attacker will do all it takes to access cardholder data. They may use different threat actions as necessary to compromise VMs hosted on the same hypervisor or host in the private cloud.

## IV. IMPACT OF SAQ METHOD ON OTHER MERCHANTS

We have shown from the risk analysis that merchant B, with the lower volumes of transactions, may create a risk which may expose other cardholder data of merchant A, with higher volumes of transaction to compromise. The potential risk of having merchants using SAQ assessment method to share the same virtual environment with a merchant using QSA should be revisited by the card brands in order to enhance the overall security of the cardholder data in the shared environment.

Table 3 estimates the potential numbers of transactions that can be compromised in a private cloud when using two mixed assessment methods. From the table 3, merchant B processes 700,000 and merchant A processes 6.5million annual Visa transactions, a successful compromise of VMs (J) can lead to compromise of 700,000 transactions. At the same time this may further lead to the compromise of VMs(D) of merchant A through VM-to-VM escape or exploitation vulnerabilities that exist in the private cloud. Potentially, over 6million of merchant A’s payment transactions can be compromised. 7.2 payment transactions can be compromised in a multi-tenancy private cloud with two mixed level of merchants. The risk exposure can even be higher than the 7.2million transaction described above depending on the numbers of mixed level merchants that are co-mingling in a private cloud.

**Table 3: Summary of annual transactions of merchants in the private cloud**

| Merchant | No. of Annual Transaction | Merchant Level | Method of Assessment | Enforcement |
|---|---|---|---|---|
| A | 6.5Million | 1 | QSA | Strong |
| **B** | **700,000** | **3** | **SAQ-D** | **Weak** |
| Both | 7.2million | 1 | QSA | Strong |

## V. RELATED RESEARCH

The additional information in [3], stated how PCI DSS compliance will be determined for merchants by examining the different scenarios of CDE deployments. One suggestion by PCI SSC was on how merchants will determine the in-scope virtual system components to achieve compliance. VMs that are part of the CDE and non-CDE VMs co-existing on the same hardware or hypervisor will all be in-scope of PCI DSS. The types of assessment methods that are applicable to merchants using the private cloud were not reviewed in this guideline. Rather, card brands are still using the existing criteria of the old PCI DSS V1.2 to determine type of assessment methods applicable to merchants in the new PCI DSS version 2.0. Level 2-4 merchant will use SAQ and Level 1 merchants use QSA assessment methods.

The findings of Verizon can be used to prove the importance of a third party security assessment (QSA) as against the self-assessment method (SAQ). In 2011 and 2010 report, it was noted that about 21% of organizations validated by Verizon were fully compliant at Initial Report Of Compliance (IROC) [15], [21]. It was also noted that merchants were overconfident when assessing the state of their own security practices and had high expectations they will pass the PCI DSS compliance validation done by Verizon's Qualified Security Assessors (QSAs). Out of the 200 merchants involved in 2010 compliance validation exercise, 78% merchants failed the validation at the initial on-site PCI DSS assessment. Some merchants that later passed validation at the final on-site assessment were able to remediate controls that were not implemented as identified by the external assessors before the final on-site assessment was completed. Other merchants that were not able to remediate the missing requirements in PCI DSS test, eventually failed the compliance validation done by the Verizon PCI assessor.

Balduzzi et al [14] on Amazon`s elastic compute exposed various vulnerabilities associated with the use of virtual images of a public cloud. The researchers investigated images used in the Amazon EC2 to provision virtualized servers called instances. They identified various vulnerabilities in the virtual instances of cloud customers using Amazon EC2. They found out that 98% of Windows AMIs and 58% of Linux AMIs in the Amazon EC2 contained software critical vulnerabilities. The results of the experiments were proofs that services or virtual instances deployed in the cloud (public) can expose cloud customers and their environment to higher security risks. CDEs deployed into multi-tenant private cloud may not be isolated from some of these vulnerabilities if security controls are not implemented and compliance with existing standards like PCI DSS are not properly enforced (validated).

The research by Cloud Security Alliance (CSA) [16] highlights some top threats to cloud computing. It is important to look at security holistically and to eliminate vulnerabilities as much as possible. Virtualization software used for virtualization has been identified as one of the top threat to cloud computing. Some of its underlying components like; CPU caches, Graphics Processing Unit (GPUs), etc. are not designed to offer strong compartmentalization properties for a multi-tenant architecture. The virtualization application for instance may have some flaws that can enable guest operating system of the CDE to gain elevated controls on hypervisor or influence the underlying host [16]. Attackers may exploit the flaws of the virtualization technology to compromise the hypervisor, host and VMs of the CDEs in the cloud. Other top threats are: malicious insider (cloud staff); insecure web APIs used by cloud customers to manage and interact with cloud services like provisioning, orchestration etc. Malwares are among the top threat to cloud noted by CSA (example is the Infostealer Trojan horses).

## VI. CONCLUSION

In this paper we have proposed a review of the criteria currently being used by Visa and other card brands for determining the assessment method that is applicable to merchants using a private cloud for the deployment of their CDE. The assessment method in private cloud of merchants is currently being determined by the annual number of transactions per merchant. The total sum of transactions in VMs of merchants using private cloud is not considered to determine the assessment method of merchants in this environment. Looking at security in-depth, there is need to remove single point of failure of using a weak assessment method in a mix of strong assessment method. We have been able to show that more cardholder data can be exposed to risk by SAQ merchants than it is currently been considered in the criteria used by Visa Card in determining the assessment method applicable to merchants. The VMs of merchants using SAQ are threats to the VMs of QSA merchants and the virtual host physical hardware. Vulnerabilities that may exist in VMs-J can be targeted by an attacker to compromise cardholder data stored in the VMs of merchants sharing the virtual environment. As a future research, this paper can be extended to evaluate the impact of using mix of SAQ and QSA by merchants in a public cloud. Also, an experiment can be performed to demonstrate how vulnerabilities that may exist in the VMs of SAQ merchants can exploited to compromise the other merchants using QSA in a virtualized environment.

## ACKNOWLEDGEMENT

I will like to express my very great appreciation to my supervisors: Dr Pavol, Dr Dale and Dr Ron, for their valuable time to read and give constructive suggestions during the development of this research work. I wish to thank my classmates for their critiques at class seminars. My special thanks to my family for their understanding and encouragement. Finally, I will like to give all the glory and adoration to the almighty God for giving me the strength and wisdom to complete this paper.

## REFERENCES

[1] Visa Inc., "Visa PCI DSS Data Security Compliance Program"; [Online] Available: http://usa.visa.com/download/merchants/cisp_overview.pdf¸ February 2012

[2] Visa Inc., “PCI DSS compliance validation Framework”, [Online] Available: http://usa.visa.com/download/merchants/cisp-bulletin-visa-pci-dss-framework-111808.pdf, November 2008

[3] PCI SSC, “Information supplement' PCIDSS virtualization guidelines”, June 2011.

[4] PCI SSC, “Summary of Changes from PCI DSS Version 1.2.1 to 2.0”, October 2010

[5] Visa, "US PCI DSS compliance status", [Online] Available: http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf, September 2011.

[6] Visa, "compliance validation details for Merchants", [online] Available: http://usa.visa.com/merchants/risk_management/cisp_overview.html, January 2012

[7] PCI SSC, “PCIDSS: Requirements and assessment procedures version 2.0” October 2010

[8] PCI Security standard council, ,"Validation Requirements for Qualified Security Assessors (QSA)", version 1.2, October 2008.

[9] National Institute of Science and Technology, “Cloud computing reference Architecture”, SP500- 292, September 2011

[10] National Institute of Science and Technology, “Guide to Security for full Virtualization Technology”, SP800-125, January 2011

[11] Visa, " What To Do If Compromised " , [ Online] Available : http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf, May 2011

[12] PCI SCC," ROC Reporting Instructions for PCI DSS v2.0 ", [Online] Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_2.0_ROC_Reporting_Instructions.pdf, September 2011

[13] PCI SSC, "Self-Assessment Questionnaire: Instructions and Guidelines Version 2.0" , [Online] Available: https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf, October 2010

[14] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro. "A security Analysis of Amazon`s Elastic Compute Service", 27th ACM Symposium On Applied Computing (SAC), Security Track, Trento, Italy, March 2012

[15] Verizon, "Verizon 2010 Payment card industry compliment Report: A study conducted by Verizon PCI and Risk intelligence teams", [Online] Available , http://www.verizonbusiness.com/resources/reports/rp_2010-payment-card-industry-compliance-report_en_xg.pdf

[16] Cloud security alliance, "Top Threats to Cloud computing V1.0"; prepared by cloud security alliance, [Online] Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010

[17] Symantec security Response, "The Nitro Attacks: Stealing Secrets from the chemical industry", [Online] Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf, December 2011

[18] Visa, "Visa expands Technology Innovation Program for U.S. Merchants to Adopt dual Interface Technology", [Online] Available: http://usa.visa.com/download/merchants/bulletin-tip-us-merchants-080911.pdf, August 2011

[19] Financial fraud Action, UK " The Plastic Fraud", [Online] Available: http://www.financialfraudaction.org.uk/Publications/#/10/, Slide 10-11, Accessed March 2012

[20] PCI SSC, " Information Supplement: PCI DSS Wireless Guideline ", [Online] Available: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

[21] Verizon, "Verizon 2011 Payment card industry compliment Report", [Online] Available: http://www.verizonbusiness.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf, March 2012

[22] T.Ristenpart, E.Tromer, H Shacham and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds", Available [online]: http://www.cs.cornell.edu/courses/cs6460/2011sp/papers/cloudsec-ccs09.pdf

[23] National Institute of Science and Technology, “Cloud computing Synopsis and Recommendations”, SP800-146, May 2011

[24] T. Bittman(Gartner), "Clarifying private cloud computing" , Available [Online]: http://blogs.gartner.com/thomas_bittman/2010/05/18/clarifying-private-cloud-computing, May 2010