2nd International Conference on Advanced Research (ICAR- Nov, 2017), Melbourne, Australia.
ISBN: 978-0-6481172-0-9
www.apiar.org.au

ADDRESSING PERCEIVED SECURITY CONCERNS OF CLOUD SERVICE WITH THE ENHANCEMENT OF DATA VISIBILITY

W.P. Yuen [a], K.B. Chuah [b]
EngD Candidate [a], Associate Professor [b]
City University of Hong Kong, Hong Kong
Corresponding email: wpyuen2-c@my.cityu.edu.hk

Abstract

Cloud computing is a pervasive technology and has been a platform in IT for several years. Cloud service providers have developed and offered different service platforms to accommodate different needs of enterprise subscribers. However, there still exists the situation of enterprise customers' hesitation and reluctance to deploy their core applications using cloud service platforms. Our recent user-survey results show that security is the perceived major concern of existing and prospective enterprise customers of cloud services.

This research investigated the expectation gap between enterprise customers and cloud service provider with regard to the perceived security of cloud services. Enterprise customers expected to be reassured of cloud service security in a more explicit or visible way from cloud service provider (CSP).

The term *data visibility* has been widely used in the IT industry especially from ICT product and solution vendors. However, there is not any practice guideline or standard in industry to define this term; nor any quantifying method.

This paper defines the characteristics and core elements of data visibility, and proposed to apply customer centric data visibility concept to address different security related concerns from both perspectives, and show how the enhancement of data visibility can earn the trust from enterprise customer in adopting public cloud service

Keywords: Data Visibility, Customer Centric, Perception of Cloud Service Security, Visibility Framework, Visibility Element.

1. Introduction

The pay-per-use business model of cloud computing allows their tenants to adjust their investment in IT resources dynamically, enterprise can reduce the CAPEX (capital expenditure) and OPEX (operating expenditure) on physical infrastructure such as servers, network, security, storage, application and IT administration/management. It is often attractive for many small and medium enterprises (SME). When enterprise adopted the public cloud business service, they may loss the control over their owned data. Different concerns have appeared from customer's perspective such as security, data integrity, performance, compliance etc. Amount all these concerns, security is perceived as the major concern by both existing and prospective enterprise customers of cloud services.

Perception of data security in cloud computing platform can be enhanced by data visibility. The term data visibility has been widely used in the IT industry, especially from ICT product and solution vendors. However, there is no common practice guideline or standard in industry. This paper defines the characteristic and the core elements of data visibility, and proposes the conceptual model data that enhances visibility on cloud platform. It used the customer centric data visibility concept to address different concerns, and show how the enhancement of data visibility can earn the trust of enterprise customers in adopting public cloud services.

ISBN: 978-0-6481172-0-9
www.apiar.org.au

These security and data privacy issues in different service models are related to the visibility of cloud platform from subscriber's perspective. It makes most enterprises uncomfortable with cloud platform (especially SaaS model) due to lack of traffic visibility about the way their data is stored and secured.

Today, subscribers can only trust the audit report provided by CSP with standard code of practice and certification such as ISO27001/27002/27017/27018. However, those standards only require documenting all the steps for manual procedures that touch production environment. SLA is another source for customer to trust on the service from cloud provider, but most of the SLA cover service availability (eg. 99.999% per year) more than security, confidential and integrity aspect (Rong, et al., 2013).

The responsibility of security in cloud is shared between CSP and customer (NIST Cloud Computing Security Reference Architecture, 2013; Amazon Web Services, Inc, 2016). Enterprise might not feel comfortable to adopt cloud computing service for their key applications and data because of security concern, especially lack of visibility on their valuable and sensitive data in cloud environment. This paper aim at investigating the data visibility to the consumer to enhance trustworthy cloud computing. The related work on this research is to propose a solution to address this scenario with the following contribution.

- Explore the expectation gap and concerns between CSP and customers
- Industry survey in relationship between visibility/monitoring and cloud security
- Define the core elements of data visibility in cloud from customer's perspective
- Propose the framework of data visibility model

2. Related Work

Monitoring is a common acceptable approach to keep tracking the activities in cloud. Accountability is necessary to mitigate the CSA threats [11] and enable users to adopt cloud. One important mechanism for accountability is monitoring (Wongthai, et al., 2013). Accountable Cloud (AC) or Monitoring as a service (MaaS) appear in the market. There are different products addressed to cloud monitoring as monitoring is also an optional features offered from CSP (chargeable). The aim of deploy cloud monitoring is different by users as it enables the provider or developer to maintain QoS, arrange resources for better service and support to tenants.

Amazon CloudWatch is a monitoring service cloud resources and applications, user can collect and track metrics, collect and monitor log files (Amazon Web Services, Inc, 2017). Fujitsu K5 Cloud IaaS service also provides a function to monitor the applications that users run on the system. It collects and tracks information on the monitored items of resources such as virtual servers and database instants (FUJITSU LIMITED, 2016)[9].

If enterprise customer especially SME do not deploy end to end service from multiple layer CSP, they might need to select or stipulate different cloud layer of service for monitoring. So, in order to acquire a better visibility in cloud, monitoring should be both layer specific and layer agnostic. Interoperability should cover different layers and cloud providers. There are different commercial cloud-oriented monitoring tools in the market with different capabilities and features[10]. Cloud monitoring can cover multiple dimensions, but interVM, intraVM traffic and infrastructure traffic should be addressed.

In order to enhance trust to CSP, trust attestation is another topic for researcher. Different attested trust cloud architectures are proposed, such as Open CIT from Intel.

The foundational concept is to provide monitor trust status of the platform (host OS, hypervisor and VM) in real time for dynamic trust measurement.

This paper uses the customer centric data visibility concept to address the different concerns and show how the enhancement of data visibility can gain the trust of customers in CSP.

3. The gap between CSP and tenants

According to NIST reference [15], the cloud service model is IaaS, PaaS and SaaS. Most of the large CSP in the market offer a one stop service with end-to-end solutions to customers eg. Microsoft, Oracle. Apart from that, many IaaS providers are transformed from original data center/hosting/MSP, they provide infrastructure and virtual/container platform for tenants, in such case, the PaaS service is usually combined with SaaS.

There are different research and studies related to security and issues of cloud computing. NIST proposed 9 key security issues in 2011 (Jansen & Grance, 2013), CSA proposed 12 top threats in cloud (CLOUD SECURITY ALLIANCE, 2016). This paper explored different concerns confronted by enterprise customer (tenant) and CSP and how visibility can be applied there.

Fig 1. List the relevant concerned items confronted by both enterprise customers and CSP. Most of the issues or concerns from enterprise customer are mainly related to data itself, security, privacy, and data integrity. Even technologies and operation oriented items are also related to data securities. The number of items concerned by cloud service provider is less than enterprise customer, although some of them are overlap. Items concerned by cloud service providers are more related to reliability, service quality, performance and operation. Data visibility can be applied to address 12 different concerns: data breaches, data location, unauthorized access, privacy, compliance, data loss, availability, malicious insider, shared technologies vulnerabilities, monitoring, forensic and instance response. It can be applied on five concerned items in the expectation gap (data breaches, data location, unauthorized access, privacy and compliance).

Cloud provider	Concerned item	Cloud customer
	Data breaches	√
	Data protection	√
	Data location	√
	Unauthorized access	√
	SLA	√
	Privacy	√
	Compliance	√
	Control	√
√	Data loss	√
√	Availability	√
√	Security - APT/DDoS attack	√
√	Malicious insider	√
√	Insufficient due diligence	√
√	Abuse use cloud	
√	Software isolation	√
√	Shared technologies vulnerabilities	√
√	Account hijack	√
√	Monitoring	√
√	Forensic	√
√	Instance response	√

Figure 1: Items of concerns of CSP and tenant

ISBN: 978-0-6481172-0-9
www.apiar.org.au

4. Data visibility and security

4.1 Data visibility concept

The term "visibility" has the following general characteristics:

- the state of being able to see or be seen
- the distance one can see as determined by light and weather conditions
- the degree to which something has attracted general attention prominence

Different sectors might have different interpretation of visibility.

Visibility is widely used in ICT nowadays. Product vendors like NPB (Network packet broker), application performance monitoring products, network traffic analytic product, data traffic analytic products, and system performance monitoring products, they used the term as their product features for marketing purpose. However, there is no official or standard definition or practice guideline on "data visibility" in ICT industry.

4.2 Data visibility in cloud computing

Customers have different expectations on cloud service through visibility, such as data location, data availability, data integrity, identity and access control, audit and compliance. They do not have enough visibility to acquire all those information, it leads to decrease in customer trust (Kuppuswamy & Al-Khalidi, 2014; Soofi, et al., 2014) The guideline on Security and Privacy in Cloud computing from NIST indicates that continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Collecting and analyzing available data about the state of the system should be done regularly and as often as needed by the organization to manage security and privacy risks, as appropriate for each level of the organization involved in decision making. Ideally, the consumer should have control over aspects of the means of visibility to accommodate its needs, such as the threshold for alerts and notifications, and the level of detail and schedule of reports (NIST Cloud Computing Security Reference Architecture, 2013).

According to the result of an industry survey in Melbourne, 77% of those surveyed agreed that monitoring/visibility as part of cloud service is important to enterprise users in APAC.

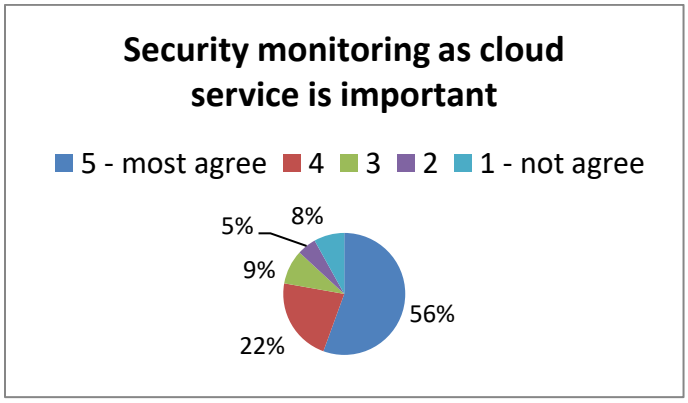

Figure 2: Industry survey result in Melbourne Jul.2013 *(sample size 74)*

The result of another industry survey in Singapore (Fig 3) shown that 75% of those surveyed from APAC agreed that more visibility in network can enhance security.

ISBN: 978-0-6481172-0-9
www.apiar.org.au

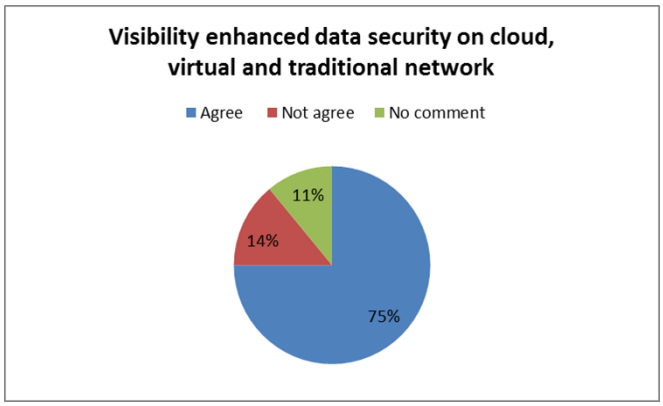

Figure 3: Industry survey result in Singapore 2013 *(sample size 264)*

4.3 Data visibility characteristics

The proposed model to enhance data visibility will have the following characteristics:

- **Customer centric** – data should belong to data owner, its policies, magnitude and dimension (both depth and width) should be defined and driven by data owner or customer. Data owner need to established a mechanism to mandate the enforcement of their own policy to ensure data confidentiality and integrity (Rong, et al., 2013)

- **End to end** – Required data status should reflect across different domains from network, server, virtual/container, application to storage (Gupta & Rai, 2015).

- **Bi-directional/Interactive** – Visibility alert in the form of pop up log message is not enough, it is desirable if driven by user to acquire enough data status anytime. Besides, any data status triggered within the condition defined by user should be reflected

5. The conceptual model

5.1 Core elements of data visibility

The 5 core elements of the proposed model adopted from the well-known "5W1H" model widely used problem management analysis are as follows:

- **Timing (When)** – When the activities happened? An accuracy time should provide on the data in different stages. The precision of the timestamp in log of each event should be accurate enough for business application use. Eg. PTP/NTP Timestamp

- **Type (What)** – What kind of data has been involved? Should detailed enough to identify what data type and data source has been involved in event or state changes. Eg. Database, table, object, filename.

- **Location (Where)** – Data location, physical storage or any virtual machine when data is at rest. Eg, IP address, domain name, mac address and geolocation.
- **User (Who)** – Who touch that specific data? Application user or system user? Eg. Aggregate the information from different IAM systems in different level.

- **Activities (How)** – How can the system, application be processed/accessed ? Is the data being inquired by normal user? or modified by unauthorized people? or dropped in network? Eg. log/SIEM retrieved from different domains and applications to identify the data status is changed in each event.

5.2 Visibility flow

The proposed data visibility mechanism is to enable cloud users to construct their required visibility condition in cloud. User visibility policies are defined according to their own requirements, and those required policies will forward to SaaS as filtering conditions on relevant activities information.

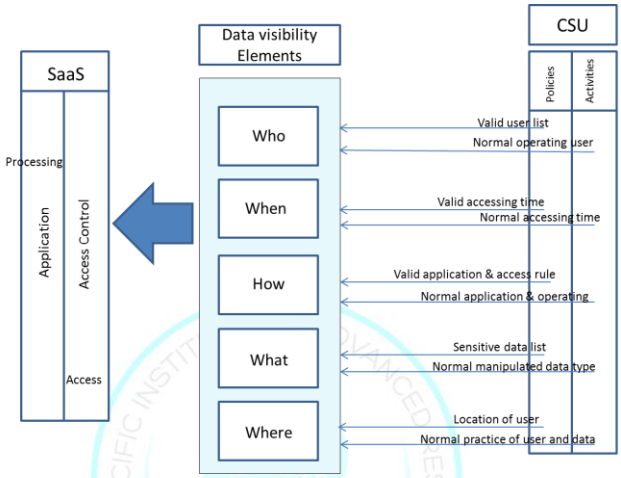

Figure 4: Data visibility requested from customer to cloud - SaaS

SaaS as an application service provider, in most cases, is the single point of contact to customer on behalf of other cloud service provider (PaaS/IaaS). So, besides the normal application data communication, SaaS can also take the role of visibility policies interface to customers. Visibility features to customer can be interactive between customer and provider, or it can also be alert based unicast to specific customer.

For some uncertain activities which happened in data center, SaaS need to get information from PaaS/IaaS. So, there is an information flow is in between them. The major characteristics of this prototype are customer centric and end-to-end visibility.

6. Framework

6.1 Components

There are three major components in the data visibility model:

1. User requested interface (URI) – User input their requirement of visibility on specific data type, user, timing, access method and location. Users can make ad hoc inquiry, and define data visibility policies

2. Policy & mapping module (PMM) – The inquiry received from URI will be converted into instruction rule resident into memory buffer. These instructions will forward to Collecting & filtering module (CFM) for visibility data collection, then mapping the specific data with source of inquiry and egress to users.

ISBN: 978-0-6481172-0-9
www.apiar.org.au

3. Collecting & filtering module (CFM) – It is a collector of all different log and events from IaaS and SaaS. Based on the instruction from PMM, the collected data will be filtered before sending back to PMM. This can make sure the visibility data meets the requirement and also discard any unrelated traffic so as to reduce the traffic over the network

Visibility requested by user through URI will be converted into policies from PMM, the instruction will then be sent to CFM to collect suitable visibility data from different CSP. From there, all collected visibility data will be filtered and sent back to PMM for mapping into specific policies which belongs to user. Finally, the visibility information will be forwarded to customer end.

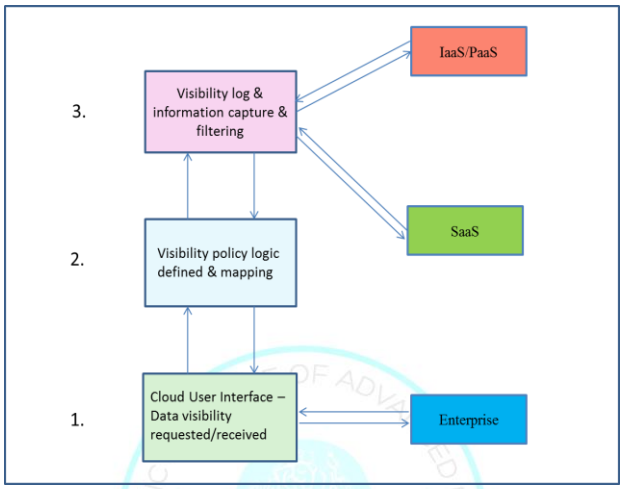

Figure 5: Components of data visibility model

6.2 Visibility traffic taxonomy

Infrastructure traffic includes :

- Event from networking and security device including NMS, IDS (host/hypervisor/network based), IPS, Firewall, DPI, load balancer, NAS
- Event and log from access device - Identity and Access Management (IAM)
- Event and log from VM/Hypervisor and host - VMI, /var/log/auth.log, /var/logs/syslog, Hyper-V log, VMM, external monitoring tools such as Solarwinds

Application traffic, log and event include:

- Event from APM, Lifecycle Management, Configuration Management, Security Management -Security Services (Runtime), DB Policy Management, HTTP Server, Database Identity Management, Database Access Management, and Directory Services Management, external application log

6.3 Architecture

Log and event traffic from infrastructure activities will be collected into log management or SIEM such as Logstash or Splunk. Related traffic will be distributed into different SaaS.

In SaaS, application activities events, access information, database management events will be collected, and aggregate with the infrastructure traffic into Collecting & filtering module (CFM) for processing. Relevant data visibility information will be filtered, mapped and egress to

ISBN: 978-0-6481172-0-9
www.apiar.org.au

relevant data owner/customer. The entired visibility traffic across the cloud is centralized and managed for data owner.

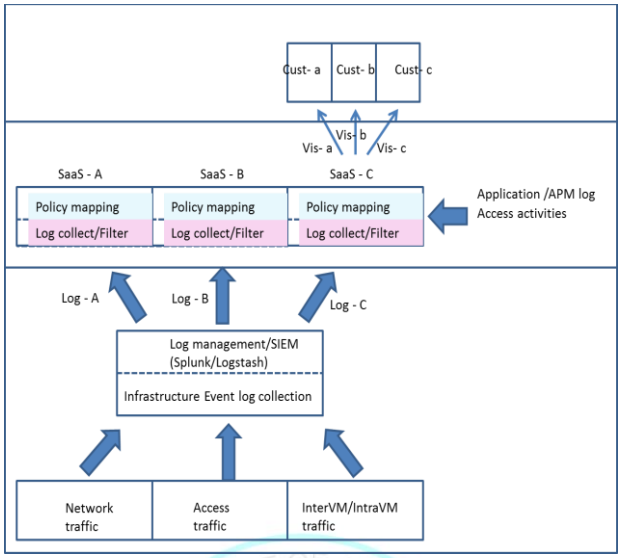

Figure 6: Data visibility model - architecture

Capturing log and event information from security device and network elements can be either from the SPAN/mirror port, or via network TAP/Probe. Most of the traffic is collected in out of band mode (except IPS). So, the service interrupt to operation is minimized. Agent can be deployed in host or VCenter/VMM to collect interVM or intraVM traffic. In some cases, CSP support third party agent aggregator eg. AWS support virtual TAP agent which can collect information from different virtual servers.

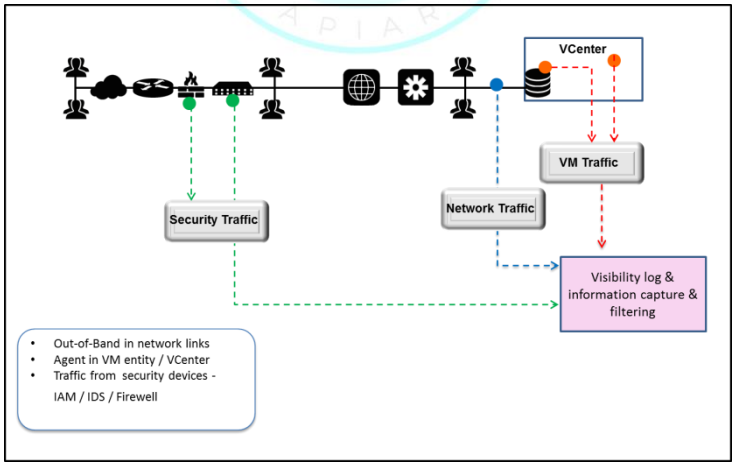

Figure 7: Data visibility model – Data capture

ISBN: 978-0-6481172-0-9
www.apiar.org.au

Conclusion & prospects

This model is expected to enable the visibility information flow through different domain across cloud to end user. When designing the conceptual mode, operation and practice of cloud providers are also need to be considered, so as to ensure that the model is practical.

This conceptual model has been introduced to different enterprises, system integrators and CSPs in Asia for their comment. The feedbacks are positive, and worthy for exploration and development.

The next stage of this research is to develop the conceptual model to a prototype. Then, put it to industry stakeholders including different cloud providers, cloudbroker (solution integrator in APAC market), and also enterprise customer, especially in SME for valuation.

It is expected to be the practice reference model for cloud provider of SI when they deliver their cloud based solution to enterprise.

References

i. Alhamazani, K. et al., 2014. An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-art. *Springer-Verlag Wien*.

ii. Amazon Web Services, Inc, 2016. *AWS Security Best Practice,* s.l.: Amazon Web Services, Inc.

iii. Amazon Web Services, Inc, 2017. *Amazon CloudWatch User Guide,* s.l.: Amazon Web Services, Inc.

iv. CLOUD SECURITY ALLIANCE, 2016. *The Treacherous 12 - Cloud Computing Top Threats in 2016,* s.l.: CLOUD SECURITY ALLIANCE.

v. Gupta, V. O. & Rai, P. Y., 2015. Threats and Vulnerability in Cloud Computing. *International Journal of Advent Research in Computer and Electronic (E-ISSN:2348-5523) special issue*.

vi. Jansen, W. & Grance, T., 2013. *Guidelines on Security and Privacy in Public Cloud Computing NIST special publication,* s.l.: Computer Security Division Information Technology Laboratory.

vii. Kuppuswamy, P. & Al-Khalidi, S. Q., 2014. Analysis of security threats and prevention in cloud storage. *Review Report, International Journal of Advanced Research in Engineering and Applied sciences,* 3(1), pp. 2278-6252.

viii. LIMITED, F., 2016. *FUJITSU Cloud Service K5 IaaS Features Handbook version 1.9,* s.l.: FUJITSU LIMITED.

ix. Mell, P. & Grance, T., 2011. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-154,* s.l.: Computer Security Division Information Technology Laboratory.

x. Modi, C. et al., 2013. A survey on security issues and solutions at different layers of Cloud computing.. *The Journal of Supercomputing,* 63(2), pp. 561-592.

xi. NIST Cloud Computing Security Reference Architecture, 2013. *NIST Special Publication 500-299,* s.l.: NIST Cloud Computing Security Working Group, NIST Cloud Computing Program.

xii. Patidar, V. & Kumbhkar, M., 2014. Analysis of Cloud Computing Security Issues in Software as a Service. *International Journal of Scientific Research in Computer Science and Engineering,* 2(3), pp. 2320-7639.

xiii. Rong, C., Nguyen, S. T. & Jaatun, M. G., 2013. Computers and Electrical Engineering. *SciVerse ScienceDirect,* 39(2013), pp. 47-54.

xiv. Soofi, A. A., Khan, M. I., Talib, R. & Sarwar, U., 2014. Security issues in SaaS Delivery model of Cloud Computing. *International Journal of Computer Science and Mobile Computing,* 3(3), pp. 15-21.

xv. Wongthai, W., Roacha, F. L. & Moorsel, A. v., 2013. *A generic logging template for infrastructure as as service cloud: Technical Report Series,* New Castle: New Castle University.