Cloud Security Proposed and Demonstrated by Cloud Computing Adoption Framework

Muthu Ramachandran and Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University, Headinley, Leeds LS6 3QR, U.K.

Abstract. This paper presents the Cloud security by Cloud Computing Adoption Framework (CCAF) from its system design, development and implementation. We illustrate the required attributes and explain its significance, including the CCAF security design. To demonstrate how it works, software schema is developed. CCAF can perform quarantine and protective actions based on "Rescue", an XML-based schema and feature for CCAF. The CCAF implementations have been illustrated to show how to enforce security and ensure all suers are protected. It provides three layers of security in Access control and firewalls; Intrusion Detection Systems (IDS) and Prevention System; and Isolation Management to maintain a high level of Cloud security. CCAF security offers a framework to serve the Cloud community. The key characteristics have been explained. We will develop more service updates and demonstrations for our forthcoming projects to ensure that CCAF security can provide more use cases and added value to the Cloud community.

1 Introduction

Cloud Computing has been an agenda for organizational adoption due to benefits in cost-savings, improvement in work efficiencies, business agility and quality of services [5, 7, 12]. With the rapid rise in Cloud Computing, software as a service (SaaS) is particularly in demand, since it offers services that suit users need. For example, Mobile applications allow users to play online games and easy-to-use applications to interact with their peers. Health informatics help medical researchers diagnose challenging diseases and cancers [3]. Financial analytics can ensure accurate and fast simulations to be available for investors [4]. While more people and organizations use the Cloud services, security and privacy become important to ensure that all the data they use and share are well protected. Some researchers assert that security should be implemented before the use of any Cloud services in place [1, 9-10]. This makes a challenging adoption scenario for organizations since security should be enforced and implemented in parallel with any services. This motivates us to develop a framework, Cloud Computing Adoption Framework (CCAF), to help organizations successfully adopt and deliver any Cloud services and projects. In this paper, we demonstrate our security design, implementation and solution for CCAF. The breakdown of this paper is as follows. Section 2 presents security overview under CCAF. Section 3 describes security design by CCAF and Section 4 explains security development schema by

Ramachandran M. and Chang V..
Cloud Security Proposed and Demonstrated by Cloud Computing Adoption Framework.
DOI: 10.5220/0004984000620070
In *Proceedings of the International Workshop on Emerging Software as a Service and Analytics* (ESaaSA-2014), pages 62-70
ISBN: 978-989-758-026-0

XML. Section 5 demonstrates CCAF security implementation. Section 6 explains how CCAF can serve the Cloud community and Section 7 sums up topics for Conslusion.

2 Security Overview under CCAF

We generalize the areas for security overview. The following are categories of CCAF security aims to cover:

- Application software security which deals with how we can build systems that can automatically protect itself.
- Network (LAN, MAN, GAN), Wireless network security, and Platform Security include Operating Systems, Virtualisation, and other systems software.
- VoIP security as the application is gaining popularity.
- Convergence network security where converging, multi-network media infrastructures, social networks and technologies, which is one of the emerging areas of research.
- Service-oriented security where issues related to system services such as denial of service attacks, distributed denial of services, and web services.
- Cloud security deals with services security, data security and privacy so that services delivered and assets are protected.
- Open-source software security deals with issues such as trust, certification and qualification models.
- Software components and architecture, security which deals with building components and architectures with security can be used as plug-ins.
- Web services security is essential to ensure secured services are delivered with integrity.
- Systems & Software security engineering deals with building security in (CCAF) right from requirements. This is also considered developing software applications with CCAF.

Caminao project [2] provides a comprehensive framework for systems engineering methods and concepts. However, it does not offer a complete solution for Cloud Computing. This motivates us to have a comprehensive design, implementation and service for Cloud security under the CCAF recommendation. CCAF is a framework for organizations that we previously demonstrate how CCAF can be offered in healthcare [3], finance [4] and education [6]. It is our goal to provide guidelines and recommendation for security and privacy. Computer security has been classified into a number of general concepts and processes such as identification, which identifies objects, functions, and actions, authentication, authorization, privacy, integrity and durability. The objective of the CCAF Cloud security is categorized and presented in Figure 1. We have so far well established basic security features with identification, authentication, authorization, and digital security encryption and decryption techniques. Key features with their explanations are as follows.

Identification is a basic and first process of establishing and distinguishing amongst

person/user & admin ids, a program/process/another computer ids, and data connections and communications. Often we use alphanumerical string as user identification key and some may use your email itself as the user identification key and this can be checked against when a user login into the system. Authentication and authorisation are two distinct form of allowing users to access what they are allowed not allowed to access any information in the system.

Privacy is the key to maintaining the success of cloud computing and its impact on sharing information for social networking and team work on a specific project. This can be maintained by allowing users to choose when and what they wish to share in addition to allowing encryption and decryption facilities when they need to protect specific information/data/media content.

Integrity is defined as the basic feature of human being as a process of maintaining consistency of actions, communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for cloud service providers to protect integrity of cloud user's data with honesty, truthfulness and accuracy at all time. In cloud computing terms, we can achieve integrity by maintaining regular redundancy checks and digital certification in addition to other basic security features of maintaining identification, authentication, and authorisation.

Durability is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

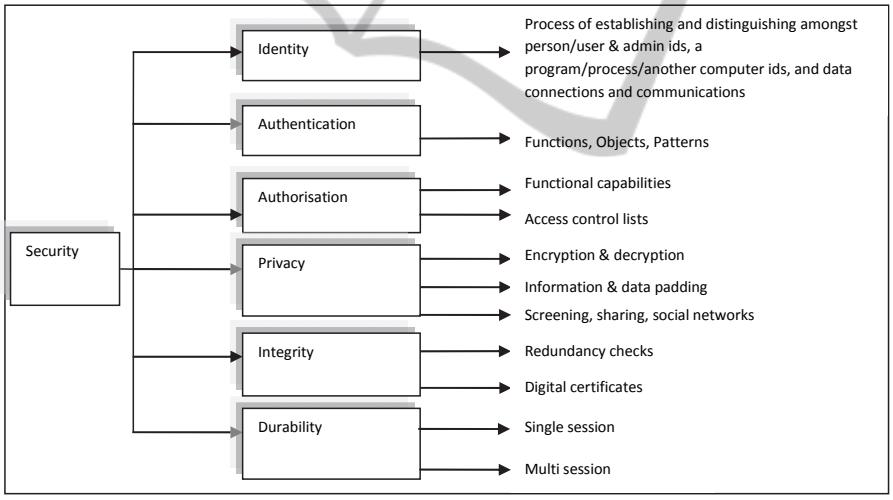

Fig. 1. CCAF digital research landscape.

3 CCAF Security Design

This section describes the system design required by CCAF. Capturing and identifying requirements for security explicitly is one of challenges in Cloud security for SaaS, which has an impact on the functionality of the system. Therefore, we need to be able specify security requirements explicitly throughout the security-specific life-

cycle phases as part of achieving CCAF (security requirements, design for security, security testing & securability testing). Tondel et al. [11] has provided an extensive survey on security requirements methods which help to identify security requirements systematically and structure them. For example, Mead [8] for the SEI's (software Engineering Institute) has identified a method known as SQUARE (Secure Quality Requirements Engineering) which has been extended SysSQUARE (Systems Engineering SQUARE) towards systems security engineering method. Our extended method consists of nine steps as follow:

- **Agree on definition** which means to define a set of acronyms, definitions, and domain-specific knowledge needs to be agreed by stakeholders. This will help identify and validate security-specific requirements clearly by stakeholders
- **Identify security goals** which means to clearly define what is expected of the system with respect to security of business drivers, policies, and procedures
- **Develop artefacts** which means to develop scenarios, examples, misuse cases, templates for specifications, and forms
- **Perform risk assessments** which means to conduct risk analysis for all security goals identified, conduct threat analysis
- **Select an elicitation technique** which includes systematic identification and analysis of security requirements from stakeholders in the forms of *interviews, business process modeling and simulations, prototypes*, *discussion and focus groups*. As part of this phase, one has also to identify level of security, cost-benefits analysis, and organizational culture, structure, and style
- **Elicit security requirements** which include activities such as producing security requirements document based security specific principle structure as part of our goal of developing CCAF earlier, risk assessment results, and techniques identifies for analysis such as *business process modeling and simulations, threat modeling, and misuse cases*, etc.
- **Categorize security requirements** which include activities such as classifying and categorizing security requirements based on company-specific requirements specification templates and to use our recommended security principles as this will help Systems Engineers to apply CCAF and track security-specific requirements for validation & verification at all stages of the systems engineering lifecycle.
- **Identify systems data security requirements** which include activities on extracting and carefully identifying data security and relevant sub-systems such as data centers, servers, cloud VM, and software security, SQL security, and other types of security that are relevant to data. This separation of concern allows systems engineers to integrate, track, design, and develop data security as part of enterprise wide systems development.
- **Prioritize security requirements** which include activities of selecting and prioritising security requirements based on business goals as well as cost-benefit analysis.
- **Inspect security requirements** which mean to conduct requirements validation process using requirements inspection and review meetings.

To achieve a fined-grained model for the iterated requirements, one can select key-words as objects and components.

4 CCAF Security Software Schema by XML

This section describes the software scheme required by CCAF. Extensible Markup Language (XML) is the language that can define the rule, permission, function and interactions in the use of SaaS and Cloud security. A proposed XML section type, Rescue, is described here as an example. “Rescue” is used to block virus, trojans and attacks such as denials of services and unauthorized access. In the event of hacking, all the files are backed up and retrieved from secure ports such as 21 for secure FTP and 443 for secure HTTPS. Instead of displaying IP addresses in the traditional method, the IP addresses in all virtual machines are assigned at runtime. There is an OVF ID that handles processing of the DR request. The syntax can be ovf:id =”rescue” presented in Table 1

Table 1. The CCAS Security Software Schema.

```
<ns: Rescue ovf:required=”true” xsi:type="ovf:Rescue_Type">

<Info>  Rescued actions for SaaS security </Info>
<Rule>
   <Info> Retrieve data and put them in safety </Info>
  <Protocol> tcp </Protocol>
  <DstAddr ovf:id=”rescue” />
  <DstPort> 21 </DstPort>
  <DstPort> 443 </DstPort>
  <SrcAddr> any </SrcAddr>
  <SrcPort> any </SrcPort>
</Rule>

<Rule>
  <Info> Destinations for quarantined files if infected </Info>
  <Protocol> tcp </Protocol>
  <DstAddr ovf:id=”rescue” />
  <DstPort> 3306 </DstPort>
  <SrcAddr ovf:id=” rescue” />
  <SrcPort> any </SrcPort>
</Rule>

<Origin>
  <Info> Firewall protection for all VMs </Info>
  <DateAdded> 2013-01-18 </DateAdded>
  <AddedBy name=”Administrator” role=”creator”</>
</Origin>

</Rescue>
```

All the OVF IDs can be mapped to the required IP addresses when a VM is deployed. This allows “Rescue” to describe not just a single VM behavior, but expected communications and actions between VMs required for rescued actions. Another feature in Table 1 shows ovf:required=”true”. This means that Rescue action is on.

What triggers Rescue is when the security software detects activities from unknown IPs in the list of unknown hosts to ensure Rescue can protect all the users in real-time.

5 CCAF Security Software Implementation

CCAF security software implementation is demonstrated by the use of the Fined-Grained Security Model (FGSM), which has layers of security mechanism to allow multi-layered protection. This can ensure reduction in the infections by trojans, virus, worms, and unsolicited hacking and denial of services attack. Each layer has its own protection and is in charge of one or multiple duties in protection, preventive measurement and quarantine action presented in Figure 2.

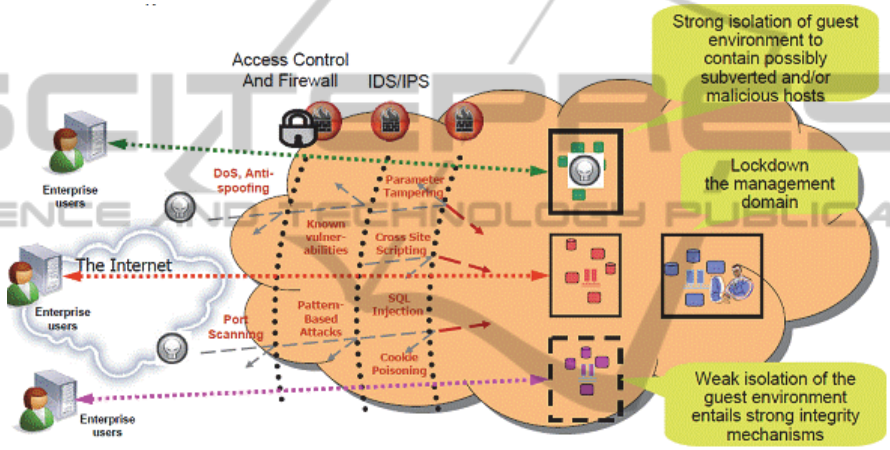

Fig. 2. The Fined-Grained Security Model offered by CCAF.

All the features in FGSM include access control, intrusion detection (IDS) and intrusion prevention (IPS), this fine-grained security framework introduced fine-grained perimeter defence. The layer description is as follows.

- The first layer of defence is **Access Control and firewalls** to allow restricted members to access.
- The second layer consists of **Intrusion Detection System (IDS) and Prevention System (IPS)**. The aim is to detect attack, intrusion and penetration, and also provide up-to-date technologies to prevent attack such as DoS, anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter tampering, cross site scripting, SQL injection and cookie poisoning.
- The third layer, being an innovative approach, **Isolation Management**, enforces top down policy based security management; integrity management. This feature monitors and provides early warning as soon as the behaviour of the fine-grained entity starts to behave abnormally; and end-to-end continuous assurance which includes the investigation and remediation after abnormality is detected.

Within isolation management, it has weak and strong isolation. Weak isolation focuses more on monitoring and captures end-to-end provenance to allow investigation and remediation to be greatly facilitated. Strong isolation and integrity management is also required when the first few vulnerabilities of the cloud are exposed. It backups data safely; quarantine infected data; and isolate quarantined data till further notice. Part of this concept has been demonstrated in Section 4 to show how rescued actions can be implemented and delivered.

6 CCAF Security – A Framework Serving the Cloud Community

This section describes how CCAF security can serve the Cloud community. Cloud security is part of a quality requirements collection process and it consists of three different requirements sub-categories: *confidential & privacy* builds the trust (trust is one of the basic and backbone for establishing quality), *integrity*, and *availability*. Therefore, security needs to be identified early, designed and to be tested as part of the SaaS explicitly.

How CCAF can serve the community is described as follows. First, we need to identify all the attributes of SaaS security so that we can assess and evaluate each requirement against a set of security attributes that will enable us to extract security related requirements. Security is an essential part of the system for achieving, protecting systems and users. Security has several attributes that are related to a simple email system (where most of the attacks, such as virus, spam, intrusions, and identity fraud occur frequently); security baselines are standards that specify a minimum set of security controls that has to be met for most organizations under normal circumstances. Second, Cloud and SaaS security also include both technical and operational security concerns. Cloud computing has emerged to address the needs of the IT cost-benefit analysis and also revolution in technology in terms of reduced cost for internet data and speed. Therefore, the demand for securing our data in the cloud has also increased as a way of building trust for cloud migration and to benefit business confidence in the cloud technology by cloud providers such as Amazon, Microsoft, Google, etc. In this way, we can ensure that our CCAF security is applicable to cloud services as well as traditional systems. Figure 3 shows a model to structure cloud security attributes to develop and integrate CCAF across system development lifecycle. This model evolves based on further research and gain knowledge and experience of our own system and therefore the model will be expanded as and when we discover new attributes.

Most of the security attributes and principles identified earlier are clearly applicable to developing cloud services with systems engineering focus. However, there are some cloud-specific security related issues such as security in virtualisation and server environments. Cloud security attributes can be found in many-fold as shown in Figure 3. Although there are many attributes available, they can be further categorized as follows:

Confidentiality, Privacy and Trust – These are well known basic attributes of digital security such as authentication and authorization of information as well protecting privacy and trust.

Cloud Services Security – This includes security on all its services such as SaaS, PaaS, and IaaS. This is the key area of attention needed for achieving cloud security.

Data Security – This category is again paramount to sustaining cloud technology. This includes protecting and recovering planning for cloud data and service centers. It is also important to secure data in transactions.

Physical Protection of Cloud Assets – This category belongs to protecting cloud centers and its assets.

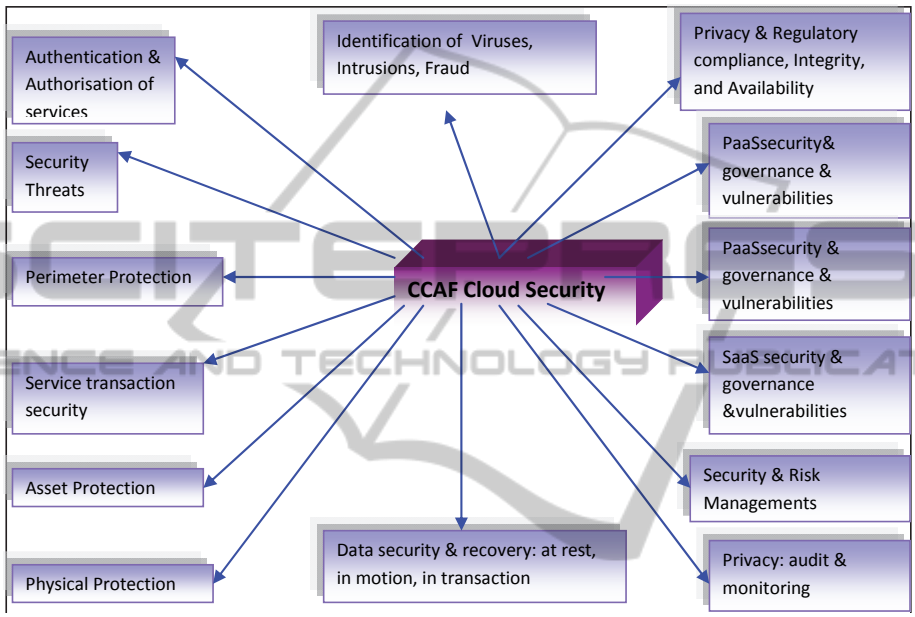

Fig. 3. CCAF Cloud Security Attributes serving for the community.

The above cloud security attributes/characteristics are essential and useful to understand non-functional aspects of services development and service provision. These attributes are also useful for building CCAF and maintaining security. The following section will use cloud security attributes and frameworks identified in this section as the main input for CCAF not developing security patches after cloud services has been delivered. Communities that have been positively influenced by CCAF in other projects include Guy's and St Thomas NHS Trusts (GSTT), King's College London (KCL), University of Southampton, University of Greenwich and Leeds Metropolitan University. Organizations that have been involved also include Commonwealth Bank of Australia (CBA), IBM in the US, SAP and University of Oxford in the development of Cloud services and projects [5]. Forthcoming Cloud projects include SAS and Mathematica for deliveries in modern education, and research and development.

7 Conclusion

We present the Cloud security presented by CCAF from its system design, development and implementation. We illustrate the required attributes and explain its significance for CCAF, including the security design. To demonstrate how CCAF works, software schema is developed. CCAF can perform quarantine and protective actions based on "Rescue", a XML-based schema and feature. The CCAF implementations have been illustrated to show how to enforce security and ensure all users are protected. It provides three layers of security in Access control and firewalls; Intrusion Detection Systems (IDS) and Prevention System; and Isolation Management to optimize Cloud security. CCAF security offers a framework to serve the Cloud community. The key characteristics have been explained. Organizations that are involved in the development and adoption of CCAF have been presented. We will develop more service updates and demonstrations for our forthcoming projects to ensure that CCAF security can provide more use cases and added value for the Cloud community.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2010), Above the Clouds: A Berkeley View of Cloud computing. Communications of the ACM, 53(4), 50-58.
2. Caminao Project, Caminao's Way: Do systems know how symbolic they are? Modelling Systems Engineering Project, http://caminao.wordpress.com/overview/?goback=%2Egde_3731775_member_251475288, accessed on 21st June, (2013).
3. Chang, V., Walters, R. J., & Wills, G., Cloud Storage and Bioinformatics in a private cloud deployment: Lessons for Data Intensive research, Springer: CLOSER 2012, CCIS 367, pp. 245–264, (2013).
4. Chang, V., Business Intelligence as Service in the Cloud, Future Generation Computer Systems, (2014).
5. Chang, V., Walters, R. J., & Wills, G., The development that leads to the Cloud Computing Business Framework. International Journal of Information Management, 33(3), pp 524-538, June, (2013).
6. Chang, V., Brain Segmentation – A Case study of Biomedical Cloud Computing for Education and Research. In, Learning Technologies Workshop, Higher Education Academy (HEA), University of Greenwich, (2013).
7. Marston, S., Li, Z., Bandyopadhyay, S. and Zhang, J. and Ghalsasi, A., Cloud computing – The business perspective, Decision Support Systems, Elsevier, 51(1): pp 176-189, (2011).
8. Mead, N.R., et. al., Security Quality Requirements Engineering (SQUARE) Methodology, TECHNICAL REPORT, CMU/SEI-2005-TR-009, (2005).
9. Ramachandran, M., Software components for cloud computing architectures and applications, Springer, Mahmmood, Z and Hill, R (eds.), (2011).
10. Ramachandran, M., Software Security Engineering: Design and Applications, Nova Science Publishers, New York, USA, 2011.ISBN: 978-1-61470-128-6, (2011).
11. Tondel, I. A et al., Security requirements for rest of us: a survey, IEEE Software, Special Issue on Security and Agile requirement engineer-ing methods, Jan/Feb. (2008).
12. Vouk, M. A., Cloud Computing – Issues, Research and Implementations, Journal of Computing and Information Technology - CIT 16, page 235–246, Volume 4, (2008).