Penerbit Akademia Baru

Journal of Advanced Review on Scientific Research
ISSN (online): 2289-7887 | Vol. 14, No.1. Pages 1-11, 2015

Cloud Computing- Double Edged Sword: An Opportunity and Big Threat

A. S. Thiab[*,1,a], *and A. S. Shibghatullahi*[2,b]

[1]Optimization, Modelling, Analysis, Simulation and Scheduling (OptiMASS) Research Group, Fakulti Teknologi Maklumat & Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[2]Department of Computer Sciences,University of Technology, Baghdad, Iraq.
[*,a]*alishawket1@gmail.com,* [b]*samad@utem.edu.my*

Abstract – *This paper provides survey of cloud computing threats and serves as an up-to-date threat identification that will help cloud users and providers to make informed decisions about risk mitigation within a cloud strategy. A literature review has been done of related works and the findings of the types of threats have been studied and the results and consequences have been laid out in the paper. The relations between the three basic platforms have been studied together and in individually but the study based on the secondary data collected from the related works on two platforms the IaaS and the PaaS have been presented in this study.*

Keywords: Cloud Computing, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service), API (Application Programming Interface), CSO (Chief Security Officer), VM (Virtual Machines)

1.0 INTRODUCTION

Cloud computing refers to software and hardware delivered as services over the Internet. The implementation of data mining techniques through Cloud computing will allow the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage. Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine.

Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest themselves of infrastructure management, and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are also very concerned about the risks of Cloud Computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable.

The services in cloud computing are provided to three platforms. IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). The computing

services are provided to clients from large data bases using virtual technology to any part of the globe. These large data centers are called 'clouds' as they virtually above the underlying structure of the system.

In the IaaS Platform the delivery system is made by the allocation of computer resources to virtual machines where the applications and the operations can be run.

In the PaaS Platform the customer can write the applications that are compatible with the service providers computing system and run them on their own machines.

In the SaaS Platform the customer is provided the applications that run on the internet in order to be able to use the facilities of the service provider through the premise machines.

Literature Review

Researches were first carried out in the University portal, with every search the search terms were refined and the minute phrases used in order to bring out the related literature that dealt with the security issues in cloud computing. Other related areas of security risks other than the IaaS Platform were also studied in order to gain an understanding of the effect that they had on the IaaS Platform security detailing [18].

Every area that was found to be a security risk was checked back with the service providers and the customers to see the risks that had threatened the customers and the service providers practically and match them to the analyzed data that has been collected from the literature review as well [19].

Out of 500 cases in practical terms that were studied it was found that 70% of them had issues with the security in the IaaS platform due to the virtualization of the machines. Despite being monitored there were sufficient loopholes in which data was extracted from the systems of the organizations. Out of these 500 cases it was found that 135 cases related to the IaaS platform, 164 cases related to the SaaS platform, 70 cases related to the PaaS platform and the rest was due to the issues with the hypervisor.

What has been confirmed is that there are security risks in cloud computing and modifications in all the platforms need to be made. What has also emerged is that the Virtual Monitoring Machine does have problems when requests are made for access and entry in another language.

Data has also been seen to be extracted from the virtual machines (VM) when the machines have been in the process of transfer. In maximum cases it has been seen that stationary data is most affected by intrusions and penetrations [20].

Objective

The purpose of this document, "Cloud Computing- a double edged sword", is to provide needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies. In essence, this threat research document should be seen as a companion to "Security Guidance for Critical Areas in Cloud Computing".

While many issues, such as provider financial stability, create significant risks to customers, we have tried to focus on issues we feel are either unique to or greatly amplified by the key characteristics of Cloud Computing and its shared, on-demand nature. We identify the following threats in our initial document:

(Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, and Account, Service & Traffic Hijacking)

Selecting appropriate security controls and otherwise deploying scarce security resources optimally require a correct reading of the threat environment. For example, to the extent Insecure APIs (Application Programming Interfaces) is seen as a top threat, a customer's project to deploy custom line of-business applications using PaaS (Platform as a Service) will dictate careful attention to application security domain guidance, such as robust software development lifecycle (SDLC) practices. By the same token, to the extent Shared Technology Vulnerabilities is seen as a top threat, customers must pay careful attention to the virtualization domain best practices, in order to protect assets commingled in shared environments.

Threat #1: Abuse and Nefarious Use of Cloud Computing Service Models: IaaS and PaaS

Description. IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Examples. IaaS offerings have hosted the Zeus botnet, Info-Stealer Trojan horses, and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used IaaS servers for command and control functions. Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist.

Remediation:

1. Stricter initial registration and validation processes.
2. Enhanced credit card fraud monitoring and coordination.
3. Comprehensive introspection of customer network traffic.
4. Monitoring public blacklists for one's own network blocks.

Impact. Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited [3].

Threat #2: Insecure Interfaces and APIs Service Models: IaaS and PaaS

Description. Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces

must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency [4].

Examples. Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

Remediation:

1. Analyze the security model of cloud provider interfaces.
2. Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
3. Understand the dependency chain associated with the API.

Impact. While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability [5].

Threat #3: Malicious Insiders Service Models: IaaS, and PaaS

Description. The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection [7].

Examples. No public examples are available at this time.

Remediation:

1. Enforce strict supply chain management and conduct a comprehensive supplier assessment.
2. Specify human resource requirements as part of legal contracts.
3. Require transparency into overall information security and management practices, as well as compliance reporting.
4. Determine security breach notification processes [8]

Impact. The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services

understand what providers are doing to detect and defend against the malicious insider threat [9].

Threat #4: Shared Technology Issues Service Models: IaaS

Description. IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc [10].

Examples. 1. Joanna Rutkowska's Red and Blue Pill exploits 2. Kortchinksy's CloudBurst presentations.

Remediation:

1. Implement security best practices for installation/configuration.
2. Monitor environment for unauthorized changes/activity.
3. Promote strong authentication and access control for administrative access and operations.
4. Enforce service level agreements for patching and vulnerability remediation.
5. Conduct vulnerability scanning and configuration audits.

Impact. Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data [11].

Threat #5: Data Loss or Leakage Service Models: IaaS, and PaaS

Description. There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment [12].

Examples. Insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures; persistence and remanence challenges: disposal challenges; risk of association; jurisdiction and political issues; data center reliability; and disaster recovery.

Remediation:

1. Implement strong API access control.

2. Encrypt and protect integrity of data in transit.
3. Analyzes data protection at both design and run time.
4. Implement strong key generation, storage and management, and destruction practices.
5. Contractually demand providers wipe persistent media before it is released into the pool.
6. Contractually specify provider backup and retention strategies.

Impact. Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications [13].

Threat #6: Account or Service Hijacking Service Models: IaaS, and PaaS

Description: Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks [14].

Examples. No public examples are available at this time.

Remediation

1. Prohibit the sharing of account credentials between users and services.
2. Leverage strong two-factor authentication techniques where possible.
3. Employ proactive monitoring to detect unauthorized activity.
4. Understand cloud provider security policies and SLAs.

Impact. Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach [15].

Threat #7: Unknown Risk Profile Service Models: Iaas and Paas

Description. One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications [16]. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs.

Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas [17].

Examples. 1. IRS asked Amazon EC2 to perform a C&A; Amazon refused. 2. Heartland Data Breach: Heartland's payment processing systems were using known-vulnerable software and actually infected, but Heartland was "willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data has been stolen [18].

Remediation:

1. Disclosure of applicable logs and data.
2. Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
3. Monitoring and alerting on necessary information.

Impact. When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

The following check-list of Cloud Security Challenges provides a guide for Chief Security Officers who are considering using any or all of the Cloud models [19].

For CSOs focused on PaaS

Challenge #1: Protect private information before sending it to the Cloud

There are already many existing laws and policies in place which disallow the sending of private data onto third-party systems. A Cloud Service Provider is another example of a third-party system, and organizations must apply the same rules in this case. It's already clear that organizations are concerned at the prospect of private data going to the Cloud. The Cloud Service Providers themselves recommend that if private data is sent onto their systems, it must be encrypted, removed, or redacted. The question then arises "How can the private data be automatically encrypted, removed, or redacted before sending it up to the Cloud Service Provider". It is known that encryption, in particular, is a CPU-intensive process which threatens to add significant latency to the process [20].

Challenge #2: Keep an Audit Trail

Usage of Cloud Services is on a paid-for basis, which means that the finance department will want to keep a record of how the service is being used. The Cloud Service Providers themselves provide this information, but in the case of a dispute it is important to have an independent audit trail. Audit trails provide valuable information about how an organization's employees are interacting with specific Cloud services, legitimately or otherwise!

The end-user organization could consider a Cloud Service Broker (CSB) solution as a means to create an independent audit trail of its cloud service consumption. Once armed with his/her own records of cloud service activity the CSO can confidently address any concerns over billing or to verify employee activity. A CSB should provide reporting tools to allow organizations to actively monitor how services are being used. There are multiple reasons

why an organization may want a record of Cloud activity, which leads us to discuss the issue of Governance [21].

For CSOs focused on IaaS

Challenge: Governance: Protect yourself from rogue cloud usage and redundant Cloud providers

The classic use case for Governance in Cloud Computing is when an organization wants to prevent rogue employees from misusing a service. For example, the organization may want to ensure that a user working in sales can only access specific leads and does not have access to other restricted areas. Another example is that an organization may wish to control how many virtual machines can be spun up by employees, and, indeed, that those same machines are spun down later when they are no longer needed. So-called "rogue" Cloud usage must also be detected, so that an employee setting up their accounts for using a Cloud service is detected and brought under an appropriate governance umbrella [22].

Whilst Cloud Service providers offer varying degrees of cloud service monitoring, an organization should consider implementing its own Cloud service governance framework. The need for this independent control is of particular benefit when an organization is using multiple SaaS providers, i.e. HR services, ERP and CRM systems. However, in such a scenario the CSO and Chief Technology Officer (CTO) also need to be aware that different Cloud Providers have different methods of accessing information. They also have different security models on top of that [23].

Some use REST, some use SOAP and so on. For security, some use certificates, some use API keys, which we'll examine in the next section. Some simply use basic HTTP authentication. The problem that needs to be solved is that these cloud service providers all present themselves very differently. So, in order to use multiple Cloud Providers, organizations have to overcome the fact they are all different at a technical level [24].

Again, that points to the solution provided by a Cloud Broker, which brokers the different connections and essentially smoothes over the differences between them. This means organizations can use various services together. In situations where there is something relatively commoditized like storage as a service, they can be used interchangeably. This solves the issue of what to do if a Cloud Provider becomes unreliable or goes down and means the organization can spread the usage across different providers. In fact, organizations should not have to get into the technical weeds of being able to understand or mitigate between different interfaces. They should be able to move up a level where they are using the Cloud for the benefits of saving money [25].

For CSOs focused on SaaS, PaaS and IaaS

Challenge: Protect your API Keys

Many Cloud services are accessed using simple REST Web Services interfaces. These are commonly called "APIs", since they are similar in concept to the more heavyweight C++ or Java APIs used by programmers, though they are much easier to leverage from a Web page or from a mobile phone, hence their increasing ubiquity. "API Keys" are used to access these services. These are similar in some ways to passwords. They allow organizations to access the Cloud Provider. For example, if an organization is using a SaaS offering, it will often be provided with an API Keys. The protection of these keys is very important [26].

Consider the example of Google Apps. If an organization wishes to enable single sign-on to their Google Apps (so that their users can access their email without having to log in a second time) then this access is via API Keys. If these keys were to be stolen, then an attacker would have access to the email of every person in that organization. The casual use and sharing of API keys is an accident waiting to happen. Protection of API Keys can be performed by encrypting them when they are stored on the file system, or by storing them within a Hardware Security Module (HSM) [27].

Conclusion: Homemade or Off-the-shelf?

When implementing a security framework to address these challenges, the CSO is faced with a buy vs. build option. They could engage developers to put together open source components to build Cloud Service Broker-like functionality from scratch. This approach creates the runtime components of a broker, such as routing to a particular Cloud Service Provider. However, other components of the solution, such as reporting and an audit trail, may not be present. An off-the-shelf Cloud Service Broker product will provide these extra features as standard and should also provide support for all the relevant WS-Security standards at a minimum [28].

As the Cloud Security Alliance notes in its Security Guidance White Paper. "Cloud Computing isn't necessarily more or less secure than your current environment. As with any new technology, it creates new risks and new opportunities. In some cases moving to the cloud provides an opportunity to re-architect older applications and infrastructure to meet or exceed modern security requirements. At other times the risk of moving sensitive data and applications to an emerging infrastructure might exceed your tolerance." I hope this article provides sufficient data points to guide readers on their journey [29].

REFERENCES

[1] A. Akinbi, E. Pensita, C. Beaumont, Identifying Security Methods & Controls For Secure PaaS Cloud Environment, Journal of Cloud Computing (2013).

[2] M. Al Morsy, J. Grundy, A.S. Ibrahim, Collaboration Based Cloud Computing Security Management Framework, pp: 364-371, IEEE 4th International Conference on Cloud Computing (2011).

[3] M. Al Morsy, J. Grundy, I. Muller, An Analysis on the Cloud Computing Security Problem Procedures, of APSEC, Cloud Workshop, Sydney-Australia, Science Direct (2010).

[4] M. Ambrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Korwinski, G. Lee, D. Patterson, A. Robbin, I. Stola, M. Zaharia, A View of Cloud Computing, Communications of the ACM 53(4) (2010) 50-58.

[5] N. Antonopoulos, L. Gillian, Cloud Computing Principles, Systems & Applications, (2010).

[6] http://dx.doi.org/10.1007/978-1-84996-2414

[7] B. Brandon, (Aug 6th 2014) Black Hat 2014: Research Reveals Amazon Cloud Security Weakness, Search Cloud Security s(1) www.techtarget.com, Retrieved on Jan 10th 2015

[8] G. Brunette, R. Mogull, Security Guidance for Critical Areas of Focus in Cloud Computing, (2009).

[9] J. Chanyung, Z. Min, L. Xiang, Research on Multi-Tenant PaaS Cloud Security on Java Platform. Information Science & Cloud Computing Journal, CISCC (2013) International Conference on Cloud Computing Security, IEEE.

[10] Chin, Katie (March 3rd 2014) Last Week on Research: Our Review of PaaS for 2014, Security & More, Gigaom.

[11] CSA, Guidance for Identity and Access Management, Cloud Security Alliance, Domain 2(1) (2010).

[12] W. Dawoud, I. Takouna, C. Meinel, Infrastructure as a Service Security: Challenges & Solutions,7th International Conference on Informatics & Systems(INFOS) (2010).

[13] A.A. Friedman, D.M. West, Privacy & Security in Cloud Computing, Issues in Technology Innovation – Brookings Institution 3 (2010).

[14] V. Fusenig, A. Sharma, Security Architecture for Cloud Networking & Communication IEEE International Conference on Cloud Computing and Networking Symposium (2012) 45-49.

[15] K. Hashizume, D. Rosado, G. Fernandez-Medina, E. Fernandez, B. Eduardo, An Analysis of Security Issues in Cloud Computing, Science Direct.

[16] A.S. Ibrahim, J. Hamlyn-Harris, J. Grundy, (2010) Emerging Security Challenges of Cloud Virtual Infrastructure, Conference Paper at Asia Pacific Software Engineering Conference,2010,Cloud Workshop, Sydney, Australia.

[17] Ibrahim, A. Mani, J. Hamlyn-Harris, (2013) Virtual Machine Security in IaaS Platform,

[18] M. Jenson, N. Gruschka, J. Schwenk, L.L. Ialono, On Technical Security Issues in Cloud Computing 2009 IEEE International Conference on Cloud Computing (2009) 109-116

[19] K. Jinzhu, A Practical Approach to Improve Data Privacy of Virtual Machines (2010).

[20] K. Julisch, M. Hall, Security & Control in the Cloud, Information Security Journal, A Global Perspective 19(6) (2010) 299-309

[21] A.U. Khan, M. Oriol, M. Jiang, K. Djemane, Security Risks & Their Management in Cloud Computing, pp: 121-128 IEEE 4th International Conference on Cloud Computing Technology & Science (2012).

[22] NIST(2014) Cloud Computing Security Standards, National Institute of Standards& Technology Cloud Computing Security,

[23] W.A. Pauley, (2013) Cloud Provider Transparency, An Empirical Evaluation, IEEE Computer and Reliability Societies

[24] P. Saripalli, B. Walters, QUIRC,A Qualitative Impact on Risk Assessment Framework for Cloud Computing Security, pp: 280-286,Journal of Cloud Computing (2010).

[25] S. Sengupta, V. Kalgud, V.S. Sharma, Cloud Computing Security Trends & Research Design, IEEE World Congress on Services (2011) 524-553.

[26] S. Subhasini, V. Kavitha, Review: A Survey on Security Issues in Service Delivery Models of Cloud Computing, Journal of Network & Computer Applications 34(1) (2011) 1-11

[27] S. Subhasini, V. Kavitha, A Survey on Security Issues in Service Delivery Models of Cloud Computing, ACM Conference on Computers, Journal of Network and Computer Applications (2014).

[28] A. Ukil, D. Jana, A. DeSarkar, A Security Framework in Cloud Computing Infrastructure, International Journal of Network Security & Its Applications 5(5) (2013) 1-14.

[29] V.J.R. Weinkler, Securing the Cloud: Cloud Computing Security Techniques & Tactics, Waltham: Syngress (2011).

[30] Paul S. Woolly, Identifying Cloud Computing Security Risks, Capstone Report, University of Oregon, Applied Information Management (2011).