Journal of Applied Technology and Innovation (eISSN: 2600-7304)
vol. 1, no. 2, (2017), pp. 79-93

Cloud Testing: Requirements, Tools and Challenges

Ahmad Dahari Bin Jarno
CyberSecurity Malaysia
Mines Resort City, 43300, Seri Kembangan, Selangor, Malaysia
Email: dahari@cybersecurity.my

Shahrin Bin Baharom
CyberSecurity Malaysia
Mines Resort City, 43300, Seri Kembangan, Selangor, Malaysia
Email: shahrin.baharom@cybersecurity.my

Maryam Shahpasand
FSec research centre
Faculty of Computing, Engineering & Technology
Asia Pacific University of Technology & Innovation
Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia
Email: dr.maryam.shahpasand@apu.edu.my

Abstract - Cloud Computing is a technology which gives computation, software, data and storage services over the network. The software industry is laying increased emphasis on Quality Assurance (QA) and Testing requirements for successful product development today. To ensure a high level of security of cloud services and applications, testing is an appropriate approach to detect possible vulnerabilities before real case scenarios occur. Therefore, many public cloud providers revealed the growing number of Testing Centre of Excellence (COE) and software test automation being encouraged by companies.This paper presents a critical review of cloud security testing. Moreover, gaps in recent related publications are revealed, testing tools and offers of software test automation. The prospective research implications are pointed out to foster the understanding and relations of current research fields.

Index Terms - Cloud Computing, Cloud Testing, Security, Vulnerability

1. Introduction

Cloud computing is a trendy and state-of-the-art solution in the information technology sector. Especially, organisations benefit from particular advantages of cloud computing like increased scalability and portability resulting in enhanced efficiency and cost reduction (Singh et al., 2016). Research on the identification of challenges and benefits of cloud computing has been done since 2008 (Buyya et al., 2008; Armbrust et al., 2010;

Riungu-Kalliosaari et al., 2016). In cloud computing, applications are hosted, deployed, and delivered as services over the Internet. New cloud application services can be developed by tailoring existing ones, while hiding the complexity of the underlying implementation. Cloud applications may be able to adapt to changes in their environment, which should be highly secure and reliable. The infrastructure on which cloud applications are built is characterized by power, storage and virtualization. Cloud Computing Security Lab focus on the software testing of the cloud and seeks to formulate new approaches, tools and techniques for improving the testability of cloud based applications.

Cloud testing refers to testing of resources such as hardware, software and etc. that are available on demand basis. Even the testing here can be viewed “as a service”. For cloud services offerings, it is essential to make sure that the services (also defined as product) not only meet its functional requirements but also non-functional requirements. Functional requirements describe the features, functioning, and usage of a product, system and software from the perspective of the product and its user. Although referred to as "requirements," they really are a form of design, albeit high-level. Functional requirements also often are called "functional specifications," and "specification" is a synonym for design. Non-functional requirements are not non-functional at all. Rather, they describe various quality factors, or attributes, which affect the functionality's effectiveness. They do not exist in the abstract but only with respect to relevant functionality. They are often called "ilities," because many end in "ility," such as, usability, reliability, and maintainability.

Cloud testing is one of the newest forms of testing in IT industry. Applications designed for cloud usage run remotely from the Internet. Many cloud applications will have large numbers of users, so performance testing and load testing are particularly important for cloud application. However, cloud applications are also subject to quality problems, security problems, and usability problems. As a general rule the applications intended to operate in the cloud will have a normal set of "ground" tests prior to "cloud" testing, which usually occur at about the same time as integration or system testing.

Security testing is defined as the process of testing specialized towards security, where testing is the process of exercising the system to verify that it satisfies specified requirements and to detect errors. SaaS testing comprises of validating SaaS applications with respect to business workflows, multi-tenancy, integrity, reliability, ease of deployment, scalability, availability, accuracy, deploy ability, ease of use, testability, portability live updating. All these applications are tested with cloud based resources and among the testing criteria mentioned above the focus will be on three key components they are performance, compatibility and security. Security testing is a great resource for identifying and rectifying vulnerabilities or flaws in applications so that they are less susceptible to compromise in the event of cyber-attacks.

2. Cloud Testing Requirements

2.1 Basic Requirements

The following is the 5 major things to consider for cloud testing.

a. Functional Testing
Functional testing of both internet and non-internet applications can be performed using cloud testing. The process of verification against specifications or system requirements is carried out in the cloud instead of on-site software testing.

b. Browser Performance Testing

Finding out thresholds, bottlenecks & limitations is a part of testing. For this, testing performance under a particular workload is necessary. By using cloud testing, it is easy to create such environment and vary the nature of traffic on-demand. This effectively reduces cost and time by simulating thousands of geographically targeted users.

c. Load & Performance Testing
Load testing of an application involves creation of heavy user traffic, and measuring its response. There is also a need to tune the performance of any application to meet certain standards. However, a number of tools are available for that purpose.

d. Latency & Bandwidth Testing
Cloud testing is utilized to measure the latency between the action and the corresponding response for any application after deploying it on cloud and measure the bandwidth capability.

e. Stress Testing
Stress Test is used to determine ability of application to maintain a certain level of effectiveness beyond breaking point. It is essential for any application to work even under excessive stress and maintain stability. Stress testing assures this by creating peak loads using simulators. But the cost of creating such scenarios is enormous. Instead of investing capital in building on-premises testing environments, cloud testing offers an affordable and scalable alternative.

f. Compatibility Testing
Using cloud environment, instances of different Operating Systems can be created on demand, making compatibility testing effortless.

2.2 Requirements in IT Security

Another consideration is the need to decide between white box or black box testing. In black box testing, the penetration tester knows as little about the system as a real-world hacker would know. This is advantageous because, as we discover and exploit vulnerabilities, no one can challenge our report by claiming "an attacker wouldn't know to do that." On the other hand, white box testing is advantageous in that it is much faster. Not only is reconnaissance and server discovery accelerated, it's easier to prioritize test efforts.

A big challenge to cloud security testing can be the lack of application logging to aid in focusing and enhancing your test efforts. Performing security testing in an isolated development environment means we will be able to tail logs and see evidence of your attacks' outcomes. In a cloud environment, we will rarely be grated this level of access. Therefore, we will only be able to gauge attack success by the application's behaviour. Some tests are such that providing input into control "A" on screen "Z" will result in invalid data on page "P". Be familiar with the data flow within our app and expect to have to poke all around the app to complete our testing. In conclusion, security testing in the cloud does change things, but it's not impossible. It's important to plan ahead, to communicate the changes in our test strategy, and to set appropriate expectations with our management. Above all, it is critical to communicate before and during our testing—primarily with our cloud provider, but also with our IT and security organizations.

2.3 Advance Requirements

Testing in a cloud has to not only ensure that the functional requirements are met, but a strong emphasis needs to be laid on non-functional testing as well.

a. Functional Testing

Goes without saying, that functional testing has to be performed to make sure that offering provides the services that the user is paying for. Functional tests ensure that the business requirements are being met. Some of the functional tests are described below.

- **Data Migration Testing:** This makes sure that the several of data modules function correctly with one another, thus making sure that their data in place.

- **Integration Testing:** Here the cloud based solution is to integrate all software tools to ensure the integration between each component and clouds working properly.

- **Interoperability Testing:** Any application must have the flexibility to work without any issues not only in different platforms, but also must work seamlessly when moving from cloud infrastructure to another.

b. Non-Functional Testing

Non-functional tests mainly focus on the web application based tests ensuring that they meet the desired requirements. Here are few forms of non-functional tests discussed below:

- **Availability Testing:** The cloud supervisor/ vendor has to make sure that the cloud is available round the clock. As there could be many mission critical activities going on, the administrator has to make sure that there is no adverse impact to the consumers

- **Multi Tenancy Testing:** Here, multiple users use a cloud offering. Testing must be performed to ensure that there is sufficient security and access control of data when multiple users are using a single instance.

- **Performance Testing:** Verification of the response time needs to be done to ensure that everything is intact even when there is a large number of a request to be satisfied. The network latency is also one of the critical factors to evaluate performance. Also, workload balancing needs to be done when there is a reduction in load, by decommissioning resources. Thus, load and stress testing are done in the cloud offering to make sure applications are performing optimally with increase/decrease in load and stress.

- **Security Testing:** Since with the cloud everything is available anytime, it's essential to make sure that all user sensitive information has no unauthorized access and the privacy of users remains intact. When maintaining the applications in cloud, user data integrity must also be verified.

- **Disaster Recovery Testing:** As already stated in availability testing, the cloud has to be available at all times and if there are any kind of failures like network outages, breakdown due to extreme load, system failures and etc., whilst measure how fast the failure is indicated and any data loss during this period.

3. Cloud Testing Tools

In this section, some of the different tools used in various kinds testing performed in a cloud are mentioned. The details of the tools are out of the scope of this article. Many of the tools are basically used for performance, load, stress testing. Some of these tools below can also be used for:

3.1 Web Functional / Regression Testing Tools:

- **SOASTA CloudTest:** CloudTest makes it easy to test to any level of expected usage – and beyond. A single interface allows to control the ramp and scale of user traffic from locations around the world and measure the effects in real time. Network emulation lets a model to test with multiple connection types. Whether it testing 100 users or a million, the CloudTest platform helps to get the most out of every test by seamlessly spanning dozens of global cloud providers, and simulating web and mobile user traffic more accurately.

- **LoadStorm:** A web-based load testing tool/service from CustomerCentrix, LLC, as a distributed application that leverages Amazon Web Services to scale on demand with processing power and bandwidth as needed. Tests for web and mobile can be built using the tool in such a way as to simulate a large number of different users with unique logins and different tasks.

- **CloudTestGo:** An on-demand Performance Testing solution using JLTT, CSS' home-grown Performance Testing tool. It enables load testing of all products including web and non-web applications and services, in the cloud. It can setup quickly and cost-effectively create a real-world Load Testing environment without having to invest in complex infrastructures, new hardware or expensive software licensing.

- **AppPerfect:** It is a fully Automated Load test, Stress test and Performance Test solution that is easy to use and cost effective. Most application performance and stability issues arise only when the server is stressed with a high user load. AppPerfect Web Load Test helps to design and simulate thousands of users in a realistic manner which can be used to load test at application infrastructure for performance, reliability and scalability.

- **Jmeter:** Java desktop application from the Apache Software Foundation designed to load test functional behaviour and measure performance. Originally designed for testing Web Applications but has since expanded to other test functions; may be used to test performance both on static and dynamic resources (files, Servlets, Perl scripts, Java Objects, Data Bases and Queries, FTP Servers and more). Can be used to simulate a heavy load on a server, network or object to test its strength or to analyze overall performance under different load types; can make a graphical analysis of performance or test server/script/object behaviour under heavy concurrent load.

- **Cloudslueth:** CloudSleuth, a free cloud monitoring service from Compuware, does the detective work on public cloud performance. With identical sample application hosted on several public cloud service provider networks, response time and availability of the application is continuously monitored from over 30 Internet backbone nodes across North America, South America, Europe, and Asia Pacific. The performance data can give a snapshot of user experience of cloud services across the globe.

- **WebdriverIO:** WebdriverIO control a browser or a mobile application with just a few lines of code. It can be test code will look simple, concise and easy to read. The integrated test runner let will write asynchronous commands in a synchronous way so don't need to care about how to handle a Promise to avoid racing conditions.

- **Selenium:** Selenium is a portable software testing framework for web applications. Selenium provides a record/playback tool for authoring tests without learning a test scripting language (Selenium IDE). It also provides a test domain-specific language (Selenese) to write tests in a number of popular programming languages, including C#, Groovy, Java, Perl, PHP, Python, Ruby and Scale.

3.2 Cloud Security Testing Tools

- **Nessus:** Nessus is a network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks. Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans.

- **Wireshark:** Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets and is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

- **Nmap:** Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. It useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

3.3 Load Test and Performance Monitoring Tools

- **Perfecto Mobiles, Keynote (Test center enterprise):** Perfecto Mobile is a global provider of cloud-based testing, automation and monitoring solutions for mobile applications and websites utilizing a wide selection of REAL and emulated mobile devices. Mobile Cloud Platform enables developers and testers to access and control a comprehensive range of the latest mobile smart phones and tablets connected to live networks around the world. Keynote Mobile Testing TCE provides enterprise platform for mobile (manual and automated) testing and service monitoring of enterprise mobile apps and websites. It gives easy remote access to all popular smart phones and tablets. Test developer can create hundreds of automation scripts and leverage them across multiple devices. It also enhances the tests scripts by using Java API to access much functionality of the remote devices. It also integrates with leading test tools like QTP and IBM ALM.* It cans plug-and-play local devices into their desktop computers for manual and automated testing. Devices can also be set-up in an enterprise lab environment (on-premise or in the Keynote Mobile Testing enterprise cloud) for sharing across local and remote teams

- **Monitis:** Monitis is a specialist provider of web and Cloud monitoring services that include website monitoring, site load testing, transaction monitoring, application and database monitoring, Cloud resource monitoring, and server and internal network monitoring within one easy-to-use dashboard. Monitis can provide of choice to increase uptime and user experience of their services and products. Monitis are fast to deploy, feature-rich in technology and provide a comprehensive single-pane view of on-premise and off-premise infrastructure and

- **BrowserMob:** BrowserMob Proxy is a simple utility that makes it easy to capture performance data from browsers, typically written using automation toolkits such as Selenium and Watir. BrowserMob Proxy can capture performance data for web apps (via the HAR format). Used to collect the performance data from the client side.

- **GFI:** GFI Software develops easier, smarter and affordable enterprise-class IT solutions for businesses. Their solutions enable IT administrators to easily and efficiently discover, manage and secure their business networks, systems, applications and communications wherever they exist. GFI is committed to its thousands of customers worldwide to deliver the trusted expertise, right-sized and smartly engineered IT solutions with a strong focus on security excellence. It also gives a complete picture of installed applications; hardware on your network; mobile devices that connect to the Exchange servers; the state of security applications (antivirus, anti-spam, firewalls, etc.); open ports; and any existing shares and services running on machines.

- **CloudHarmony:** CloudHarmony provides objective, impartial and reliable performance analysis to compare cloud services. It to be an impartial and reliable source for objective cloud performance analysis. It not affiliated with or owned by any cloud provider. It publish report on CDN and DNS services, the standard is now 100 percent uptime, while for other services, brief interruptions remain common.

- **InterMapper**: InterMapper is a cross-platform, network monitoring, and network mapping program. It comes with a variety of network probes based on ping, SNMP, http and other network protocols used to monitor the state of networked devices and servers. It displays the status of the devices it monitors in maps or lists. It also supports alarms for devices that have disappeared from the network or which are in a warning state, and can send alerts via email, pager, console alerts, or script execution

- **Blaze Meter**: Self-service, on-demand, cloud-based load testing. Simulate any user scenario for webapps, websites, mobile apps or web services. Launch a single dedicated server or a cluster of 100. Apache JMeter compatible - pre-configured JMeter environments with up to 144 CPU cores and 500 GB of memory. Set geo locations from among choices worldwide. Set up tests, access test results, view test reports, compare past test reports and more, all on a unitary console. Generate traffic using public cloud providers or install the on-premise load generator software on your own machines and test behind the firewall on your internal network. Free tools and resources for tips and tricks to optimize website and app performance.

4. Challenges

As exciting as cloud sounds, all is not hunky-dory here. There are some challenges with relying and using cloud as an infrastructure as well. Let's take a look at some of the primary concerns using the cloud.

Challenge #1: With everything available on demand to any user, security is a primary issue for the businesses as currently there is still a lot of discussion and research going on in the industry to set up security standards. User privacy protection, security standards on cloud, security of applications running within the cloud, security testing techniques are some of the primary issues that need to be addressed in the cloud infrastructure

Challenge #2: Another big challenge is the performance of an application in a cloud: specifically, in private clouds. It will be shared across many users and hence could lead to delays. Also in case of some maintenance or outage related activities, the bandwidth may seem insufficient.

Challenge #3: Sometimes for testing purposes, we require certain configurations: with respect to servers, storage or networking which may not be supported by the cloud provider. This sometimes makes it difficult to emulate customer environments.

Challenge #4: Another commonly faced challenge is with respect to integration testing whereby the testers test the network, database, servers, etc. In such situations, the tester will not have control on the underlying environment. Secondly, the challenge is doubled when there has to be an interaction between these components because the tester will have to anticipate risks like crashes, network breakdown or servers going kaput. Cloud computing has today become one of those "big bangs" in the industry. Most organizations are now leaning to adopting the cloud because of its flexibility, scalability and reduced costs. The following table lists the main challenges in cloud computing environment.

Challenge #5: Having an automatically set testing environment according to user preferences is essential for cloud based software testing but is a challenge to engineers because of the lack of cloud enablement in several existing testing tools. Moreover, several cloud providers offer restricted. Configuration capabilities for their cloud service which leads to constraints in emulating dynamic testing environments.

Challenge #6: Performance testers usually execute their test plans on pre-fixed environments with agreed upon metrics, evaluation parameters, etc. But for cloud testing, the effect of dynamic scalability plays the role of a villain, if you were to ask us. On-demand scalability poses extra loads on testing tools to execute new test cases in real time without prefixed metrics or evaluation statistics.

Challenge #7: With lack of proper control of the underlying cloud environment, testers face a huge challenge there is interaction between these components.

Challenge #8: Due to the lack of universal standards in integrating public resources on the cloud with internal data architectures of organizations, there is a serious challenge to testing teams to maintain dynamic testing environments to offer testing as a service. Changing vendors would lead to the requirement of new solution architectures and platform modifications for test tools to operate smoothly.

Challenge #9: Testing teams often prepare test cases and scenarios with pre-determined data sets but when testing is offered as a dynamic cloud service, then the costs involved in encrypting test data on cloud systems have to be considered since they need to evaluate the security aspects of cloud testing as well.

5. Limitations and challenges on Security Cloud Testing

In the early state of the newly emerged cloud computing paradigm, most researchers focused on a broader and coherent understanding, including definitions, challenges and benefits (Armbrust et al., 2010; Riungu-Kalliosaari et al., 2016). Subsequently, security of cloud environments became one of the most crucial concerns in adopting and using the new technology (Ali et al., 2015; Singh et al., 2016). The recent survey of RightScale Inc. (2016) revealed, that security challenges are the second highest concerns in cloud computing. Distributed systems are possible targets for attacks causing radical extra charges such as data modifications or downtimes. Data loss or leakage represents 24.6% and cloud-related malware 3.4% of threats causing cloud outages (Ko & Lee, 2013). Most of the software security incidents are exploited vulnerabilities. Hence, Akhgar (2016) recommends developing security metrics to identify vulnerabilities. To ensure application security, security testing techniques are important and effective countermeasures for improvement (Felderer et al., 2016). Thus, implemented systems should be tested by the use of analytical techniques and engineering principles to detect security issues as early as possible (Bos et al., 2014). However, according to Shrivastva et al. (2014), is security testing one of the major challenges in cloud testing environments. Besides, Nachiyappan & Justus (2015) indicated that present cloud security testing has many open queries, such as quality assurance and security validation. The authors also stated the challenge of testing security measures in cloud environments. Kumar & Singh (2014) revealed the research issue of performing quality checks within cloud environments. Beyond, Madan et al. (2016) pointed out the need to develop an approach for cloud privacy testing. Although the body of knowledge on cloud testing is growing, the literature review reveals an enormous gap of sophisticated security testing approaches for testing the cloud. Researchers mostly focused on Test as a Service (TaaS) rather than on testing the cloud.

Security of the data is the biggest disadvantage. Storing data in a cloud means the data is, in theory, accessible to anyone and data and code are mostly stored in a remote location beyond an organization's legal and regulatory jurisdiction. Yet another challenge is that some cloud providers offer only limited types of configurations, technology, servers and storage, networking and bandwidth, making it difficult to create real-time test environments. Improper choice of cloud-based use and pricing options is another risk. While some vendors offer pay-as-you-go services, they are only cost-effective when the right plan and service provider are chosen for the anticipated needs (e.g. space vs. RAM vs. bandwidth). Costs can quickly spin out of control if resource estimates differ wildly from actual usage.

Integration testing in clouds - Although we have seen numerous published research papers addressing software integration testing issues and strategies, not much research results have been applied in the real engineering practice. One of the major reasons is the existing software and components are developed without enabling technology and solution to support and facilitate systematic software integration. In a cloud infrastructure, engineers must deal with integration of different SaaS and applications in/over clouds in a black-box view based on their provided APIs and connectivity protocols. This could cause a lot of extra integration costs and difficulties due to the following issues:

- There is a lack of well-defined validation methods and quality assurance standards to address the connectivity protocols, interaction interfaces, and service APIs provided by SaaS and clouds APIs; and
- There is a lack of cost-effective integration solutions and framework to facilitate software application integration and assembly inside clouds and over clouds.

Infrastructure requirements: It is vital that Infrastructure requirements are rigorously set, because the very flexibility that the cloud offers for testing environments can itself be a risk if the requirements for those environments are inappropriate. Results will then be poor and negative perceptions of the cloud as a test environment will result from what was really an inattention to requirements.

6. Summary

Using the cloud for testing is immensely helping organizations to acquire the required tools, software licenses, infrastructures at a very low cost without having to set it up themselves and then worry about its maximum utilization.

For Cloud Security Lab/Test Lab: NeXpose is a tool for auditing cloud infrastructure. It also provides Vulnerability Management for cloud assessment. NeXpose can scan the entire infrastructure, application, database or Virtual Machine to detect vulnerability across them. Vulnerability management tools include the ability to detect and identify assets in an IT infrastructure, detect vulnerabilities, provide descriptions of vulnerabilities as well as links to patches and other forms of remediation, and generate a host of reports -- all from a central console. The other tool will be proposed using SAINT, Burpsuite, NetSkope, Qualys, Retina, VIM and GFI LanGuard.

Though offering testing as a service through cloud based automation throws up a lot of challenges down the line, organizations continue to focus on this trend, thanks to its numerous benefits. This is evident from another World Quality Report insight which shows that the share of testing budgets for transformational projects has increased from 41% in 2011 to 43 % in 2013.

The core philosophy behind a majority of the challenges stated is because of the underlying characteristics of the cloud platform. A closely-knit approach with the cloud service provider can help to minimize this risk considerably as testing teams can built a solid cloud platform to deploy their tools.

Partnering with a reliable testing service provider is the perfect answer for organizations to eliminate testing related challenges and overheads especially with regards to automated test services. With decades of experience in offering world class testing services to a plethora of global giants, Cigniti is your road to eliminating testing overheads once and for all. Moreover, functional testing may take specific forms such as:

i. User acceptance testing: Also, known as beta testing, this category of testing evaluates an application's performance in the real world among its intended audience. It has the added benefits of helping to minimize change requests down the road and keeping overall project costs to a minimum. User acceptance testing can also build goodwill with end users and improve their satisfaction with the software in question.

ii. Interoperability testing: With interoperability testing, testers are looking to see that programs work with others on a variety of platforms. Many applications are now cross-platform and must meet mission-critical requirements such as exchanging data between different medical records systems. With the emergence of cloud computing, this type of testing may also check whether software can hand off workloads across both cloud and on-premises infrastructure.

iii. System verification testing: Here we get into slightly more technical testing. System verification may include code audits, revisions to any documentation, and testing of hardware and software components under normal as well as adverse environmental conditions. Voting machines are a prime example of appliances that require thorough system verification.

iv. How has the emergence of cloud computing affected the general practice of functional testing? We can already see signs of its influence on the applications testing that have been "hybridized," i.e. designed to leverage both internal and external (public cloud) IT resources. More specifically, these programs require careful attention to the interoperability of all the systems involved, as we noted above.

The cloud computing paradigm is a nascent technology with many benefits for organisations. On the other side, security of clouds is still one of the major concerns of clients to adopt and use the new computing paradigm. The review of the recent academic literature revealed that cloud security in general is still a major concern in the industry and academics alike. To make it clearer, a data breach revealed vulnerabilities at Yahoo! Inc., whereby 32 million user accounts were accessed by forged cookies to log in without a password (Yahoo! Inc., 2017). Another example is the Distributed Denial-of-Service (DDoS) attack against Dyn, which was just recently acquired by Oracle, causing a major breakdown of its Domain Name System (DNS) servers also affecting enterprises relying on SaaS (York, 2016). Besides, the survey unfolded that security and related testing activities are current research fields with a lot of open queries. Thus, many academic papers have been published to identify and address challenges in cloud security, vulnerabilities and threats. However, most of the researchers focused on TaaS rather than on testing the cloud. Hence, this survey reveals a current gap in academic research in terms of testing the cloud security using an appropriate approach for SaaS applications. The authors imply to conduct further research on cloud security testing approaches, especially in SaaS and public environments, whereby internal and external factors need to be differentially considered.

References

Zafar, F., Khan, A., Ur, S., Malik, R., Ahmed, M., Anjum, A., Khan, M.I., Javed, N., Alam, M. & Jamil, F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. Computers & Security. 65. p.pp. 29–49.

Yahoo! Inc. (2017). Annual Report. [Online]. Delaware. Available from: https://investor.yahoo.net/secfiling.cfm?filingID=1193125-17-65791&CIK=1011006&soc_src=mail&soc_trk=ma. [Accessed: 27 March 2017].

Vohradsky, D. (n.d.). Cloud Risk - 10 Principles and a Framework for Assessment. Retrieved from http://www.isaca.org/Journal/archives/2012/Volume-5/Pages/Cloud-Risk-10-Principles-and-a-Framework-for-Assessment.aspx

The 10 Worst Cloud Outages (and What We Can Learn From Them). (2011, June 27). Retrieved from http://www.infoworld.com

Security of OpenStack Cloud. (n.d.). Retrieved from http://www.stratoscale.com

Security Authorization Process Guide. (n.d.).

Roadmap NIST, cloud application security and operations policy. (2015, July).

Red-hat OpenStack platform. (n.d.).

Private Cloud Providers Comparison. (n.d.). Retrieved from http://www.tomsitpro.com

National standard for cloud NIST. (n.d.).

Mirantis Reference Architecture VHC for Cloud Native Apps. (2016, March 3).

ISACA. (2011). IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. Retrieved from http://www.isaca.org/cloud

ISACA. (2010). Business Model for Information Security. Retrieved from http://www.isaca.org/bmis

Goldsmith, R. F. (n.d.). Search software quality. Retrieved from http://searchsoftwarequality.techtarget.com/answer/Functional-vs-non-functional-requirements-what-is-the-difference

Enisa. (2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security. Retrieved from http://www.enisa.europa.eu

Cloud Pentest. (n.d.).

Boucher. (2013). Boucher Testing Challenge.

Boucher, P. f. (n.d.). Security Authorization Process Guide Security Software.

Hofmann, D. W. (2010, November). Cloud Computing: The Limits of Public Clouds for Business Applications', IEEE Internet Computing.

Blake, M. B. (2010, November). Service-Oriented Computing and Cloud Computing: Challenges and Opportunities', IEEE Internet Computing.

Architecture, N. S. (2013, May 15). Architecture, NIST Security.

Boucher. (2013, June 18). Standard Roadmap NIST.

Penetration Testing Guidance. (2015, March).

Kirsch, B. (2015, April 7). Private cloud provider comparison. Retrieved from http://www.tomsitpro.com/articles/private-cloud-providers-comparison,2-899.html

Roadmap NIST. (July, 2015).

Julie Mathew, L. K. (2016, August 22). Best practice configure IBM cloud manager with OpenStack. Retrieved from http://www.ibm.com/developerworks/cloud/library/cl-best-practices-configure-ibm-cloud-manager-with-openstack-trs/index.html

York, K. (2016). Dyn Statement on 10/21/2016 DDoS Attack. [Online]. 2016. Available from: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/. [Accessed: 27 March 2017].