Review Article

International Journal of Advanced Technology and Engineering Exploration, Vol 5(48)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2018.C02

Modular responsibility distribution for vulnerability management process

Shaz Alam[1*] and Mohd Muqeem[2]
Research Scholar, Department of Computer Application, Integral University, Lucknow, India[1]
Associate Professor, Department of Computer Application, Integral University, Lucknow, India[2]

Abstract
The world of computing rapidly changed from mainframe to client server architecture and towards the new world of cloud computing. This new generation of computing has tremendous advantages over traditional offerings. Irrespective of all, security is one of the biggest hurdles which hold the migration of business towards cloud. Main reason is client unawareness about the security counters and their roles. Security control can be normally implemented around three levels such as vulnerability, attack and threat. It is better to identify and pre analyse the concerns at earliest level. The purpose of research is to visualize the vulnerability management process in the modular form and make a transparent responsibility picture for each actor. In the end of the research a new term threshold limit was highlighted in vulnerability life cycle.

Keywords
Cloud security, Vulnerability, Vulnerability management.

1.Introduction
From beginning, experts have made significant efforts to reduce the hardware dependency. Cloud computing is among dream concepts for the realisation of the resources from remote location. It has tremendous offering not only limited to provide hardware independence but also bring the storage, software application independence for the organisation [1]. Irrespective of all, many organisations lose trust to migrate business over cloud due to its security reason [2]. Main reason for security concern is client unawareness about the existing security counter and their roles. In cloud architecture, all the resources of individual organisation are maintained by the cloud provider. It always raised question of trust on provider security abilities. But it does not imply that, cloud provider is always responsible for all the causes. In somewhat sense client is also equally responsible to have the complete information about the security counters. To maintain the trust metrics between provider and user, it is necessary to make the vulnerability management process transparent with defined roles for both the actors [3]. Security control normally implement at three levels such as vulnerability, attack and threat. As we all know, all three level are highly correlated to each other [4]. So it is better to pre analyse the cause at earliest level.

*Author for correspondence

Main aim of the paper is in two folds one is to give a modular form to vulnerability management process and second is to define responsibility of actors to manage different modules. This may act as a guideline to bring the appropriate solution on time. It helps us to maintain the trust between cloud provider and user with exact responsibility transparency. This paper snapshot is divided into three sections. Section 1 describes all the module should be maintained at provider side, Section 2 describes module of responsibility for client organisation to nullify the existing vulnerability impact. Section 3 consists of final result and conclusion.

2.Provider site management
Cloud computing is the concept consisting of two important actors one is cloud provider, and second is individual client organisation. Both the actors are equally responsible to manage the existing flaws [5]. This section briefly explains the modules of responsibilities for cloud provider. There are three important modules.

- Monitoring module
- Development module
- Reporting module

All the above three modules at provider are highly correlated with each other. Monitoring module is responsible for highlighting newly identified system or network flaw and its proper verification and

analysis. Development module is responsible for timely generation of patch for the issues reported by monitoring module. Reporting module is the most important part as it provides the access to existing problem and its solution details to client organization.

2.1Monitoring module

A rough layout of the monitoring module is illustrated in *Figure 1*. It consist of three important steps one is to gather the information timely, second is to verify its existence and last one its impact over the cloud. Obviously to provide an effective solution to a problem, it should be well defined and understandable. All cloud providers should implement a separate monitoring module. The purpose is very clear, to timely identify the problem, verify its existence and proper severity analysis using user guide [6]. It is managed by the group of internal expert, researcher, hacker's community or client organisation reporting volume. All the information gathered in this module will report at restricted access database and forward to patch development module. The purpose of restricted access database is to provide the access to significant most actors who are highly getting affected with this [7, 8]. This is the most important functioning module in the process of vulnerability management. This module consists of four very important steps such as monitoring, verification, impact analysis and bug filling report.

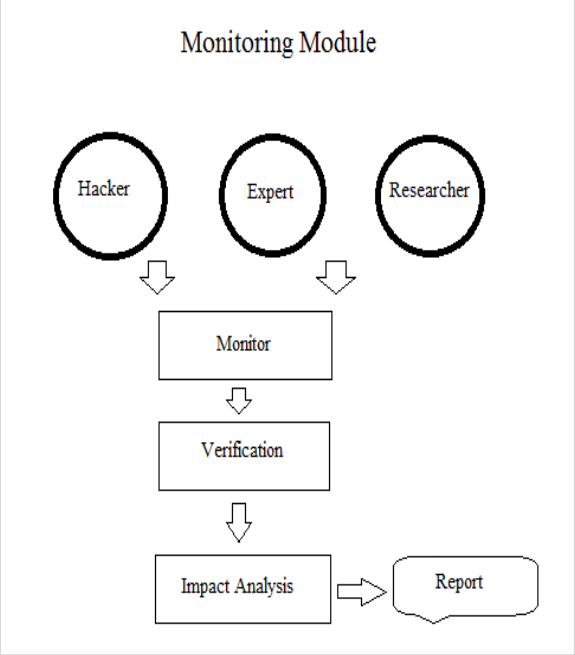

Figure 1 Skelton of monitoring module

2.2Development module

Figure 2 illustrated layout of the development module in which a new term threshold limit is introduced with the aim to release the vulnerability information publically after an specified time either patch is developed on time or not. This module is managed by the team of internal dedicated experts for patch generation. It works on three important functional domains like development of patch, testing of patch validity and reporting. Most of the cloud provider prefers not to disclose the vulnerability before its patch development. But due to economy of issues and lack of expertise, it happened many times that patch may not generate on time within the specified disclosure time as per vulnerability life cycle [9]. In vulnerability life cycle, to reduce the impact of grey risk zone want to introduce a new term "threshold extended limit". This term has two fold aims one is to provide more flexibility to provider to generate patch on time and second is to restrict the provider to disclose the details after a specified limit. Threshold extended limit is defined as a limit decided by the cloud provider itself up to which he should wait for patch generation. After the specified threshold extended limit either the patch is developed or not, it should be disclosed publically through various channels. Cloud provider generally does not prefer to disclose vulnerability before its patch generation. The main reason is to restrict the access to lacking without its solution to malicious actors [9]. This is a challenging area for the provider to ensure the generation of patches on time. To understand about the severity of the problem, consider the vulnerability life cycle model explained in the paper [9]. In vulnerability life cycle it was noticed that, there is enough duration between vulnerability disclosure and patch time in majority of cases. It makes the lacking of the system publically available without the appropriate patch. It is highly recommended for the provider does not disclose the vulnerability before its patch if possible. If not possible to generate patch on time, then should enforce agreement between provider and public database channels to restrict or control over the access of such information via publically available database. It is the most important part of the vulnerability management process (VMP). It let the provider to think over enhancing the abilities of expertise to generate patch on time and to build a strong agreement with the public access database to provide control access.

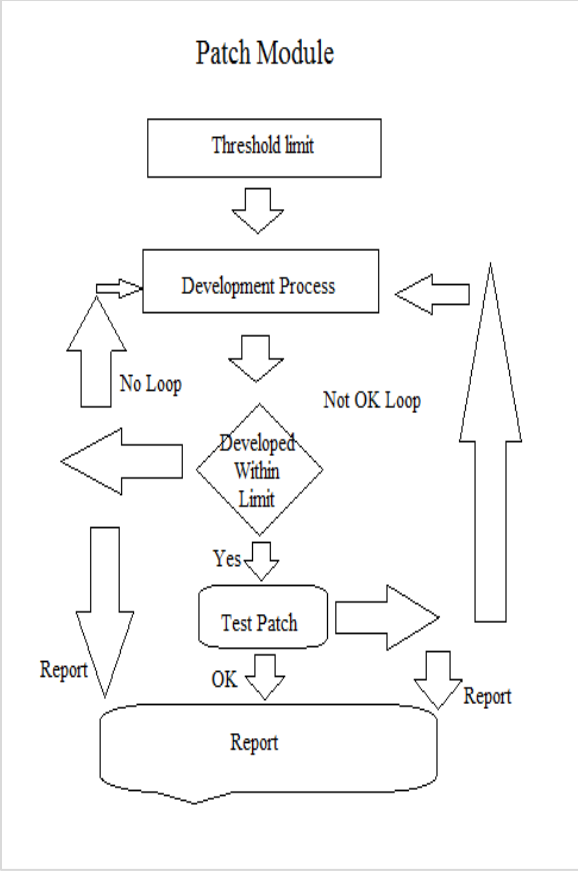

Figure 2 Development module

2.3Reporting module

Figure 3 illustrated layout of the reporting module which is generally connected with two types of databases one is easily accessible and other one has restricted access. It receives the information from monitoring and development module stores it into these databases as per the rules. Reporting Module is generally used to announce the details about the vulnerabilities either in restricted access database or publically accessed database.

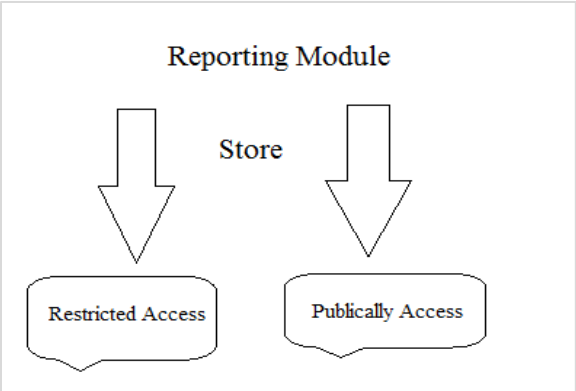

Figure 3 Reporting module

3.Client site management

Cloud provider is responsible for timely identification of flaws in network or software, generate appropriate patch and reported to the existing channels like national vulnerability database (NVD), open source vulnerability database (OSVDB) etc. [9]. Now it is the responsibility of client to install an appropriate scanner in scanning module. This scanning module scans the client architecture using the publically available channel to report about the flaws with their solution recommendation.

As per the study of vulnerability life cycle, it was noticed that there is always enough duration between patch time and its inclusion [9].This duration comes under the category of white attack risk that can be easily removable with the help of timely patch information for existing lacking. It is the sole responsibility of the cloud user to implement appropriate scanner structure to get these updates soon.

Figure 4 illustrated layout of the scanning module which is present at client site. This module consists of one main component known as scanner to scan the network or cloud to generate the timely report of vulnerabilities to install appropriate solution. It is highly recommended to select or deploy most appropriate for these tasks as per the requirement.

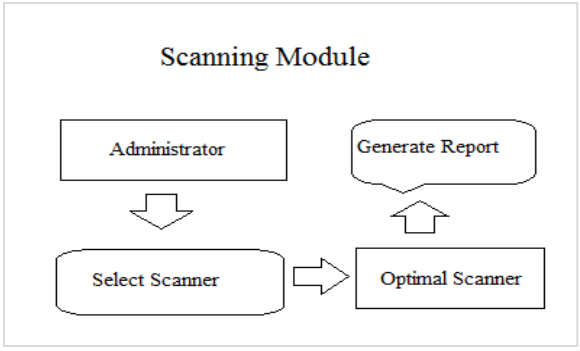

Figure 4 Scanning module

4.Result and discussion

This research visualised the process of vulnerability management in modular form.

- Three modules are listed under the sole responsibility of cloud provider while one is listed under the section of client organisation.
- It helps us to separate the roles and responsibilities for cloud provider and client organisation.

- Based on all the analysis of different literature in vulnerability life cycle a new term threshold limit is introduced in development module.

5.Conclusion and future work

With the help of all above description, would like to highlights few recommendations, core challenges and limitation in modules. These recommendation, limitation and challenges are as.

- Limitation of expertise to generate patch on time.
- Existing scanners normally consider the publically access database for reporting in scanning module
- Recommend to include the concept of "extended threshold limit" with two fold aim to reduce the impact of grey attack zone in vulnerability life cycle.
- Recommend to support scanner switching automate process of scanning in scanning module to reduce the impact of white attack zone in vulnerability life cycle.
- Recommend to make a strong agreement with publically access database to provide control access.

Acknowledgment

This work is acknowledged by Integral University manuscript No IU/R&D/2018-MCN000410.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Zhang Q, Cheng L, Boutaba R. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications. 2010; 1(1):7-18.
[2] Zhang X, Wuwong N, Li H, Zhang X. Information security risk management framework for the cloud computing environments. In international conference on computer and information technology 2010 (pp. 1328-34). IEEE.
[3] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. 2012; 28(3):583-92.
[4] Alam S, Muqeem M, Khan SA. Review on security aspects for cloud architecture. International Journal of Electrical and Computer Engineering. 2018; 8(5): 3129-39.
[5] Kandukuri BR, Rakshit A. Cloud security issues. In international conference on services computing 2009 (pp. 517-20). IEEE.
[6] https://www.first.org/cvss/userguide. Accessed 5 January 2018.
[7] https://www.bugzilla.org. Accessed 10 January 2018.
[8] https://www.exploit-db.com/. Accessed 15 January 2018.
[9] Torkura KA, Cheng F, Meinel C. A proposed framework for proactive vulnerability assessments in cloud deployments. In ICITST 2015 (pp. 51-7).

Shaz Alam completed his graduation BSc. (CPM) from Lucknow University and post-Graduation MSc. Tech (IMCA) from Jamia Millia Islamia New Delhi and currently deployed as an active Research Scholar in Department of Computer Application, Integral University Lucknow and has 5 year of experience as Corporate Trainer in Centre for Career Guidance & Development Integral University Lucknow. His area of interest includes Cloud Computing, Java Technology, and Formula Independent Approaches.
Email: shaz.alam62@gmail.com

Dr. Mohd. Muqeem has completed his doctoral from Integral University, Lucknow. He is presently working as Associate Professor in the Department of Computer Application, Integral University Lucknow. He has more than 14 year of experience in the field of Academics. He is currently working in the area requirement Engineering and Web Technologies. He has published paper in reputed journal with impact factor. He is a member of CSI, ISTE, CSTA, IAENG and other societies.