International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.4, pp : 395-399 1April 2014

Cloud Computing Security Challenges and their Compromised Attributes

[1]Muhammad Aamir, [2]Prof. Xiang Hong,[3]Atif Ali Wagan,[4]Muhammad Tahir,[5]M.Asif
[1,2,3,4]School of Software Engineering Chongqing University China
[5]School of Electrical Engineering Chongqing University China
Corresponding Email: aamirshaikh86@hotmail.com

Abstract— **Cloud computing is a revolutionary modern computing platform in the field of information technology. It has promptly became famous and considered the emerging field of recent times due to its potential for better utilization of computer resources like flexible IT architecture, scalability, availability, fault tolerance, computational power, computational platforms, storage and applications and to cut down costs of operations and supports. Nevertheless the security is the biggest threat to its consumers and more research needs to be done to deal with this security breach. In this paper, the better understanding of cloud computing and their security is discussed. And I investigated the major cloud computing security challenges, examined their compromised attributes and delivers the most threaten attribute to cloud computing.**

Keywords— **Cloud Computing, Security Challenges, Attributes, SLR.**

I. Introduction

The outcomes of contemporary technologies depend on its efficiency, competence, performance, its feature of user friendliness and most importantly its level of information security and control.

Cloud computing is a new model which is taking place at very high speed in Information Technology services and became a prominent model of present days due to its fascinating features which are elastic, shared resources, immense scalability, pay as you go, self-provision of resources and zero maintenance cost.

Cloud computing can be implemented in an extensive variety of architectures, within different service and deployment models where the services availability is the responsibility of service provider , and it can also be implemented with different technologies and software design approaches.

Cloud computing is self-determining computing technology which is entirely different from grid and other computing technologies and Google apps is the greatest example of it.

Cloud Computing makes novel progress in processors, virtualization technology, storage, broadband Internet connection, and fast, economical servers have combined to make the cloud a more credible solution.

However several researchers have attempted to describe cloud computing and the definition all agreed upon didn't come up yet. But the most appropriate definition which is considered a standard definition presented by the federal technology agency "National Institute of Standards and Technology" shortly NIST:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1].

According to the NIST definition numerous cloud computing key characteristics include; rapid elasticity, broad network access, on demand self service, resource pooling, metered service and multi tenacity that are advocated by "Cloud Security Alliance" shortly CSA.

The three key modes of service offered in cloud computing is [1]:

Software as a Service:
It allows the user to utilize the hosted services on server according to their requirements, and the cloud users are responsible for controlling configurations of the applications.

Platform as a Service:
The hosting of environment is in charge of user and users are allowed to place their customized applications on cloud server and they are allowed to use development tools to develop their applications.

Infrastructure as a Service:
The cloud user in charge of controlling all services except data centre infrastructure and all computing resources such as storage, virtual machines processing, network capacity and others provided on demand over internet except data centre infrastructure.

Further, according to the NIST classification, the cloud model is composed of four core deployment models:

Public clouds:
The cloud models accessible to all common, public and big industrial organizations.

Community clouds:
The cloud models which serve number of organizations or groups specifically and it may be managed by more than one organizations or group.

Private clouds:
The cloud models bound to particular group or organization with multiple users. It might be managed, and controlled by the single organization, and grouping of them.

Hybrid clouds:
The cloud models combination of two or more clouds of deployment model.

Cloud computing is rapidly taking up since past few years, and its demand is relatively increasing. Cloud computing is an emerging technology and gaining popularity in the field of information

technology and growing area in IT security space. The foremost Cloud providers present in the recent marketplace are Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Sales force, and Rack space and there are many different vendors offering different Cloud services.

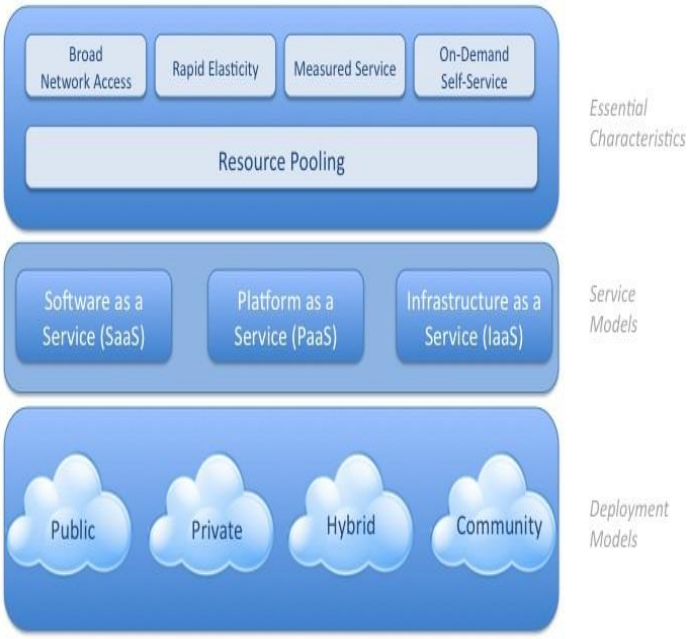

Figure: 1 NIST Visual Model of Cloud Computing

II. Cloud Computing Security Significance

The cloud computing is the promising development platform of IT industry which provides organizations with an efficient, flexible and cost effective substitutes to host their resources. Cloud computing delivers various advantages to the organizations who decide to adopt it.

Regardless of potential benefits to the organizations in implementing cloud model, there are several issues which are threat to the cloud consumers and that impact the model reliability and passiveness. Cloud security is the main fear that hinders the implementation of the cloud computing model and it is the key prerequisite for any service which presented cloud computing platform.

To cope with the security is not an easy task, it is not a minute challenge and there are several security challenges which are threats from different factors and levels and it is obvious that the security concerns has played the main significant role in hindering cloud computing. In this paper, I identify the security challenges, their compromised attributes and find the most influential attribute which would be the toughest obstacle to overcome.

The factors such as a computing on demand, storage on demand, elastic computing, virtualization requirement, and multi processing which makes the cloud dynamic and multifaceted. Because of these features it is hard and premeditated to apply the exact security technique at the exact places.

Cloud computing offers a novel business model for organizations to implement IT services with no in advance investment. Regardless of the potential gains accomplished from the cloud computing, the organizations are unhurried in admitting it due to security issues and challenges related with it.

Due to cloud's very nature cloud security is one of the major issues which obstruct its growth and probably the biggest reason why organizations fear to move their data to cloud and has become priority concern for organizations.

The cloud users and providers are showing their keen interest in cloud computing and both are willing to use it, with a condition which guarantees that their data and information will remain confidential and protected [2].

The popularity of cloud computing is largely due to the factuality that various enterprise applications and data are moving into cloud platforms; nevertheless, inadequacy of security is still the key hurdle for cloud implementation [3].

To understand the need to keep the cloud secure, the not-for-profit organization is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholder's Cloud Security Alliance (CSA) is formed with a mission to promote the use of the best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing [4].

International Data Corporation shortly IDC an American market research, analysis and advisory firm conducted surveys in 2008 and 2009 successively, amongst senior business executives and IT professionals regarding the challenges/issues which mainly affect the performance of cloud computing.

According to the survey 2008, respondents rated 74.6% to security and it shows security is the biggest concern emerged in cloud service [5].

In the survey year of 2009, the result reveals many of the same challenges but the respondents rated security topped with 87.5% masses which declares its importance compared to other cloud services challenges.

On January.20, 2010 at the Brookings Institute forum on Cloud Computing for business, Brad Smith Microsoft General Counsel and the Senior Vice President conveyed a very important message.

Throughout his crucial speech to the forum, he brought to light data from a survey amongst business leaders and the general population about their measuring attitude on cloud computing which is organized by Microsoft.

The survey uncovered that 86 percent of business leaders chief concern is potential of cloud computing and 58 percent of the general population also believe the same, while other more than 90 percent of the same people are worried about cloud computing security, privacy and access for their personal information and data in the cloud [6].

III. Methodology

In this research work, the method, systematic literature review shortly SLR has been chosen in order to analyze the on hand literature concerning the security issues of cloud computing and to answer the designed research question: what are the cloud computing security challenges and their compromised attributes? And mention the most threaten attribute to its security.

Most of the earlier research works were done with conventional literature review which has low scientific value due to non-rigorous and unfair approach, where the systematic literature review has is of highly defined characteristics with more clear scientific perspective.

In this paper we have undertaken the systematic literature review (SLR) as a primary research method and the guidelines and

systematic process by Kitchenham is adopted to conduct this research work [7].

A Systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, topic or phenomenon of interest and their primary aim is to outline a search strategy to find out the primary studies to answer the research questions [7].

The view of the research methods which are used to answer the research questions is shown in figure 2.

Figure: 2 Research Design

The most important features that distinguish a systematic literature review from a conventional literature review are [7]:

- Particular question addressed by defining a review protocol in systematic literature review.
- A search strategy defines in order to attain as much of the relevant information in Systematic literature review.
- The inclusion and exclusion criteria are requiring evaluating each potential main study Systematic literature review.

Systematic review is carried out mostly in three phases:

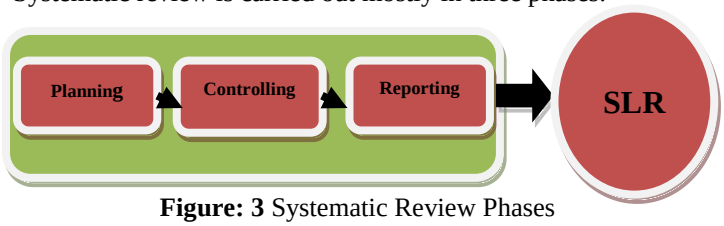

Figure: 3 Systematic Review Phases

In order to attain the research objectives, research question is developed mentioned above. The most important intend of research questions is to recognize the cloud security challenges and their compromised attributes.

PICO criteria are used to explain keywords which have impact on this research. The PICO is an acronym which stands for Population Intervention Comparison Outcomes. It is criteria of placing a search strategy together that permits to obtain a further proof based approach to literature searching [7].

Population:

The population might be any of the specific role, application and area. In this research "Cloud Computing" has chosen as Population.

Intervention:

The intervention is the tool or technology or procedure that addresses an exact concern. In this research "Security" is an intervention.

Comparison:

This is the tool or technology or procedure with which intervention is being compared. In this research, we are not comparing any of the technology or procedure.

Outcomes:

Outcomes are supposed to relate to factors of importance of specific tool or technology. All related outcomes should be particular and different security challenges and their compromised attributes are the outcomes of this research.

The quality assessment is done in order to make sure that the proper and related studies were integrated throughout the SLR and must accomplish the overall aim and research objectives.

A review protocol states the methods that are used to carry out an exact systematic review [7].

In this research the SLR is carried out to determine the published papers related to the security challenges and their compromised attributes. In order to attain the research objectives the related research papers selected, by following the selection criteria as mentioned by Kitchenham [7].

During the SRL, to identify the related research papers, required information and to ensure that the selected material is relevant to our research work the following search string was constructed the search string ((Cloud Computing) AND (security) AND (issues* OR threats* OR challenges*)).

Then search was conducted from four databases which include IEEE Xplore, Springer link, Science direct and Scopus using search string which provided number of papers, to filter the papers which do not contain Irrelevant information the criteria of exclusion is done and which do contain relevant information the criteria of inclusion is done which is necessary to assess our potential primary study.

IV. Results and Analysis

In the process of SLR, the number of relevant papers has extracted to meet the objectives of the research from the huge number of papers published.

Data analysis is the method of collection and summarization the results of the studies. And these methods are used to structure the data properly based on the findings.

In our research, the Narrative Analysis for analyzing the results is used. Narrative analysis is a method of non-quantitative synthesis which represents the extracted information about studies should be tabulated in a manner consistent with the review questions.

From the analysis, 62 security challenges has identified throughout the SLR. The complete description of these challenges is presented in Table A.

Nos.	Challenges	Compromised Attributes
1	WS-Security	Integrity, Confidentiality
2	Account or service hijacking	Confidentiality
3	Limited Audit ability	Audibility
4	Longer Chain of Trust	Security
5	Data scavenging	Availability
6	Customer-data manipulation	Integrity
7	XML-related attacks	Integrity
8	Browser Security	Security
9	Dictionary attacks	Security
10	VM security	Confidentiality ,Integrity
11	input validation attack	Confidentiality , Integrity
12	Computer hardware security	Confidentiality
13	VM escape	Integrity
14	VM hopping	Confidentiality
15	Sniffing/Spoofing virtual network	Security
16	Data management security	Confidentiality
17	Network transport security	Integrity
18	Data storage security	Security , Integrity , Availability
19	Phishing attack	Confidentiality
20	wrapping attack	Integrity
21	Injection Attack	Availability
22	IP Spoofing	Confidentiality
23	Tampering	Integrity
24	Repudiation	Audibility
25	Information Disclosure	Confidentiality
26	Denial of Service	Availability
27	Elevation of Privilege	Confidentiality
28	Physical security	Security, Availability
29	WLAN‟s security	Usability, Accountability
30	Direct attacking method	Confidentiality
31	Replay attack	Integrity
32	Man-in-the-middle attack	Availability, Integrity
33	Reflection attack	Confidentiality
34	Interleaving attack	Integrity, Confidentiality
35	Timeliness attack	Usability, Availability
36	Self-adaptive storage resource management	Integrity, Confidentiality
37	Client monitoring and security	Security
38	Lack of trust	Confidentiality
39	Weak Service Level Agreements (SLAs)	Availability, Confidentiality
40	Perceived Lack of Reliability	Availability
41	Auditing	Security, Confidentiality
42	Back-Door	Usability
43	TCP Hijacking	Confidentiality, Integrity
44	Social Engineering	Confidentiality
45	Dumpster Diving	Availability
46	Password Guessing	Confidentiality
47	Trojan Horses and Malware	Usability
48	Completeness	Availability
49	Roll back attack	Availability, Usability
50	Fairness	Confidentiality
51	Data Loss or Leakage	Availability
52	Computer Network Attack	Integrity, Confidentiality
53	Denial of service attack	Availability
54	Service Availability	Availability
55	Data Privacy	Confidentiality
56	Data security	Security
57	Network security	Integrity, Security
58	Data locality	Reliability
59	Data integrity	Integrity
60	Data segregation	Security, Confidentiality
61	Data Backups	Availability
62	Data manipulation	Availability, Integrity

Table A: List of Challenges and Compromised Attributes

And it is found that Confidentiality is the most threaten compromised attribute in the security of cloud computing in contrast to others attributes. The result is shown below in the figure 4.

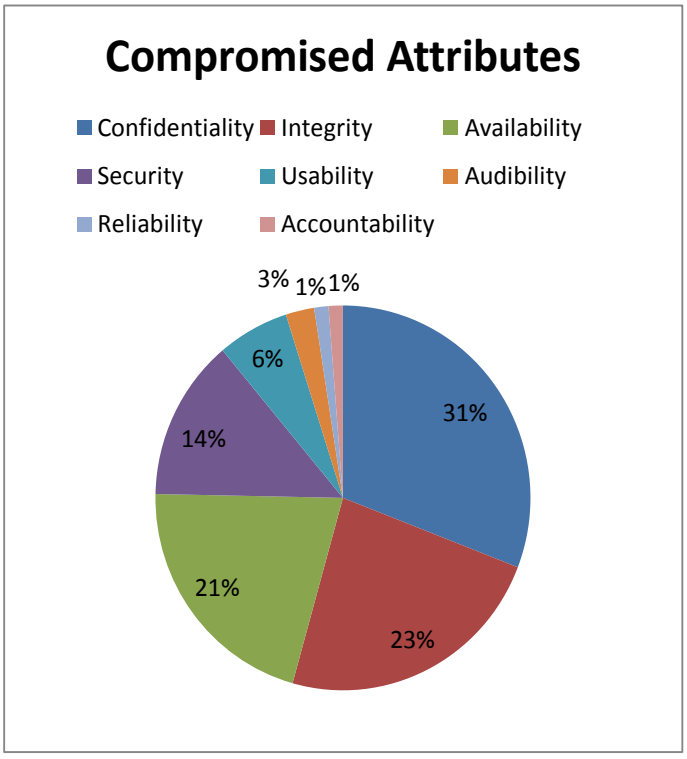

Figure: 4 Compromised Attributes

IV. Conclusion

Cloud computing is the rapidly growing and adopting technologies of recent times. It provides plentiful potential benefits; despite numerous security challenges.

The paper efforts to bring to light the security challenges of cloud computing, their compromised attributes and mentioned the most threaten attribute. The numerous security challenges have been identified has strong impact on cloud users, and providers of cloud computing and it is found that compromised attribute confidentiality, is most threatening attribute in security of cloud computing.

As the cloud computing technology is improving continuously, the new security challenges have to be faced in future too. It is necessary for the future, the users and providers has to be more risk aware , security aware and should have potential to face and cope with upcoming challenges, in order to protect their information.

Acknowledgement

The authors are thankful to Prof. Xiang Hong for his valuable suggestions and support.

References

[1]The NIST Definition of Cloud Computing Peter Mell Timothy Grance NIST Special Publication 800-145,2011.

[2]Eystein Mathisen, "Security Challenges and Solutions in Cloud Computing", 5th IEEE International Conferenceon Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.

[3]Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing Cloud computing Environment against DDoS Attacks", IEEE, , pp. 1-5,2011.

[4]https://cloudsecurityalliance.org.

[5]Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, pp. 214-216,2011.

[6]http://www.microsoft.com/en-us/news/press/2010/jan10/1-20brookingspr.aspx.

[7]Kitchenham B, Charters S. ,Guidelines for performing Systematic Literature Reviews in Software Engineering, Keele University and Durham University Joint report,2007.