Vol. 5, No. 3 March 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Cloud Computing and Associated Mitigation Techniques: A Security Perspective

[1]Muhammad Aamir, [2]Xiang Hong, [3]Muhammad Tahir, [4] Atif Ali Wagan
[1, 3, 4]Student, School of Software Engineering, Chongqing University, P.RChina
[2]Prof. Dr., School of Software Engineering, Chongqing University, P.R China

E-mail: [1]aamirshaikh86@hotmail.com, [3]muhammad.tahir.shaikh@gmail.com

ABSTRACT

Cloud Computing is the contemporary technology in the field of Information Technology. It is rapidly turning into one of the most prominent technologies due to its growing and revolutionary nature in recent times. It assures to delivers a wide range of resources like flexible IT architecture, scalability, availability, fault tolerance, computational power, computational platforms, storage and applications to consumers using internet in a low cost. On the other hand, there are various issues need to be discussed and one of the major challenges faced by the Cloud Computing is security. This paper presents a better understanding of Cloud Computing and its security, and identifies the Cloud Computing mitigating techniques and their impact on security.

Keywords: *Cloud Computing, Mitigating Techniques, Security, SLR*

1. INTRODUCTION

The Cloud Computing technology is rising rapidly in recent times due to its attractive features; it is applied extensively in the industrial community, businesses, consumer services, academics and government organizations [1].

Numerous definitions are proposed and available in the literature of Cloud Computing, and the most appropriate of which is considered a standard definition presented by 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"[5].

Cloud Computing is the foundation of numerous features which are elastic, shared resources, immense scalability, pay as you go, and self-provision of resources, it 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 [3].

The primary objective of Cloud Computing is the finest use of distributed resources, mingle them to achieve higher throughput and be capable to resolve large scale computation dilemmas [4].

Based on NIST definition, the Cloud Computing has the following main important characteristics: on demand self service, broad network access, resource pooling, rapid elasticity, metered service and multi tenacity advocated by Cloud Security Alliance shortly CSA.

There are also three key modes of service which are software as a service shortly SAAS, only the cloud user is responsible for controlling configurations of the applications; platform as a service shortly PAAS, hosting of environment is be in charge of user; and infrastructure as a service shortly IAAS, the cloud user in charge of controlling all except datacenter infrastructure.

Moreover, the four core deployment models which are public clouds; which is accessible to all common public and or big industrial organizations; community clouds, serve number of organizations or groups; private clouds, bounded to a particular groups organizations; and hybrid clouds, a mixture of two or more clouds of deployment model.

Cloud Computing is rapidly growing field since past few years, and its demand is relatively increasing. The renowned Cloud providers on hand in the market are Amazon, Google and Microsoft. IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Sales force, Rack space and many more. The Cloud Computing is one of the significant technical learning roadway platforms, the platform yet to have numerous problems to be resolved, amongst which security is the toughest obstacle to overcome.

Being the users of Cloud Computing platform, client's data has to be stored in the cloud. Its security is a major issue to be dealt with which plays an important role of gaining and maintaining customers trust in Cloud Computing services and hence is vital for its development [2].

The Cloud Computing market is increasing very fast, in 2010 it was USD 68 million and will reach to 148 billion in 2014, this revenue imply that Cloud Computing is a very promising platform and will make more impact on development of information technology [1].

Vol. 5, No. 3 March 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

However, beside development, research, and application of cloud computing, the security problems appeared to be a major issue in its development. In cloud computing, or in any online environment, an important component of strong privacy safeguards is security and is one of the biggest concerns among its user.

The cloud users and cloud 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 [6].

Cloud security is essential and probably the biggest reason why organizations fear to move their data to cloud. Because of the cloud's very nature security is of particular concern. In Data operations and other potentially vulnerable areas, security has become a priority for organizations using Cloud Computing and with their associated providers.

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 [7].

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 [8].

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 [9].

In the survey year of 2009, the result reveals many of the same challenges but the respondents rated security topped with 87.5 percent 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 [10].

The survey results proved that the security is the most important challenge among entire parameters that influence the performance and development of Cloud Computing. This paper, attempts to give the clear view of Cloud Computing and its security and spot the different mitigating techniques and analyze their impact on security.

2. REASEARCHMETHODOLOGY

This study is set out to answer the research question: what are the mitigating techniques being used in Cloud Computing and what is their impact on security? The majority of the existing research work has made using conventional literature review which has low scientific value due to inaccurate and undue approach.

In this research work, a method named systematic literature review selected as a primary research method to review the existing literature concerning mitigating techniques and their impact on security. The view of the research methods which are used to answer the research questions is shown in figure 1.

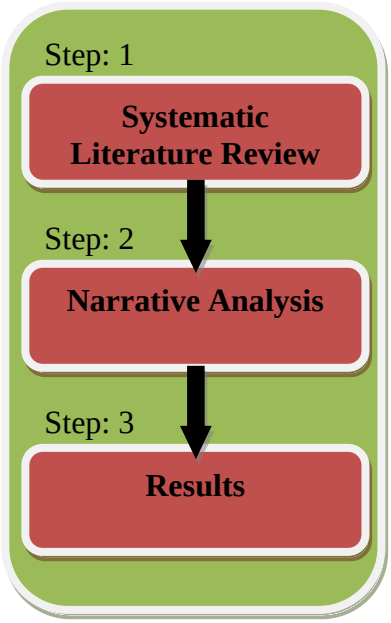

Fig: 1 Research Design

A Systematic literature review is a mean 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 form a search strategy to find out the primary studies related to research questions [11].

Systematic reviews intend to give a reasonable evaluation of a research topic by means of a reliable, accurate and auditable methodology and it combines the present work in a way that is fair and perceived to be fair.

A systematic review should be conducted according to the predefined search approach and this approach has to permit the comprehensiveness of the research to be conducted. And there are number of key features that distinguish a systematic literature review from a conventional literature review.

The SLR addresses the particular research question by defining a review protocol; it defines search strategy that intends to discover a large amount of existing information related to the research and the Systematic reviews entail the criteria of inclusion and exclusion to assess possible research study.

In order to accomplish research objectives, Kitchenham systematic process and procedure is adopted [11]. A large number of papers have selected that related to the research questions published between 2001 and 2013.

PICO criteria [11] 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.

2.1 Population

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

2.2 Intervention

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

2.3 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.

2.4 Outcomes

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

The following search string was constructed and used to find the required information during the SLR. (Cloud Computing) AND (security OR vulnerability* OR challenge*) AND (technique* OR method* OR framework* OR approach* OR model*)) and to ensure that the selected papers are relevant to our research work.

To identify the papers, the search was conducted from four databases which include IEEE Xplore, Springer link, Science direct and Scopus using search string. And study selection criteria spot the most important studies which give facts concerning research questions [11].

The criteria of inclusion and exclusion are completed; to filter out the papers which do contain the relevant and irrelevant information about research question. At first a study selection criterion excludes the searches by title and abstract. The study selection process followed by refining the search according to defined inclusion and exclusion criteria, that reflects the information related to Cloud Computing mitigating techniques and their impact on security.

2.5 Inclusion criteria

- Studies providing the basic understanding of Cloud Computing environment, and importance of security in Cloud Computing environment.
- Studies that covering the Cloud Computing mitigating techniques which are being used in cloud environment and also formalizing their impact on security.

2.6 Exclusion criteria

- Studies which are not in English language.
- Studies which are not replicating security techniques and importance of security.

3. RESULT AND ANALYSIS

In recent years, the huge amount of research has been done in the area of Cloud Computing. In the process of SLR, we have extracted 100 papers relevant to meet the goals of the research from the large number of papers published since the year 2001 to 2013.

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, we have identified 65 security techniques during the systemic literature review. The detailed list of these techniques is presented in table 1. The mentioned mitigation techniques have strong impact on the Performance, Security, Efficiency, QoS, Privacy and Access control of Cloud Computing.

The defined mitigation techniques somehow improve the overall services in Cloud Computing environment some of the commonly employed security techniques that are identified in SRL are Role-Based Access Control (RBAC), Identity-Based Authentication (IBA), Advance Encryption Standard (AES), Triple Data

Encryption Standard (DES) and DES, Intrusion Detection System (IDS), Public Key Based Homomorphic Authenticator with Random Masking, Third party auditor (TPA), The Service Level Agreement (SLA), and Trusted Platform Module (TPM).. The result is shown in figure 2.

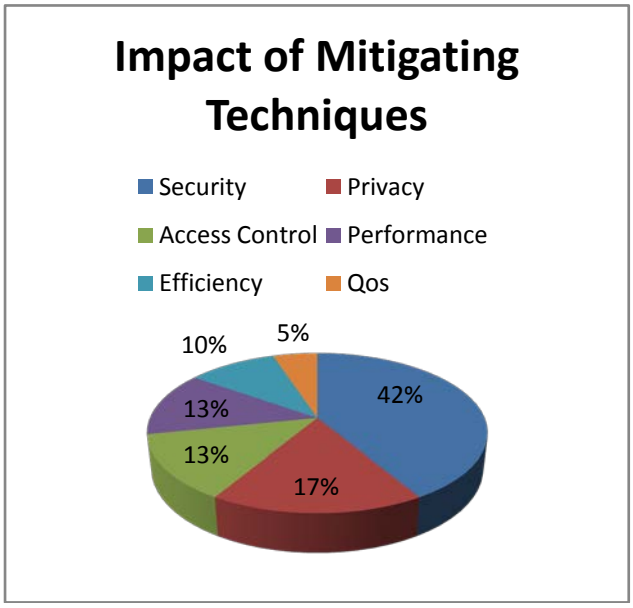

Fig 2: Impact of Mitigating Techniques

4. CONCLUSION

Cloud Computing is appearing as one of the rapidly adopted technologies in the computing field of information Technology and it provides plentiful potential benefits; despite security is the prime consideration. Cloud Computing mitigating techniques are in great consideration by large number of services and big challenge for the stakeholders during their method of identification. Form the systematic literature review it is noted that Cloud Computing in the future will result leading and flexible transactions of information despite of security issues.

Because it provides the user with flexible services, simple, individual access control to the cloud services. During the SLR, the satisfactory number of mitigating techniques in Cloud Computing has identified are tabulated in systematic method. And mainly used mitigating techniques in Cloud Computing are listed in the table 1.

Few of the widely used security techniques that are recognized in SRL are Role-Based Access Control (RBAC), Identity-Based Authentication (IBA), Advance Encryption Standard (AES), Triple Data Encryption Standard (DES) and DES, Intrusion Detection System (IDS), Public Key Based Homomorphic Authenticator with Random Masking, Third Party Auditor (TPA), The Service Level Agreement (SLA), and Trusted Platform Module (TPM).

And the impact of these mitigating techniques on Performance, Security, Efficiency, Quality of services, Privacy and Access control services of Cloud Computing are mentioned in the figure: 2 and it comes across that security has major and strong impact among identified services, and it is the key concern amongst researchers, users and providers of cloud computing.

If it is required to exchange confidential information between a browser and a web server, Encryption is an obvious means for secure communication, and appropriate encryption of information and transmission is essential. The security issues in Cloud Computing are always one of the main research topics for researchers and developers to investigate the appropriate solutions every time.

In the future there is need of further investigation, Cloud Computing security issues are burning and key issues for researchers and developers to find the suitable solution always. And it is recommended that there is need to find a most favorable and proper security solutions for the specific services in the Cloud. And In the future the research can be continue by proposing, Cloud Computing security compromised attributes can be identified and the most threatening compromised attribute to the Cloud Computing can be proposed.

Vol. 5, No. 3 March 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Table 1: Security Techniques

S.NO	Security Techniques	Impact
1.	Machine learning techniques	Security
2.	Attribute-based DRM scheme in Cloud Computing by combining the techniques of cipher text policy attribute-based encryption (CP-ABE) and proxy re encryption (PRE)	Access control , Performance
3.	A trust-aware access control policy	Access control , Privacy
4.	Distributed intrusion detection technique	Security
5.	Outsourced attribute-based encryption (OABE)	Security
6.	Conceptual categorization (CC) and mathematical underpinning technique that model checking techniques	Access control
7.	Public key encryption with RSA	Security
8.	Encryption(separate symmetric encryption keys)	Security
9.	Cipher text policy attribute-based encryption(CP-ABE) and combined with identity-based encryption (IBE) techniques	Security
10.	Role-based encryption (RBE) scheme	Access control , Security
11.	Role-based access control (RBAC)	Access control, Privacy , Efficiency
12.	AES, Triple DES and DES	Security , QOS
13.	Identity-based group signature	Access control , Privacy
14.	RC6	Security
15.	Symmetric and asymmetric searchable encryption techniques	Security , Access control
16.	Privacy preserving algorithm approach	Security, Privacy
17.	Attribute-based encryption (ABE), and Attribute-based signature(ABS)	Security , Privacy , Access control
18.	Identity-based cryptography (IDC)	Security
19.	Secure data sharing framework using homomorphic encryption and proxy re-encryption schemes	Privacy
20.	Network based IDS	Security
21.	Parallel processing in cryptographic algorithms	Security , Efficiency
22.	Cryptographic techniques	Security , Privacy
23.	(Secure Socket Layer) 128-bit encryption	Security
24.	Multi-dimensional password generation	Security , Access control, Privacy
25.	High order object oriented modeling technique(HOOMT)	Security
26.	ECC elliptic curve cryptography Encryption	Security , Privacy , Access control
27.	Public key encryption	Security
28.	Intrusion prevention system(IPS), authentication, authorization and accounting (AAA) controls	Security
29.	SOA-based trace back approach (SBTA)	Security
30.	Identity-based cryptography (IBC) security mediated cryptography	Access control , Security
31.	Shamir's secret sharing algorithm, triple modular redundancy (TMR) technique with sequential method	Privacy, Security
32.	Hidden Markov model based clustering using data mining techniques	Security
33.	RBAC with identity management	Security
34.	File-centric and data-centric logging mechanisms	Security
35.	Identity-based authentication (IBA	Privacy, Security
36.	RSA algorithm	Security, Efficiency
37.	Dynamic intrusion detection system	Performance
38.	Multi-tenancy based access control model (MTACM)	Security, Access control

39.	TLS handshake	Security
40.	Public key based homomorphic authenticator with random masking	Privacy, Performance
41.	Third party auditor (TPA)	Efficiency, QoS
42.	Probabilistic sampling technique	Security, Privacy
43.	Diffie-Hellman key exchange	Security, Access control
44.	Private face recognition	Privacy, Performance
45.	Message authentication codes (MACs)	Efficiency
46.	Data colouring and software water marking techniques	Performance, Security
47.	A novel cloud dependability model	QoS, Security
48.	Key policy attribute-based encryption (KP-ABE)	Privacy, Efficiency
49.	Proxy re-encryption (PRE)	Performance, Security
50.	Application-oriented remote verification trust model (ARVTM)	Qos, Security
51.	Security assertion mark-up language (SAML)	Performance, Privacy
52.	Trusted platform module (TPM)	Qos, Security
53.	Proof of retrieve ability (POR)	Efficiency, Performance
54.	Fair MPNR protocol	Security, Performance
55.	Sobol sequence	Security, Performance, Efficiency
56.	Redundant array of independent net-storages (RAIN)	Privacy, Efficiency
57.	Hadoop distributed file system	Performance
58.	Self-cleansing intrusion tolerance (C-SCIT)	Security, Privacy
59.	Searchable symmetric encryption (SSE)	Security, Privacy, Performance
60.	Provable data possession(PDP)	Security, Performance, Efficiency
61.	Time bound ticket based mutual authentication scheme	Efficiency, Security, Performance
62.	Security access control service (SACS)	Access control, Security
63.	The service level agreement	Qos, Performance
64.	Hypervisor	Access control
65.	Identity management	Privacy, Security

REFERENCES

[1] AkhilBhel and KanikaBhel," An Analysis Of Cloud Computing Security Issues", World congress on Information and Communication Technologies, 2012.

[2] F. Cheong, C. Cheong, Xu Xiaoping, Yan Junhu," Research on Cloud Computing Security Platform", Fourth International Conference on Computational and Information Sciences,2012.

[3] Eman M.Mohamed, Hatem S. Abdelkader," Enhanced Data Security Model for Cloud Computing", The 8th International Conference on Informatics and Systems, 14-16 May, 2012.

[4] YashpalsinhJadeja, KiritModi, "Cloud Computing-Concepts, Architecture and Challenges", International Conference on Computing, Electronics and Electrical Technologies [CCEET], 2012.

[5] The NIST Definition of Cloud ComputingPeter Mell Timothy Grance NIST Special Publication 800-145, 2011.

[6] EysteinMathisen, "Security Challenges and Solutions in Cloud Computing", 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.

[7] Bansidhar Joshi, A. SanthanaVijayan, Bineet Kumar Joshi, "Securing Cloud ComputingEnvironment against DDoS Attacks", IEEE, , pp. 1-5,2011.

[8] https://cloudsecurityalliance.org.

[9] HaoyongLv and Yin Hu, "Analysis and Research about Cloud ComputingSecurity Protect Policy", IEEE, pp. 214-216, 2011.

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

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

AUTHOR PROFILES

Muhammad Aamir received the degree in Computer Systems Engineering from Mehran UET Jamshoro, Pakistan, in 2009. He is a research student of Software Engineering. Currently, he is a student of MSE Software Engineering at Chongqing University China.

Prof. Xiang Hong received his Ph.D. degree, form University of Alberta, Canada in 1998. Currently, he is Professor of Software Engineering at Chongqing University China.

Muhammad Tahir received his Bachelor degree in Software Engineering from Institute of Information & Communication Technology University of Sindh Jamshoro, Pakistan in 2009. Mr.Tahir has been awarded Chinese Government Scholarship for his master degree in Chongqing University in 2012.

Atif Ali Wagan received the degree in Computer Science from University of Sindh Jamshoro, Pakistan, in 2009. He is a research student of Software Engineering. Currently, he is a student of MSE Software Engineering at Chongqing University China.