International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-3, Issue-1, March 2013

A Study on Security Requirements in Different Cloud Frameworks

Ramandeep Kaur, Pushpendra Kumar Pateriya

Abstract- Cloud computing provides the capability to use computing and other storage resources which are required by various users on a metered basis and reduce the expenditure in an organization's computing infrastructure. The virtual machines running on physical hardware and being controlled by hypervisors is a cost-efficient and flexible computing technique that is used as a key technology in cloud computing and provides transparency to different cloud users as there is no actual physical allocation of the machine. As cloud computing provides various benefits nowadays, it also brings some of the concerns about the security and privacy of information. In this paper, we made a study about different security risks that pose a greatest threat to the cloud computing. This paper describes about the different security issues that are occurring in the various cloud computing frameworks and the areas where security lacks and measures can be taken to enhance the security mechanisms.

Keywords-Internet protocol, Infrastructure as a service, Platform as a service, Software as a service, Virtual machine

I. INTRODUCTION

Cloud computing is defined as a style of computing where massively scalable IT- enabled capabilities are delivered 'as a service' to external customers using Internet technologies. The cloud computing offers several benefits like fast deployment, pay-for- use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services. Cloud computing basically stores all of its applications and databases in the data centers which are placed at different locations. Due to this movement of application software, data and services are not trustworthy. So this give rise to many security challenges that are: accessibility vulnerabilities, virtualization vulnerabilities, web application vulnerabilities, privacy and control issues arising from third parties having physical control of data, issues related to identity and credential management, data verification, tampering, integrity, confidentiality, data loss and theft, issues related to authentication of the respondent device or devices and IP spoofing.

Manuscript received on March, 2013.

Ramandeep Kaur, Department of computer science and technology, Lovely Professional University, Jalandhar(Punjab), India.

Pushpendra Kumar Pateriya, Department of computer science and technology, Lovely Professional University, Jalandhar (Punjab), India.

This paper describes the various securities issues of cloud computing in various security frameworks. Cloud computing model consist of 5 major characteristics that are:

a. On demand self service
b. Resource pooling
c. Rapid elasticity
d. Broad network access
e. Measured service

There are 3 service models provided by cloud computing that are SaaS, PaaS and IaaS.

a. SaaS: Use provider's applications over a network.
b. PaaS: Deploy customer-created applications to a cloud.
c. IaaS: Rent processing, storage, network capacity, and other fundamental computing resources.

Cloud computing was made possible and is influenced by the variety of architectural, technological, and operational influences. The key drivers of cloud computing are high-performance computing, grid computing, autonomic computing, Web services, virtualization, universal connectivity, and open-source software. We can divide the working of cloud computing into 2 sections and that are: front end and back end. They connect to each other through a network usually the Internet. The front end is the client, sees when using an application. The back end is the "cloud" section of the system. The front end includes the client's computer and the application required to access the cloud computing system. The various services that constitute front end are: Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox.

The back end of the system consist of various computers, servers and data storage systems that create the "cloud" of computing services and is beneficial for the different users. Each application will have its own dedicated server which it is suppose to use.

A central server has full rights of administering the system, monitoring all the incoming and outgoing traffic and listening to the client demands. It follows a set of rules which in more technical terms is called **protocols** and uses a special kind of software called **middleware**. Middleware allows networked computers to communicate with each other. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy.

II. SECURITY ISSUES IN VARIOUS CLOUD COMPUTING FRAMEWORKS

The various security issues in cloud computing frameworks are discussed in the following section of the paper and that require a lot of scope for providing the security in the cloud computing frameworks:

A. *Data security:*

The sensitive and confidential data of each enterprise stores within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. In the SaaS model offered by cloud computing, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. So the SaaS vendor must adopt additional security checks to ensure data security at every entry point and prevent breaches due to security vulnerabilities in the application or through unauthorized employees [15]. This scheme involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Malicious or unauthorized users can exploit weaknesses in the data security model to gain unauthorized access to data. The following assessments test and validate the security of the enterprise data stored at the SaaS vendor:

a. Cross site scripting
b. Access control weaknesses
c. Insecure storage(in terms of data centers)
d. Insecure configuration of system

B. *Network security:*

All the data flow over the network needs to be secure in order to prevent leakage of sensitive and confidential information. So this basically involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. In case of Amazon Web Services (AWS), the network layer provides significant protection against traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, DOS(denial of service) attacks, port scanning, packet sniffing, etc [16]. However, malicious and unauthorized users can exploit weaknesses in network security configuration to get the access of network packets due to session management weaknesses and insecure SSL trust configuration.

C. *Browser Security:*

when we are studying about cloud environment then it is very clear that in a Cloud environment, remote servers are basically used for various computations. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform independent client software useful for all users throughout the world. In cloud environment this can be categorized into various different types for example: Software-as-a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication.

D. *Data integrity:*

It is one of the most important elements of data security and privacy. It is very easy to achieve data integrity in standalone system with single database by simply adopting ACID properties but in distributed systems it s not a easy task to maintain data integrity like in cloud computing. Most of the SaaS vendors expose their web services APIs without any support for transactions. Each SaaS application may have different levels of availability and SLA (service-level agreement), which further complicates management of transactions and data integrity across multiple SaaS applications [3]. The lack of integrity controls at the data level could result in various problems leading to insecure data integrity.

E. *Data confidentiality issue:*

Cloud computing involves the sharing or storage by users of their own information on remote servers owned and operated by others whom we are not known with and accesses through the Internet or other connections [3]. Confidentiality issues arise due to:

a. A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider.
b. Disclosure of the remote storage may have adverse consequences for the legal status of protections for personal or business information.
c. The storage of information in the cloud may have an effect on the privacy and confidentiality protections of information.

F. *Data breaches:*

Data from various users and business organizations lie together in a cloud environment which is called pooling of resources, breaching into the cloud environment will potentially attack the data of all the users. In this way, the cloud becomes a high value target. In the Verizon Business breach report blog (Russ Cooper, 2008) it has been stated that external criminals pose the greatest threat (73%), but achieve the least impact (30,000 compromised records), resulting in a Pseudo Risk Score of 67,500. Insiders pose the least threat (18%), and achieve the greatest impact (375,000 compromised records), resulting in a Pseudo Risk Score of 67,500 [14].

G. *Virtual threats:*

Some threats to virtualized systems are general in nature and in cloud computing this is a very common attack as everything in cloud environment is based upon the principle of virtualization. Other threats and vulnerabilities, however, are unique to virtual machines. Many VM vulnerabilities generates from the fact that vulnerability in one VM system can be exploited to attack other VM systems or the host systems, as multiple virtual machines share the same physical hardware so this will leave all other VMS also infected and will hamper the security of the cloud architecture.

H. *Host and network intrusion:*

The provider in PaaS might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and the provider has to offer strong assurances that the data remains inaccessible between different applications. Strong Attention should be paid to how malicious and unauthorized actors react to new cloud application architectures that obscure application components from their area.

I. *Man in middle attacks:*

MIMA is commonly taking place when different cloud users across the cloud are communicating with each other or sharing the resources from the cloud environment. Any third person can try to hack the information during the transmission. To prevent this, strong mechanisms should be used so that identity of any third person can be determined

International Journal of Soft Computing and Engineering
IJSCE
www.ijsce.org
Exploring Innovation

and if he/she is unauthorized user, there should be scheme to block the further communication with that user so that he/she cannot hamper with the data integrity and data privacy which can further reduce the impact of MIMA in cloud computing.

III. CURRENT SOLUTIONS PROVIDED IN THE FIELD OF CLOUD COMPUTING

As there are number of entry points of information when we are communicating with the cloud like servers, firewalls or mobile devices so we need to focus on these points and enhance the security mechanisms [5]. For data encryption and host authentication basically TLS (transport layer security) is used. For identity and access management and network security controls like intrusion prevention and detection systems are used.

So basically security issues can occur when one user is using the cloud services or two users are sharing the same cloud services. Attacks can be man in middle attack, third party interruption, and DOS attacks.

NIST architecture described by peter Mell in 2012 is also used to handle secure big-data sets. We also explored some real business issues in adoption of cloud with Security [7]. Cloud is indeed an impactful technology that is sure to transform computing in business but parallelization problems may arise from communication between multiple clients and access to shared resources [1]. So basically this architecture describes the various parallelization problems that may arise while communicating.

The Effective Privacy Protection Scheme (EPPS) is proposed by Hsun Chuang in 2011 to provide the appropriate privacy protection which is satisfying the user demand privacy requirement and maintaining system performance simultaneously, At first, we analyze the privacy level users require and quantify security degree and performance of encryption algorithms[8]. Then, an appropriate security composition is derived by the results of analysis and quantified data. Finally, the simulation results show that the EPPS not only fulfills the user demand privacy but also maintains the cloud system performance in different cloud environments. Cloud computing moved the data and the application software of the various enterprises to the centralized large data centre, where the security issue arises [2].

In Cloud Computing Architecture, brokers are responsible to provide services to the end users. An Effective Cost Management System (ECMS) which works over Secure Cloud Communication Paradigm (SCCP) helps in finding a communication link with overall minimum cost of links [10]. There has been increasing interest in storing data securely in the cloud environment. To provide owners of data stored in the cloud with flexible control over access to their data by other users, a role-based encryption (RBE) scheme for secure cloud storage can also be used [13].

IV. PROPOSED MODEL

For reducing the high utilization of time and effort during the implementation of the security in the various cloud computing frameworks and enhancing the privacy requirements of the various users, we are proposing a model in which security is enhanced by assigning the roles to the different users depending upon the level of privacy a user demands and next step will be selection of the appropriate encryption algorithm.

Steps of the proposed model are described in the figure below:

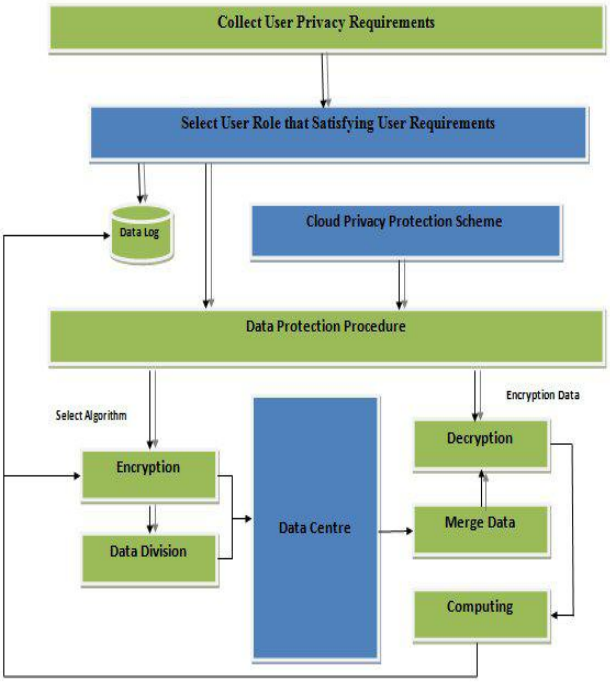

Fig 1: Proposed model for security and privacy

V.CONCLUSION

We talked about different cloud frameworks and there are number of security issues that occur in various cloud computing frameworks. Depending upon the study of various security challenges in cloud computing, we have proposed a model which can be beneficial in terms of security and privacy of different cloud users. Cloud computing is an emerging technology and meeting the user demands on time from remote areas due to its characteristic of resource pooling. Currently there are number of frameworks discussed in this study which enhance the security mechanisms in the cloud computing framework but still it lacks as implementing the various encryption techniques require more CPU utilization. So still there is a need of such a framework that must be developed and which will provide better encryption as well as less effort. Depending upon the study of various security challenges in cloud computing, we have proposed a model which can be beneficial in terms of security and privacy of different cloud users. This paper is a study of various security issues in cloud computing frameworks and current provided solutions provided to various cloud security challenges.

ACKNOWLEDGMENT

I would like to place on record my deep sense of gratitude to Assistant Prof. Pushpendra Kumar Petriya of Computer Science Engineering, LPU (Jalandhar) India for his generous guidance, help and useful suggestions. His assistance is very much beneficial for me to carry out the process of research in this field. Key improvements in the proposed research work would not be possible without the valuable suggestion and the feedback of my guide. I would also like to thanks to all my colleagues and classmates for their co-operation and support.

REFERENCES

[1] Wayne Jansen, Timothy Grance (2011) *"Guidelines in security and privacy in cloud computing"* National institute of standards and technology U.S department of commerce, NIST special publication 800-144.

[2] Yashpal Kadam(2011) *"Security issues in cloud computing- A transparent view"* Int. J Comp Sci. Emerging Tech, Vol- 2 No 5 October, 2011.

[3] Kevin Hamlen, The University of Texas at Dallas, USA (2010) *"Security issues in cloud computing"* International Journal of Information Security and Privacy, 4(2), 39-51.

[4] Volker Fusenig and Ayush Sharma (2012) "*Security Architecture for Cloud Networking"* International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium 978-1-4673-0009-4/12.

[5] V.Krishna Reddy (2011) *"Security Architecture of Cloud Computing"* International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462 Vol. 3.

[6] Pankaj Arora, Rubal Chaudhary Wadhawan(2012) *"Enhancing security and privacy in the cloud computing"* ijccr volume 2.

[7] Peter Mell(2012) *"What's special about cloud security"* IEEE computer society, 1520-9202/12.

[8] Hsun Chuang (2011*) "An Effective Privacy Protection Scheme for Cloud Computing"* ICACT ISBN 978-89-5519-155-4.

[9] Pardeep kumar, Vivek Kumar Sehgal(2011*) "Effective Ways of Secure, Private and Trusted Cloud Computing"* IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3,ISSN (Online): 1694-0814.

[10] Gaurav Raj, Kamaljit Kaur(2012) *"Secure Cloud Communication for Effective Cost Management System through MSBE"* International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.3.

[11] Jianyong Chen, Yang Wang, and Xiaomin Wang (2012) *"On-Demand Security Architecture for Cloud Computing"* IEEE Computer Society, 0018-9162/12.

[12] Abhishek Gupta, Jatin Kumar(2012)*"Design and Implementation of the Workflow of an Academic Cloud"* Indian Institute of Technology, Delhi[pdf].

[13] Lan Zhou, Vijay Varadharajan and Michael Hitchens(2011) *"Enforcing Role-Based Access Control for Secure Data Storage in the Cloud"* The Computer Journal, Vol. 54 No.10, 2011.

[14] Cooper R. Verizon Business Data Breach security blog, 2008.

[15] Kandukuri BR, Paturi VR, Rakshit A. "*Cloud security issues*". In: IEEE international conference on services computing, 2009, p. 517–20.

[16] Kaufman LM. *"Data security in the world of cloud computing, security and privacy"* IEEE 2009; 7(4):61–4.

Ramandeep Kaur, She has achieved her B.tech Degree from Punjab Technical University in 2010 and pursuing her M.tech from Lovely Professional University (Jalandhar), Punjab. Currently she is working at LPU, Jalandhar (Punjab). She is pursng her M.tech(CSE) in the field of cloud computing focusing on the security issues and various cloud frameworks.

Pushpendra Kumar Pateriya, He is an Assistant Professor in the Department Of Computer Science in Lovely Professional University, Phagwara (Punjab) India. Pushpendra's Research interests include Cloud Computing, Grid Computing, Network Security and Cryptography, Image Processing, Selective Image Encryption and Software Engineering. Some of the Publications are:

1. "Analysis on Man in the Middle Attack on SSL", International Journal of Computer Applications (0975 – 8887) Volume 45– No.23, May 2012, http://research.ijcaonline.org/volume45/number23/pxc3879816.pdf
2. "PC1-RC4 and PC2-RC4 Algorithms: Pragmatic Enrichment Algorithms to Enhance RC4 Stream Cipher Algorithm", International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420, http://ijcsn.org/IJCSN-2012/1-3/IJCSN-2012-1-3-36.pdf
3. "PC-PC-RC4 Algorithm: An Enhancement over Standard RC4 Algorithm", International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420, http://ijcsn.org/IJCSN-2012/1-3/IJCSN-2012-1-3-21.pdf
4. "Effective Resource Provisioning in Hybrid Cloud Environment", International Journal of Computer Science & Technology (IJCST)-Vol III Issue II, Ver 3, April to June 2012, http://ijcst.com/?page_id=1656
5. "RC4 Enrichment Algorithm Approach for Selective Image Encryption", International Journal of Computer Science & Communication Networks,Vol 2(2),181-189, http://www.ijcscn.com/Documents/Volumes/vol2issue2/ijcscn2012020207.pdf
6. "A Case Study on Software Development Projects in Academic Knowledge Centers using SCRUM", International Journal of Computer Applications (IJCA) April 2012 Edition, http://research.ijcaonline.org/volume43/number10/pxc3878385.pdf
7. "A Pragmatic Study on Different Stream Ciphers And On Different Flavors of RC4 Stream Cipher", International Journal of Computer Applications (0975 – 8887) Volume 43– No.10, April 2012, http://paper.ijcsns.org/07_book/201203/20120306.pdf