ISSN 2395-1621

Multi-layer Data Security with the Cloud Computing Adoption Framework

[#1]Rohit Polbhune, [#2]Suraj Baviskar, [#3]Aarti Tadole, [#4]Vinay Waghmare

[1]polbhunerohit78@gmail.com,
[2]surajbaviskar30@gmail.com,
[3]vinaypal.waghmare21@gmail.com,
[4]aratitadole567@gmail.com

[#1234]Computer Department

JSPM's Imperial College of Engineering and Research,
Wagholi, Pune University, Pune.

ABSTRACT

Offering real-time data security for petabytes of data is important for Cloud Computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. We believe this can only be able to achieve with an approach that is systematic, adoptable and well-structured. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. This paper explains the overview, rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. Since our Data Center has petabytes of data, there is a huge task to provide real-time protection and quarantine. This paper discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related\ to it concerning security. The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats.

Keywords: Cloud Computing Adoption Framework (CCAF),Security Framework, Multi-layered Security Protection

ARTICLE INFO

Article History

Received: 11th December 2017

Received in revised form :

11th December 2017

Accepted: 14th December 2017

Published online :

14th December 2017

I. INTRODUCTION

Cloud computing provides the next generation of internet-based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model is introduced by NIST [1] as "a model for enabling 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.". Multitenancy and elasticity are two key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability.

Cloud Computing and its adoption has been a topic of discussion in the past few years. It has been an agenda for organizational adoption due to benefits in cost-savings, improvement in work efficiencies, business agility and quality of services . With the rapid rise in Cloud Computing, software as a service (SaaS) is particularly in demand, since it offers services that suit users need. For example, Health informatics can help medical researchers diagnose challenging diseases and cancers . Financial analytics can ensure accurate and fast simulations to be available for investors . Education as a Ser-vice improves the quality of education and delivery Mobile applications allow users to play online games and easy to use applications to interact with their peers.

II. RELATED WORK

Data security for the private clouds hosted in the Data Center :-

As discussed in the introduction, the rapid data growth poses challenges for data security for the private clouds hosted in the data center. Literatures for different security solutions are as follows. Zhang et al [11] provide reviewof the Cloud Computing and explain the research challenges

associated with security. However, they only provide an overview of important security challenges but do not provide a full detailed solution on Cloud security. Liuet al [7] explain their software security analysis with their rationale and an example. However, there is a lack of details about the software design and implementation process involved, and empirical results to evaluate its performance and effectiveness of their proposed solution, which looks like the combination of UML and workflows.Yu et al [13] and Wang et al [14] propose their fine grained security model for Cloud storage. Both are similar, except that proposal from Yu et al [14] are more indetails and they explain theories and users associated with their proof of concept. However, both proposals [13,14] do not have any experiments, simulation and empirical data to prove the effectiveness and robustness of their fine grained security model. Thus, both proposals do not address in depth data security issues, when the rapid growth of data is a challenge for the Data Center. There are common observations in the security proposed methods: Each paper [7, 8, 10, 12, 14] only proposes a single solution. In the event of fraud, cyber criminal activities and unauthorized hack, the security solution is insufficient to protect the data security and the data center if only a single solution is adopted. Hence, a better alternative is required.

We proposed the multilayered security to integrate security techniques to illustrate the essence and effectiveness of the framework with advantages of doing so. First, the strength of each technique is enhanced. Second, since each technique can not always fully prevent hacking or provide a full solution without fallacy, the multilayered security can improve the extent of security since it is more difficult for viruses and trojans to break different types of security in one go. The aim is to maximize security protection and reduce the threats. To demonstrate the data security of the private clouds hosted in the data center, we propose the use of ethical hacking to demonstrate whether our CCAF multilayered security can withstand a large amount of viruses and trojans attacks, if the rapid data increase is from the external malicious hacking. We will provide detailed process and results.

III. PRESENT SYSTEM AND CHANGES

Key data security issues that are: critical personal data (personal and financial information such as credit card) during data transmission. Network and packet sniffers can be used to steal such information.

• Falsifying User Identities deals with identity theft by gaining access to data and can also threaten digital signatures with non
repudiation attacks .

• Password related threats deals with stealing and cracking passwords.

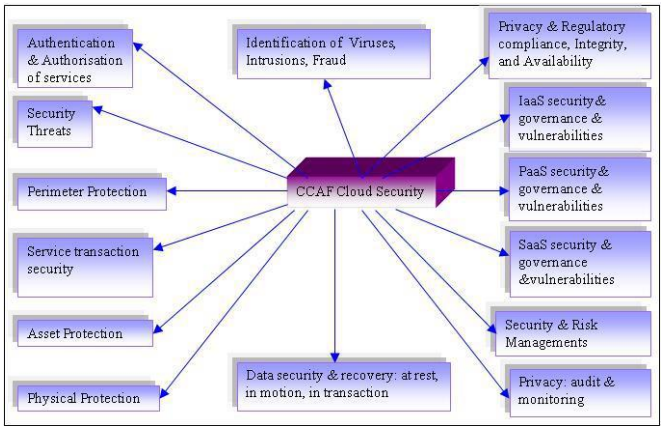
• Authorized access to tables, columns, and rows deals with security at the database level.

• Lack of accountability deals with system administrators for monitoring and protecting data access and user account management.

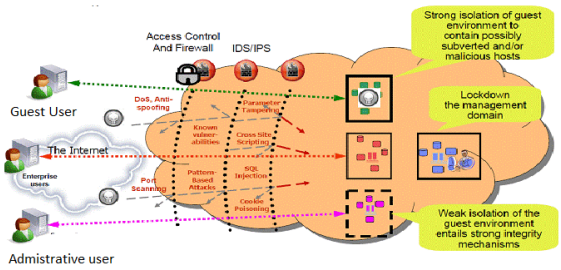
• Complex User Management Requirements deal with user account management strategies.

• Multitier Systems deal with providing access to other services and application layers.

• Scaling the security administration of multiple Systems poses extra complexity of managing cloud security as it deals with providing multiple accesses to multiple applications.



ARCHITECTURE CHANGES IN CIOUD COMPUTING



IV. METHODOLOGY

Select an elicitation technique :-

To include systematic identification and analysis of security requirements from stakeholders in the forms of interviews, business process modeling and simulations, prototypes, discussion and focus groups. As part of this phase, one should identify level of security, cost benefits analysis, organizational culture, structure and style.

Elicit security requirements :-

To include activities such as producing security requirements document based security specific principle structure as part of our goal of developing CCAF earlier, risk assessment results, and techniques identifies for analysis such as business process modeling and simulations, threat modeling, and misuse cases, etc.

Categorize security requirements :-

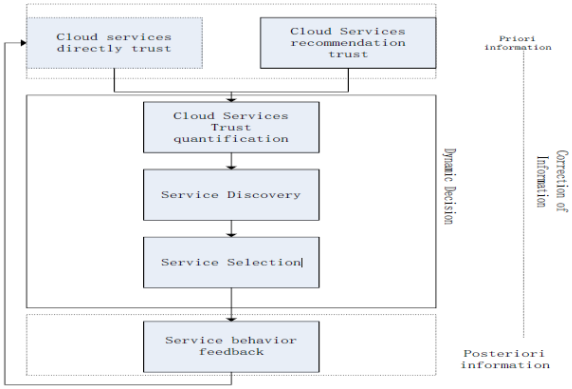
To include activities that classify and categorize security requirements based on company specific requirements specification templates and use our recommended security principles as this will help Systems Engineers to apply CCAF and track security specific requirements to validate and verify at all stages of the systems engineering life cycle.

Identify systems data security requirements:-

To include activities on extracting and carefully identifying data security and relevant subsystems such as data centers, servers, cloud VMs, and software security, SQL security, and other types of security that are relevant to the data. This separation of concerns allows systems engineers to integrate, track, design, and develop data security as part of enterprise wide systems development.

Prioritize security requirements:-
to include activities of selecting and prioritizing security requirements based on business goals as well as cost benefit analysis.

Inspect security requirements :-
To conduct requirements validation process using requirements inspection and review meetings.



Layer 1: Firewall
This section describes the intrusion protection used in CCAF to ensure that all data is safeguarded all the times. The Intrusion Prevention System (IPS) is used with the core syntax includes: crypto key pubkey-chain rsa named-key realm-cisco.pub signature key-string

While typing these three lines, an encrypted key string is generated to protect the data from potential malicious hack. The key string may look like this: B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
Once the key generation is done, the IPS configuration can be saved. Similar to "Rescue" XML tag in Section 3.1, the next step is to create a rule for IPS, followed by co n-figuring IPS signature storage location. The final step I ncludes IPS event notification. Their respective steps are presented as follows.

```
ip ips name <rule name> < optional ACL>
router#configure terminal
router(config)# ip ips name iosips
ip ips config location flash:<directory name>
router(config)#ip ips config location flash:ips
ip ips notify sdee
router(config)#ip ips notify sdee
```

Layer 2: Identity Management:

```
While trigger(status(job)) d o
   check(status(job)); / / to check the status
is 0 or 1
 if (security == 1)
     firew all(status(job));
 id entity(status(job));
   encryption(status(job));
 else
action((status(job));
quarantine(status(job));
report(status(job)); / / report the system ;do not stop
CCAF end ;
 end ;
```

Layer 3: Convergent Encryption:

After the identity management phase, all data has to undergo the security test offered by Convergent encryption (CoE), which uses the hash of plaintext to work out the encryption key (K). Here is a sample example to illustrate how it works. Adam obtains the encryption key from his message M such that K = H(M), where H is a cryptographic hash function; he uses this key to encrypt his message, hence: CoE= E(K, M)= E(H(M);M), where E is a block cipher. By applying this technique, two dif ferent users with two identical plaintexts will obtain two identical ciphertexts since the encryption key is the same. This allows the cloud storage provider to perform efficient storage (such as deduplication, which means the same file is only stored and archived at one place without duplication) on such ciphertexts without having any knowledge on the original plainexts.

V. CONCLUSION

CCAF multilayered security for the data security in the datacenter under the proposal and recommendation of CCAF guidelines. We explained the rationale, overview, omponentsin the CCAF, where the design was based on the requirements and the implementation was illustrated by its multilayered security. We explained how multilayered security was a suitable method and recommendation, since it offered multiple protection and improvement of security for 10 PB of data in the Data Center based at the University of London Computing Center (ULCC). We explained the technical details in each layer of security and propose an integrated solution to check all the data when data is intensively used. We used the Business Process Modeling Notation (BPMN) to simulate the cases of how the data can be used, either at rest, in use, or in motion. All simulations could be completed within 2 seconds.

REFERENCES

[1] S., Marston, Z., Li, S., Bandyopadhyay, J., Zhang, A., Ghalsasi, "Cloud computing – The business perspective". Decision Sup-port Systems, Elsevier, 51(1): pp 176-189, 2011.
[2] M. A., Vouk, "Cloud Computing Issues, Research and Implementations".Journal of Computing and Information Technology-CIT 16, page 235–246, Volume 4, 2008.
[3] A. K., Jha, C. M., DesRoches, E. G., Campbell, K., Donelan, S. R.,Rao, T. G., Ferris, D., Blumenthal. "Use of electronic health records in US hospitals. New England Journal of Medicine",360(16), 1628-1638,2009.
[4] H. T., Peng, W. W., Hsu, C. H., Chen, F., Lai, J. M. Ho, "FinancialCloud: Open Cloud Framework of Derivative

Pricing. In Social Computing (SocialCom), 2013 International Conference on (pp. 782-789). IEEE, 2013, September.
[5] M., Mircea, A. I., Andreescu, "Using cloud computing in higher education: A strategy to improve agility in the current financial crisis". Communications of the IBIMA, 2011, 1-15.
[6] M., Armbrust, A., Fox, R., Griffith, A. D., Joseph, R. H., Katz, A.,Konwinski, G., Lee, D., Patterson, A., Rabkin, I., Stoica, M.,Zaharia, "Above the Clouds: A Berkeley View of Cloud computing". Communications of the ACM, 53(4), 50-58, 2010.
[7] L., Liu, E., Yu, J., Mylopoulos,"Security and privacy requirements analysis within a social setting".In Requirements Engineering Conference, 2003. Proceedings,11th IEEE International (pp. 151-161),IEEE,2003, September.
[8] T., Mather, S., Kumaraswamy, S. Latif, (2009), "Cloud security and privacy: an enterprise perspective on risks and compliance". ISBN: 978-0-596-80276-9, O'Reilly Media, Inc.
[9] M., Pop, S. L., Salzberg, "Bioinformatics challenges of new sequencing technology". Trends in Genetics, 24(3), 142-149, 2008.
[10] A., Greenberg, A., J., Hamilton, D. A., Maltz, P., Patel, "The cost of a cloud: research problems in data center networks". ACM SIGCOMM computer communication review, 39(1), 68-73, 2008.
[11] Q., Zhang, L., Cheng, R., Boutaba, "Cloud computing: state of the art and research challenges". Journal of internet services and applications, 1(1), 718, 2010.
[12] J.J. Cebula, L.R. Young, "A Taxonomy of Operational Cyber Security",Technical Note: CMU/SEI-2010-TN-028,Software Engineering Institute,USA, December 2010.
[13]G., Wang, Q., Liu, J., Wu, "Hierarchical attribute based encryption for finegrained access control in cloud storage services". In Proceedings of the 17th ACM conference on Computer and communications security (pp. 735-737), ACM, 2010, October.
[14] X., Zhang, M., Nakae, M. J., Covington, R., Sandhu, "Toward a usage based security framework for collaborative computing systems", ACM Transactions on Information and System Security (TISSEC), 11(1), 3, 2008.
[15] G. McGraw, " Software security: building security in, Addison Wesley, USA, 2006.
[16] P., Brooks, J., Chittenden, "Metrics for Service Management:Designing for ITIL". Van Haren Publishing,ISBN: 978 90 87536480,2012.
[17] V.,Chang, R. J. Walters, G. Wills, "Cloud Storage and Bioinformatics in a private cloud deployment: Lessons for Data Intensive research".Springer: CLOSER 2012, CCIS 367, pp. 245–264,2013.
18] V.,Chang, "Business Intelligence as Service in the Cloud".Future Generation Computer Systems, DOI:http://dx.doi.org/10.1016/j.future.2013.12.028, 2014.
[19] I. A., Tondel, et al., "Security requirements for rest of us: a survey". IEEE Software, Special Issue on Security and Agile requirement engineering methods, Jan/Feb, 2008.

