IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

# Cloud Computing Security Techniques for Enhancing Utilization Efficiency

**Jaya[1], Kiranbir Kaur[2]**

**Available online at: www.ijcseonline.org**

Received: 08/Mar/2018, Revised: 15/Mar/2018, Accepted: 26/Mar/2018, Published: 30/Apr/2018

***Abstract***- Cloud computing provides resources or services both in terms of hardware and software using network (typically internet). Physical machines thus can perform operations beyond their capabilities. Cloud provides services including IaaS, PaaS and SaaS. Everything user needs is physically close to them hence extensive use of cloud is on the prospect. As users increases so does security threats. Cloud resources could be the target through application of attacks. Several techniques being suggested and research over to avoid critical consequence of threats. This paper provides comprehensive study of techniques used to enhance security within cloud computing environment. Comparative study also list best possible techniques which can work upon in the future.

***Keywords***- Cloud, Services, Attacks, Threats

## 1. INTRODUCTION

[1]Cloud computing becomes need of the hour since unlimited resources are up for grabs at absolutely low cost. Cost is encounters on the basis of pay per use. Due to benefits associated with cloud, large number of users interacted with cloud to use resources provided by cloud computing. Intention of users is uncertain and some users may be malicious causing threats to cloud resources. Security threats in cloud significantly reduce performance of system. [2]Data loss and increased cost due to security threats potentially reduce benefits provided through cloud.

To improve significance of cloud computing, security mechanism must be enforced within cloud computing. Before discussing security threats and attacks, cloud services are discussed as under

### 1.1 IaaS

[3]Cloud provides virtualised computing resources over the internet through the use of IaaS(Infrastructure as a Service). It can be scaled up or down depending upon requirement of users. IaaS is extremely useful in continues changing environment. Characteristics of IaaS are listed as under

- Virtualised computing resources provided by IaaS.
- IaaS service size is dynamic indicating that it can be scaled up or down depending upon requirements.
- Policy based services critically associated with IaaS.
- Automated administrative tasks being used in IaaS.
- Pay per use eliminate capital expenses from Iaas.

### 1.2 PaaS

[4]Platform as a service is also crucial service generated through cloud computing. User does not have to worry about the infrastructure through PaaS. Platform provided through cloud, utilized by users as if platform including operating system is loaded within user's machine. PaaS is also known as application platform service. Following features accompanied with PaaS

- Application execution platform is provided through the use of PaaS.
- Support for higher level programming without additional cost and overhead.
- Application maintenance and enhancement is easy.
- Useful in multi user environment where multiple developers are operating on single development project.

### 1.3 SaaS

[5]Software as a service is another asset associated with cloud owing to its success. Software plus services is another designated name assigned to SaaS. Licensed software are centralised hosted within cloud are accessed by users on pay

 

per use basis. Features associated with SaaS are described as under

- Multitenant architecture is followed within SaaS.
- It is possible to use software meant for specific business industry known as vertical SaaS.
- It is possible to use software meant for general business industry known as horizontal SaaS.
- Open integration protocol is used within SaaS for customization.

The security and authentication mechanisms are required to be enforced at each level of service provided with the help of cloud. Various security concerns and mechanisms used to tackle the issue is discussed in next section

## 2. LITERATURE SURVEY

Cloud computing as per now is heart and soul of new era. Internet based computing is supported through the services provided by cloud computing. Interactive services including infrastructure, network access, provisioning and platform is provided through distributed or cloud computing. As services grows so does the users. Users can be malicious in nature and may lead to attack. This situation is required to be prevented. Security of cloud hence becomes critical. Security technique suggested by [6] includes one to many probabilistic order preserving encryption. Differential attacks are explored over the OPE(order preserving encryption). Background information of outsources document can lead to accurately predicting attacking nodes and preserving cipher text. Another security mechanism suggested by [7]. You et al. uses channel estimation error as base criteria for security breech detection. Channel estimation errors as increases security breech becomes more common. Outage and intercept probability is used to minimize the error in channel estimation to reduce attack probability. Data access control mechanism proposed by [8] is considered for analysis in which private or secret keys are used at sender and receiver end. These keys can be used to easily encrypt and decrypt the information. These security strategies become critical as more and more users interact with the cloud. [9]proposed bidirectional authentication mechanism, statistical analysis and load balancing strategy was also suggested through analysed approach. Primarily storage security was considered. [10]proposed techniques and challenges associated with cloud computing. Comparison of techniques used for security purposes were mentioned and described through this literature. Because of security issues enterprises prefer to keep less sensitive data within cloud. [11] proposed memory replication mechanism to enhance security concern within LTE cloud. Replication procedure includes copying of sensitive information at multiple places. In case of failure sensitive information can be recovered from other replicated images. Storage space was heavily used in this approach. [12]proposed credit based scheduling using deadline mechanism for enhancing security and allowing the task to finish well within suggested time period. [13]proposed block level encryption within cloud. Block level encryption mechanism allows reduces redundancy along with encryption for security. Primarily public key encryption mechanism was used in block level encryption. [14]proposed analysis of various cloud computing security techniques along with issues associated with security concerns. Techniques described in tabular manner and parameters associated with cloud security techniques were mentioned comprehensively.

This paper presents concise but all round analysis of security concerns associated with cloud computing. Finally this paper present future security work leading to protection of cloud data.

## 3. COMPARATIVE ANALYSIS OF VARIOUS SECURITY MEASURES WITHIN CLOUD COMPUTING

Comparison of security concern technique is presented in this section. Parameters described in this comparison table can be optimised further.

| Paper / Parameters | Technique | ACCESS RIGHTS | ROLES | AUTHURIZATION | DATA PORTABILITY | FAIL OVER AND BACK UP |
|---|---|---|---|---|---|---|
| [15] (Xiao, Song, & Chen, 2013) | Cloud storage in terms of keys is considered | Read and Write | Not defined | Not Defined | Data from data centers can be transferred to other data enters | Not provided |
| [16] (C.-N. Yang & Lai, 2013) | Review is conducted of security | Read and Write | Defined for Sharing | Administrator is used to decide data values to be shared | Data from data centers can be transferred to other | Back up server is used |

 

| | | | | | | |
|---|---|---|---|---|---|---|
| | mechanism | | | | data enters | |
| [17] (Li, Li, & Huang, 2015) | Source and destination analysis for secure data transfer | Not Used | Defined to ensure safe passage of data | Administrator used to ensure duplicate file is not uploaded | Inter platform data transfer is supported | Back Server is used |
| [18] (Guillotteau, Orange, France, & Mauree, 2012) | Privacy and security handling mechanism | International privacy handling is used | Not Applicable | Technical standards are used for authorization | Data portability is provided | Not used |
| [19] (Noor, Sheng, Yao, Dustdar, & Ngu, 2016) | Trust based technique | Trust based Access rights | Trust based Roles are used | Administrator is used as a authority | Interdependence is used | Proxy servers are used for back up |
| [20] (C. Wang, Cao, Li, Ren, & Lou, 2010) | 128 bit key size is used for security | Key based access rights | Key based roles in terms of sender and receiver | Certification agency is used | Data moved between client and server | Provided with back up server |
| [21] (Harfoushi et al., 2014) | 32 bit, 64 bit, 128 bit key is analysed | Review of various access rights used in encryption algorithms are considered | Not Specified | Review is conducted of various techniques having distinct administration policies | Data moved between client and server | Provided with back up server |
| [22] (Hwang et al., 2016) | Benchmark mechanism instead of Keys is used | Analysis in terms monitoring and certification agencies | Defined for sharing | Certification and monitor nodes are used | Data movement is supported | Provided with back up server |
| [23] (H. Wang, Kang, & Wang, 2016) | Fitness enabled technique is used | Mutation is used as a update mechanism | Sharing is specified | Offspring mechanism is used for the same | Data is moved and altered depending upon fitness | Not specified |
| [24] (K. Yang & Jia, 2013) | Dynamic auditing technique is used | Verification mechanism as access right | Successful auditing is used for sharing | Administrator conduct Auditing | Data movement between source and destination | Provided with back up server |

Table 1: Comparison of Techniques used within cloud computing

Transfer of data from source to destination is of prime concern in case of advanced computing. Virtual machines in terms of nodes exist in advance computing. Users of advance computing could be fair or malicious in nature. In case of malicious nodes some defence mechanism is needed. This defence mechanism is provided in terms of encryption. In advance computing, cost is encounter on the basis of pay per use. So, security along with space conservation is issues to tackle in case of advance computing. Both of these issues are tackled by the use of data deduplication.

## 4. CONCLUSION AND FUTURE SCOPE

Security techniques are critically accompanied requirement within cloud system. Cloud system comes into exposure to wide variety of users. Some users out of millions at exposure to cloud may able to distort the working of cloud system hence forth many of the enterprise do not prefer sensitive data storage within cloud system. In order to resolve the problem access control, roles and other distinct mechanisms were defined within cloud system to enhance security. In future, key based mechanism for enhancing security within cloud system can be used. This may lead to enhance trust of users within cloud for storing sensitive data.

## 5. REFERENCES

[1] N. Wahidah, B. Ab, K. Jenni, S. Mandala, and E. Supriyanto, "Review On Cloud Computing Application In P2P Video Streaming," *Procedia - Procedia Comput. Sci.*, vol. 50, pp. 185–190, 2015.
[2] J. Aikat, N. Carolina, J. S. Chase, A. Juels, C. Tech, T. Ristenpart, and C. Tech, "Rethinking Security in the Era of Cloud Computing," no. June, 2017.
[3] B. Nicolae, "BlobCR : Efficient Checkpoint-Restart for HPC Applications on IaaS Clouds using Virtual Disk Image Snapshots."
[4] C. Pahl and I. Centre, "Containerization and the PaaS Cloud," 2015.
[5] R. Buyya, "Introduction to the IEEE Transactions on Cloud

 

Computing," vol. 1, no. 1, pp. 3–21, 2013.
[6] K. Li, W. Zhang, C. Yang, and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption Based Cloud data Search," vol. 6013, no. c, pp. 1–9, 2015.
[7] J. I. A. You, Z. Zhong, G. Wang, B. O. Ai, and S. Member, "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors," vol. 2, 2014.
[8] X. Wu, R. Jiang, and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," pp. 1–14, 2015.
[9] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, T. Qiu, and S. Member, "An Efficient Protocol with Bidirectional Verification for Storage," vol. 3536, no. c, pp. 1–13, 2016.
[10] F. Sabahi, "Cloud Computing Security Threats and Responses," pp. 245–249, 2011.
[11] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, "R EPLISOM : Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud," vol. 4662, no. c, 2015.
[12] A. Sharma and S. Sharma, "Credit Based Scheduling Using Deadline in Cloud Computing Environment," pp. 1588–1594, 2016.
[13] Y. Zhao and S. S. M. Chow, "Updatable Block-Level Message-Locked Encryption," pp. 449–460, 2017.
[14] P. You, Y. Peng, W. Liu, and S. Xue, "Security Issues and Solutions in Cloud Computing," 2012.
[15] Z. Xiao, W. Song, and Q. Chen, "Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1107–1117, Jun. 2013.
[16] C.-N. Yang and J.-B. Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing," in *2013 International Symposium on Biometrics and Security Technologies*, 2013, pp. 259–266.
[17] X. Li, J. Li, and F. Huang, "A secure cloud storage system supporting privacy-preserving fuzzy deduplication," *Soft Comput.*, Jan. 2015.
[18] S. Guilloteau, F. T. Orange, France, and V. Mauree, "Privacy in Cloud Computing," *Media Informatics*, no. March, p. 26, 2012.
[19] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.
[20] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," in *2010 IEEE 30th International Conference on Distributed Computing Systems*, 2010, pp. 253–262.
[21] O. Harfoushi, B. Alfawwaz, N. a. Ghatasheh, R. Obiedat, M. M. Abu-Faraj, and H. Faris, "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review," *Commun. Netw.*, vol. 06, no. 01, pp. 15–21, 2014.
[22] K. Hwang, X. Bai, Y. Shi, M. Li, W.-G. Chen, and Y. Wu, "Cloud Performance Modeling with Benchmark Evaluation of Elastic Scaling Strategies," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 130–143, Jan. 2016.
[23] H. Wang, Z. Kang, and L. Wang, "Performance-Aware Cloud Resource Allocation via Fitness-Enabled Auction," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 1160–1173, Apr. 2016.
[24] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

 