Identity Verification In Hybrid Cloud Computing

S. K. Jha, Ankit Kapahi

Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India, Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India.
Email: skjha2@amity.edu; ankitkapahi@gmail.com

ABSTRACT: Organizations are adopting cloud in their business to gain cost-efficiency and to survive amongst the best. Moving to cloud, customer organizations can utilize pay-per-usage pattern of service and innumerable advantages that cloud offers over traditional methodologies. With the diversity of purposes that cloud computing is used for, data storage is the major adopted service. This includes the storage of sensitive data like employee personal information, which increases the demand for privacy and high security in cloud. For ensuring the safety of data and information sensitive to the business, organizations must know what type of cloud to be used. Public cloud, wherein costs are low with minimum or no guarantee of safety of the data or Private cloud, wherein the customer can rely on a third party cloud vendor for safeguarding their data with complete privacy. The tug of war between public cloud and private cloud came to an end with hybrid cloud which is a connected cluster of public clouds and private clouds.Hybrid cloud can viewed as the solution for many organizations needs in terms of security and usage. The paper provides a proposed algorithm for hybrid cloud security and the comparative study between the existing security algorithm and proposed security algorithm of hybrid cloud.

Keywords: Cloud Computing, Hybrid Cloud, Data Security, Cloud Identity, Public Cloud, Private Cloud

1 INTRODUCTION

Today needs to match their requirements with strategic approach. The organization must know what suits their requirement the best. Right decisions are essential for improved outcomes and high profits. Thus, what type of cloud to be used is an important decision which needs adequate planning. Organizations wanting both scalability (that public cloud offers) and security (that private cloud offers) turned to hybrid model [11]. Hybrid cloud model provides new possibilities in terms of security. One of the major issues in using cloud services is security and to verify authentication of the user or cloud and identify misuse if any [15]. Traditional methods to detect unauthorized activities in cloud are not enough. Identity verification is essential mechanism in all cloud services. The paper explains existing identity verification mechanism in detail about the algorithm it follows. Also, the paper provides a proposed algorithm which can enhance the security of hybrid cloud, making it more reliable for the customer organizations. The paper is organized as follows: In Section 3, various challenges in hybrid cloud security are discussed. In section 4, existing algorithm for hybrid cloud model is explained. In section 5, an effective algorithm for hybrid cloud model is proposed with some advancement that can be incorporated into the existing algorithm. Section 6 comprise of a comparative study between the existing and the proposed algorithm. In section 7 the conclusion is provided.

2 LITERATURE REVIEW

2.1 Methodology

In this paper, we have tried to study all research papers defining cloud computing, types of cloud, hybrid cloud security, security algorithms, published in various journals and conferences. Based on the results and inferences from each paper, we have tried to understand the existing algorithm and propose an algorithm for hybrid cloud computing.

2.2 About Hybrid Cloud

A Hybrid cloud as the name suggests is an integration of public cloud services and private cloud services performing various functions within the same organization [8]. Public cloud provides cost efficiency whereas a private cloud provides enhanced security with complete trust on a third party cloud vendor. Hybrid cloud is thus a solution, utilizing public cloud for non-sensitive data to reduced costs and relying on the private cloud for ensuring safe computation and storage [3]. Hybrid cloud model can be deployed in the following ways:

1. Different Cloud service providers come together to provide both private and public services in an integrated manner.

2. Cloud service providers offer complete hybrid package.

3. Organizations with private cloud take up public cloud services which they further integrate in their infrastructure.

There are various advantages that hybrid model offers:

1. Scalable: By moving non-sensitive data from private to public cloud, organizations reduce requirement and demand on a private cloud.

2. Cost Efficient: Public clouds offers low costs and provide to be more economic than private cloud. Therefore Hybrid cloud allows the organizations to save on extra costing along with keeping sensitive data secure.

3. Flexible: Combination of cost effective public cloud and secure private cloud, organizations can explore different operational methods. Hybrid cloud is thus an answer to many questions that organizations face while choosing the right type of cloud service.

3 HYBRID CLOUD SECURITY CHALLENGES

There are various complex security challenges in the hybrid cloud:

1. Increased malicious attacks: Due to large number of users and their sensitive data stored, cloud becomes more prone to black hat hackers.

2. Virtualization: Unquestionably, virtualized environment with its advantages isalso a loophole in cloud security. Virtualization can lead attackers to ways of hacking the server, affecting the very existence of the organization.

3. Application security: When an application is being executed in the cloud, it's available to every single security threat. The CSA (Cloud Security Alliance) divides application security itself into authentication, authorization, and compliance, identity management, application authorization management, application monitoring.

4. Identity and access management: Identity management itself is a very vast topic. The objective of identity management is to control access to computer resources, applications, data, and services. This paper is limited till Identity Verification, not including other factors of identity management

4. EXISTING ALGORITHM

As with the high deployment of hybrid cloud, Intra-cloud communication has become a very common phenomenon and data is being transferred between clouds at a tremendous rate. A number of algorithms exist for cloud safety. Here is the existing algorithm [5] for secured intra-cloud communication using challenge text based communication which works like this:

A. Step 1 – This presumes that there is a secured and trusted environment established between them because of SLA's and whenever one cloud needs data from another cloud it will just send a data request.

B. Step 2 – In response to data request second cloud will send a challenge text asking requesting cloud to decrypt it with its public key and send it back to give proof of identity and to maintain confidentiality.

C. Step 3 – If the received decrypted challenge text matches with the original one then encrypted data will be send to requesting cloud else request is discarded.

5. PROPOSED ALGORITHM

Hybrid cloud offers many security challenges due to the nature of its functionality, that is, the data flow between clouds. Increased security issues are evident in such functionality. When hybrid cloud emerged, its primary objective was to make this cluster of clouds work. Only encryption was done before moving the data through the network. Here, we provide a method by proposing an extra level of security via an algorithm with identity verification. Following are the steps of the proposed algorithm:

A. *Step 1:* Suppose there are two clouds "Cloud A" and "Cloud B" composing into a hybrid cloud. Both have a trusted environment already created between them using Service-level agreement and standardized API's. These programming interfaces will contain the instructions of how clouds can communicate with each other.

B. *Step 2*: If "Cloud A" wants to access some data of "Cloud B", it will send a data request (DRQ) to "Cloud B" but with this data request, "Cloud A" will be sending (IDC) identification code also. This IDC is the current time and date in encrypted form as per Caesar cipher or RSA algorithm.

C. *Step 3*: Cloud 'B' receives the packet and decrypts the Identification code using its public key.

D. *Step 4:* "Cloud B" will check the authenticity of the request by comparing date with decrypted IDC date and also checks if the difference between current time and decrypted IDC time is less than 120 sec. If the difference is less than 120 seconds, the data would be sent.

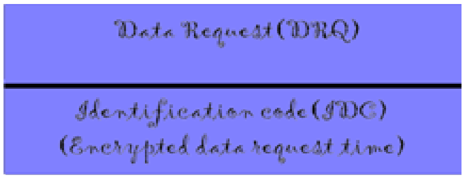
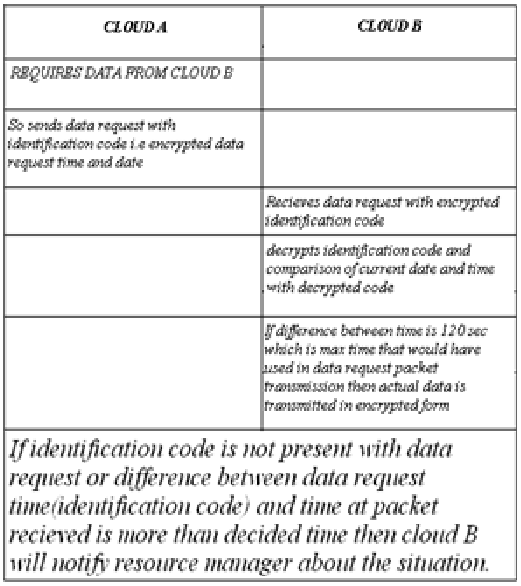


Fig. 1 *Data Request packet*

E. *Step 5*: .data transferred will be encrypted using various layers of encryption so that it cannot be accessed without a key.

F. *Step 6:* If date does not match or the difference between the current time and decrypted IDC time is more than 120 seconds, "Cloud B" will discard the request and notify about this request to resource manager.

This proposed algorithm adds time as a parameter for increasing hybrid cloud security. The existing algorithm does not incorporate time for identity verification.



CLOUD A	CLOUD B
REQUIRES DATA FROM CLOUD B	
So sends data request with identification code i.e encrypted data request time and date	
	Recieves data request with encrypted identification code
	decrypts identification code and comparison of current date and time with decrypted code
	If difference between time is 120 sec which is max time that would have used in data request packet transmission then actual data is transmitted in encrypted form
If identification code is not present with data request or difference between data request time(identification code) and time at packet recieved is more than decided time then cloud B will notify resource manager about the situation.	

TABLE 1
Steps for Identity Verification

6. ADVANTAGES OF THE PROPOSED HYBRID CLOUDALGORITHMFOR IDENTITY VERIFICATION OVER EXISTING ALGORITHM

This algorithm can resolve or can be useful in the following cases:

1. In the proposed algorithm, Identity Proof is sent with the data request itself. So the number of steps or transmissions will be reduced. As a result, less time will be taken to process the request.
2. As the number of transmissions gets reduced, the network traffic will also get reduced, unlike existing algorithm, where there happen to be three steps before sending the data.
3. Even if the system encounters heavy traffic or congestion in the network, it would be easily cleared with difference between the times of data request and receiving time. No such mechanism present in the existing algorithm.

7. CONCLUSION

The paper has introduced an algorithm for identity verification within hybrid cloud to make the hybrid model more secure. The algorithm uses time as factor for identifying abnormal behavior and unauthorized access. The difference between the current time and decrypted IDC time will decide if the user has access to the requested information and data or not. Thus, the proposed algorithm is an advancement of the existing one with enhanced security in hybrid cloud.

REFERENCES

[1] Mladen A. Vouk, “Cloud Computing – Issues,Research and Implementations”, Journal of Computing and Information Technology - CIT 16, 2008, 4

[2] Bhushan Lal Sahu, Rajesh Tiwari, “a Comprehensive study on Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012

[3] R.Balasubramanian,M.Aramudhan, “Security Issues: Public vs Private vs Hybrid Cloud Computing”, International Journal of Computer Applications (0975 – 8887) Volume 55– No.13, October 2012

[4] Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satapathy, “Cloud Computing: Security Issues and Research Challenges”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

[5] Anukrati Dubey, GunjitaShrivastava& Sandeep Sahu, “Security in Hybrid Cloud”, Global Journal of Computer Science and Technology Cloud and Distributed, Volume 13 Issue 2 Version 1.0 Year 2013

[6] Deyan Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, 2012 International Conference on Computer Science and Electronics Engineering

[7] Rahul Bhoyar, Prof. Nitin Chopde, “Cloud Computing: Service models, Types, Database and ssues”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013

[8] VaibhavKhadilkar, KerimYasinOktay, Murat Kantarcioglu and SharadMehrotra, “Secure Data Processing over Hybrid Clouds”

[9] Wei Wang, Baochun Li, and Ben Liang, “Towards Optimal Capacity Segmentation with Hybrid Cloud Pricing”, Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada

[10] Bandaru A Chakravarthi, Bharat Kumar Saki, Ch Raju, P V S Sarma, IndranilSaaki, “Improving Utilization Infrastructure Management in Private and Hybrid Clouds”, International Journal of Engineering Research and Development e-ISSN : 2278-067X, p-ISSN : 2278-800X, www.ijerd.com Volume 2, Issue 5 (July 2012), PP. 20-30

[11] Kaustav Choudhury, Diptam Dutta, KasturiSasmal, “Resource Management in a Hybrid Cloud Infrastructure”, International Journal of Computer Applications (0975 – 8887) Volume 79 – No 12, October 2013

[12] Hui Zhang, Guofei Jiang, Kenji Yoshihira, Haifeng Chen and Akhilesh Saxena, “Intelligent Workload Factoring for A Hybrid Cloud Computing Model”

[13] Sujay. R, “Hybrid Cloud: A New Era”, IJCST Vol. 2, Issue 2, June 2011

[14] Sunita Rani, AmbrishGangal, “Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints”, International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4302 – 4304

[15] Hong-Linh Truong, SchahramDustdar, and Kamal Bhattacharya, “Programming Hybrid Services in the Cloud”, IBM Research – India

[16] Amanjot Kaur, Manisha Bhardwaj, “Hybrid Encryption for Cloud Database Security”, International Journal of Engineering Science and Technology, Volume-2, Issue-3, 737 – 741

[17] Sarojadevi K, Jeevitha R, Uncloud the Cloud of Cloud Computing”, International Journal of Computer Applications in Engineering Sciences, VOL I, SPECIAL ISSUE ON AISC , DECEMBER 2011