International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Multilayered Security Approach for Cloud Data Centers using Hash Functions

Jashanpreet Pal Kaur[1], Rajbhupinder Kaur[2]

[1]M.Tech Research Scholar, [2]Assistant Professor
Department of Computer Engineering, Yadavindra College of Engineering,
Talwandi Sabo, Punjab, India

Abstract: ***Cloud Computing provides computing over the internet. The cloud is not a trust worthy because there is no control of users on the data. Hence, the cloud data centers are vulnerable to assorted attacks. It is required for the cloud service providers to ensure the secured data transmission in the cloud framework. There is also dependency among the layers. So attack at any layer may affect the other layers. This paper proposed a new multilayered security approach means the security at different levels of different cloud layers to secure the data stored at cloud data centers based on dynamic hybrid key then performance of proposed algorithm is evaluated at last based on execution time, security improvement percentage and delay.***

Keywords: Security Issues in Cloud computing, Cryptography, MD5 and SHA1 Algorithms, Static and Dynamic Keys

1. Introduction

The Cloud Computing stores the data is at remote location and available on demand. By data outsourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid the extra expenses on software, hardware, information resources and data maintenance. In traditional on premises deployment model the data of enterprise must resides within its boundary and follow their own access control and security policies [1][2]. Whereas in cloud computing data reside at data centers of cloud with the lack of control and without the knowledge of how their data resides. Due to the nature of cloud system there are many questions that arise as to weather a cloud is secure enough or not from various threats and vulnerabilities [3]. The protection is paramount and users need to regain control over the protection of their data from Cloud Service Provider. Hence the security and privacy are two main issues in cloud computing. Multilayered security means security at different levels of the different cloud layers. It means security of Infrastructure as a service, software as a service, platform as a service, virtual machine security, network level security, host level security. The security can be maintained without having privacy but privacy is not maintained without having security. So, Security is considered a key requirement for cloud computing [3][4]. The better way to secure cloud data centers from the potential threats and vulnerabilities by using cryptography. The information is encrypted by the users using cryptography techniques before uploading into the cloud data centers [5]. There are basically three kinds of cryptographic techniques: 1) Symmetric Key 2) Asymmetric Key 3) Hash Function cryptography [6]. The cryptography can also be defined into two categories Dynamic Key Cryptography and Static key cryptography. The dynamic key cryptography is used to enhance the security and computational efficiency of any system. The dynamic keys are similar in nature to one- time pad, every message in the system is encrypted by a different cryptographic key. In case of static key cryptography the same key is used every time. Hence it is more vulnerable to attacks[14]. We have proposed a new security scheme based on hash functions. This approach provides a security with a set dynamic hybrid keys or hash keys. The single algorithm does not provide the better security. Hence, multiple algorithms or hybrid approach used for proposed approach.

2. Problem Formulation and Objective

2.1 Problem formulation

As discussion towards the security and how best to protect data in the Cloud data centers is provided. The notion of data privacy and security is addressed. The degree of trust afforded to a Cloud Service Provider is analyzed.

There exists a dependency among the cloud layers. The attack on any layer affects the other layers. There are different kinds of attacks on each level of cloud security architecture that makes cloud data centers vulnerable to assorted attacks. Hence, it's required for the cloud service providers to ensure the secure data transmission in the cloud framework.

The proposed algorithmic approach provides a multilayered security by using encryption based on the hash keys to secure the data centers and cloudlets.

2.2 Objectives

- To propose a new algorithm for security of cloud data centers.
- To provide an effective scheduling and security with **e**ncryption.
- The implementation of encryption module with hash functions in CloudSim (Java based simulator)
- To test the performance of proposed algorithm with some parameters.

3. Research Methodology

The main design scenario of such approach is as following.

1) Implementation of cryptography and secured layered in the proposed algorithmic approach.
2) The dynamic hash keys are generated for the authentication purpose using hybrid approach.

3) The cloud data centers are accessed by authenticated clients using secured shell and encrypted transmission via brokers. If the client's authentication failed then it terminates the execution.
4) When cloudlet is submitted to the datacenter for execution. The cloudlet has a specific key used as a private key. Once the key is identified and recognized, the cloud service provider will approve.

The implementation of algorithm goes through various steps:
STEP 1: Initialize CloudSim package
STEP 2: Activation of the Cloud Objects and Related Parameters
STEP 3: Generation of dynamic hybrid keys (Encryption module)
STEP 4: Activation of cloudlets and virtual machines for communication.
STEP 5: Authentication of participating clients
STEP 6: Logging of Parameters
STEP 7: Detailed Report Generation and Stop.

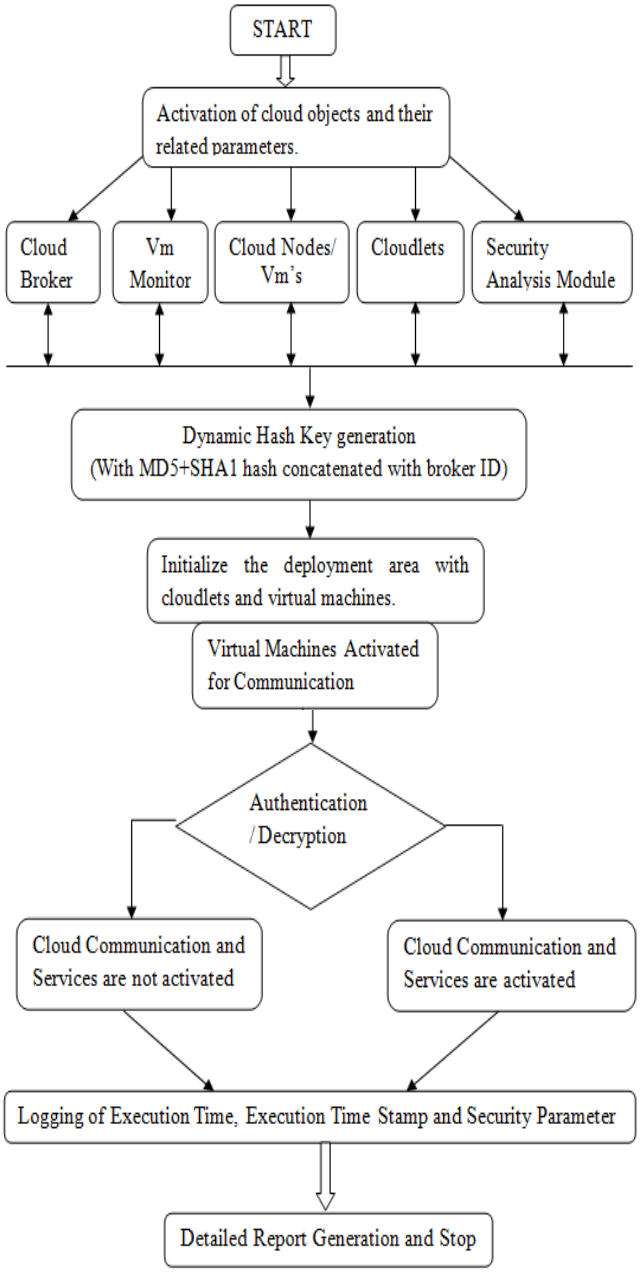


Figure1: Flow chart of proposed approach

4. Simulation Results and Discussion

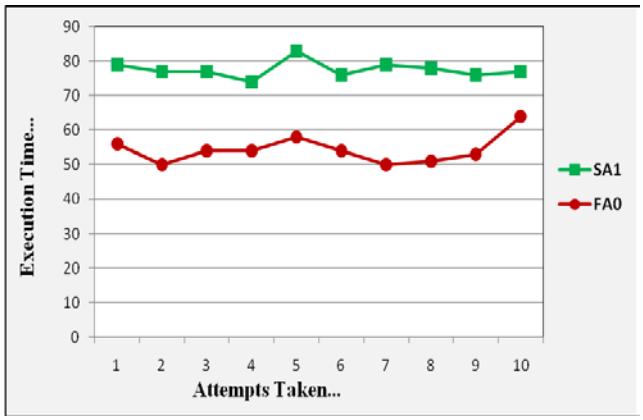
The tools used for the implementation of proposed algorithm are as following:
1) CloudSim simulator is a toolkit for the modelling and simulation of Cloud computing environments.
2) Eclipse IDE (Simulation Engine)
3) Spreadsheet Plug-ins for parameter analysis

The whole research work is carried out by using CloudSim with Eclipse IDE. From the reports generated at last, the parameter execution time, security parameter and delay are analysed to check the performance of proposed approach.

4.1 In Case of Dynamic Hybrid Key

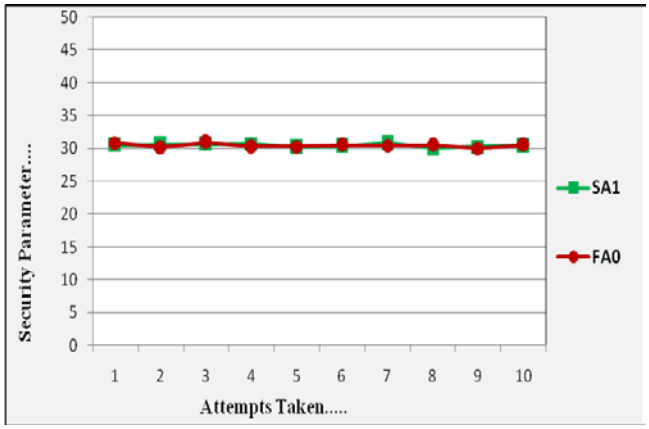
This section shows the results of our proposed scheme for execution time parameter and Security parameter. Here,
DHK-1 denotes: Successful Authentication of dynamic hybrid key
DHK-0 denotes: Failed Authentication of dynamic hybrid key

1) Execution Time
The execution time for successful authentication is always more than the failed authentication. Because when authentication is failed the algorithm terminates the operation. It doesn't process the cloudlets. The execution time is near about 90ms but it is less than 70ms and more than 40 ms in case of failed authentication.



Graph 1.1: Execution Time

2) Security Parameter
The security improvement percentage is approximate to 30 percent in both cases on every attempt.



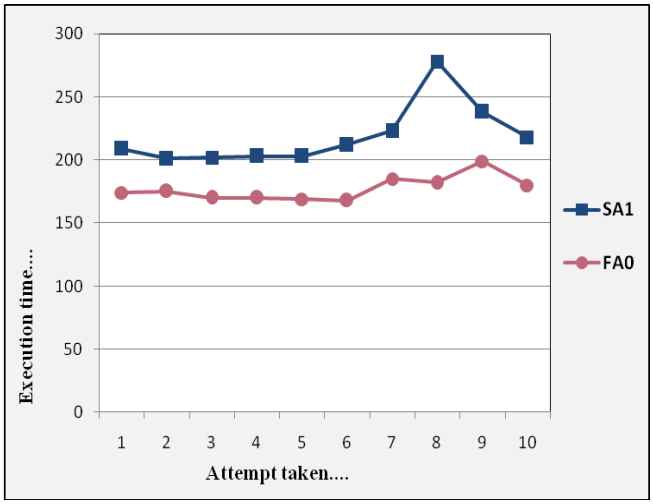
Graph 1.2: Security Parameter

4.2 In case of Static Key

This section shows the results of static key approach that is used only to check the performance of our algorithm for execution time and security parameter value. Here, **SK-1 denotes:** Successful Authentication of Static Key. **SK-0 denotes:** Failed authentication of Static Key.

1) Execution Time

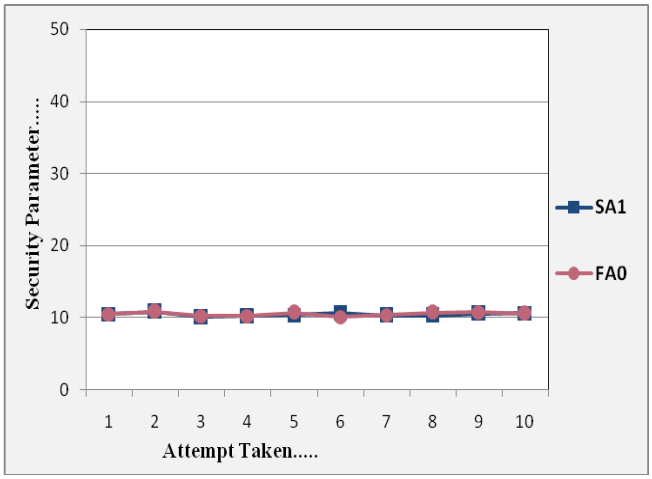
The Execution Time is more than 200 milliseconds on every run when authentication is successful but less than 200 milliseconds and more than 500 ms when authentication failed.



Graph 1.3: Execution time

2) Security Parameter

The security parameter is approximate to 10 percent in both when authentication is successful and when authentication is failed.

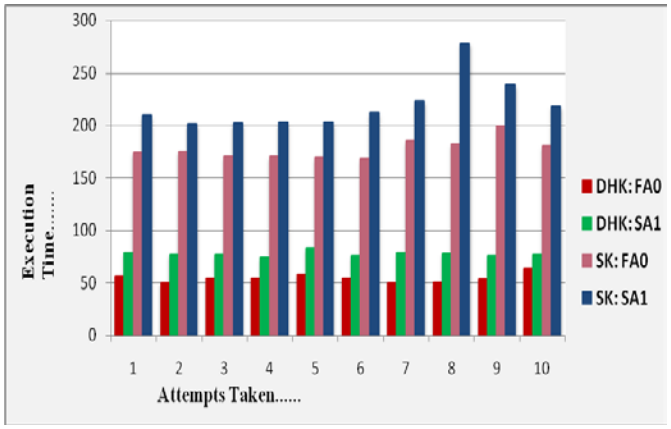


Graph 1.4: Security Parameter

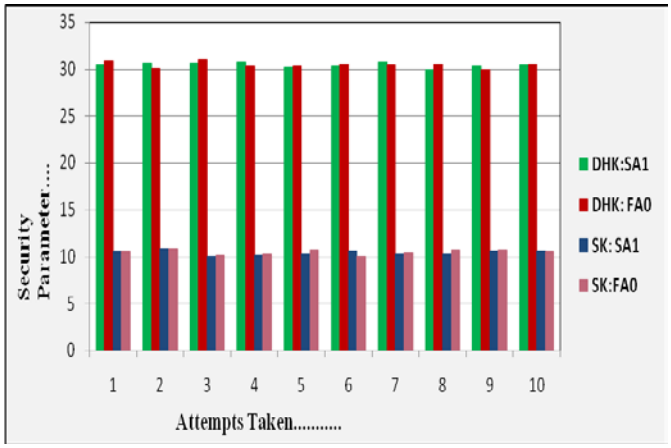
4.3 Comparative Analysis of both approaches

The comparative analysis of execution time and security parameter in case of both static key and dynamic hybrid key concludes that The algorithm execution time is less in case of Dynamic Hybrid Key than the Static Key either the key is successfully authenticated or not. Similarly, the security parameter or security improvement percentage is better in case of Dynamic Hybrid Key (approximate to 30) than the static key (Approximate to 10). Here,

DHK-SA1: denotes Dynamic Hybrid Key: Successful Authentication
DHK-FA0: denotes Dynamic Hybrid Key: Failed Authentication
SK-SA1: denotes Static Key: Successful Authentication
SK-FA0: denotes Static Key: Failed Authentication



Graph 1.5: Comparison of execution time for both keys



Graph 1.6: Comparison of security parameter for both keys

5. Conclusion and Future Scope

A new and innovative algorithm for cloud environment is proposed in this work which provides a security at different levels of different layers of architecture using hash functions. The security at the host level is provided with encryption using the dynamic hash or hybrid keys. The dynamic hash keys are used for a security at data center and virtualization level security. The security at application level is provided by authentication process. The security at the network level is provided with a Broker ID. At last the approach with a simple static key is taken for just a comparison purpose. The proposed algorithm is then also analyzed in terms of some parameters. The analysis concludes that dynamic hybrid keys provide a better security improvement percentage and execution time. The data selection is random hence there are no delays for receiving input.

But these results are not enough and there are several directions in which this investigation can go in. The cryptographic techniques are essential, but not the only one, method to protect private data against partially trustworthy cloud server. Therefore, future scope of work is:

- To test the proposed model for checking it against its fault tolerant power.
- The QOS (quality of service) of proposed model may be determined in terms of some availability, throughput and delay.
- The algorithm with keyed hash function will be designed to check the performance against this keyless hash function algorithm.

References

[1] Liu, P. You, Y. Peng, "Security Issues and Solutions in Cloud Computing", IEEE-computer society, 2012.
[2] R. Padhy, M.Patra, S.Satapathy, "Cloud Computing: Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.
[3] M.Walloschek, B.Grobauer,Stöcker,"Understanding of Cloud Computing Vulnerbilities", IEEE Compter and Reliability Society, 2011.
[4] S. Hariri, and Y.Al-Nashif, "Resilient Cloud Data Storage", ACM-NSF Center for Cloud and Autonomic Computing, 2013
[5] A. Jaber, M. Fadlili, "The Use of Cryptography in Cloud environment", IEEE International Conference and Computing and Engineering, December 2013.
[6] William Stalling, A Handbook on "Cryptography and network Security" by Pearson Education, 2009
[7] D.Rajesh Kumar, R. Gupta, Tanisha, "File Security in Cloud using Two-tier Encryption and Decryption", IJARCSSA, vol.3, issue 7, July 2013.
[8] Gurpreet Kaur, Manish Mahajan, "Analyzing the Data Security for a Cloud Computing Using Cryptographic Algorithms", International Journal of Engineering Research and Applications, vol.3, issue 5, pp.782-786, Sep-Oct 2013.
[9] H. Galli, Padmanabham, "Data Security in Cloud using the Hybrid Encryption and Decryption", IJARCSSE, vol.3, issue 10, Oct.2013.
[10] Hashem, K. Nafi, Tonny S. Kar, S. Hoque, "The Newer user authentication, File encryption & Distributed server based Cloud Computing security architecture", International Journal of Advanced Computer Science and Applications, vol.3, no.10., 2012
[11] K. Kaur, Er. Seema, "The Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", International Journal of Engineering Research and Applications, vol.2, issue 5, Sep-Oct 2012.
[12] K. Dubey, M. Namdev, S. Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE sixth international conference, 2012.
[13] D. Subbiah, S. Muthukumaran, T. Ramkumar,, "The enhanced survey and proposal to secure the data in cloud computing environments", IJEST, vol.5, no.01, January 2013.
[14] X.Wu, P.D.Le, H.Ngo, C.Wilson, B.Srinivasan, "Dynamic Key Cryptography and Applications", IJNS, Vol.10, No.3, PP.16, May 2010.

Author Profile

Er. Jashanpreet Pal Kaur has received her B.Tech degree in Computer Science and Engineering from MIMIT, Malout under PTU, Jalandhar in 2012. She is pursuing M.Tech (Regular) degree in computer engineering from Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo (Bathinda). Her research interest is in field of networking.

Er. Rajbhupinder Kaur has received her M.Tech Degree from Punjabi University, Patiala in 2010 and B.Tech degree from Punjab Technical University, Jalandhar in 2006. She is working as Assistant Professor in Yadavindra College of Engineering, Talwandi Sabo, Bathinda Punjab. Her research interests are in the fields of Mobile Ad-Hoc Network, Network Security, Nanotechnology, wireless sensor networks. She has published many national &international papers.