Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review Paper on 3 Step Mechanism Using RSA, AES and MD5 to Improve the Security in Cloud Environment

Pankaj Kamboj*, Er. Lovnish Bansal
Department of CSE, I.K Gujral, PTU,
Punjab,India

Abstract— Cloud computing is a computing paradigm in which software, platform or infrastructure are delivered as ondemand services, thus providing a highly scalable and costeffective environment for running IT applications such as high performance computing, multimedia services and enterprise applications, which require ever-increasing computational resources. A new data security algorithm by using the hybrid approach of RSA, AES and MD5 has been proposed in this research paper. This research work will provide the solutions to the various data security attacks and vulnerabilities in the cloud environment.

Keywords— Cloudlets, RSA, AES, Virtual Machine, MD5, Datacenter, Security

I. INTRODUCTION

Cloud Computing is one of the biggest technology advancement in recent times. It has taken computing in initial to the next level. Cloud computing is one of the biggest thing in computing in recent time. Cloud computing is a broad solution that delivers IT as a service. Cloud computing uses the internet and the central remote servers to support different data and applications. It is an internet based technology. It permits the users to approach their personal files at any computer with internet access. The cloud computing flexibility is a function of the allocation of resources on authority's request. Cloud computing provides the act of uniting. Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet. In the cloud computing, the internet is viewed as a cloud. By the use of cloud computing, the capital and operational costs can be cut.

II. RELATED WORK

Dinesh Devkota et al. (2015) introduces a new security mechanism that will enforce cloud computing services against breaches and intrusions. Existing techniques for securing servers used for cloud computing and storage of data has also been surveyed. In addition to these techniques, a newly developed technique for security in cloud-based servers (MIST) has been described. Due to the relevance of cloud systems in gathering sensitive information in aerospace platforms, the techniques will also need to prevent common attacks through weak password recovery, retrieval, authentication and hardening systems, otherwise hackers will be able to compromise even the protected systems.

Neha Kajal et al. (2015) analyzed the various security aspects that are vulnerable to the cloud computing and needed to be resolved. This will help to upgrade promising benefits of cloud computing so that consumers cannot have a second thought regarding its adoption.

Mehdi Ezzarii et al. (2015) focuses on the performance of intrusion detection solutions (IDS) by analyzing their performance in terms of recognition, security and capacity. The main aim of this research work is to help engineers to implement adequate solution (IDS) depending on the security levels of cloud computing. The proposed method is based on two-stage. The first stage consists on studying the needed requirements of IDS solution in cloud computing. The second stage classifies security attacks based on four levels. The classification identifies attacks that we should treated with the fitting solution.

Priyanka Ora et al. (2015) proposes the solution to maintain data security and data integrity. This scheme contains a combination of RSA Partial homomorphic and MD5 hashing algorithm .In this solution data is encrypted by RSA Partial before uploading it on cloud server. After uploading its hash value is calculated by MD5 hashing scheme. All these approaches undergo through the following steps Encryption/Decryption, Data uploading on a cloud, Hashing and Verification.

Nivedita Shimbre et al. (2015) discusses the file distribution and SHA-1 technique. When file is distributed then data is also segregated into many servers. So here the need of data security arises. Every block of file contains its own hash code, using hash code which will enhance user authentication process; only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on cloud. Third party auditor is used for public auditing. The research work discusses the handling of some security issues like Fast error localization, data integrity, data security. The proposed design allows users to audit the data with lightweight

communication and computation cost. Analysis shows that proposed system is highly efficient against malicious data modification attack and server colluding attack. Performance and extensive security analysis shows that proposed systems are provably secure and highly efficient.

III. PROBLEM FORMULATION

The only way to increase data protection, confidentiality and integrity is to keep in mind that the data is protected during transmission and at rest within the cloud using file-level encryption. As the CSA Security Guidance points out, "encryption offers the benefits of on the cloud service provide reliable data transmission on cloud provider and lack of dependence on detection of operational failure.

- In the existing work, direct connection has been established with the client and cloud service provider. The provider will easily come to know about the client's identity, thereby leading to the data mining based attacks.
- The cloud service provider can easily extract the valuable information from the data stored at the cloud end.
- No back up server is defined at the cloud provider that can lead to permanent loss of data in the case of any failure in the hardware.

IV. OBJECTIVE

- To study the existing security based solutions in cloud environment.
- To implement the 3-step mechanism to enhance the security in cloud computing by making use of gateway between the client and cloud provider.
- To implement the RSA homomorphic algorithm while sending the data from the client to the cloud gateway.
- To implement the AES encryption algorithm while sending the data from the cloud gateway to the cloud service provider (CSP).
- To implement the concept of client based read/write policies.
- To maintain the integrity of data stored at the Cloud service provider using MD5 hashing algorithm
- To implement the proposed security solution in cloud environment and compare the performance of existing algorithm with the proposed algorithm.

V. PROPOSED WORK

- Client will enter the data that has to be sent to the Cloud Provider.
- The RSA homomorphic algorithm will be performed at the client side which will encrypt the data before sending the data to the gateway.
- This encrypted data is then transferred to the gateway.
- Gateway will receive the data and will perform the MD5 hashing algorithm and will further apply the AES (Advanced Encryption Standard) algorithm.
- Gateway will store the details of the user and the uploaded file in the user identity table.
- Afterwards Gateway will transfer the encrypted file to the cloud provider for storage.
- Cloud provider will store the data received from the gateway and is also backed up inside the backup server.
- The cloud provider will store the data and will perform the MD5 hashing algorithm on it to generate the hash values. These hash values are stored at the gateway.

By making use of this approach, we will be able to achieve following purposes:

- If anyone tries to hack the data while transferring from client to the gateway, he/she will get only encoded data.
- If anyone tries to perform the mining on the files stored at the cloud provider, no results will be retrieved as there is no identity of user at the cloud provider.

During downloading the file from cloud end, the client will follow the following steps:

1. Client will ask the gateway to download his/her stored file.
2. Gateway will forward the request to the cloud provider and cloud provider will send the new generated hash value of the requested file.
3. The gateway will match the hash value with the previously stored hash value. If the values have been matched then the downloading will take place, else there is violation of integrity policy at the cloud provider.
4. If the hash values have been matched, then the cloud provider will send the encrypted file to the gateway and gateway will perform the AES decryption algorithm.
5. Now, the gateway will generate the hash value and will further match the newly generated hash values with the value stored at the client side.
6. The gateway will further send the decrypted file to the client and client will finally perform the RSA decryption mechanism and the original data is obtained.

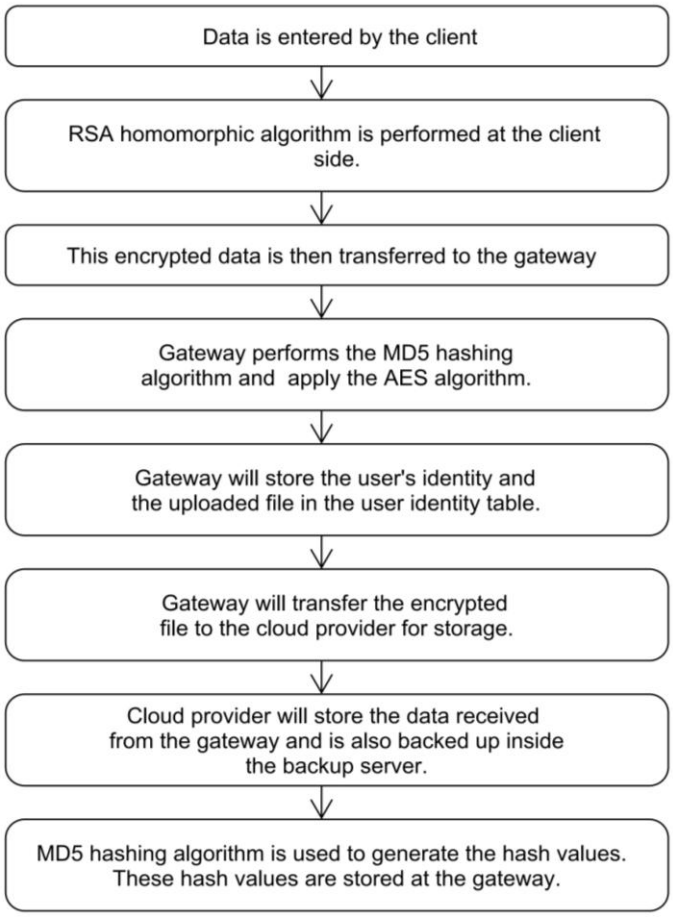

Figure: Flowchart of the Proposed Work

VI. IMPLEMENTATION TOOLS

Implementation Language Java:

Java is a general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that code that runs on one platform does not need to be recompiled to run on another. Java applications are typically compiled to bytecode [16] that can run on any Java virtual machine (JVM) regardless of computer architecture. Java is, as of 2014, one of the most popular programming languages in use, particularly for client-server web applications, with a reported 9 million developers.

Cloud Sim:

CloudSim is an extensible simulation toolkit that enables modeling and simulation of Cloud computing systems and application provisioning environments. The CloudSim toolkit supports both system and behavior modeling of Cloud system components such as data centers, virtual machines (VMs) and resource provisioning policies. It implements generic application provisioning techniques that can be extended with ease and limited effort. Currently, it supports modeling and simulation of C loud computing environments consisting of both single and internetworked Clouds (federation of Clouds).

VII. CONCLUSION

Security is the key for the success of the cloud environment. In order to avail the benefits of cloud, we must ensure the security of data being transferred between the client and user. New attacks have been appearing day by day and we need some strong mechanism to handle with all the types of attacks. In this paper we have analyzed the different solutions given by the authors and have proposed a new security solution by using the hybrid combination of encryption algorithms link AES and RSA. We will be using the MD5 hashing algorithm along with the encryption algorithms for the verification process.

REFERENCES

[1] D. Devkota, P. Ghimire, D. J. Burris and D. I. Alkadi, "Comparison of Security Algorithms in Cloud Computing," IEEE , pp. 1-7, 2015.
[2] N. Kajal , N. Ikram and P. , "SECURITY THREATS IN CLOUD COMPUTING," IEEE, pp. 691-694, 2015.
[3] M. EZZARII, H. . E. GHAZI, , H. ELGHAZI and T. SADIKI, "Performance Analysis of a Two Stage Security Approach in Cloud Computing," IEEE, 2015.

[4] P. Ora and D. Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography," IEEE International Conference on Computer, Communication and Control (IC4-2015)., 2015.

[5] N. Shimbre and P. P. Deshpande, " Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm," IEEE, pp. 35-39, 2015.

[6] V. k. pant, J. Prakash and A. Asthana, "Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques," IEEE, pp. 490-494, 2015.

[7] Y. Zhu and J. Zuo , "Research on Data Security Access Model of Cloud Computing Platform," IEEE, pp. 424-428, 2015.

[8] Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013

[9] Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013

[10] Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012.

