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 a Hybrid Model of Steganography and Blowfish to Ensure Data Security in Cloud Environment

Amanpreet Kaur*, Er.Khushdeep Kaur
Department of CSE, I.K Gujral PTU,
Punjab, India

Abstract: ***Cloud Computing is a model for enable infinite network access, convenient usage, on-demand service and scalable resources that are billed on utility basis.Cloud Computing model provides five essential characteristics, four deployment models and three service models.In this paper, we have proposed a new security algorithm with efficient use of AES algorithm , steganography and blowfish algorithm.We will be implementing the above proposed work in cloud sim simulation tool.***

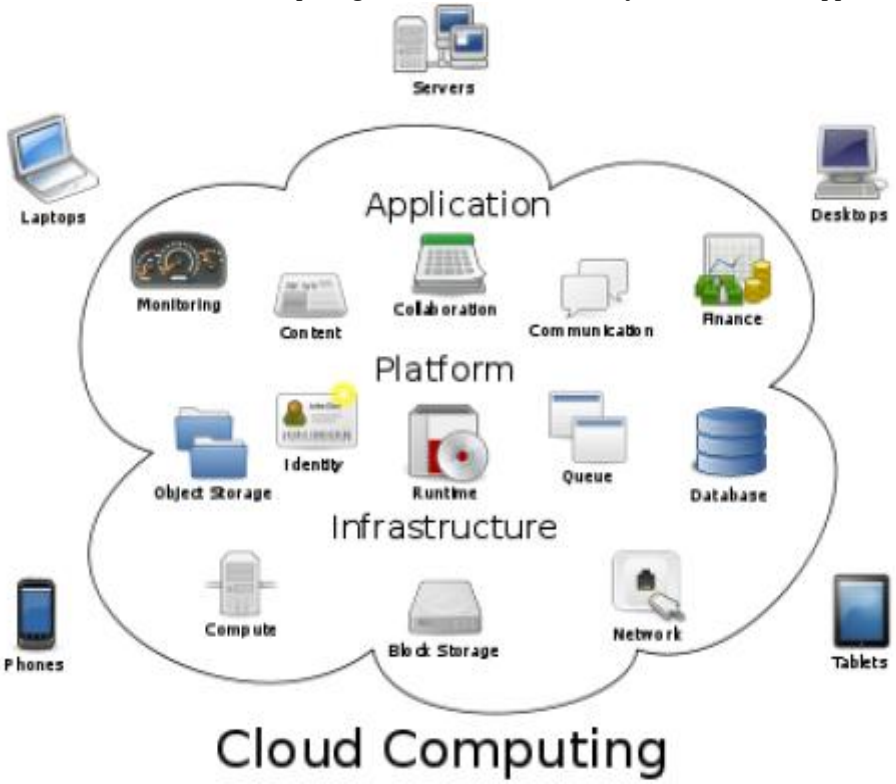
Keywords: cloud computing, Datacentre, Blowfish, AES, Steganography

I. INTRODUCTION

Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud is a broad solution that delivers IT as a service. Cloud computing is an internet based technology uses the internet & central remote servers to support data and applications. It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access. Cloud computing also provided shared resources like electricity distributed on the electrical grid. Before cloud computing, websites and server based applications were executed on a specific system. The cloud computing flexibility is a function of the allocation of resources on authority's request. And the cloud computing provides the act of uniting. The definition of cloud computing provided by National Institute of Standards and Technology (U.S Department of Commerce) is as follows:

"Cloud Computing is a model for enable infinite network access, convenient usage, on-demand service and scalable resources that are billed on utility basis. Cloud Computing model provides five essential characteristics, four deployment models and three service models."

There is no doubt that the convenience and low cost of cloud computing services have changed our daily lives; however, the security issues associated with cloud computing make us vulnerable to cybercrimes that happen every day



II. RELATED WORK

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.

Vinay Kumar et al. (2015) describes how to secure data and information in cloud environment in time of data sharing or storing by using cryptography and steganography technique. Cloud computing is based on network and computer applications. In cloud data sharing is an important activity. Small, medium, and big organization are use cloud to store their data in minimum rental cost. In present cloud proof their importance in term of resource and network sharing, application sharing and data storage utility. Hence, most of customers want to use cloud facilities and services. So the security is most essential part of customer's point of view as well as vendors. There are several issues that need to be attention with respect to service of data, security or privacy of data and management of data.

Pallavi Kulkarni et al. (2015) provides platform for providing business or consumer IT services over the Internet. The computing capability of mobile systems is enhanced by Cloud computing. Mobile devices can rely on cloud computing and information storage resource, to perform computationally intensive operations such as searching, data mining, and multimedia processing. Along with traditional computation services it provides, mobile cloud also enhances the operation of traditional ad hoc network by treating mobile devices as service nodes, e.g., sensing services. The sensed information, such as location coordinates, health related information, should be processed and stored in a secure fashion to protect user's privacy in the cloud.

Saakshi Narula et al. (2015) provides the review of security research in the field of cloud security. After security research we have presented the working of AWS (Amazon Web Service) cloud computing. AWS is the most trusted provider of cloud computing which not only provides the excellent cloud security but also provides excellent cloud services.

Patil Madhubala et al. (2015) studies the various data security concerns such as various reconnaissance techniques, denial of service, account cracking, hostile and self-replicating codes, system or network penetration, Buffer overflow, SQL injection attack.

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.

1. No Integrity checks have been implemented that will verify the originality of the data stored at the cloud provider. Verification is an important domain of cloud computing model. In this part data present on cloud is verified by data owner just to check data integrity. This task is performed at cloud server end. A hash value is calculated of the uploaded data and is returned back to the data owner. In future data owner can verify their data by requesting for verification option. As owner requests for this option hash value of the data present at cloud is calculated. This calculated hash value is matches with the old hash value which is present at owner end. If this value match's then data present at the cloud is safe and no modification has been done if it does not match then there are some changes on cloud data.
2. No Authentication and authorization mechanism is mentioned in the paper that will provide proper rules and permissions to the users. No read/write policies have been implemented in the present work that will provide the grants and permissions to the user for different types of tasks.
3. A single encryption algorithm is used to encrypt the data which can be risky at the times when we have to store our credentials or utmost important data at the cloud provider. A hybrid mechanism containing multiple sequences or multiple iterations should be used to provide the security that is needed at the cloud end.

IV. OBJECTIVES

- To study the existing security based solutions in cloud environment.
- To implement the OTP (One Time Password) based authentication and authorization mechanism for granting the permissions to the cloud users.
- To implement the data verification process while uploading and downloading of the data using SHA1 hashing algorithm.
- To implement the Blowfish encryption algorithm along with steganography while sending the data from the cloud gateway to the cloud service provider (CSP).
- To implement the proposed security solution in cloud environment and compare the performance of existing algorithm with the proposed algorithm.

V. PROPOSED WORK

Methodology

- Client registers with the cloud service provider using his/her ID and password.
- The cloud provider will fetch the client's data and will register the client with the database stored at the cloud service provider.
- After successful registration, the client will try to login using his/her ID and Password. The provider will authenticate the client's credentials.
- If the Username and password are correct, then the cloud provider will generate the OTP based on client's data using SHA1. The OTP can be alpha-numeric and is encrypted using Blowfish and is sent to the client's registered E-mail Id.
- The client will enter the retrieved OTP and will send it to the cloud provider. The cloud provider will match the incoming OTP with the generated OTP and will check the user's read/write permissions.
- Based on the user's permissions, the cloud provider will generate the user authorization ticket.
- Now the client will choose the data to be sent to the cloud provider. At the client side, Blowfish encryption will take place and will convert the original data into ciphers.
- The encrypted data is then encoded into an image using the concept of steganography. An image is chosen randomly and the edges of the image are filtered out using canny edge detection methodology. The least significant bit is then replaced with the data bytes.
- This encoded image is sent to the cloud service provider.
- The SHA1 algorithm has been chosen for implementing the hash values at the cloud provider. The hash value is stored at the client side for verifying the originality of the data.

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

- During downloading the file from cloud end, the client will follow the following steps:
- Client will ask the cloud provider for downloading his/her stored data.
- The cloud provider will generate the new hash value of the client's stored data. This hash value is matched with the previously generated hash values.
- If the values have been matched then the downloading will take place, else there is violation of integrity policy at the cloud provider.
- If the hash values have been matched, then the cloud provider will send the encoded image to the client.
- The client will retrieve the image and will apply the steganography mechanism to decode the image and will retrieve the data from the edges using canny edge detection.
- After fetching the data, the client will again apply the blowfish decryption mechanism to obtain the original data.

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 byte code [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

All the cloud service models not only provide different types of services to end users but also disclose information security issues and risks of cloud computing systems. There is a risk of data loss in cloud environment. The data of the client needs to be transferred and should be stored with proper encryption algorithms. In this paper we have proposed a solution that will enhance the security of the cloud data by using the BlowFish encryption algorithm along with steganography. The SHA1 verification algorithm is used to verify the user's data. The OTP(One-time-password) mechanism will be implemented to authenticate the user's identity before accessing the cloud data.

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.

