Cloud Computing Using Encryption and Intrusion Detection

Tony Durgadas Jagyasi[1]
[1]Dept. of Computer Science and Engineering
[1]Nagpur Institute of Technology Nagpur, India

Abstract— Cloud computing provides many benefits to the users such as accessibility and availability. As the data is available over the cloud, it can be accessed by different users. There may be sensitive data of organization. This is the one issue to provide access to authenticated users only. But the data can be accessed by the owner of the cloud. So to avoid getting data being accessed by the cloud owner, we will use the intrusion detection system to provide security to the data. The other issue is to save the data backup in other cloud in encrypted form so that load balancing can be done. This will help the user with data availability in case of failure of one cloud.

Keywords: Cloud Computing, Encryption, Intrusion Detection, Encryption Algorithm.

I. INTRODUCTION

The use of cloud computing has increased rapidly in recent years in many organizations. Cloud computing provides many benefits to the users such as accessibility and availability. As the data is available over the cloud which is accessed by number of different users, so there are some security issues related to the storage of the data over the cloud. There may be sensitive data of organization which is stored over the cloud which can be accessed by any user. This is the one issue to provide authentication of the user to access the data whether it's the owner of the cloud service provider or the top management of the company.

The other issue can be if the cloud where the data is stored if fails. If such things happen then there will be need to store the same data in multiple clouds, so that if one cloud fails then the user will get the data from the other cloud i.e. to create backup of the encrypted data. With this, the cloud will not get heavy due to access of the same data by multiple authenticated users.

II. LITERATURE SURVEY

Cloud computing is used to describe platform and type of application. This platform dynamically provides provisions, configures, reconfigures, and servers as needed by the cloud. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices [3]. Cloud computing also describes applications that are extended to be accessible through the Internet. These cloud applications use large data centers and powerful servers that host Web applications and Web services. Anyone with a suitable Internet connection and a standard browser can access a cloud application.

Security in cloud is one of the major areas of research. The survey shows that, the researchers are focusing on efficient algorithms and encryption techniques to enhance the data security in cloud.

Cloud Computing allows customers to utilize resources and software's which are hosted by service providers. It mainly reduces infrastructure investment and maintenance cost. Computing infrastructure is not known to the users and resources are provided virtually in cloud. High Performance Computing (HPC) allows scientists and engineers to solve scientific, engineering and business problems using different applications that require high computational capabilities.

Cloud computing build a decades of research in virtualization, utility computing, and web and programming administrations [5]. It suggests an administration arranged structural planning, diminished data innovation overhead for the close client, extraordinary adaptability, decreased aggregate cost of proprietorship, on-interest administrations and numerous different things. Cloud computing alludes to both the provisions conveyed as administrations over the Internet and the fittings and frameworks programming in the datacenters that furnish those administrations. Cloud computing portrays both a stage and a sort of requisition. A cloud computing stage powerfully designs, reconfigure, and provisions servers as required. Cloud provisions are requisitions that are broadened to be approachable through the Internet. These cloud provisions utilize vast server farms and effective servers that have Web requisitions and Web administration.

Intrusion detection (NIDS) and prevention systems (NIPS) serve a critical role in detecting and dropping malicious or unwanted network traffic [8]. These have been widely deployed as perimeter defense solutions in enterprise networks at the boundary between a trusted internal network and the untrusted Internet. This traditional deployment model has largely focused on a single-vantage point view of NIDS/NIPS systems, placed at manually chosen (or created) chokepoints to provide coverage for all suspicious traffic.

Intrusion detection systems (IDS) that are used to find out if someone have gotten into or are trying to get into your network. The most popular IDS are Snort, which is available at http://www.snort.org [9].

III. PROBLEM STATEMENT

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with single cloud providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

We have also addressed the problem of Accuracy, Authenticity and Efficiency arises for building robust and efficient intrusion detection systems.

So to solve the problem of cloud computing, we can make the data available in multiple clouds in the encrypted form, so that only the authenticated users can only access the data from the cloud. This helps the cloud to share

the load for load balancing and make the data available in case of failure of one cloud.

The problem is to provide security to the data from different users getting access over the sensitive data and get the cloud balanced by load balancing methods and give the access of the data to the authenticated users only.

The problem of authentication can be solved by using the layered approach of the intrusion detection system. In this method all the layers will work autonomously. There will be no problem of the authentication of the user accessing the data from the cloud due to the different layers of the system performing independent functions to check the user authenticity.

IV. PROPOSED APPROACH

The proposed approach will consist of multiple clouds where the user's data will be available in the encrypted form. The same data will be available in the different clouds, so this will help the authenticated users to access the data easily and allows the cloud to balance the load while data being retrieved by the number of authenticated users at the same time. With this the data will be retrieved by the authenticated users only. If the other user tries to access the data from the cloud, the user will have to pass from the various security points i.e. different layers of the Intrusion detection layers where the authentication of the user is done. If the user seems to be authenticated then only the user will get access to the data.

V. METHODOLOGY

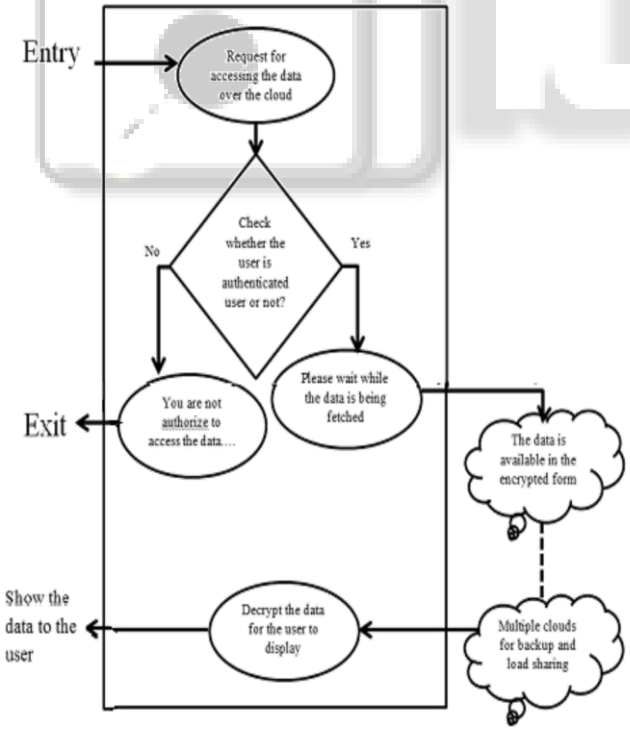

Fig. 1: Flow Diagram

With the help of different security algorithms such as RSA algorithm, Brute force attack algorithm, Shamir's algorithm etc. we are going to provide the security to the data available over the cloud to maintain the integrity of the stored data. With the help of different load balancing, the load of the clouds will be shared among different clouds so that the availability of the data should be maintained and the data retrieval can be done easily by the authorized users.

Network security is of primary concerned for large organizations. Various types of Intrusion Detection Systems (IDS) are available in the market like Host based, Network based or Hybrid depending upon the detection technology used by them. Modern IDS have complex requirements. With data integrity, confidentiality and availability, they must be reliable, easy to manage and with low maintenance cost. Various modifications are being applied to IDS regularly to detect new attacks and handle them. In this we will use genetic algorithm (GA) and data mining based Intrusion Detection System.

With this all, the security of the data is maintained with availability of the integrated data within the durable time to access/ retrieve the data by the user.

VI. TOOLS FOR DEVELOPMENT AND VERIFICATION OF RESULT

- Hardware requirement: Personnel Computer, Pentium processor PIII and above, Ram 512 and above, Hard disk 20GB, Internet connection.
- Software requirement: HTML, Java, JavaScript.
- Database Connectivity: MySQL/VB.

ACKNOWLEDGMENT

We would like to thanks to all those who has given the proper support and guidance. We would also like to thanks to the dept. head and all the staff.

REFERENCES

[1] Privacy Preserving Public Auditing for secure cloud storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE.
[2] Insider Threats to Cloud Computing: Directions for New Research Challenges BY William R Claycomb, Alex Nicoll Carnegie Mellon University.
[3] Efficient Computing With Cloud. Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[4] Cloud Computing Security: From Single to Multi-Clouds 2012 45th Hawaii International Conference on System Sciences.
[5] Impact of Cloud Computing on IT Industry: A Review & Analysis International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 01– Issue 02, November 2012
[6] Network-Wide Deployment of Intrusion Detection and Prevention Systems
[7] IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 1, JANUARY-MARCH 2010 Layered Approach Using Conditional Random Fields for Intrusion Detection
[8] Intrusion Detection System using Genetic Algorithm and Data Mining International Journal of Computer Science and Informatics ISSN (PRINT): 2231 –5292, Vol-1, Iss-4, 2012
[9] Intrusion Detection Systems with Snort 2003 Pearson Publication.

