Data Leakage Detection In Cloud Computing

Saurabh Yadav[1], Shivam Prajapati[2], Ashfaq shaikh[3], Avinash Yadav[4]

[1,2,3,4] *Student, Diploma(Computer), Thakur Polytechnic, Mumbai*

---***---

Abstract - *A sensor network is a group of specialized transducer with a communications infrastructure for monitoring and recording conditions at diverse locations. Cloud computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unprecedented advantages: on-demand self-service, ubiquitous network access***.** *And This system develops a strengthened security model for considering data security against data leakage attack in cloud and the storage server in the upload phase of an integrity verification scheme. And presents an efficient verification scheme for ensuring remote data integrity in cloud storage.*

Key Words: In packet bloom-filter, Cloud Sim, Tight lip, Cipher Trust, Private data, Cloud Audit Server

1. INTRODUCTION

A sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable.

2. EXISTING SYSTEM

Privacy Oracle also employs a similar technique, which the authors term differential black-box fuzz testing, to monitor perturbations in network traffic from different inputs. However, the system requires executing the application and rolling back to re-execute with different input providing no real-time protection and the algorithm to detect divergent output in network. Another recently common approach to mitigating information leakage is information flow tracking.

2.1 WORKING IN EXISTING SYSTEM

Stations called sensor nodes, each of which is small, lightweight and portable.

All marks of weekly test and unit test are displayed on notice board; timetable of daily class routine is displayed on notice board.

3. PROPOSED SYSTEM

In proposed system, the system proposes a new cloud storage scheme in proof of retrievable for cloud storage, in which a trustworthy audit server is introduced to preprocess and upload the data on behalf of the clients. On the other side we improve the semi-honest trust worthy and ensure dynamic data process in cloud.

3.1 USE CASE DIAGRAM

In the current interface there is an : User data has upload in cloud while satisfy the user integrity proof.

- In this Module We Verify the cloud user authentication
- The user doesn't trust the process has been abort
- Its proved secure against recent attacks in strengthened security model while supporting efficient public verifiability

3.2 FLOW DIAGRAM

- The cloud server reduces the clients burden by maintaining their files and sequentially monitor user's cloud account while end of user's action it dynamic update user's account .
- The process takes over by using Integrity Verification algorithm.
- Its work carrying out multiple challenges-responses. Under the Shacham and Waters proposed a security model for PoR system which achieve number of checking.

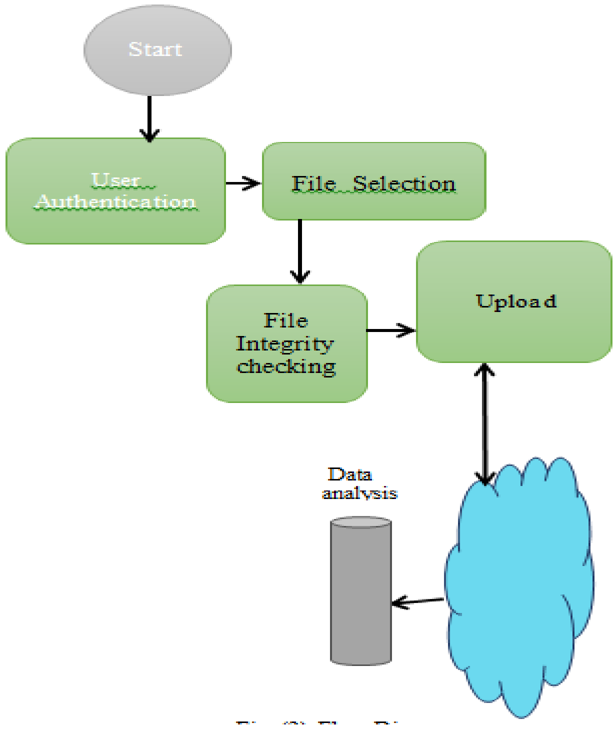

Fig .(2) Flow Diagram

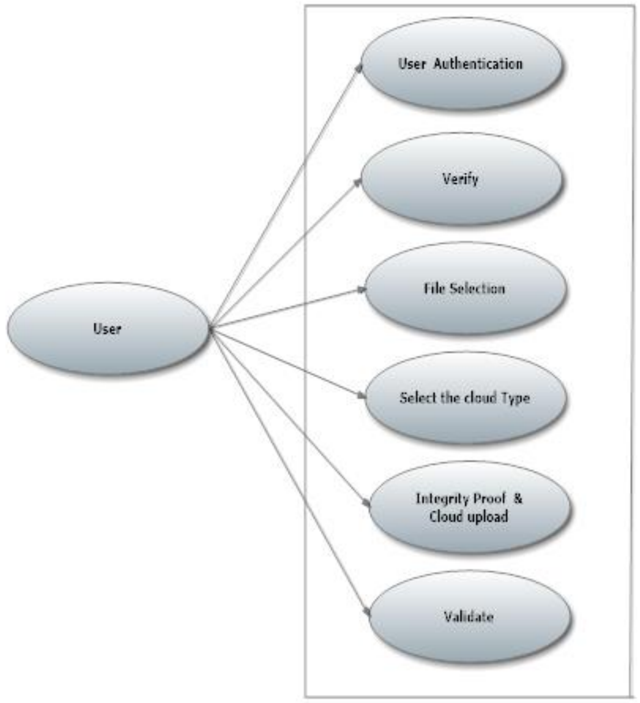

Fig .(1) Use Case Diagram

4.1 ADVANTAGES

1. Computation cost is low.
2. The computation burden is not huge for the users. Data Process also work in very efficient manner.
3. The cloud audit server (CAS) is not required to have high storage capacity.
4. It proved secure against reset attacks in the strengthened security model while supporting efficient public verifiability and dynamic data operations simultaneously.

4.2 FUTURE SCOPE

we have shown it is possible to assess the likelihood that an user is responsible for a leak, based on the overlap of his data with the leaked data and the data of other users, and based on the probability that objects can be ‘guessed´ by other means. Our model is relatively simple, but we believe it captures the essential tradeoffs. The algorithms we have presented implement a variety of data distribution strategies that can improve the distributor’s chances of identifying a leader in further research work.

5. CONCLUSION

Preventing sensitive data from being compromised is an important and practical research problem. The algorithms in this project achieve precise results by discounting fields that are repeated or constrained by the protocol. Specifically, in our scheme tags should be authenticated by the client in each protocol execution other than calculated or prestored by the client.

REFERENCES

[1] Adobe Systems Incorporated. Adobe Flash Player. HTTP://www.macromedia.com/software/flash/about, 2008.

[2] R. Anderson and F. Petit colas. On the Limits of Steganography. IEEE Journal of Selected Areas in Communications, 16(4):474-481, 1998.

[3] K. Borders and A. Prakash. Web Tap: Detecting Covert Web Traffic. In Proc. of the 11th ACM Conference on Computer and Communications Security (CCS), 2004.

[4] K. Borders and A. Prakash. Towards Quantification of Network-Based Information Leaks Via HTTP. In Proc. of the3rdUSENIX Workshop on Hot Topics in Security, 2008.

[5] J. Gailly and M. Adler. The gzip Home Page. http://www.gzip.org/, 2008.