**A Survey on Data Integrity Checking and Enhancing Security for Cloud to Fog Computing**

**ABSTRACT:**

Cloud computing plays an important role in the computing world as it provides a cost-effective way of delivering services to customers through the internet. The Cloud Service Providers (CSPs) offer an enormous amount of storage space with low cost and eliminates the data management burden of the customers. As the operational details are not transparent, the CSPs may be untrusted. They may steal the user data, tamper the data, remove the rarely accessed data or hide the data loss by duplicating the data. In such cases, data integrity fails and needs to be addressed. The emerging fog computing paradigm extends the cloud platform to provide services for IoT applications. So the data integrity verification techniques are not only to be incorporated over the cloud but also to be extended for fog computing. This survey discusses the various data integrity checking methodologies for both cloud and fog environment.

**EXISTING SYSTEM:**

Existing cloud data integrity verification methods are not suitable for fog environment because of its cryptographic nature. So there is a need for a lightweight scheme to verify the data integrity in the fog environment. Cloud storage reduces the capital cost, application deployment time, information management and maintenance but it raises security challenges like confidentiality, availability and integrity since the data are not under the control of the user

**DISADAVANTAGES:**

* Cloud storage reduces the capital cost, application deployment time, information management and maintenance but it raises security challenges like confidentiality, availability and integrity since the data are not under the control of the user
* Data might get deleted either due to technical glitch or due to administration errors.
* Security issues
* Maintenance and Power Consumption

**PROPOSED SYSTEM:**

The intent of this survey is to study the various techniques based on the authentication structures used for data integrity verification in the cloud and fog environment and to analyze their pitfalls.The classifications are root signature-based, BF-based, tag regeneration-based and tablebased schemes. This survey concludes that root signaturebased schemes are suitable for integrity verification in a single copy of dynamic data, BF-based schemes are suitable for a single copy of static data, tag regeneration-based schemes are suitable for IoT data and table-based schemes are suitable for multiple copies of dynamic data.

**ADAVANTAGES:**

* Data redundancy
* Ability of users to access information without any interruption.
* Traditional techniques (RSA, MD5) that are used for integrity verification require the user to download the data, compute the metadata and verify it with the already stored one.
* It is an efficient authenticated structure

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

❖ System : Pentium Dual Core.

❖ Hard Disk : 13 GB.

❖ Monitor : 15’’ LED

❖ Input Devices : Keyboard, Mouse

❖ Ram : 32GB.

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 7.

Coding Language : Java

Tool : Netbeans

Database : MYSQL

**REFERENCE:**

K.Uma Maheswari Department of CSE National Institute of Technology Tiruchirappalli 620015, India 406118003@nitt.edu,“ **A Survey on Data Integrity Checking and Enhancing Security for Cloud to Fog Computings**”, 978-1-7281-4167-1/20/$31.00 ©2020 IEEE