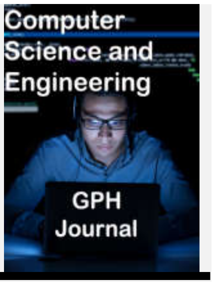
GPH JOURNAL

Global Publication House Journal
Computer Science & Engineering



Securing Coding-based Cloud Storage opposed to malignant Attacks

Srinithy.S, Meena.R, Kavipriya.P *(Students[1,2,3])*

R Charanya *Assistant Professor (Senior)*

Vellore Institute of Technology, Vellore, Tamilnadu, India

ABSTRACT

Nowadays cloud storage is becoming an emerging technology where the user can store their data and access it remotely using the internet. But the security to the user data has become a major concern. Pollution attack, a set to corrupt our stored data in the cloud, which is considered as one of the major risks that affects data security in cloud storage. In our proposed technique, we show how to prevent the pollution attack and how to store our files safely. The following techniques and algorithm are implemented in our projects. our first technique is, the user send the data by encrypting it using **RC5 ALGORITHM**.

The user can able to upload the following file format only(.jpg, .txt). Another technique is **Checksum Method**, a user send an encrypted file to the admin by using this method. This generates a key for that particular encrypted file. The encrypted file has to be verified by the admin. By this verification the checksum method generates a key to the file.

if the file has same key means the file not hacked or not attached. After verification the admin has to upload the file safely in cloud. If the user need that file, means he/she has to send a request to the admin. Only after getting the response key from admin the user able to download the file. Our Approach is to very robust and the polluters can be easily isolated.

KEYWORDS: - Checksum Method, RC5 Algorithm, Cloud Storage, Malignant Attacks.

****

Research Article

Corresponding Author

Name: R Charanya. *Assistant Professor*
Email: ************
Contact: ************

Article Info

Received on: 03-19-2019
Revised on: 03-24-2019
Accepted on: 03-25-2019

INTRODUCTION

Block Level Cloud Storage is providing many facilities by allowing the users to store and retrieve their data in a remote storage resource which can be used as their local disks. this has become more use since the user can store to recover the original data items. However two problems arrive a very large data set as per the pay per use model. When the user need to unlock their full capacity, he/she has to address the various problems including performance, data access, integrity, confidentiality etc. The security of data in cloud requires a key for both user and admin (service provider).

Among many of the risks in cloud security pollution attack is considered as one of the major risk in ensuring trustworthiness Of the data. In this type of attack the adversary takes in control any of the storage resource and attempt to pollute the data to make the data availability difficult. This pollution attack becomes more difficult when coding techniques are employed to represent data in the storage resource.

In this case the data items are subdivided into parts, these are then encoded to get a suitable number of coded fragments which are to be placed on independent storage resources. These coded fragments are further computed such that the subset of it allows the user.

(1) Every sequence of bits will be a valid coded fragment, so there is no way to find out whether the data has been altered by third party or not unless the user recovers the corresponding data item.

(2) Even when we assume that data has been recovered and the pollution also been detected, but becomes difficult to identify in which place the data has polluted.

LITERATURE SURVEY

In this world every one using smart phones, so that each person has personal information (i.e files, photos etc..) they need to save their files in their phone device. saving in our phone device it's not safe nowadays. By saving our files in cloud storage is safe when compared to system device[1]. Many users and IT operators are getting very enthusiastic and eager about the benefits of cloud storage, such as to be developed and lead to future success so that they need to store and control data in the cloud and to gain advantage on the promise of higher-performance., so that they can access them from any location via the Internet. It provides multi-tenant model and cloud computing architecture to implement cloud storage.

The block level storage in cloud offer its users the access to virtual disks which can be accessed and used directly as if their own storage disk. A traditional Block –Level Cloud Storage should enable its users or application ,a sufficient levels of performance, availability, integrity, confidentiality for the storage of data . But this is mostly affected by performance and availability leading to the delay of process. In this paper they show how the Luby Transform(LT) codes are used to overcome the above mentioned problem.

Here are the LT codes are used to store the fragments of sectors on the storage nodes. For this an architecture of a back-end for Block –Level Cloud Storage system to achieve performance, availability, integrity, confidentiality with the use of LT codes . The performance of this system is evaluated by providing real workloads and subsequently compared with traditional BLCS .The final results showed that it can be simultaneously possible to achieve the above mentioned objectives by using LT coding based BLCS[2]. Moreover it works like typical BLCS in all aspects providing the confidentiality to the data.

In this paper they discuss the impact of pollution attack (a security threat)on coding based distributed storage systems for Wireless Sensor Network(WSN). Pollution attack a major problem whereby a third party attempt to corrupt the stored data by injecting some fake coded fragments into original data resulting in corruption of entire data. To relieve from such attacks an algorithm has been proposed[3]. Their approach is not involving any traditional methods like digital signatures or hashing techniques like checksum .The finalanalysis shows that their algorithm is suitable for practical systems and environment specially in Wireless Sensor Network.

The presentation of desultory web cipher can grief expressively when malignant nodule pollute the idea of the interchanged chocks. Foregoing effort have established fault rectifying cipher by observing few familiar enclose in ciphering view. So cipher are depend on presenting excess in length sector. Another techniques need the method of homomorphic hashing functions, which are estimate too high. In this paper, we existent a exceptional and recording powerful security algorithm, refer the invalid Keys, to identify and involve malignant violence depend on the subspace properties of unexpected even web cipher.

The cooperate nodule check the honest of a block by verifying if it appears with the subspace connected by the origin blocks. This is achievable when whole nodule has a vector orthogonal to all the compounds of the origin blocks. These vectors, related to invalid keys, refer to the invalid space of the origin blocks and analyze a uncalculated compound when separated by the origin. Unlike earlier security modus, our invalid Keys algorithm enables nodule to promptly discover demoralizing blocks without altering the cipher or venerable excess on the interchanged data. We systematically sort out the violation caused by immediate betrays, and determine the capabilities of invalid Keys by variable the capability of the malignant nodules. We also view, through wide performances, that the invalid Keys viewpoint is more powerful than generous security using homomorphic hashing when come near restraining the violation reduction.

ARCHITECTURE DIAGRAM

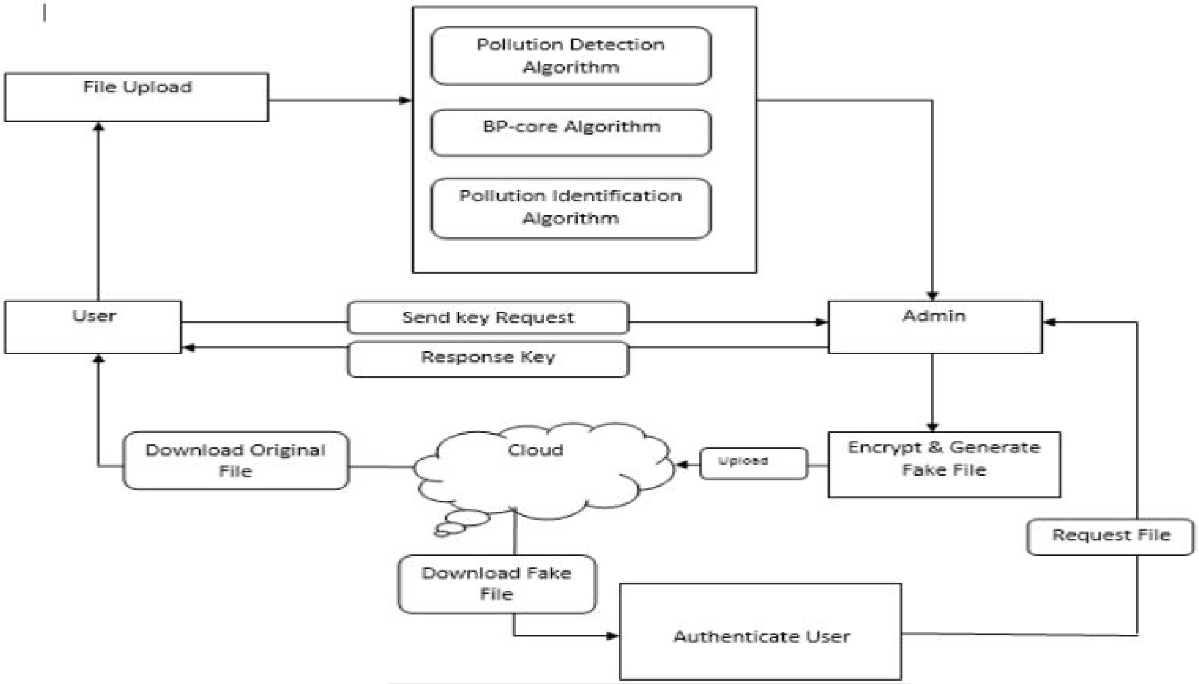


Figure 1: Architecture diagram

PROPOSED SYSTEM

In figure 1, the user sends the data by encrypting it using RC5 Algorithm. The user can able to upload the following file format only(.jpg, .txt),and the next step is Checksum Method, a user send an encrypted file to the admin by using this method.

This generates a key for that particular encrypted file. The encrypted file has to be verified by the admin. By this verification the checksum method generates a key to the file if the file has same key means the file not hacked or not attached. After verification the admin has to upload the file safely in cloud. If the user need that file means, he has to send a request to the admin. Only after getting the response key from admin the user able to download the file.

PROPOSED SYSTEM	EXISTING SYSTEM
our first technique is ,the user send the data by encrypting it using RC5 ALGORITHM. The user can able to upload the following file format only(.jpg, .txt). The another technique is Checksum Method, a user send an encrypted file to the admin by using this method. This generates a key for that particular encrypted file. The encrypted file has to be verified by the admin. By this verification the checksum method generates a key to the file if the file has same key means the file not hacked or not attached. After verification the admin has to upload the file safely in cloud. If the user need that filemeans,he has to send a request to the admin. Only after getting the response key from admin the user able to download the file.	Even though we have save our information in clouds, there is a chance to corrupt our data by untrusted parties. An attackers can easily corrupt our data by using some cryptographic keys, keystroke timing or identifying the password by using some tricks etc..

ADVANTAGE	DISADVANTAGE
Should have enough data redundancy. Very Robust approach. Able to affectively isolate the polluters. Efficient to store data with highly secured.	If one file got affected, there is more chance to all file infected by that file.

PROPOSED SYSTEM

This paper says that relative less codes permit one to pattern a effortless poisonous exposure process that can be used to examine data incorruptibility throughout the usual read performance of a cloud-based storage system. Regardless, the exposure process alone is not sufficient to interpret the almost necessary issue, i.e. to locate the spiteful, storage nodes in sequence to eliminate them from the system. Here we had initiate an algorithmic solution that utilize both poisonous exposure, authorized by relative less codes, and statistical assumption to repeatedly recognize the spiteful nodes.

We had furnish an logical model to evaluate, the time need to distinguish all defilers in a absolute cloud storage system; we also examined the successfulness of our proceed as a task of many system frameworks. At last, we had imitated a cloud storage scenario and, also by taking a account in cloud, we also convey that the initiate technique reach the expected level.

REFERENCE

[1]. [1]H. Dewan and R. Hansdah, "A survey of cloud storage facilities," in IEEE SERVICES, jul 2011, pp. 224 –231.

[2] C. Anglano, R. Gaeta, and M. Grangetto, "Exploiting rateless codes in cloud storage systems," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1313–1322, May 2015.

[3] L. Buttyan, L. Czap, and I. Vajda, "Detection and recovery from pollution attacks in coding-based distributed storage schemes," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 6, pp. 824–838, 2011.

[4] L. Buttyn, L. Czap, and I. Vajda, "Pollution attack defense for coding based sensor storage," in Proceedings of the IEEE Interna- tional Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010.

[5] E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via null space properties of network coding," in INFOCOM 2009, IEEE.

[6] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," Security and Privacy, IEEE Symposium on, 2004.

[7] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in IEEE INFOCOM, 2006.

[8] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signaturebased scheme for securing network coding against pollution attacks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008.

[9] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient scheme for securing xor network coding against pollution attacks," in INFOCOM 2009, IEEE.

[10] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT codes-based secure and reliable cloud storage service," in IEEE INFOCOM, 2012, pp. 693–701.