Dogo Rangsang Research Journal
ISSN : 2347-7180

UGC Care Group I Journal
Vol-08 Issue-15 No. 03: 2021

+Secured Image Storage Using Data Integrity Convergent Encryption Protocol

H N S Bhavani Eshwari[1], P N Ramya[2]
Computer Network and Information Security, Jawaharlal Nehru Technological University
[1]Department of Information Technology, GNITS, Telangana, Hyderabad dhansu93@gmail.com
[2]Assistant Professor, Department of Information Technology, GNITS, Telangana, Hyderabad
ramyapn1@gmail.com

ABSTRACT: Cloud Computing is an emerging technology and plays key role. Cloud service provider provides the flexibility and allows users to offload their data to the cloud and leave all the data management, maintenance and security issues to the Cloud Service Provider (CSP) who manages the services.CSP charge nominal fee to the users on usage of the resources provided by them. In the cloud storage, Security of data has become a prime concern, replication and dissemination of multimedia data become increasingly. Due to the increase in data usage, the storage space had been compromised for redundant data which means occurrence of the same data provided by millions of users creates wastage of available space on the cloud. To overcome the above problem data deduplication techniques are employed. Those techniques eliminate the redundant data on cloud by using Data Integrity Convergent Encryption Protocol. In this proposed system, we employee the protocol where each image in the formats of .jpeg, .png and .tiff is divided into blocks, rehashed, encrypted and these blocks which are common between images are stored only once at the cloud and performed integrity check for the uploaded images whether the images are remained same or corrupted during data transmission by generating hamming code. We provide detailed analyses based on the theory, experiment and security aspects of the proposed scheme.

Keywords: Deduplication, Integrity, Encryption, Storage.

I. INTRODUCTION

Cloud computing is the emerging technology. Cloud computing is the availability of system resources as cloud storage, networking and computational power to the user on demand. Cloud technology offers many services e.g. Software as a Service known to be SaaS, Platform as a Service known to be PaaS, Infrastructure as a Service known to be IaaS. Cloud computing has empowered users with the expediency of data storage, data availability, data accessibility, etc. cloud computing methodology offers tremendous flexibility and allows users to offload their data to the cloud and leave all the data management, maintenance and security issues to the Cloud Service Provider (CSP) who manages the services.CSP charge nominal fee to the users on usage of the resources provided by them. This is important for CSP to maintain balance between the cost of the services they provide and the fees they charge to the users, as maintaining and storing the huge volume of user's data, along with the bandwidth usage incur costs for the service providers of cloud.

The data stored can be in various forms like text, image, audio, video and hosting applications on the cloud by users. Some of the most popular Cloud Storage Providers are Dropbox, icloud, flicker, google photos. The uses of digital cameras and social media sites such as Facebook and YouTube have contributed to the rapid growth of data being uploaded to the cloud. Images are used to communicate and convey meaningful information. The widespread usage of digital images on the internet requires a reliable, fast and powerful security to store and transmit them over the network. The use of images and multimedia content for sharing purposes is one of the most significant factors causing issues of duplicate data in the storage and increase in the bandwidth, communication.

Securing images from unauthorized users and adversaries is very important and needed in the fields of medical processing, remote sensing, military, government documents, telecommunications and other similar fields. Image encryption is needed to enforce content access control, privacy, confidentiality and provide protection of images by transforming the original content of the image into texture-like or noise-like information that is hard to understand as the quantity of data storage increases is becoming a serious issues in cloud storage services. In 2020 the amount of data storage growing about 40 trillion gigabytes and more, it will occupy lots of space in cloud storage. To overcome the problem of removing duplicate data, providing the security is explained and implemented in this paper. To remove duplicate data, where we are considering image kind of data, we proposed a method that is Data Integrity Convergent

Dogo Rangsang Research Journal
ISSN : 2347-7180

UGC Care Group I Journal
Vol-08 Issue-15 No. 03: 2021

Encryption (DICE) Protocol at client side. We are presenting a secure block level image deduplication method. In this method, identical images are identified and eliminated in encrypted form. In Data integrity convergent encryption (DICE) Protocol [1], the image uploaded by user are set into blocks, keys are generated by hashing each block of the image. Each block is encrypted using Advanced Encryption Standard (AES) which is a symmetric based algorithm with a key that is obtained from hashing the blocks of image using SHA-256 algorithm. A tag for each block is generated by hashing the cipher generated by encrypting the block and stored in the tag store to check the block availability. It means that identical blocks generate the same tags, which allows service provider to perform deduplication based on the tags generated for the image blocks. To check the integrity of the uploaded image, we use hamming code which is

II. RELATED WORK

Bellare et al. have proposed the Message Locked Encryption (MLE) scheme [2], where protocol standards are defined. Convergent Encryption (CE), Convergent Encryption without Hash (HCE1), Convergent Encryption With Hash (HCE2) and Randomized Convergent Encryption (RCE) several other MLE based strategies are available [3]. These mentioned strategies provide deduplication [4].

Gang et al. [5] considered the entire image for deduplication of and applied the Convergent Encryption (CE) scheme coupled with Attribute Based Encryption to perform deduplication of image.

Fatema et al. [6] used partial encryption along with SPIHT compression characteristics and image hashing to perform deduplication. Security is provided the Cloud Service Provider using the partial