www.ijiarec.com

NOV 2013

International Journal of Intellectual Advancements and Research in Engineering Computations

ENHANCING SECURITY IN CLOUD COMPUTING BY COMBINING DYNAMIC BROADCAST ENCRYPTION, BIT TORRENT AND GROUP SIGNATURE

[*1]Ms.R.Malar Priya, [*2]Ms.R.Kalpana, [3]S.Saravanakumar,M.E.,

ABSTRACT

Cloud computing refers to a network that distributes processing power, applications, and large systems among many computers. Cloud computing seems to offer some incredible benefits for communicators: the availability of an incredible array of software applications, access to lightning-quick processing power, unlimited storage, and the ability to easily share and process information. All of this is available through your browser any time you can access the Internet. While this might all appear enticing, there remain issues of reliability, portability, privacy, and security. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. We are in great need of encrypting the data. This paper combines the techniques of cloud data storage and content Distribution by dynamic broadcast encryption algorithm along with the Bit Torrent application results in minimizing the difficulties of bulky data and aims in resulting efficient sharing of the secure storage services in cloud computing.

Index terms: Bit torrent, content distribution, Dynamic broadcast encryption, group signature.

I INTRODUCTION

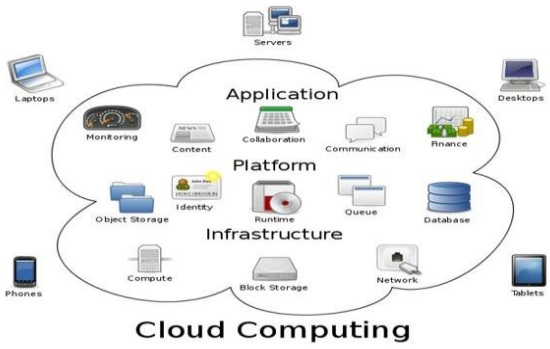
Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources .Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. Cloud computing is about moving services, computation and/or data—for cost and business advantage—off-site to an internal or external, location-transparent, centralized facility or contractor. By making data available in the cloud, it can be more easily and ubiquitously accessed, often at much lower cost, increasing its value by enabling opportunities for enhanced collaboration, integration, and analysis on a shared common platform. Considering the installation of network infrastructure a cloud environment can be broadly categorized into three types- public cloud, private cloud and hybrid cloud. Though from operation and maintenance point-of-view cloud computing is a great cost-effective IT solution for business of any magnitude, but it has at least two major concerns-technical developments, security and privacy. Since cloud computing is relatively a new technology in comparison to other existing computing solutions, it still has lots of scope of becoming a mature system as a reliable and cost-effective computing technology downloading a file provide content to other clients interested in the same file.

II PROBLEM AND ANALYSIS

The users require that their data remain secure and they need to have a strong assurance from the cloud servers to store their data correctly without tampering or partially deleting because the

Author for Correspondence:
[*1]Ms.R.Malar Priya, PG Scholar, Department of CSE, Aditya Institute of Technology, Coimbatore, India.
E-mail: malarpriya91@gmail.com
[*2]Ms.R.Kalpana, PG Scholar, Department of CSE, Aditya Institute of Technology, Coimbatore, India.
E-mail: Kalpaname91@yahoo.com
[3]Mr.S.Saravanakumar, M.E., Asst.Professor Department of CSE, Aditya Institute of Technology, Coimbatore, India.

internal operation details of service providers may not be known to the cloud users. In this paper, an efficient and secure scheme for cloud data storage has to be in a position to ensure the data integrity and confidentiality. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.



Objectives:

The main goal is to provide the security and reduces the bulky data for the user data application in the cloud.

1. An effective and flexible distributed scheme with explicit dynamic data support to ensure the privacy of users' data and guarantee the data dependability in the cloud.
2. Content distribution makes the bulky data to distribute in to various files and the file can be downloaded by using bit torrent application in the cloud.
3. The data mounted in the cloud can be well secured by providing group signature algorithm.

III SOLUTION AND MECHANISM

A. DATA STORAGE ON CLOUD:

Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualize the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers and multiple locations. The safety of the files depends upon the hosting companies, and on the applications that leverage the cloud storage. When data is distributed it is stored at more locations increasing the risk of unauthorised physical access to the data. For example, in cloud based architecture, data is replicated and moved frequently so the risk of unauthorised data recovery increases dramatically. (e.g. disposal of old equipment, reuse of drives, reallocation of storage space) The Manner that data is replicated depends on the service level a customer chooses and on the service provided. Different cloud vendors offer different service levels. Risk of unauthorized access to data can be mitigated through the use of encryption, which can be applied to data as part of the storage service or by on-premises equipment that encrypts data prior to uploading it to the cloud.

The number of people with access to the data who could be compromised (i.e. bribed or coerced) increases dramatically. A single company might have a small team of administrators, network engineers and technicians, but a cloud storage company will have many customers and thousands of servers and therefore a much larger team of technical staff with physical and electronic access to almost all of the data at the entire facility or perhaps the entire company. Encryption keys that are kept by the service user, as opposed to the service provider limit the access to data by service provider employees. It increases the number of networks over which the data travels. Instead of just a local area network (LAN) or storage area network (SAN), data stored on a cloud requires a WAN (wide area network) to connect them both. By sharing storage and networks with many other users/customers it is possible for other customers to access your data. Sometimes because of erroneous actions, faulty equipment, a bug and sometimes because of criminal intent. This risk applies to all types of storage and not only cloud storage. The risk of having data read during transmission can be mitigated through encryption technology. Encryption in transit protects data as it is being transmitted to and from the cloud service.

Encryption at rest protects data that is stored at the service provider. Encrypting data in an on-premises cloud service on-ramp system can provide both kinds of encryption protection.

B. CONTENT DISTRIBUTION:

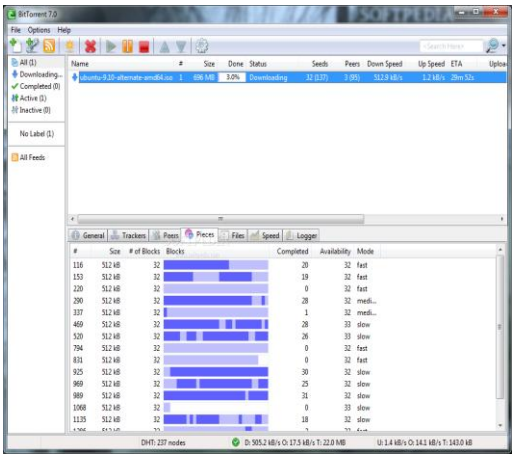
A cloud provider provides two cloud-based services: storage and content delivery. A content provider utilizes these two services to store and distribute her content to multiple subscribers. The content provider and subscribers can access content via a cloud-based application service, which reads and manages the content stored in the storage service via cloud storage APIs. The application service is an application deployed in the cloud by the content provider or a third party. The content provider can use multiple cloud-based services from different cloud service providers to host her application service, content storage service, and content delivery service. The problem identifies in the systems with a Minimum distributed peer-to- peer systems. To achieve An MDT objective for a group of client requires judicious use of client uplink and downlink capacities, which are typically highly asymmetric as offer their clients, download speeds that are significantly larger than upload speeds. In support of the MDT objective for bulk-synchronous content distribution, in this paper we investigate the potential benefit from the on- demand deployment of cloud resources to upload capacity, we propose the use of Bit Torrent in receiving the entire content. Content distribution provides the major aspects are

1. **Integrity and Authenticity:** Safeguarding the accuracy and typically completeness of data and processing methods. Unauthorized a single entities cannot change data; adversaries cannot substitute a forged document for a requested one.
2. **Availability and Persistence:** Ensuring that authorized users have access to data and associated assets when required. For a content distribution system this often means always. This property entails stability in the presence of failure or changing node populations.
3. **Performance:** The time required for performing the operations allowed by the system, typically publication, searching and retrieval of documents.

C. BIT TORRENT APPLICATION:

A BitTorrent client is a computer program that manages downloads and uploads using the Bit Torrent protocol. Bit Torrent is for distributing large amounts of data over the Internet. Bit Torrent is one of the most common protocols for transferring large files and it has been estimated that networks collectively have accounted for roughly 43% to 70% of all Internet Traffic. The Bit Torrent protocol can be used to reduce the server and network impact of distributing large files. Rather than downloading a file from a single source server, the Bit Torrent protocol allows users to join a file of hosts to download and upload from each other simultaneously.

BIT TORRENT APPLICATION RESULTS:

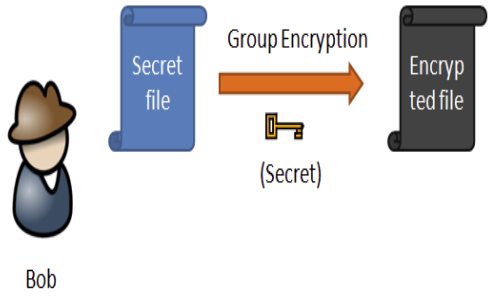


D. DYNAMIC BROADCAST ENCRYPTION ALGORITHM:

Broadcast encryption (BE) schemes enable the sender of a message to specify a subset of the registered (the target set or privileged set), who will be able to decrypt the cipher text sent to all users via a broadcast channel. The complement of the target set (in the set of the registered users) is called the revoked set. To accomplish user revocation when sending a message, a BE generally generates three parts: the Id Header, that is a bit-string that unambiguously identifies the target set/revoked set; the Key Header, that encapsulates a session key for the privileged users; and the Message Body, that contains the payload encrypted under the session key.

Broadcast encryption is the cryptographic problem of delivering encrypted content (e.g. TV programs or data on DVDs) over a broadcast channel in such a way that only qualified users (e.g. subscribers who have paid their fees or DVD players conforming to a specification) can decrypt the content. The challenge arises from the requirement that the set of qualified users can change in each broadcast emission, and

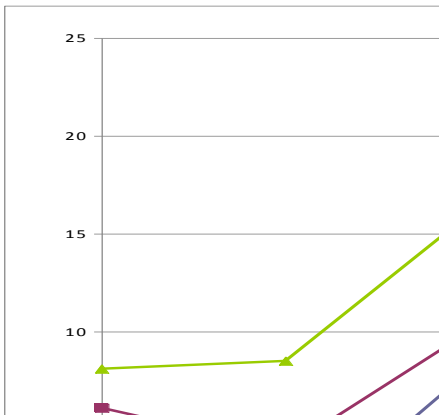
therefore revocation of individual users or user groups should be possible using broadcast transmissions, only, and without affecting any remaining users.



Simulated graph:

A group signature scheme GS = (GKg, GSig, GVf, Open) consists of four polynomial-time algorithms:

1. The randomized group key generation algorithm GKg takes input 1k , 1n , where k ∈ N is the security parameter and n ∈ N is the group size (ie. the number of members of the group), and returns a tuple (gpk, gmsk, gsk), where gpk is the group public key, gmsk is the group manager's secret key, and gsk is an n-vector of keys with gsk[i] being a secret signing key for player i ∈ [n].
2. The randomized group signing algorithm GSig takes as input a secret signing key gsk[i] and a message m to return a signature of m under gsk[i] (i ∈ [n]).
3. The deterministic group signature verification algorithm GVf takes as input the group public key gpk, a message m, and a candidate signature σ for m to return either 1 or 0.



The graph results are shown here:

4. The deterministic opening algorithm Open takes as input the group manager secret key gmsk, a message m, and a signature σ of m to return an identity i or the symbol ⊥ The first graph results depicts the result On the Basis of applying the technique of Content distribution. Once the file is get Uploaded in the cloud its distribution time Of uploading is get minimized .This feature Is obtained by combining the technique the Bit torrent and content distribution algorithm After uploaded the file the third graph Represents the Security enhancement.

IV CONCLUSION

The overarching goal of this setting is to get minimizing the maximum time of bulk synchronous content distribution where it takes any client in a set to download content of the required file. In the paper, we have developed a formulation of Bit Torrent to split the content over the file, through the cloud resources .In our future work we use another content distribution algorithm by implementing RSA algorithm along with dynamic broadcast encryption algorithm to provide security in the cloud.

REFERENCES:

[1]. Raymond sweha, vatche Ishakian, Azer Bestavros, Angels in the Cloud, 2011 IEEE 4th International conference.

[2]. M. Piatek, T. Isdal, T. Anderson, A. Krishnamurthy, and Venkataramani "Do incentives build robustness in BitTorrent," in NSDI, 2007. International conference on cloud computing.

[3]. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[4]. Robert Gellman and World Privacy Forum, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", February 23, 2009.

[5]. K. D. Bowers, A. Jules, and A. Opera, "HAIL: A High-Availability and Integrity Layer for

Cloud Storage," http://eprint.iacr.org/2008/489.

[6]. Reducing upload and Download Time on Cloud using Content Distribution Algorithm published at International Journal on Recent and Innovation Trends in Computing and Communication, ISSN 2321 – 8169.

[7]. Pardeep Kumar, Vivek Kumar Sehgal, DurgSingh Chauhan, P. K. Gupta, Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No.2, 2011.

[8]. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 2009. L. Ferrara, M. Green, S. Hohen Berger, M. Pedersen (2009),"Practical short signature batch verification", in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, pp. 309–324.

[9]. Cloud Security Alliance, (2009) "Security guidance for critical areas Of focus in cloud computing," Available http://www.cloudsecurityalliance.org

[10]. H. Sachem, B. Waters (Dec 2008), "Compact proofs of secure irretrievability", In Proc. of Asia crypt 2008, vol. 5350, pp. 90–107

[11]. P. Mell, T. Grance, (2009) "Draftnist working definition of cloud computing," Referenced on June. 3rd, 2009 on linear http: //csrc.nist.gov/groups/SNS/cloud-computing/index.html.