International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Fast Handling of Cloud Data Based on user Level Virtualization and Resource Scheduling

P. Aron Bami[1], M. Velladurai[2]

[1]PG Scholar, Department of M.Sc(Software Engineering), PSN College of Engineering & Technology, Tirunelveli,Tamilnadu, India
[2] Research Supervisor, Department of M.Sc(Software Engineering), PSN College of Engineering & Technology, Tirunelveli,Tamilnadu, India

ABSTRACT

Many believe the future of gaming lies in the cloud, namely Cloud Gaming, which renders an interactive gaming application in the cloud and streams the scenes as a video sequence to the player over Internet. This paper proposes GCloud, a GPU/CPU hybrid cluster for cloud gaming based on the user-level virtualization technology. Specially, we present a performance model to analyze the server-capacity and games' resource-consumptions, which categorizes games into two types: CPU-critical and memory-io-critical. Consequently, several scheduling strategies have been proposed to improve the resource-utilization and compared with others. Simulation tests show that both of the First-Fit-like and the Best-Fit-like strategies outperform the other(s); especially they are near optimal in the batch processing mode. Other test results indicate that GCloud is efficient: An off-the-shelf PC can support five high-end video-games run at the same time. In addition, the average per-frame processing delay is 8_19 ms under different image-resolutions, which outperforms other similar solutions.

Keywords : Application Programming Interface, Representational State Transfer, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Performance Counter Monitor, Remote Frame Buffer.

I. INTRODUCTION

Cloud computing is an internet-based computing in which large groups of remote servers are networked to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources. Clouds can be classified as public, private or hybrid.

Cloud computing or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions.

The expression cloud is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of things whose details are not inspected further in a given context. In analogy to above usage the word cloud was used as a metaphor for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics.

The cloud symbol was used to represent the Internet as early as 1994. Cloud computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take resources from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of

being impeded by IT obstacles items belong to the long tail of the item distribution. Following the spirit of extensive research on the Long Tail Phenomena, these types of items should not be discarded or Ignored but gainfully utilized in recommendation methods. The long tail of recommender systems and Purpose a new methods of managing such items from long tail. To split items into the head and tail parts and group items in the tail parts using certain clustering methods. Splitting and grouping improves recommendation performance as compared to some of the alternative non- grouping and fully- grouped methods. Performance improvement by running various experiments on two "real-world" datasets. Head/tail Splitting strategies reducing error rates of recommendations and demonstrate that this partitioning often outperforms clustering of the whole item set.

The long Tail problem in the context of recommender systems has been addressed Previously. In particular, analyzed the impact of recommender systems on sales concentration and developed an analytical model of consumer purchases that follow product recommendations provided by a recommender system. The recommender system follows a popularity rule, recommending the bestselling product of consumers, and they show that the process tends to increase the concentration

As a result, the treatment is somewhat akin to providing product popularity information. The model in does not account for consumer preferences and their incentives to follow recommendation or not. Also studied the effects of recommender systems on scales concentration and did not address the problem of improving recommendations for the item in the Long Tail , which constitutes the focus of this paper. In a related question has been studied; to which extent recommender system account for an increase in the long tail of the scales distribution shows that recommender systems increase firm's profits affects scales concentration.

The cold start problem for the items in the Long Tail that have only very few ratings. A popular Solutions to the cold start problem utilizes content- based methods When two items with no or only few ratings are inferred to be similar based on their content. In our work, we use grouping of items in the long tail, rather than the content-based methods to identify similar items and to leverage their combined ratings to provide better recommendations. Clustering methods used in recommender system. In particular, clusters similar users into the same cluster to overcome the data sparsity problem for collaborative filtering. Also in, item clustering Is used to improve the prediction accuracy of collaborative filtering where items were divided into smaller groups, and existing cf algorithms were applied to each group category separately .we use related clustering ideas but in the context of the Long tail phenomenon to leverage few ratings of the Items in the Long tail.

II. METHODS AND MATERIAL

A. Literature Survey

S. Ruj, M. Stojmenovic, and A. Nayak, Privacy Preserving Access Control with Authentication for Securing Data in Clouds [1] An area where access control is widely being used is healthcare. Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. It is important to control the access of data so that only authorized users can access the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys.

Existing work on access control in cloud are centralized in nature. All other schemes use attribute based encryption. The scheme uses a symmetric key approach and does not support authentication. The other drawback was that an user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In this paper, we extend the work with added features which enable to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. Access control in online social networking has been studied. Such data are being stored in clouds. It is very important that only the authorized users are given access to that information. A similar situation arises when data is stored in clouds, for example in Dropbox, and shared

with certain groups of people. Attribute based signature scheme to achieve authenticity and privacy. Unlike, our scheme is resistant to replay attacks, in which an user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy. This is an important property because an user, revoked of its attributes, might no longer be able to write to the cloud

C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, TowardSecure and Dependable Storage Services in Cloud Computing, [2] In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attacks. To address these problems, our main scheme for ensuring cloud data storage is presented.

The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded data. Subsequently, it is shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. The procedure for file retrieval and error recovery based on erasure correcting code is also outlined. Finally, we describe how to extend our scheme to third party auditing with only slight modification of the main design.

S. Kamara and K. Lauter, Cryptographic Cloud Storage, [3] To support lazy-revocation and hierarchies, Key to Compute uses scheme that is based on Key-Policy Attribute-Based encryption scheme. A general cryptographic library is developed and released it as an independent open source project . It provides a short overview of the library. Our library implements the KP-ABE scheme and fixes a non-trivial limitation existed in the construction of KP-ABE is a large universe construction, meaning that it does not require the attributes to be fixed during the initialization process. However, the maximum number of attributes should be known in advance – a limitation which is not desirable in many practical cases. To overcome this limitation, adoption of the random oracle model and replace function by a secure hash function. This modification also improves the efficiency of the library. Therefore, our library does not put any limitation on the number of attributes that can be used in the system. It supports numerical attributes and comparisons.

Simplicity and extendability are two major design goals of K2C framework. K2C framework is independent of any specific cloud provider. It has two simple interfaces which abstract away the details of the cloud providers: IDataStore and IMetadataDirectory. A new cloud service provider can be supported easily by implementing these interfaces. Out of the box, framework comes with a data store driver for Amazon S3 and a meta-data directory driver which uses Amazon Simple. To make it easier for the developers to learn and use our framework, we expose its services through a set of APIs which are very similar to the Java APIs for accessing the file system. Lazy revocation was first introduced in Cephues to eliminate re-encryption required for each revocation at the cost of slightly lowered security. Lazy revocation, which is widely being used in recent cryptographic file systems, requires a key-updating scheme to support key regression.

Key-updating schemes are studied and formalized. Grolimund et al introduced Cryptree which can support access hierarchies and lazy revocation simultaneously. However, due to the explicit and physical dependency of these links, file system operations – especially revocations – require updating large number of these cryptographic links. For example, the revocation of write privilege requires updating keys, where n is the number of data objects contained in that folder and its sub-folders.

H. Li, Y. Dai, L. Tian, and H. Yang, Identity-Based Authentication for Cloud Computing, [4] The application of ID-Based Cryptography, in a distributed environment, is an emerging and interesting area, which has been partially investigated in the literature.

IBC was first adapted to grid networks. The idea of applying IBC to grid security was explored by Lim and Robshaw in 2004. In their proposal, each virtual organization has its own PKG, and all of its users share the same IBC– PE certified by a grid certification authority. Their scheme offers to the encrypting entity more flexibility during the key generation process, and permits to add granularity to the ID-based public key. In fact, Lim and Robshaw propose to include the security policy into the identifier used as input for the public key computation algorithm. However, their proposal has two drawbacks.

The user needs to maintain an independent secure channel with the PKG for the retrieval of his private key. Second, the PKG is able to achieve a key escrow attack, due to its knowledge of the clients private keys X.509 certificate to allow users to act as their own trusted authorities for the purpose of delegation and single sign-on. Therefore, they remove the need for a proxy certification. On one hand, this technique avoids the key escrow attack and the need for a secure channel for private key distribution in an ID-based system. Unfortunately, users have to support the cumbersome task of verifying the parameter sets of other entities. In addition, this paper does not address the arising risk of Man In The Middle attacks. In 2005, Lim and Paterson proposed to use IBC in order to secure a grid environment.

They describe several scenarios in which IBC simplifies the current grid solutions, like the elimination of the use of certificate, simple proxy generation, easy revocation of proxy certificates and the savings of bandwidth by using the pairing based approach proposed by Boneh and Franklin. In the same way, Li et al propose to use IBC as an alternative to the SSL authentication protocol in a cloud environment. However, these schemes still suffer from the needed trust hierarchy to ensure a secure working system.

H. Li, Y. Dai, L. Tian, and H. Yang, [5] Identity-Based Authentication for Cloud Computing,Cloud computing is a style of computing in which dynamically scalable and commonly virtualized resources are provided as a service over the Internet. This paper, first presents a novel Hierarchical Architecture for Cloud Computing (HACC). Then, Identity-Based Encryption (IBE) and Identity-Based Signature (IBS) for HACC are proposed. Finally, an Authentication Protocol for Cloud Computing is presented. Performance analysis indicates that APCC is more efficient and lightweight than SSL Authentication Protocol (SAP), especially for the user side. This aligns well with the idea of cloud computing to allow the users with a platform of limited performance to outsource their computational tasks to more powerful servers. Cloud computing provides a number of advantages that include economies of scale, dynamic provisioning, increased flexibility and low capital expenditures; it also introduces a range of new security risks. IBE-based systems do not require certificate management, eliminating the need for certificate lookups and complex certificate revocation schemes.

B. Existing System

The Data are accessed in centralized form on the basis of key distributed center. Key distributed center does not support for authentication. A single failure of KDC can affect the maximum number of data in cloud storage. It is most difficult to maintain the large number of data in cloud for centralized form. Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. we propose our privacy preserving authenticated access control scheme. According to our scheme a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS, as discussed in Sections 3.4 and 3.5, respectively.We will first discuss our scheme in details and then provide a concrete example to demonstrate how it works. There are three users, a creator, a reader, and writer. Creator Alice receives a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token. There are multiple KDCs which can be scattered. For example, these can be servers in different parts of the world.

A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. Secret keys given for decryption, Kx are keys for

signing. The message MSG is encrypted under the access policy X.

C. Proposed System

Maintaining the large number of data in cloud, decentralized access control approaches is proposed. Involving distribution of secret keys and attributed of all users. Authentication access control only allows the user for reading purpose. Accessing the data by user only satisfying the access policy and authentication. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication.

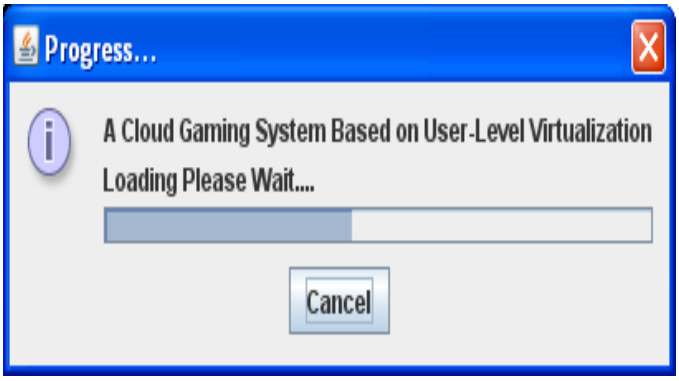
It provides access control based on user information. In this module cloud verifies the users who are authenticated. Anonymous users are authenticate in cloud by some encryption method. This original user creates and shares data with other users in the group through the cloud. Shared data is further divided into a number of blocks. The Figure.2 represents the process. The original user is the original owner of data. Data is divided into many small blocks, where each block is independently signed by the owner.

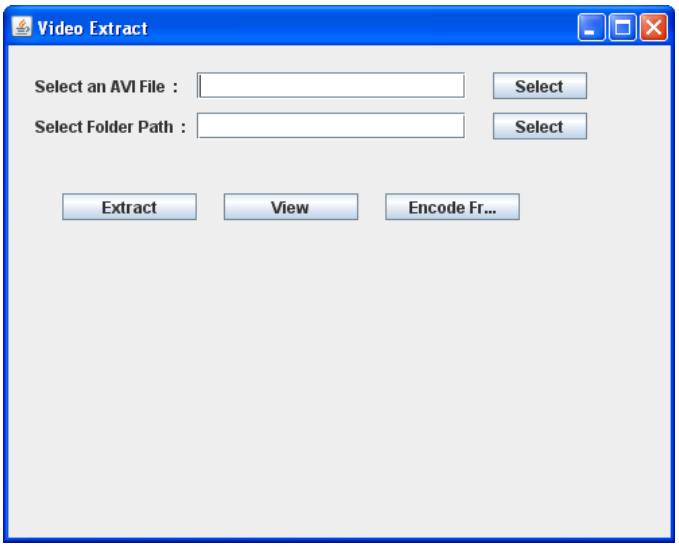
Authorization for individual users are provided for authenticated users and anonymous users. Authorizations are given to users on the basis on key generation. The user easily upload the encrypted datas to cloud the ring key for each file uploaded by the user is generated automatically. After that the user note their member ring key for that data access to others. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. The benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data.

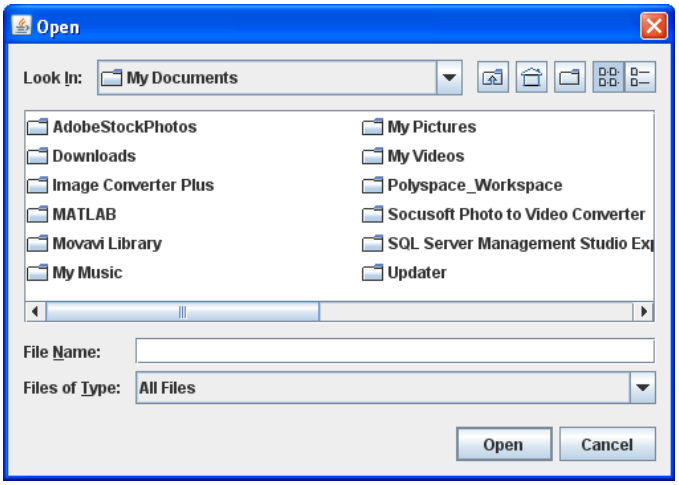
It provides access policy based on users information. It provides security for user information based on the attribute based encryption technique. We only consider how to audit the integrity of shared data in the cloud with static groups keys. It means the group key is pre-defined before shared data is created in the cloud and the membership of users in the group key is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. Another interesting problem is how to audit the integrity of shared data in the cloud with dynamic Datas. A new user can be added into the group and an existing group member can be revoked during data sharing.

III. EXPERIMENTAL RESULTS

The experimental results can be shown as figure below







IV. CONCLUSION

The data, which is stored in the cloud, is made secure with highly secure access control. A decentralized way to access control technique along anonymous authentication, which provides the user security and prevents replay attacks. The cloud is not aware of the identity of the user storing the information, but verifies the user's credentials. Key distribution center supply in a decentralized way. Data stored in clouds is highly secure. The data corruption will not happen. Efficient search on encrypted data is also an important distress in clouds. Access control is also gaining importance for users. Users can have either read or write or both accesses to a file stored in the cloud. The access policy decides who can access the data stored in the cloud.

V. REFERENCES

[1]. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving AccessControl with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "TowardSecure and Dependable Storage Services in Cloud Computing,"IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[3]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "FuzzyKeyword Search Over Encrypted Data in Cloud Computing,"Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[5]. H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authenticationfor Cloud Computing," Proc. First Int'l Conf. Cloud Computing(CloudCom), pp. 157-166, 2009.

[6]. C. Gentry, "A Fully Homomorphic Encryption Scheme," PhDdissertation, Stanford Univ., http://www.crypto.stanford.edu/craig, 2009.

[7]. A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-BasedCloud Computing," Proc. Third Int'l Conf. Trust and TrustworthyComputing (TRUST), pp. 417-429, 2010.

[8]. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Frameworkfor Accountability and Trust in Cloud Computing," HP TechnicalReport HPL-2011-38, http://www. hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[9]. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: TheEssential of Bread and Butter of Data Forensics in CloudComputing," Proc. Fifth ACM Symp. Information, Computer andComm. Security (ASIACCS), pp. 282-292, 2010.

[10]. D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc.15th Nat'l Computer Security Conf., 1992.