JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING

IMPLEMENTATION OF SECURITY SERVICES BY USING SLA IN MULTICLOUD COMPUTING

[1]S.SHANAWAZ BASHA [2]A.D.SIVARAMA KUMAR

[1]Assistant Professor, AVSV Engineering College of JNTUA, Dept.CSE
[2] M.Tech Student, AVSV Engineering College of JNTUA, Dept.CSE

ABSTRACT : *Cloud computing has been envisioned as the next-generation architecture of IT enterprise.we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server.Data security and access control when users outsource sensitive data for sharing on cloud servers. Our proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption. Cloud storage moves the user's data to large data centers, which are remotely located, on which user does not have any control. However, this unique feature of the cloud poses many new security challenges which need to be clearly understood and resolved. We provide a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA).Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability and achieves fine - graininess, scalability and data confidentiality for data access control in cloud computing. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.*

Keywords: ABE, Proxy Encryption, Cloud Computing,Cloud Storage, Data Integrity, Data Intrusion, Service Level Agreement, Lazy Re-Encryption.

I.INTRODUCTION:

Advantages of cloud computing Low initial capital investment and Shorter start-up time for new services and Lower maintenance and operation costs and Higher utilization through virtualization, Easier disaster recovery Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorized users. These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

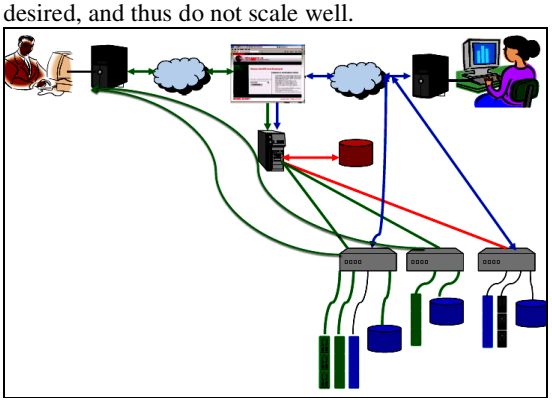

Fig1:cloud computing security archetecture

The use of cloud computing has increased rapidly in many organizations. As shown in fig1. Two persons [1] argue that small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs. Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds". This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed.

II.IMPLEMENTATION OF SECURITY SERVICE:

Key Policy Attribute-Based Encryption (KP-ABE):

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE,[2,3,4] data are associated with attributes for each of which a public key component is defined. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. A KP-ABE scheme is composed of four algorithms which can be defined as follows:

- Setup Attributes
- Encryption
- Secret key generation
- Decryption

2.1Setup Attributes:

Fig2 and this algorithm is used to set attributes for users. From these attributes public key and master key for each user can be determined. The attributes, public key and master key are denoted as Attributes- U = {1, 2. . . N}

Public key- PK = (Y, T1, T2, . . . , TN)

Master key- MK = (y, t1, t2, . . . , tN)

Encryption: This algorithm takes a message M, the public key PK, and a set of attributes I as input. It outputs the cipher text E with the following format: E = (I, ˜ E, {Ei}i)

where ˜E = MY, Ei = Ti.

2.2.Secret key generation:

This algorithm takes as input an access tree T, the master key MK, and the public key PK. It outputs a user secret key SK as follows. SK = {ski}

This algorithm takes as input the cipher text E encrypted under the attribute set U, the user's secret key SK for access tree T, and the public key PK.

Finally it output the message M if and only if U satisfies T.

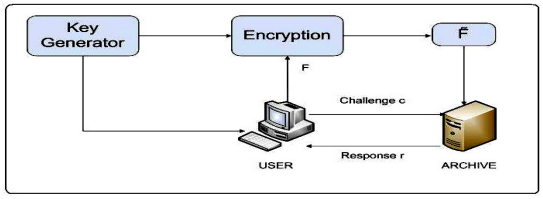

Fig2:security service using key generator

2.3. Proxy Re-Encryption (PRE):Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under Alice's public key into another cipher text that can be opened by Bob's private key without seeing the underlying plaintext. A PRE scheme allows the proxy, given the proxy re-encryption key rka↔b, to translate cipher texts under public key pk1 into cipher texts under public key pk2 and vise versa.

2.4.Lazy re-encryption: The lazy re-encryption technique and allow Cloud Servers to aggregate computation tasks of multiple operations. The operations such as Update secret keys Update user attributes.

III.META-DATA GENERATION:

Let the verifier V wishes to the store the file F with the archive. Let this file F consist of n file blocks. We initially preprocess the file and create metadata to be appended to the file. Let each of the n data blocks have m bits in them. A typical data file F which the client wishes to store in the cloud. [2,3] Each of the Meta data from the data blocks mi is encrypted by using a suitable algorithm to give a new modified Meta data Mi. Without loss of generality we show this process by using a simple XOR operation. The encryption method can be improvised to provide still stronger protection for verifier's data. All the Meta data bit blocks that are generated using the above procedure are to be concatenated together. This concatenated Meta data should be appended to the file F before storing it at the cloud server. The file F along with the appended Meta data e F is archived with the cloud. As data generation is far outpacing data storage it proves costly for small firms to frequently update their hardware whenever additional data is created. Also maintaining the storages can be a difficult task. It transmitting the file across the network to the client can consume heavy bandwidths.

IV.SERVICE LEVEL AGREEMENT (SLA):

The problem is further complicated by the fact that the owner of the data may be a small device, like a PDA (personal digital assist) or a mobile phone, which have limited CPU power, battery power and communication bandwidth.One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. In this paper we provide a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA). It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted. Advantages are part from reduction in storage costs data outsourcing to the cloud also helps in reducing the maintenance. Avoiding local storage of data. and By reducing the costs of storage, maintenance and personnel. and It reduces the chance of losing data by hardware failures. and Not cheating the owner.

4.1CLOUD STORAGE: in fig3 Data outsourcing to cloud storage servers is raising trend among many firms and users owing to its economic advantages.[2,3]This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which is supposed to - presumably for a fee - faithfully store the data with it and provide it back to the owner whenever required.

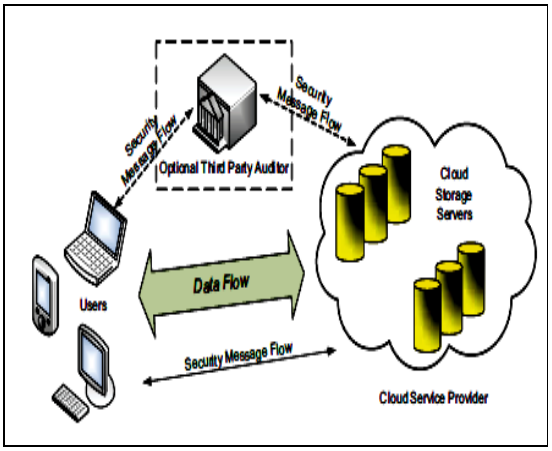

Fig3:Data flow service in cloud computing

This problem tries to obtain and verify a proof that the data that is stored by a user at remote data storage in the cloud (called cloud storage archives or simply archives) is not modified by the archive and thereby the integrity of the data is assured. Cloud archive is not cheating the owner, if cheating, in this context, means that the storage archive might delete some of the data or may modify some of the data. While developing proofs for data possession at untrusted cloud storage servers we are often limited by the resources at the cloud server as well as at the client. 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.

V. CRYPTOGRAPHIC PRIMITIVES:

5.1 Firstly, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. 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.

5.2 Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.These techniques, while can be useful to ensure the storage correctness without having users possessing data, can not address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely [3.4,5] on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

VI. KEY-HASH APPROACH SCHEME:

In this scheme, unlike in the key-hash approach scheme, only a single key can be used irrespective of the size of the file or the number of files whose retrievability it wants to verify. Also the archive needs to access only a small portion of the file F unlike in the key-has scheme which required the archive to process the entire file F for each protocol verification. If the prover has modified or deleted a substantial portion of F, then with high probability it will also have suppressed a number of sentinels.

6.1 Verification Phase: fig4 contains the verifier before storing the file at the archive, preprocesses the file and appends some Meta data to the file and stores at the archive. At the time of verification the verifier uses this Meta data to verify the integrity of the data. It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted. It does not prevent the archive from modifying the data.

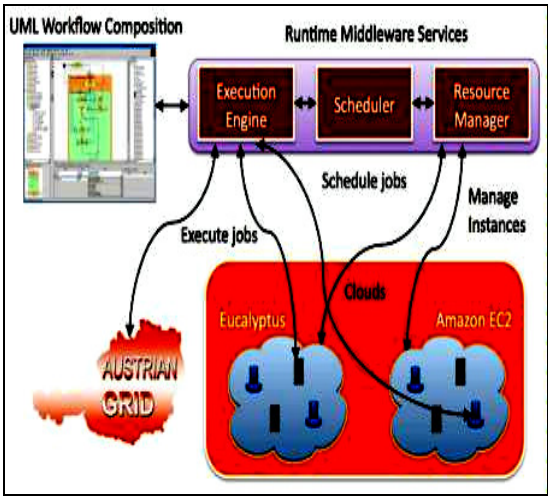

Fig4:implementation services in cloud computing

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service

(PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, data storage and computing services.In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. An example of PaaS is GoogleApps. [4,5]Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. An example of SaaS is the Salesforce.com. A private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud).This model represents the third layer in the cloud environment architecture.

VII.SECURITY RISKS IN CLOUD COMPUTING:

7.1 Fault tolerance and service availability: When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider, as system failures will mean that data will become unavailable if the data depends on a single service provider. Similarly, when deploying IT systems over a single cloud, services may be unavailable if the cloud goes out of operation.

7.2data migration: Users that adopt cloud computing may subject to the risk that their data cannot be migrated to other clouds. Without the capability of migrating data to other clouds, users may be forced to stay with a cloud if they have considerable dependence on the data.

7.3Data confidentiality and integrity: Data generated by cloud computing services are normally kept in the clouds as well. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control[4] thus they may not be able to prevent unauthorized disclosure or malicious modification of their data. Various security related issues and concerns in cloud computing have been identified and are studied, including data privacy, data protection, access control availability [5], authentication, Scalability. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data [5,6]. Ristenpartet al. [5] claim that the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact in the private cloud. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. In addition, the path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices[6]. As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services.

VIII. DATA INTEGRITY:

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al.[7] give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers [8]. Another example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services [8]. One of the solutions that they [9] propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. [9] state that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al.claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place. Although this protocol solves the problem from a cloud storage perspective, Cachinet al. [10] argue that they remain concerned about the users' view, due to the fact that users trust the cloud as a single reliable domain or as a private cloud without being aware of the protection protocols used in the cloud provider's servers. As a solution, Cachinet al. [10] suggest that using Byzantine fault-tolerant

protocols across multiple clouds from different providers is a beneficial solution.

8.1 Data Intrusion: According to Garfinkel[11], another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see [18] for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

8.2 Service Availability: Another major concern in cloud services is service availability. Amazon [6] mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers [12]. Both Google Mail and Hotmail experienced service downtime recently [13]. If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (MediaMax) as a cloud storage provider [13]. Garfinkel[14] argues that information privacy is not guaranteed in Amazon S3. Data authentication which assures that the returned data is the same as the stored data is extremely important. Garfinkel claims that instead of following Amazon's advice that organizations encrypt data before storing them in Amazon S3, organizations should use HMAC [15] technology or a digital signature to ensure data is not modified by Amazon S3. These technologies protect users from Amazon data modification and from hackers who may have obtained access to their email or stolen their password [19].

IX. FUTURE WORK:

We have used this technique in previous databases-as-a-serves research [17]. In other words, hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. Therefore, if the attacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider to know the secret which is the worst case scenario. Hence, replicating data into multi-clouds by using a multi-share technique [18] may reduce the risk of data intrusion and increase data integrity.

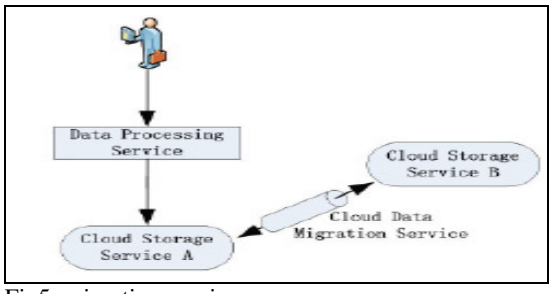

Fig5: migration service

When data on clouds can only stay on the clouds where they are kept, users will be forced to stay with the clouds unless they decide to give up their data. This is not an acceptable situation. the fig5 Migration model where the migration of data is guaranteed. Users process their data via a Data Processing Service, where the data are kept on Cloud Storage Service A. The Cloud Data Migration Service can interact with Cloud Storage Service A and another cloud storage service, namely Cloud Storage Service B. The Cloud Data Migration Service can move data from Cloud Storage Service A to Cloud Storage Service B, and vice versa. By being able to move data from Cloud Storage Service A to Cloud Storage Service B, users need not worry about their data being excessively controlled by a cloud provider, knowing that they can switch to another service provider by moving the data out from the current cloud storage service provider to another .This fact has been discovered from [16] this survey and we will explore dealing with different cloud provider interfaces and the network traffic between cloud providers. Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers.

X.CONCLUSION:

This paper describes the architecture of a cloud computing, types of cloud computing, different delivery models, storage architecture, security issues and different proposed deployment models. The cloud computing mainly focuses availability, flexibility, scalability, and reliability issues. Based on the availability the cloud computing can be divided into four different types like public cloud, private cloud, community cloud and hybrid cloud. Based on the services offered by the NIST has provide three different delivery models of a cloud like Software as a Service (SaaS), Platform as a Service (PaaS)[17,18],and Infrastructure as a Service (IaaS). A SAN file system (that is, a storage area network file system) is programming that enables the sharing of the same copies of files stored on common storage media among multiple servers that may have different operating systems. Without a SAN file system, although different servers may share common storage media (using virtualization approaches), they cannot share the same files. Some of the benefits of SANs include High Bandwidth,

Modular Scalability, High Availability, Fault Tolerance , Manageability, Ease of Integration ,Reduced Total Cost of Ownership Fiber Channel The security concerns that users may have when adopting cloud computing, including fault tolerance and service availability, data migration, and data confidentiality and integrity. To eliminate these security concerns, five deployment models are proposed and described in detail, showing various architecture of deploying IT systems on cloud computing infrastructure. These deployment models address the different security concerns.

XI. REFERENCES

[1] Junjie Peng, School of computer science & High performance computing center Shanghai University, Shanghai, 200072 P.R. China

[2] K. Keahey and T. Freeman, "Science Clouds: Early Experiences in Cloud Computing for Scientific Applications," in proceedings of Cloud Computing and Its Applications 2008, Chicago, IL. 2008.

[3] AbiCloud homepage. http://www.abiquo.com/en/products/abicloud.

[4] Elastic Compute Cloud Amazon Web Services. http://aws.amazon.com/ec2.

[5] Microsoft Azure. http://www.microsoft.com/azure.

[6] Google App Engine. http://code.google.com/appengine.

[7] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

[8] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.

[9] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.

[10] A. Singh, M. Srivatsa, and L. Liu. "Search-as-a-Service:Outsourced Search over Outsourced Storage". ACM TRANSACTIONS ON THE WEB, 3(4), September 2009

[11] T. Uemura, T. Dohi, and N. Kaio. "Availability Analysis of a scalable intrusion tolerant architecture with two detection modes". In The First International Conference on Cloud Computing, pages 178–189, 2009

[12] G. Zhao, J. Liu, Y. Tang, W. Sun, F. Zhang, X. ping Ye, and N. Tang. "Cloud computing: A statistics aspect of users".In The First International Conference on Cloud Computing, pages 347–358. Springer, 2009.

[13] Introduction to Cloud Computing architecture White Paper, Sun Microsystems 1st Edition, June 2009. [15] G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.

[14] Open Nebula. http://www.opennebula.org.

[15] Nimbus. http://workspace.globus.org.

[16] http://www.eweek.com/c/a/Cloud-Computing/Eucalyptus-Offers-OpenSource-MwareBased -Cloud-Platform-100923/.

[17] D. Nurmi, R. Wolski, etc., "The Eucalyptus Open-source Cloud-computing System," in Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, Shanghai, 2009, 124-131.

[18] B. Sotomayor, K. Keahey, I. Foster. Combining Batch execution and Leasing Using Virtual Machines, HPDC 2008, Boston, MA, 2008, 1-9 [7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.