CRYPTOGRAPHY BASED DATA SECURITY TECHNIQUES FOR THE CLOUD COMPUTINGH

A.S.THARUNGANDHI, M.Sc(computer science specialization with information security and cyber forensics).,

Rathinam college of arts and science , Eachanari, Coimbatore-641021

Bharathiyar University

ABSTRACT

over the last years, cloud computing has become an important theme in the computer field. Essentially, it takes the information processing as a service, such as storage, computing. It relieves of the burden for storage management, universal data access with independent geographical locations. In PKI (public key infrastructure), provable data possession protocol needs public key certificate distribution and management. It will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity. In addition to the heavy certificate verification, the system also suffers from the other complicated certificates management such as certificates generation, delivery, revocation, renewals, etc. In cloud computing, most verifiers only have low computation capacity. Identity-based public key cryptography can eliminate the complicated certificate management. In order to increase the efficiency, identity-based provable data possession is more attractive. Thus, it will be very meaningful to study the ID-DPDP.

1. INTRODUCTION

The authoring of the Domain Module is cost and labor intensive, but its development cost might be lightened by profiting from semiautomatic Domain Module authoring techniques and promoting knowledge reuse. To determine how it might help in the Domain Module authoring process, it has been tested with an electronic textbook, and the gathered knowledge has been compared with the Domain Module that instructional designers developed manually.

Advantages

Cryptography plays a crucial role in ensuring data security in cloud computing environments. By employing cryptographic techniques, sensitive information can be protected from unauthorized access, ensuring confidentiality, integrity, and authenticity of the data. Here are some advantages of cryptography-based data security techniques for cloud computing.

Confidentiality: Cryptography allows for secure communication and storage of data by encrypting it. Encryption transforms the original data into an unreadable format, which can only be decrypted using the appropriate key.

In the cloud computing context, this ensures That even if a breach occurs, the encrypted Data remains unintelligible to unauthorized Parties

Data Integrity: Cryptographic techniques, such as hash functions and digital signatures, provide mechanisms to verify the integrity of data. Hash functions generate a fixed-size "digest" of the data, which acts as a unique identifier. Any changes to the data will result in a different hash value, enabling detection of tampering. Digital signatures use public-key cryptography to sign data, providing a means to authenticate the sender and verify data integrity

Existing system

Essentially, it takes the information processing as a service, such as storage, computing. The integrity checking**TIT** protocol must be efficient in order to make it suitable for capacity-limited end devices. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost.

1.2 Proposed system

Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification, and public verification. We will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi cloud storage. First ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

Literature Survey

TITLE : Efficient Remote Data Possession Checking In Critical Information Infrastructures Ensuring Data Storage Security In Cloud Computing

AUTH :Dr.T.Nalini,Dr.K.Manivannan, Vaishnavi Moorthy

YEAR : 2013.

DESCRIPTION

Cloud computing has been envisioned as the on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. Today, technical research works focus on Remote data possession Checking protocols permit to check that a remote server can access an uncorrupted file with the help of third party verifiers. In this paper, Seb´e et al.'s protocol is adapted to support efficient remote data possession checking in critical information infrastructure without the help of a third party auditor. This design allows users to audit the cloud storage with very lightweight communication and computation cost. In addition, the auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving remote server. The design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.

TITLE : Efficient Remote Data Possession Checking in Critical Information Infrastructures

AUTHOR : Francesc Sebe, Josep Domingo-Ferrer

YEAR : 2008

DESCRIPTION

Checking data possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, and so forth) is a matter of crucial importance. Remote data possession checking protocols permit checking that a remote server can access an uncorrupted file in such a way that the verifier does not need to know beforehand the entire file that is being verified. Unfortunately, current protocols only allow a limited number of successive verifications or are impractical from the computational point of view. In this paper, we present a new remote data possession checking protocol such that 1) it allows an unlimited number of file integrity verifications and 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier.

TITLE **:** Identity-Based Remote Data Possession Checking in Public Clouds

AUTHOR **:** Huaqun Wang, Qianhong Wu, Bo Qin, and Josep Domingo-Ferrer

YEAR **:** 2010.

DESCRIPTION

Checking remote data possession is of crucial importance in public cloud storage. It enables the users to check that their outsourced data have been kept intact without downloading the original data. The existing remote data possession checking (RDPC) protocols have been designed in the PKI (public key infrastructure) setting. The cloud server has to validate the users' certificates before storing the data uploaded by the users in order to prevent spam. This incurs considerable costs since numerous users may frequently upload data to the cloud server. This paper addresses this problem with a new model of identity-based RDPC (ID-RDPC) protocols. We present the first ID-RDPC protocol proven to be secure assuming the hardness of the standard computational Diffie-Hellman (CDH) problem. In addition to the structural advantage of elimination of certificate management and verification, our ID-RDPC protocol also outperforms existing RDPC protocols in the PKI setting in terms of computation and communication.

TITLE : Identity-Based Distributed Provable Data Possessionin Multi-Cloud Storage

AUTHOR : A. Juels, B. S. Kaliski Jr.

YEAR : 2012

DESCRIPTION

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

TITLE : Designated-Verifier Provable Data Possession in Public Cloud Storage

AUTHOR : Yongjun Ren, Jiang Xu1, Jin Wang and Jeong-Uk Kim

YEAR : 2013.

DESCRIPTION

Cloud storage is now an important development trend in information technology. However, information security has become an important problem to impede it for commercial application, such as data confidentiality, integrity, and availability. In this paper, we propose designated verifier provable data possession (DV-PDP). In public clouds, DV-PDP is a matter of crucial importance when the client cannot perform the remote data possession checking. We study the DV-PDP system security model and use ECC-based homomorphism authenticator to design DV-PDP scheme. The scheme removed expensive bilinear computing. Moreover in DV-PDP scheme, the cloud storage server is stateless and independent from verifier, which is an important secure property in PDP schemes. Through security analysis and performance analysis, our scheme is provable secure and high efficiency.

TITLE : Scalable and Efficient Provable Data Possession

AUTHOR : Hadassa Katta, Vivek Kolla, P Raja Rao.

YEAR : 2013

DESCRIPTION

Cloud storage has become an attractive and cost effective alternative for enterprises to outsource their valuable business data. However, there are security concerns pertaining to the integrity of data as the cloud server is treated as “untrusted”. To overcome this problem many security schemes came into existence. Recently Zhu et al. presented a technique known as Provable Data Possession (PDP) for data integrity in cloud with distributed storage mechanisms. They considered multiple cloud service providers to store data in cooperative fashion. Their solution makes use of homomorphic verifiable response indeed and multi-prover zero-knowledge system for ensuring data integrity. In this paper we practically implement the PDP scheme proposed by Zhu et al. and build a prototype application to demonstrate the proof of concept. The empirical results reveal that the PDP scheme is very effective and can be used in real time multi-cloud environments.

TITLE : Integrity Verification in Multi-Cloud Storage Using Cooperative Provable Data Possession

AUTHOR : Megha Patil, Prof. G.R.Rao

YEAR : 2014

DESCRIPTION

Storage outsourcing in cloud computing is a rising trend which prompts a number of interesting security issues. Provable data possession (PDP) is a method for ensuring the integrity of data in storage outsourcing. This research addresses the construction of efficient PDP which called as CooperativePDP (CPDP) mechanism for distributed cloud storage to support data migration and scalability of service, which considers the existence of multiple cloud service providers to collaboratively store and maintain the clients' data. CooperativePDP (CPDP) mechanism is based on homomorphism verifiable response, hash index hierarchy for dynamic scalability, cryptographic encryption for security. Moreover, it proves the security of scheme based on multi-prover zero knowledge proof system, which can satisfy knowledge soundness, completeness, and zero-knowledge properties. This research introduces lower computation and communication overheads in comparison with non-cooperative approaches.

TITLE : Dynamic Provable Data Possession

AUTHOR : C. Chris Erway, Alptekin K¨upc¨u, Charalampos Papamanthou , Roberto Tamassia

YEAR : 2009

DESCRIPTION

As storage-outsourcing services and resource-sharing networks have become popular, the problem of efficiently proving the integrity of data stored at untrusted servers has received increased attention. In the provable data possession (PDP) model, the client preprocesses the data and then sends it to an untrusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP scheme applies only to static (or append-only) files. We present a definitional framework and efficient constructions for dynamic provable data possession (DPDP), which extends the PDP model to support provable updates to stored data. We use a new version of authenticated dictionaries based on rank information. The price of dynamic updates is a performance change from O(1) to O(log n) (or O(nọ log n)), for a file consisting of n blocks, while maintaining the same (or better, respectively) probability of misbehavior detection. Our experiments show that this slowdown is very low in practice (e.g., 415KB proof size and 30ms computational overhead for a 1GBfile). We also show how to apply our DPDP scheme to outsourced file systems and version control systems (e.g., CVS)

2.MODULES DESCRIPTION:

- Private Key Generator.
- Combiner

- Cloud Server.
- User Integrated Output

The detailed description of the modules are ,

Private Key Generator:

In this module is used to help the Key Generator to generate keys to the cloud owners data and check their data is in safe also provide protection to the data. Because of providing private key any unknown persons are not easily identify our data. when receiving the identity, it outputs the corresponding private key.

Combiner:

Combiner an entity, which receives the storage request and distributes the block-tag pairs to the corresponding cloud servers. When receiving the challenge, it splits the challenge and distributes them to the different cloud servers. When receiving the responses from the cloud servers, it combines them and sends the combined response to the verifier.

Cloud Server:

In this module is used to help the cloud server which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data. Cloud Servers reside in our world-class data centers, with memory, and fully redundant networking and power all the way to the Client.

User Integrated output

This module has developed an efficient method to outsource the policy updating to the cloud server, which can satisfy all the requirements. We have also proposed an expressive attribute-based access control scheme for big data in the cloud, and designed policy updating algorithms for different types of access policies.

3. System Features:

3.1 System Feature

SOFTWARE USED:

- Language: JAVA
- Front End: J2EE
- Back End: MySQL 5.5
- IDE : Eclipse

HARDWARE USED:

- PENTIUM IV 2.6 GHz, Intel Core 2 Duo processor
- 40GB hard disk
- 1GB RAM

SYSTEM TECHNIQUES:

Identity-Based Distributed Provable Data Possession (ID-DPDP) We adopt the idea that overall trust degree (OTD) comprises two parts: First-hand trust (trust based on real-time and multisource service data) and second-hand trust (feedback). This hybrid trust calculation approach is based on a combination of two kinds of known trust methodologies: feedback-based trust and experience-based trust. The Firs-Hand-Trust is collect data from cloud provider and Second-Hand-Trust is collect feedback from users. So finally we are compare two trust and providing best cloud providers.

SYSTEM DESIGN

Design Engineering deals with the various UML [Unified Modeling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

EXPLANATION:

what system functions are performed for which actor. Roles of the actors in the system can be depicted. Client login or register into user window then if it is a valid user means then it can goes to the next process. If a Client enters into a system by providing correct user name and password and validate from database.

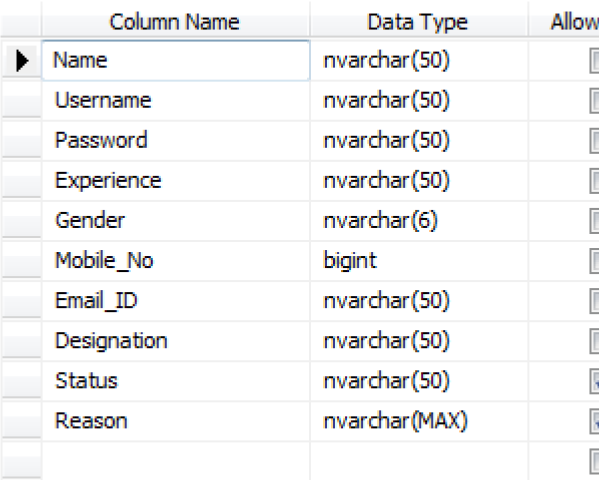
That describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. HttpSession session = request.getSession(true);

DATABASE TABLE DESIGN STRUCTURE

Database design is the process of producing a detailed data model of a database. This logical data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a Data Definition Language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity.

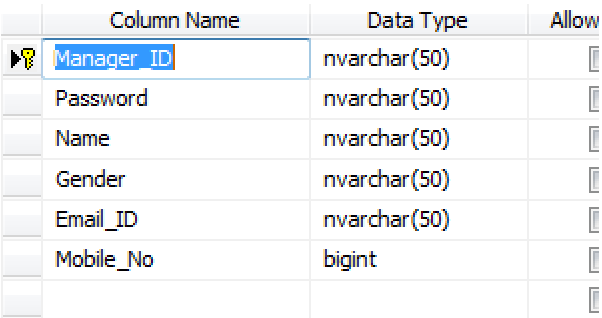
Database Name: User authendication

Table Name:Registration



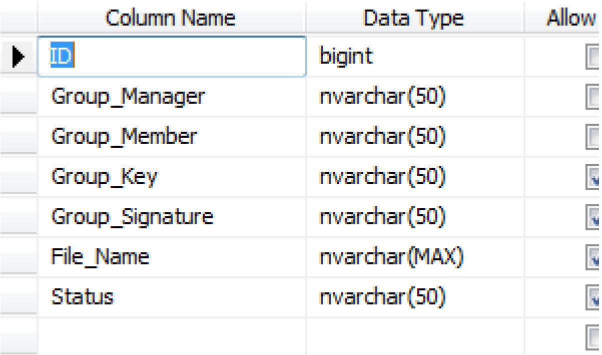
Column Name	Data Type	Allow
Name	nvarchar(50)	□
Username	nvarchar(50)	□
Password	nvarchar(50)	□
Experience	nvarchar(50)	□
Gender	nvarchar(6)	□
Mobile_No	bigint	□
Email_ID	nvarchar(50)	□
Designation	nvarchar(50)	□
Status	nvarchar(50)	☑
Reason	nvarchar(MAX)	☑
		□

Table Name: Owner Details



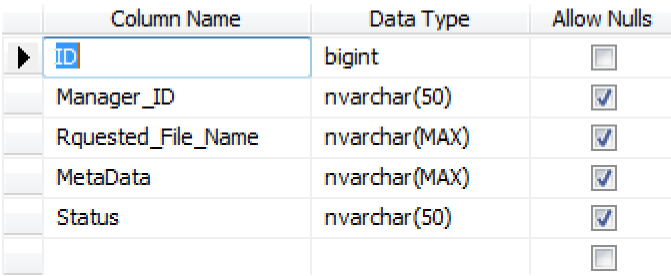
Column Name	Data Type	Allow
Manager_ID	nvarchar(50)	□
Password	nvarchar(50)	□
Name	nvarchar(50)	□
Gender	nvarchar(50)	□
Email_ID	nvarchar(50)	□
Mobile_No	bigint	□
		□

Table Name: Group user Details



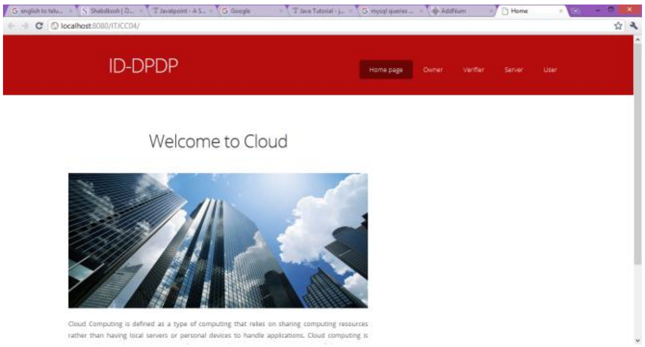
Column Name	Data Type	Allow
ID	bigint	□
Group_Manager	nvarchar(50)	□
Group_Member	nvarchar(50)	□
Group_Key	nvarchar(50)	☑
Group_Signature	nvarchar(50)	☑
File_Name	nvarchar(MAX)	☑
Status	nvarchar(50)	☑
		□

Table Name: Verification Details



Column Name	Data Type	Allow Nulls
ID	bigint	□
Manager_ID	nvarchar(50)	☑
Rquested_File_Name	nvarchar(MAX)	☑
MetaData	nvarchar(MAX)	☑
Status	nvarchar(50)	☑
		□

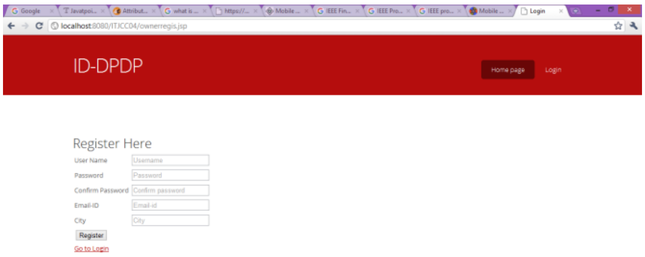
EXPERIMENTAL RESULTS:



localhost:8080/ITJCC04/

Welcome to Cloud

Cloud Computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is



localhost:8080/ITJCC04/ownerregis.jsp

Register Here

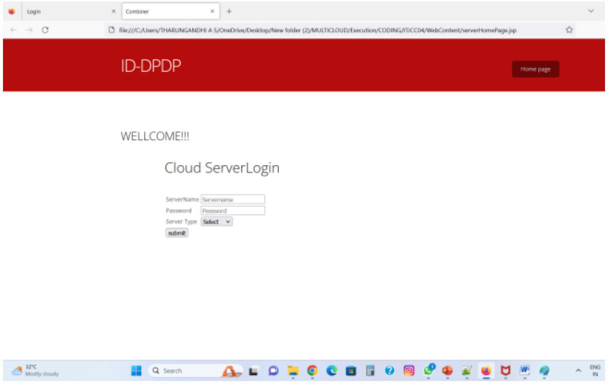
User Name: Username

Password: Password

Confirm Password: Confirm password

Email-ID: Email-id

City: City

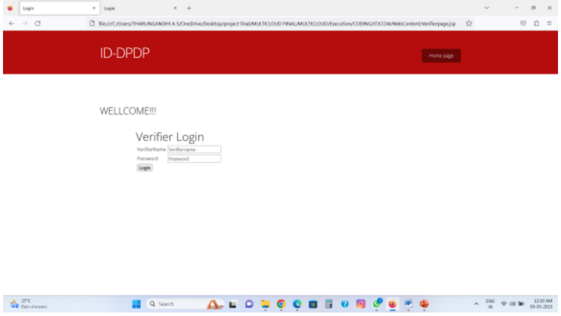


ID-DPDP

WELLCOME!!!

Cloud ServerLogin

Login
Combiner
file:///C:/Users/THARUNGANDHI A S/OneDrive/Desktop/New folder (2)/MULTICLOUD/Execution/CODING/ITCC04/WebContent/serverHomePage.jsp
Home page
ServerName
Servername
Password
Password
Server Type
Select
submit
32°C
Mostly cloudy
Search
ENG
IN

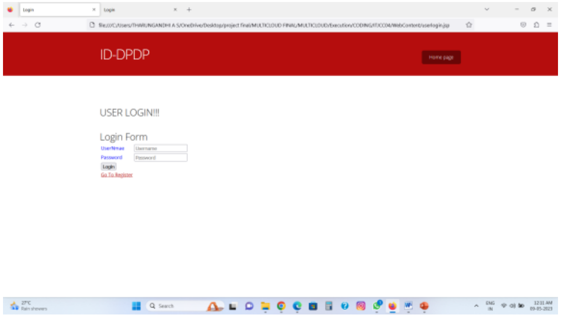


ID-DPDP

WELLCOME!!!

Verifier Login

Login
Login
file:///C:/Users/THARUNGANDHI A S/OneDrive/Desktop/project final/MULTICLOUD FINAL/MULTICLOUD/Execution/CODING/ITCC04/WebContent/Verifierpage.jsp
Home page
VerifierName
Verifiername
Password
Password
Login
27°C
Rain showers
Search
ENG
IN
12:10 AM
09-05-2023



ID-DPDP

USER LOGIN!!!

Login Form

Login
Login
file:///C:/Users/THARUNGANDHI A S/OneDrive/Desktop/project final/MULTICLOUD FINAL/MULTICLOUD/Execution/CODING/ITCC04/WebContent/userlogin.jsp
Home page
UserNmae
Username
Password
Password
Login
Go To Register
27°C
Rain showers
Search
ENG
IN
12:11 AM
09-05-2023

6.1 CONCLUSION

The above combination of secret key and public key cryptography can be applied mainly in military where data security is given more importance. Thus usage of two set of keys numbers in this technique ensures that the data is transmitted securely and accessed only by authorized people.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, ‘‘Provable Data Possession atUntrusted Stores,’’ in Proc. CCS, 2007, pp. 598-609.

[2] G. Ateniese, R. DiPietro, L.V. Mancini, and G. Tsudik, ‘‘Scalableand Efficient Provable Data Possession,’’ in Proc. SecureComm,2008, pp. 1-10.

[3] C.C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,‘‘Dynamic Provable Data Possession,’’ in Proc. CCS, 2009,pp. 213-222.

[4] F. Sebe´, J. Domingo-Ferrer, A. Martı´nez-Balleste´, Y. Deswarte,and J. Quisquater, ‘‘Efficient Remote Data Integrity Checkingin Critical Information Infrastructures,’’ IEEE Trans. Knowl.Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[5] H.Q.Wang. (2013, Oct./Dec.). Proxy Provable Data Possession inPublic Clouds. IEEE Trans. Serv. Comput. [Online]. 6(4), pp. 551-559. Available.

[6] Y. Zhu, H. Hu, G.J. Ahn, andM. Yu, ‘‘Cooperative Provable DataPossession for Integrity Verification in Multicloud Storage,’’IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244,Dec. 2012.

[7] Y. Zhu, H.Wang, Z. Hu, G.J. Ahn, H. Hu, and S.S. Yau, ‘‘EfficientProvable Data

Possession for Hybrid Clouds,'' in Proc. CCS, 2010,pp. 756-758.

[8] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ‘‘MR-PDP:Multiple-Replica Provable Data Possession,'' in Proc. ICDCS,2008, pp. 411-420.