CRYPTOGRAPHY BASED DATA SECURITY TECHNIQUES FOR THE CLOUD COMPUTING

PHASE 1 REPORT

Submitted by

THARUNGANDHI A S (RCAS2021MCS201)

in partial fulfillment for the award of the degree of

MASTER OF SCIENCE SPECIALIZATION IN INFORMATION SECURITY AND CYBER FORENSICS

DEPARTMENT OF COMPUTER SCIENCE RATHINAM COLLEGE OF ARTS AND SCIENCE (AUTONOMOUS) COIMBATORE - 641021 (INDIA) **DECEMBER-2022**

RATHINAM COLLEGE OF ARTS AND SCIENCE
(AUTONOMOUS) COIMBATORE - 641021

BONAFIDE CERTIFICATE

This is to certify that the thesis entitled **CRYPTOGRAPHY BASED DATA SECURITY TECHNIQUES FOR THE CLOUD COMPUTING** submitted by **A.S.THARUNGANDHI**, for the award of the Degree of Master in Computer Science specialization in **"INFORMATION SECURITY AND CYBER FORENSICS"** is a bonafide record of the work carried out by him/her under my guidance and supervision at Rathinam College of Arts and Science, Coimbatore

Mr.Ravishankar **Mr.P.Sivaprakash**

Supervisor Mentor

Submitted for the University Examination held on 02.12.2022

INTERNAL EXAMINER **EXTERNAL EXAMINER**

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS) COIMBATORE - 641021

DECLARATION

I, **A.S.THARUNGANDHI**, hereby declare that this Phase-I entitled **"CRYPTOGRAPHY BASED DATA SECURITY TECHNIQUES FOR THE CLOUD COMPUTING",** is the record of the original work done by me under the guidance of **Mr. Ravishankar M.E.,**, Faculty Rathinam college of arts and science, Coimbatore. To the best of my knowledge this work has not formed the basis for the award of any degree/diploma/ associateship/fellowship/or a similar award to any candidate in any University.

Signature of the Student:

A.S.THARUNGANDHI

Place: Coimbatore

Date: 02.12.2022

COUNTERSIGNED

Mr.Ravisankar M.E., Supervisor

Contents

Acknowledgement

On successful completion for project look back to thank who made in possible. First and foremost, thank **"THE ALMIGHTY"** for this blessing on us without which I could have not successfully our project.I am extremely grateful to **Dr.Madan.A. Sendhil, M.S., Ph.D.,** Chairman, Rathinam Group of Institutions, Coimbatore and **Dr. R.Manickam MCA., M.Phil., Ph.D.,** Secretary, Rathinam Group of Institutions, Coimbatore for giving me opportunity to study in this college.I am extremely grateful to **Dr.R.Muralidharan, M.Sc., M.Phil., M.C.A., Ph.D.,** Principal Rathinam College of Arts and Science(Autonomous), Coimbatore.Extend deep sense of valuation to **Mr.A.Uthiramoorthy, M.C.A., M.Phil., (Ph.D),** Rathinam College of Arts and Science (Autonomous) who has permitted to undergo the project.

Unequally I thank **Mr.P.Sivaprakash, M.E., (Ph.D).,** Mentor and **Dr.Mohamed Mallick, M.E., Ph.D.,** Project Coordinator, and all the Faculty members of the Department - iNurture Education Solution pvt ltd for their constructive suggestions, advice during the course of study.I convey special thanks, to the supervisor **Mr.Ravisankar M.E.,** who offered their inestimable support, guidance, valuable suggestion, motivations, helps given for the completion of the project.

I dedicated sincere respect to my parents for their moral motivation in completing the project.

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.

Chapter 1

Introduction

1.1 GENERAL:

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.

1.2 OBJECTIVE:

The objective of our project is Identity-based public key cryptography can eliminate the complicated certificate management.

SCOPE OF THE PROJECT

In this project we are going to ID-DPDP protocol can realize private verification, delegated verification, and public verification

1.3 EXISTING SYSTEM:

Essentially, it takes the information processing as a service, such as storage, computing. The integrity checking 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.

1.4 DRAWBACKS IN EXISTING SYSTEM:

Data Checking is more complex using multiple servers. Needed large storage space. Insufficient data loss.

1.5 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.

1.6 ADVANTAGES IN PROPOSED SYSTEM:

- It has more significant storage space.
- It provides secure public data's.
- Using private key Generation.

Chapter 2

DISTRIBUTED PROVABLE DATA POSSESSION MODULES

2.1 GENERAL

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. There are Six modules for the generation of Data possession.

2.2 METHODOLOGIES

Following modules involves

2.3 MODULES

- **User Interface Design.**
- **Client**
- **Private Key Generator.**
- **Combiner**
- **Cloud Server.**
- **User Integrated Output**

User Interface Design:

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

Client Module:

This module is used to help the cloud owner to view details and upload files with the security. The individual cloud owner contains the key. The

Cloud owners view the user searching details and the counting of file request details. which has massive data to be stored on the cloud for maintenance and computation, can be either individual consumer or corporation.

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.

2.4 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.

REFERENCE PAPER: "Dynamic Provable Data Possession".

2.5 GENERAL

These are the requirements for doing the project. Without using these tools and software's we can't do the project. So we have two requirements to do the project. They are

1. **Hardware Requirements.**
2. **Software Requirements.**

2.6 HARDWARE REQUIREMENTS:

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the system does and not how it should be implemented.

PROCESSOR : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.

RAM : 512 MB DD RAM

MONITOR : 15" COLOR

HARD DISK : 40 GB

2.7 SOFTWARE REQUIREMENTS:

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the team's and tracking the team's progress throughout the development activity.

Front End : J2EE.

Back End : MY SQL 5.5

Operating System : Windows 07

IDE : Eclipse

Chapter 3

DESIGN ENGINEERING

SYSTEM DESIGN AND DEVELOPMENT

FILE DESIGN

The design base files are the most important of the app. The performance of the app depends on how the app is design. It has been given at most attention to reduce the size of files and redundancy. At the same time all the files are design to incorporate all relevant information regarding each entity. A single database with information about all the entities will make the app more complicated. The functions and structure of each of the database files are given below. In this the file contains the details of industries with their rates for low, medium and high quality material.

INPUT DESIGN

The Input design is mainly concerned with an input screen in the software. In the input design, user-oriented inputs are converted into a com-

puter based system format. User can also select desired options from the menu, the provides all possible facilities. Also the important input format is designed in such a way that accidental errors are avoided. The user has to input only just the minimum data required, the also helps in avoiding the errors that the users may make. Accurate designing of the input format is very important in developing efficient software.

OUTPUT DESIGN:

Outputs from computer systems are required primarily to communicate the results of processing to users. They are also used to provide permanent copy of the results for later consultations. The outputs are needed to be generated as a hard copy and as well as queries to be viewed on the screen. Keeping in view these outputs, the format of the output is taken from the outputs, which are currently being obtained after a processing. The standard printer is to be used as output media for hard copies. The main objective of output design is to interrupt and communicate the result of the computer part of the system to user in a form, which they meet their requirements and also to communication the output specification to the programmers in a way, this is unambiguous, comprehensive. This application gets an input from user for number of floors, number of rooms and square feet and when the user selects for quality of material they need, application initiates the calculation, perform, finalize and generates the report to user.

Chapter 4

DEVELOPMENT TOOLS

4.1 GENERAL

This chapter is about the software language and the tools used in the development of the project. The platform used here is JAVA.

4.2 FEATURES OF JAVA

4.3 THE JAVA FRAMEWORK

Java is a programming language originally developed by James Gosling at Sun Microsystemsand released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to bytecode that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, concurrent, class-based, and object-oriented, and is specifically designed to have as few implementation dependencies as possible. It

is intended to let application developers "write once, run anywhere".

Java is considered by many as one of the most influential programming languages of the 20th century, and is widely used from application software to web applications the java framework is a new platform independent that simplifies application development internet. Java technology's versatility, efficiency, platform portability, and security make it the ideal technology for network computing. From laptops to datacenters, game consoles to scientific supercomputers, cell phones to the Internet, Java is everywhere!

4.4 OBJECTIVES OF JAVA

To see places of Java in Action in our daily life, explore java.com.

Why Software Developers Choose Java

Java has been tested, refined, extended, and proven by a dedicated community. And numbering more than 6.5 million developers, it's the largest and most active on the planet. With its versatility, efficiency, and portability, Java has become invaluable to developers by enabling them to:

- Write software on one platform and run it on virtually any other platform
- Create programs to run within a Web browser and Web services
- Develop server-side applications for online forums, stores, polls, HTML forms processing, and more

- **Combine applications or services using the Java language to create highly customized applications or services**

- **Write powerful and efficient applications for mobile phones, remote processors, low-cost consumer products, and practically any other device with a digital heartbeat**

Some Ways Software Developers Learn Java

- **Today, many colleges and universities offer courses in programming for the Java platform. In addition, developers can also enhance their Java programming skills by reading Sun's java.sun.com Web site, subscribing to Java technology-focused newsletters, using the Java Tutorial and the New to Java Programming Center, and signing up for Web, virtual, or instructor-led courses.**

Object Oriented

To be an Object Oriented language, any language must follow at least the four characteristics.

1. Inheritance :It is the process of creating the new classes and using the behavior of the existing classes by extending them just to reuse the existing code and adding addition a features as needed.

2. Encapsulation: It is the mechanism of combining the information and providing the abstraction.

3. Polymorphism: As the name suggest one name multiple form, Polymorphism is the way of providing the different functionality by the functions having the same name based on the signatures of the methods.

4. Dynamic binding: Sometimes we don't have the knowledge of objects about their specific types while writing our code. It is the way of providing the maximum functionality to a program about the specific type at runtime.

4.5 Java Server Pages - An Overview

Java Server Pages or JSP for short is Sun's solution for developing dynamic web sites. JSP provide excellent server side scripting support for creating database driven web applications. JSP enable the developers to directly insert java code into jsp file, this makes the development process very simple and its maintenance also becomes very easy.

JSP pages are efficient, it loads into the web servers memory on receiving the request very first time and the subsequent calls are served within a very short period of time.

In today's environment most web sites servers dynamic pages based on user request. Database is very convenient way to store the data of users and other things. JDBC provide excellent database connectivity in heterogeneous database environment. Using JSP and JDBC its very cceasy to develop database driven web application.

Java is known for its characteristic of "write once, run anywhere." JSP

pages are platfJavaServer Pages

JavaServer Pages (JSP) technology is the Java platform technology for delivering dynamic content to web clients in a portable, secure and well-defined way. The JavaServer Pages specification extends the Java Servlet API to provide web application developers with a robust framework for creating dynamic web content on the server using HTML, and XML templates, and Java code, which is secure, fast, and independent of server platforms.

JSP has been built on top of the Servlet API and utilizes Servlet semantics. JSP has become the preferred request handler and response mechanism. Although JSP technology is going to be a powerful successor to basic Servlets, they have an evolutionary relationship and can be used in a cooperative and complementary manner.

Servlets are powerful and sometimes they are a bit cumbersome when it comes to generating complex HTML. Most servlets contain a little code that handles application logic and a lot more code that handles output formatting. This can make it difficult to separate and reuse portions of the code when a different output format is needed. For these reasons, web application developers turn towards JSP as their preferred servlet environment.

4.6 Evolution of Web Applications

Over the last few years, web server applications have evolved from static to dynamic applications. This evolution became necessary due to some

deficiencies in earlier web site design. For example, to put more of business processes on the web, whether in business-to-consumer (B2C) or business-to-business (B2B) markets, conventional web site design technologies are not enough. The main issues, every developer faces when developing web applications, are:

1. Scalability - a successful site will have more users and as the number of users is increasing fastly, the web applications have to scale correspondingly.

2. Integration of data and business logic - the web is just another way to conduct business, and so it should be able to use the same middle-tier and data-access code.

3. Manageability - web sites just keep getting bigger and we need some viable mechanism to manage the ever-increasing content and its interaction with business systems.

4. Personalization - adding a personal touch to the web page becomes an essential factor to keep our customer coming back again. Knowing their preferences, allowing them to configure the information they view, remembering their past transactions or frequent search keywords are all important in providing feedback and interaction from what is otherwise a fairly one-sided conversation.

Apart from these general needs for a business-oriented web site, the necessity for new technologies to create robust, dynamic and compact server-side web applications has been realized. The main characteristics of today's

dynamic web server applications are as follows:

1. Serve HTML and XML, and stream data to the web client

2. Separate presentation, logic and data

3. Interface to databases, other Java applications, CORBA, directory and mail services

4. Make use of application server middleware to provide transactional support.

5. Track client sessions.

4.7 Benefits of JSP

One of the main reasons why the JavaServer Pages technology has evolved into what it is today and it is still evolving is the overwhelming technical need to simplify application design by separating dynamic content from static template display data. Another benefit of utilizing JSP is that it allows to more cleanly separate the roles of web application/HTML designer from a software developer. The JSP technology is blessed with a number of exciting benefits, which are chronicled as follows:

1. The JSP technology is platform independent, in its dynamic web pages, its web servers, and its underlying server components. That is, JSP pages perform perfectly without any hassle on any platform, run on any web server, and web-enabled application server. The JSP pages can be accessed from any web server.

2. The JSP technology emphasizes the use of reusable components. These components can be combined or manipulated towards developing more purposeful components and page design. This definitely reduces development time apart from the At development time, JSPs are very different from Servlets, however, they are precompiled into Servlets at run time and executed by a JSP engine which is installed on a Web-enabled application server such as BEA WebLogic and IBM WebSphere.

4.8 Servlets

Earlier in client- server computing, each application had its own client program and it worked as a user interface and need to be installed on each user's personal computer. Most web applications use HTML/XHTML that are mostly supported by all the browsers and web pages are displayed to the client as static documents.

A web page can merely displays static content and it also lets the user navigate through the content, but a web application provides a more interactive experience.

Any computer running Servlets or JSP needs to have a container. A container is nothing but a piece of software responsible for loading, executing and unloading the Servlets and JSP. While servlets can be used to extend the functionality of any Java- enabled server.

They are mostly used to extend web servers, and are efficient replacement

for CGI scripts. CGI was one of the earliest and most prominent server side dynamic content solutions, so before going forward it is very important to know the difference between CGI and the Servlets.

4.9 Java Servlets

Java Servlet is a generic server extension that means a java class can be loaded dynamically to expand the functionality of a server. Servlets are used with web servers and run inside a Java Virtual Machine (JVM) on the server so these are safe and portable.

Unlike applets they do not require support for java in the web browser. Unlike CGI, servlets don't use multiple processes to handle separate request. Servets can be handled by separate threads within the same process. Servlets are also portable and platform independent.

A web server is the combination of computer and the program installed on it. Web server interacts with the client through a web browser. It delivers the web pages to the client and to an application by using the web browser and he HTTP protocols respectively.

The define the web server as the package of large number of programs installed on a computer connected to Internet or intranet for downloading the requested files using File Transfer Protocol, serving e-mail and building and publishing web pages. A web server works on a client server model.

Chapter 5

IMPLEMENTATION

5.1 GENERAL

In this we implement the coding part using eclipse. Below are the coding's that are used to generate the domain module for electronic text books. Here the proposed techniques are used in the coding part to generate the e-books. Data security is one of the major concerns in Information Technology, particularly in Cloud Computing. When it comes to Multi-cloud storage, it is also very important to maintain Data Integrity across the cloud servers since they may be located anywhere around the globe. One cannot ignore the threats to a user's data on cloud even though cloud provides wide range of services like storage capacity, cost savings and high speed. Enterprises and businesses use cloud services to store their files, but this exposes confidential and sensitive file to new risks. The proposed Multi-cloud storage provides a secure mechanism for file storage by abstracting the process of storing files across multiple servers to the users and enhancing the security and

privacy of data with a trustworthy environment. The user of the cloud need not worry about the way data is stored in multi cloud servers or about the way it is uploaded or downloaded. The methodology adopted ensures the integrity of data in files is maintained when the data is retrieved by the user. This paper describes the implementation of a secure Multi-cloud storage for files by adopting encryption and file splitting concepts to improvise the security of file stored. Here, the user's file is fragmented into segments and each segment is loaded into a different cloud server. The files parts are encrypted by making use of keys unique to each cloud server before being loaded. Double encryption is provided when the user first encrypts the file before it can be uploaded to the cloud server and the integrity is ensured by hashing each file part before encryption. All the metadata corresponding to a file's fragmentation and encryption is maintained by a combiner module. The suggested model ensures both Data privacy and security, and Data Integrity.

5.2 Identity Based Distributed provable Data possession in Multi Cloud Storage.

Registrationpage.jsp

¡!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"¿

¡html xmlns="http://www.w3.org/1999/xhtml"¿

¡head¿

¡meta name=”keywords” content=”” /¿

¡meta name=”description” content=”” /¿

¡meta http-equiv=”content-type” content=”text/html; charset=utf-8” /¿ ¡title¿Login¡/title¿

¡link href=”http://fonts.googleapis.com/css?family=Open+Sans:400,300,600” rel=”stylesheet” type=”text/css” /¿

¡link href=’http://fonts.googleapis.com/css?family=Abel—Satisfy’ rel=’stylesheet’ type=’text/css’ /¿

¡link href=”style.css” rel=”stylesheet” type=”text/css” media=”screen” /¿

¡/head¿

¡script type=”text/javascript”¿

function validateForm()

var x = document.forms[”myForm”][”Uname”].value;

if (x == null —— x == ””)

alert(”Name must be filled out”);

return false;

var x1 = document.forms[”myForm”][”Passwd”].value;

if (x1 == null —— x1 == ””)

alert(”Password must be filled out”);

return false;

var x2 = document.forms["myForm"]["Confirm"].value;

if (x2 == null —— x2 == "")

alert("Confirm Passout must be filled out");

return false;

var x3 = document.forms["myForm"]["Emailid"].value;

if (x3 == null —— x3 == "")

alert("Email Id must be filled out");

return false;

var x4 = document.forms["myForm"]["City"].value;

if (x4 == null —— x4 == "")

alert("City must be filled out");

return false;

var x5 = document.forms["myForm"]

["UserType"].value;

if (x5 == null —— x5 == "")

alert("User Type must be filled out");

return false;

5.3 Conclusion And sFuture Work

Conclusion:

FUTURE CONCEPT:

• Store pre computed answers as metadata (at the client, or at the server

in an authenticated and encrypted manner). Because of this approach, the number of updates and challenges a client can perform is limited and fixed a priori.

• We want to store block in each cloud so the request has to go from each Cloud Service Provider.

FUTURE TECHNIQUE:

• Cooperative PDP (CPDP).

TECHNIQUE DEFINITION:

• Homomorphism verifiable response, hash index hierarchy for dynamic scalability, cryptographic encryption for security.

• CPDP technique is based entirely on symmetric key cryptography without requiring any bulk encryption.

5.4 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 in-Public 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, "Efficient-Provable 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.

[9] A.F. Barsoum and M.A. Hasan, "Provable possession andreplication of data over cloud servers," Centre Appl. Cryptogr.Res., Univ. Waterloo, Waterloo, ON, Canada, Rep. 2010/32.

[10] Z. Hao and N. Yu, "A Multiple-Replica Remote Data PossessionChecking Protocol with Public Verifiability," in Proc. 2nd Int.Symp. Data, Privacy, E-Comm., 2010, pp. 84-89.