

On The Security of Data Access Control for Multi-Authority Cloud Storage Systems

Shaik Javeed Basha¹, M.N Malli Karjuna Reddy²

¹P.G. Scholar, ²Assistant Professor

^{1,2} Branch: Computer Science & Engineering

^{1,2} S V R Engineering College, Nandyal, Kurnool (Dist.).

Email: ¹javeedbasha70@gmail.com, ²mali51arjun@gmail.com

Abstract

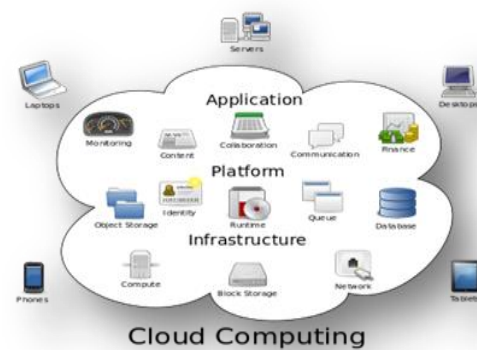
Data access control has turning into a testing issue in cloud storage systems. A few methods have been proposed to accomplish the protected data access control in a semi confided in cloud storage system. As of late, K.Yang et al. proposed a fundamental data access control scheme for multiauthority cloud storage system (DAC-MACS) and an extensive data access control scheme (EDAC-MACS). They asserted that the DAC-MACS could accomplish productive decryption and quick disavowal and the EDAC-MACS could likewise accomplish these objectives despite the fact that nonrevoked users uncover their Key Update Keys to the repudiated user. Be that as it may, through my cryptanalysis, the repudiation security of the two schemes can't be ensured.

Keyword: Data Access Control, Cloud Computing, attribute revocation, revocation security, CP-ABE, multiauthority cloud

INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-

party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together.

Often, virtualization techniques are used to maximize the power of cloud computing.

EXISTING SYSTEM

Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server

DISADVANTAGES OF EXISTING SYSTEM

- Cloud storage service separates the roles of the data owner from the data service provider, and the data owner does not interact with the user directly for providing data access service, which makes the data access control a challenging issue in cloud storage systems.
- The cloud server cannot be fully trusted by data owners, traditional server-based access control methods are no longer applicable to cloud storage systems.

PROPOSED SYSTEM

We first construct a new multi-authority CPABE scheme with efficient decryption and design an efficient attribute revocation method for it. Then, we apply them to design an effective access control scheme for multi-authority systems. The main contributions of this work can be summarized as follows.

We propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme for multi-authority cloud storage systems, which is provably secure in the random oracle model and has better performance than existing schemes.

We construct a new multi-authority CP-ABE scheme with efficient decryption. Specifically, we outsource the main

computation of the decryption by using a token based decryption method.

We also design an efficient immediate attribute revocation method for multi-authority CP-ABE scheme that achieves both forward security and backward security. It is efficient in the sense that it incurs less communication cost and computation cost of the revocation.

ADVANTAGES OF PROPOSED SYSTEM

NEDAC-MACS can withstand the two vulnerabilities even though the non-revoked users reveal their received key update keys to the revoked user.

The performance simulation shows the overall storage, computation, and communication overheads of the NEDAC-MACS are superior to that of DACC and relatively same as that of DAC-MACS.

REQUIREMENTS ANALYSIS

Preliminary Investigation

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games. When it is approved by the organization and our project guide the first activity, i.e. preliminary investigation begins. The activity has three parts:

- Request Clarification
- Feasibility Study
- Request Approval

Request Clarification

After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires.

Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network(LAN). In today's busy schedule man need everything should be provided in a readymade manner. So taking into consideration of the vastly use of the net in day to day life, the corresponding development of the portal came into existence.

INPUT DESIGN AND OUTPUT DESIGN

INPUT DESIGN

The input design is the connection between the information system and the user. It involves the creating particular and strategies for data readiness and those means are important to put exchange data in to a usable shape for preparing can be accomplished by reviewing the PC to peruse data from a composed or printed archive or it can happen by having individuals keying the data straightforwardly into the system. The design of input centers around controlling the measure of input required, controlling the mistakes, maintaining a strategic distance from deferral, evading additional means and keeping the procedure straightforward. The input is designed in such a route in this way, to the point that it furnishes security and usability with holding the protection. Input Design thought about the accompanying things:

- What data ought to be given as input?
- How the data ought to be orchestrated or coded?
- The exchange to control the working faculty in giving input.
- Methods for getting ready input approvals and ventures to pursue when mistake happen.

OBJECTIVES

1. Input Design is the way toward changing over a user-arranged depiction of the input into a PC based system. This design is essential to evade blunders in the data input process and demonstrate the right bearing to the administration for getting right information from the mechanized system.

2. It is accomplished by making user-accommodating screens for the data passage to deal with expansive volume of data. The objective of designing input is to make data passage less demanding and to be free from blunders. The data section screen is designed so that every one of the data controls can be performed. It additionally gives record seeing offices.

3. At the point when the data is entered it will check for its legitimacy. Data can be entered with the assistance of screens. Proper messages are given as when required so the user won't be in maize of moment. Along these lines the goal of input design is to make an input format that is anything but difficult to pursue

OUTPUT DESIGN

A quality yield is one, which meets the necessities of the end user and presents the data obviously. In any structure eventual outcomes of taking care of are granted to the users and to other system through yields. In yield plan it is settled how the data is to be removed for fast need and moreover the printed form yield. It is the most basic and direct source data to the user. Capable and adroit yield setup improves the structure's relationship to help user fundamental initiative.

1. Organizing PC yield should proceed in a created, well altogether thought about way; the right yield must be delivered while ensuring that each yield segment is arranged with the objective that people will find the

system can use easily and satisfactorily. Exactly when examination plan PC yield, they should Identify the specific yield that is relied upon to meet the necessities.

2. Select methods for showing data.
3. Make file, report, or diverse associations that contain data made by the structure.

The yield kind of a data structure should accomplish somewhere around one of the going with goals.

- Convey data about past activities, current status or projections of the
- Future.
- Signal basic events, openings, issues, or alarms.
- Trigger an action.
- Confirm an action.

SYSTEM DESIGN

MODULES

MODULES:

- Global trusted certificate authority
- Attribute Authority
- Cloud Server
- Data Owner
- User

MODULES DESCRIPTION:

Global trusted certificate authority:

The CA is a global confided in authentication authority in the framework. It sets up the framework what's more, recognizes the enrollment of the extensive number of users and AAs in the system. The CA is accountable for the course of global secret key and global public key for each legal user in the structure. In any case, the CA isn't locked in with any attribute organization and the creation of riddle keys that are connected with attributes. For example, the CA can be the Social Security Administration, a free association of the United States government. Each user will

be issued a Social Security Number (SSN) as its global identity.

Attribute Authority:

Every AA is an independent attribute authority that is responsible for issuing, repudiating and reviving user's attributes according to their activity or identity in its territory. In DACMACS, each attribute is connected with a lone AA, yet every AA can manage a self-self-assured number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is accountable for making a public attribute key for each attribute it manages and a secret key for each user accomplices with their attributes.

Cloud Server:

The cloud server stores the owners' data and gives data get to organization to users. It creates the decryption token of a ciphertext for the user by using the riddle keys of the user issued by the AAs. The server moreover does the ciphertext revive when an attribute disavowal happens.

Data Owner:

The data owners characterize the entrance arrangements and encode the data under the strategies previously facilitating them in the cloud. They don't depend on the server to do the data get to control. Rather, the ciphertext can be gotten to by all the lawful users in the framework. Be that as it may, the entrance control occurs inside the cryptography. That is just when the user's attributes fulfill the entrance strategy characterized in the ciphertext, the user can decrypt the ciphertext.

User:

Every user is appointed with a global user identity from the CA. Every user can uninhibitedly get the ciphertexts from the server. To decrypt a ciphertext, every user may present their mystery keys issued by a few AAs together with its global public key

to the server and request that it create a decryption token for some ciphertext. After accepting the decryption token, the user can decrypt the ciphertext by utilizing its global mystery key. Just when the user's attributes fulfill the entrance strategy characterized in the ciphertext, the server can create the right decryption token. The mystery keys

and the global user's public key can be put away on the server; hence, the user does not have to present any mystery keys if no mystery keys are refreshed for the further decryption token generation.

DIAGRAMS SYSTEM ARCHITECTURE



Fig. 3: System model for MONA [5]

4.1 DATA DICTIONARY











































Authority

Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/> file_name	varchar(45)	latin1_swedish_ci		No	None		
<input type="checkbox"/> request	varchar(45)	latin1_swedish_ci		No	None		
<input type="checkbox"/> date	timestamp		on update CURRENT_TIMESTAMP	No	CURRENT_TIMESTAMP	on update CURRENT_TIMESTAMP	
<input type="checkbox"/> size	varchar(45)	latin1_swedish_ci		No	None		
<input type="checkbox"/> status	varchar(45)	latin1_swedish_ci		No	No		
<input type="checkbox"/> status2	varchar(45)	latin1_swedish_ci		No	No		
<input type="checkbox"/> author	varchar(45)	latin1_swedish_ci		No	No		











































f-download

Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/> id	int(10)		UNSIGNED	No	None	auto_increment	
<input type="checkbox"/> file_name	varchar(45)	latin1_swedish_ci		No	None		
<input type="checkbox"/> down	varchar(45)	latin1_swedish_ci		No	None		

Files

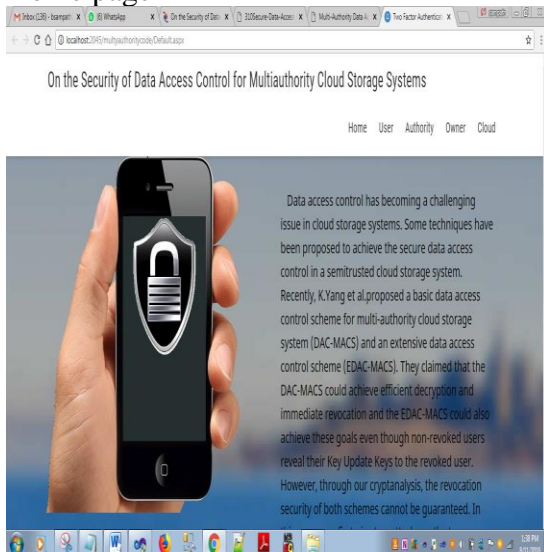
	Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/>	file_name	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	size	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	date	timestamp			No	CURRENT_TIMESTAMP		      
<input type="checkbox"/>	file	blob		BINARY	No	None		      
<input type="checkbox"/>	data	blob		BINARY	No	None		      
<input type="checkbox"/>	key	varchar(45)	latin1_swedish_ci		Yes	NULL		      

Register

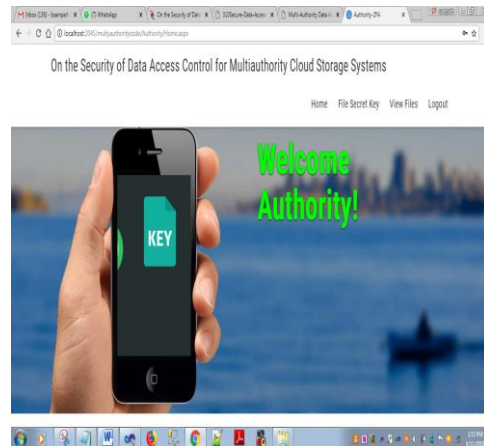
	Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/>	username	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	name	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	password	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	mail	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	phoneno	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/>	one_key	varchar(45)	latin1_swedish_ci		Yes	NULL		      

SCREEN SHOTS

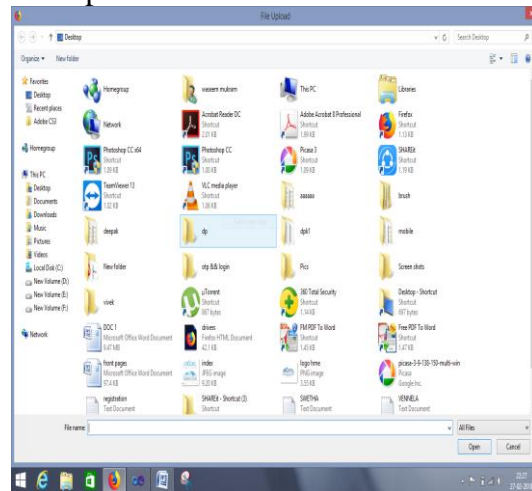
Home page



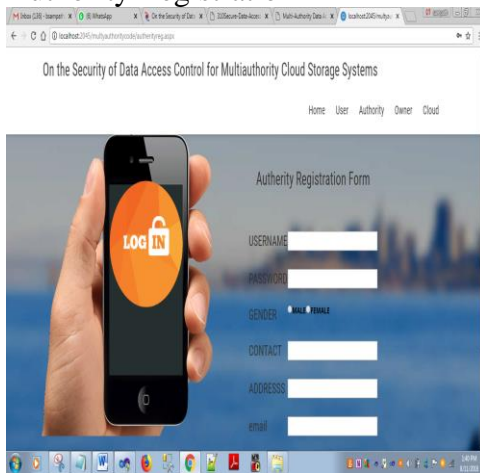
Authority login



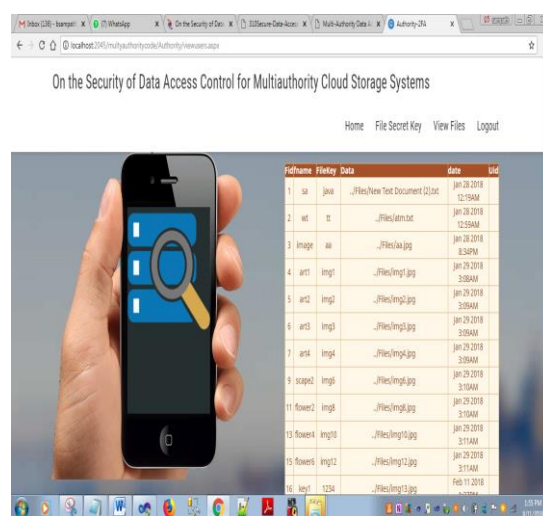
File upload



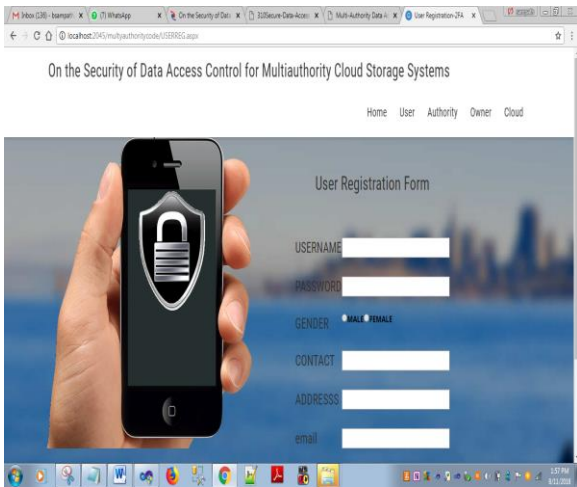
Authority Registration



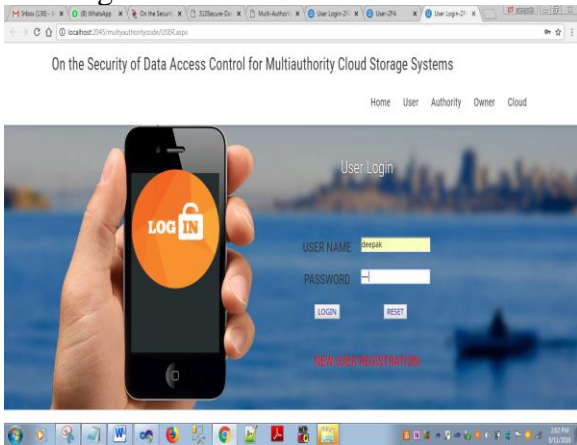
Authority Homepage



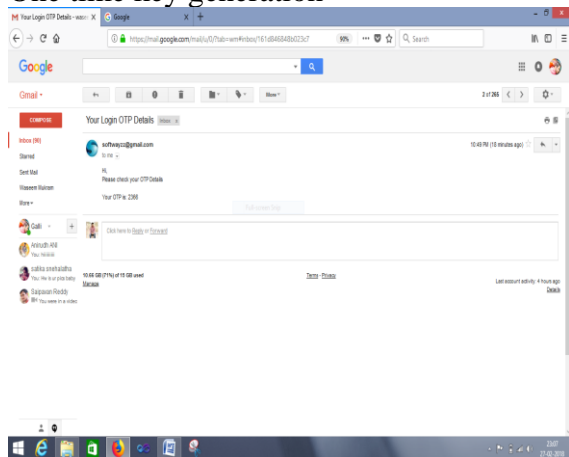
User registration



User login



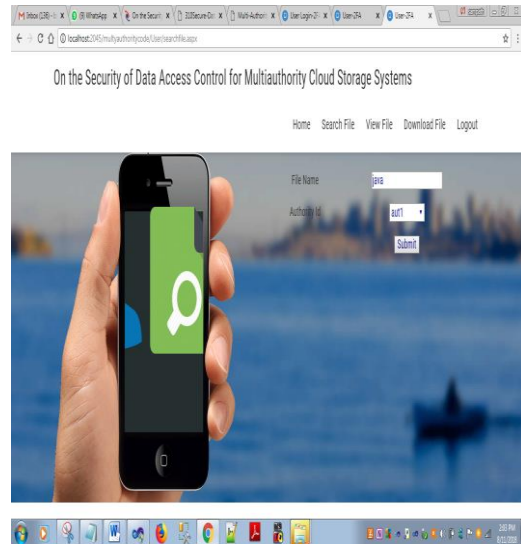
One time key generation



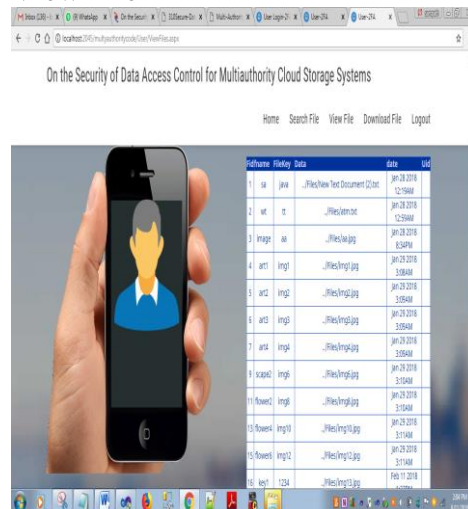
User's home page



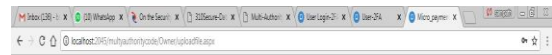
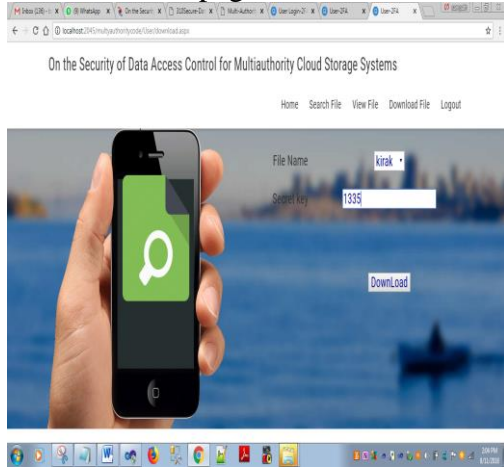
Search file



View File

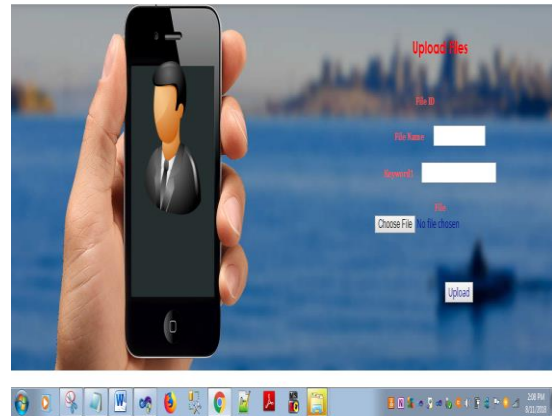


File download page

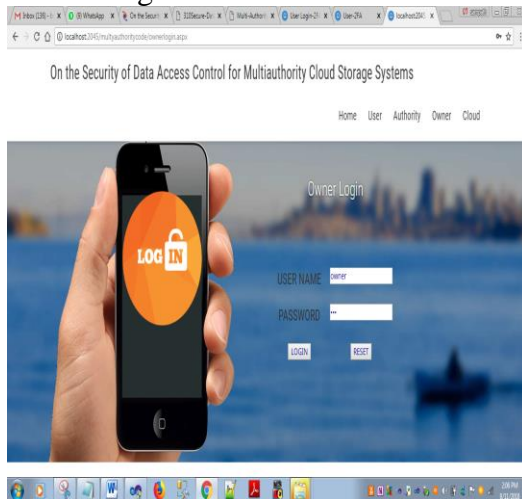


On the Security of Data Access Control for Multiauthority Cloud Storage Systems

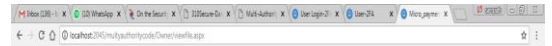
Home File Upload View Files Logout



Owner Login



View File:



On the Security of Data Access Control for Multiauthority Cloud Storage Systems

Home File Upload View Files Logout



File Upload

CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we have presented and proposed a protected revocable multi-authority CP-ABE scheme that can bolster secure attribute disavowal. At that point, I built a successful information get to control scheme for multi-authority distributed storage frameworks. The revocable multi-authority CP-ABE is a promising system, which can be connected in any remote.

BIBLIOGRAPHY

- [1] Kan Yang and Xiaohua Jia, —Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage —, in IEEE Trans. Parallel Distributed System, vol 25, No.7, pp 1735- 1744, July 2014.
- [2] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” in Proc. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321-334.
- [3] B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.
- [4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded Ciphertext Policy Attribute Based Encryption,” in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008, pp. 579-591. [5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully Secure Functional Encryption: AttributeBased Encryption and (Hierarchical) Inner Product Encryption,” in Proc. Advances in Cryptology EUROCRYPT’10, 2010, pp. 62-91.
- [6] M. Chase, “Multi-Authority Attribute Based Encryption,” in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), 2007, pp. 515-534.
- [7] M. Chase and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), 2009, pp. 121-130.