Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity checking in Public Cloud

B.Swarajya Lakshmi[1], A.D.Sivarama Kumar[2]
[1]P.G. Scholar, [2]Assistant Professor
[1,2]BRANCH: CSE
[1,2] SVR Engineering college .
Email: [1] lakshmi.jun@gmail.com,[2]sivaram.cse@svrec.ac.in

Abstract

The Identity based plan gives proficient dynamic data operations to data in distributed computing. This is on the grounds that client wishes to do different block level operation on the data document by assuring the data integrity. It accept that CSS will give the right data to client without deceiving the client. The block Level operation performed in fine grained updates. To accomplish this, this plan uses an adaptable data segmentation strategy and a data auditing convention. The data segmentation is the method for splitting the entire document into countable number of parts and are put away in various server areas. This strategy is improved the situation data security. The enemy does not know the document areas of different divided parts of record. Subsequently, he can't see the entire gathered single record.
In this way we can secure the data. In the mean time, it address a potential security issue in supporting open unquestionable status to make the plan more ensured and strong, which is accomplished by adding an extra authorization process among the three partaking gatherings of customer, server and a Manager. For better security, our plot incorporates an extra authorization process with the point of eradicating dangers of unapproved review difficulties from pernicious or imagined outsider inspectors, which we term as 'approved auditing'. Subsequently, the portioned records are encoded and put away in various server areas for enhancing the security purposes.

Keywords: Cloud computing, Identity-based cryptography, Proxy public key cryptography, Remote data integrity checking, time server.,

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.

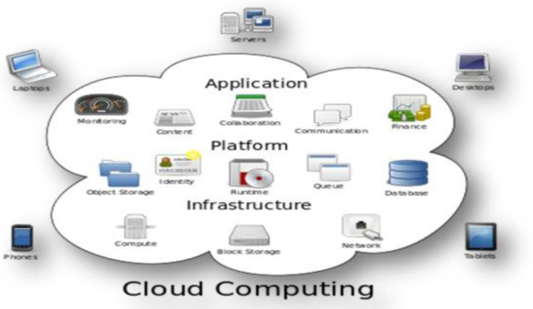


Fig 1.1 Structure of cloud computing

How Cloud Computing Works?

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.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage ca nbe managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

LITERATURE SURVEY

Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing

AUTHORS: Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu

Cloud computing is becoming increasingly popular. A large number of data are outsourced to the cloud by data owners motivated to access the large-scale computing resources and economic savings. To protect data privacy, the sensitive data should be encrypted by the data owner before outsourcing, which makes the traditional and efficient plaintext keyword search technique useless. So how to design an efficient, in the two aspects of accuracy and efficiency, searchable encryption scheme over encrypted cloud data is a very challenging task. In this paper, for the first time, we propose a practical, efficient, and flexible searchable encryption scheme which supports both multi-keyword ranked search and parallel search. To support multi-keyword search and result relevance ranking, we adopt Vector Space Model (VSM) to build the searchable index to achieve accurate search results. To improve search efficiency, we design a tree-based index structure which supports parallel search to take advantage of the powerful computing capacity and resources of the cloud server. With our designed parallel search algorithm, the search efficiency is well improved. Extensive experiments on the real-world dataset validate our analysis and show that our proposed solution is very efficient and effective in supporting multi-keyword ranked parallel searches.

Mutual verifiable provable data auditing in public cloud storage

AUTHORS: Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee

Cloud storage is now a hot research topic in information technology. In cloud storage, date security properties such as data confidentiality, integrity and availability become more and more important in many commercial applications. Recently, many provable data possession (PDP) schemes are proposed to protect data integrity. In some cases, it has to delegate the remote data possession checking task to some proxy. However, these PDP schemes are not secure since the proxy stores some state information in cloud storage servers. Hence, in this paper, we propose an efficient mutual verifiable provable data possession scheme, which utilizes Diffie-Hellman shared key to construct the homomorphic authenticator. In particular, the verifier in our scheme is stateless and independent of the cloud storage service. It is worth noting that the presented scheme is very efficient compared with the previous PDP schemes, since the bilinear operation is not required.

1. 3) Proxy signatures for delegating signing operation

AUTHORS: M. Mambo, K. Usuda, and E. Okamoto

In this project a new type of digital proxy signature is proposed. The proxy signature allows a designated person, called a proxy signer, to sign on behalf of an original signer. Classification of the proxy signatures is shown from the point of view of the degree of delegation, and conditions of a proposed proxy signature for partial delegation are clarified. The proposed proxy signature scheme is based on the discrete logarithm problem. Compared to the consecutive execution of the ordinary digital signature sch.emes, it has a direct form, and a verifier does not need a public key of a user other than the original signer in the verification stage. Moreover, it requires less amount of computational work than the consecutive execution of the signature schemes. Due to this efficiency together with the delegation property, an organization, e.g. a software company, can very efficiently create many signatures of its own by delegating its signing operations to multiple employees. Another attractive feature of the proposed schemes is their high applicability to other ordinary signature schemes based on the discrete logarithm problem. For instance, designated confirmer proxy signatures can be constructed..

2. 4) New ID-based proxy signature scheme with message recovery

AUTHORS: E.-J. Yoon, Y. Choi, and C. Kim

In 2012, Singh-Verma proposed an ID-based proxy signature scheme with message recovery. Unfortunately, by giving two concrete attacks, Tian et al. showed that Singh-Verma's scheme is not secure. This project proposes an improvement of Singh-Verma's scheme to eliminate the security problems.

3. 5) Secure proxy signature schemes from the weil pairing

AUTHORS: B.-C. Chen and H.-T. Yeh

A proxy signature scheme is a method which allows an original signer to delegate his signing authority to a designated person, called a proxy signer. Up to now, most of proxy signature schemes are based on the discrete logarithm problem. In this paper, we propose a proxy signature scheme and a threshold proxy signature scheme from the Weil pairing, and also provide security.Proof .language is a high-level language that can be characterized by all of the following buzzwords:

EXISTING SYSTEM:

In public cloud environment, most clients upload their data to *PCS* and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager's legal business will go on during the the period of investigation. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking.

1. Chen *et al.* proposed a proxy signature scheme and a threshold proxy signature scheme from the Weil pairing.
2. By combining the proxy cryptography with encryption technique, some proxy re-encryption schemes are proposed. Liu *et al.* formalize and construct the attribute-based proxy signature.
3. Guo*et al.* presented a non-interactive CPA (chosen-plaintext attack)-secure proxy re-encryption scheme, which is resistant to collusion attacks in forging re-encryption keys.

DISADVANTAGES OF EXISTING SYSTEM:

- Public checking will incur some danger of leaking the privacy.
- Less Efficiency.
- Security level is low

PROPOSED SYSTEM:

This project is based on the research results of proxy cryptography, identity-based public key cryptography and remote data integrity checking in public cloud.

In public cloud, this project focuses on the identity-based proxy-oriented data uploading and remote data integrity checking.

By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a novel proxy-oriented data uploading and remote data integrity checking model in public cloud. We give the formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairings, we designed the first concrete ID-PUIC protocol.

In the random oracle model, our designed ID-PUIC protocol is provably secure. Based on the original client’s authorization, our protocol can realize private checking, delegated checking and public checking.

We propose an efficient ID-PUIC protocol for secure data uploading and storage service in public clouds.

Bilinear pairings technique makes identity-based cryptography practical. Our protocol is built on the bilinear pairings. We first review the bilinear pairings.

ADVANTAGES OF PROPOSED SYSTEM:

High Efficiency.

Improved Security.

The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis.

On the other hand, the proposed ID-PUIC protocol can also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the original client’s authorization.

Private Checking, Delegated Checking And Public Checking

Our arranged ID-PUIC convention fulfills the non-open checking, appointed checking and open checking. Within the remote information integrity checking system, R1, Ro, Rp zone unit indispensable. Accordingly, the technique will exclusively be performed by the element UN office has R1, Ro,Rp. When all is said in done, since R1, Ro,Rp territory unit solid mystery by the first customer, our convention will exclusively be performed by the primary customer. Along these lines, it's non-open checking. On a few cases, the first customer has no capacity to picture its remote learning integrity, for example, he's taking a get-away or in prison or in combat zone, and so on. Subsequently, it'll delegate the outsider to play out the ID-PUIC convention. It might be the third examiner or the intermediary or elective substances. The principal customer sends R1, Ro, and Rp to the appointed outsider. The appointed third party has the adaptability to play out the ID-PUIC convention. In this way, it's the property of appointed checking. On the inverse hand, if the principal customer makes R1,Ro,Rp open, any element has the adaptability to play out the ID-PUIC convention. Consequently, our convention has conjointly the property of open.

Time Server

We include time server with in framework to indicate each record a particular day and age, and for that particular day and age document is available to client or customers. After time stamp is lapse record will be on cloud are not available to customers. So cloud can't get records those exist on cloud for long time.

Intermediary Server

While uploading documents on cloud intermediary stores duplicate of record so that if documents on cloud are hacked or tainted or integrity of

records isn't guarantee then those documents are again recover from intermediary.

MODULES:

MODULE DESCRIPTIONS:

ORIGINAL CLIENT:

Original Client is an Entity, Who is going to go about as a transfer the enormous data into people in general cloud server (PCS) by the assigned intermediary, and the main reason for existing is integrity checking of gigantic data will be through the remote control. For the Data uploading and Downloading customer need to pursue the following Process steps:

Customer can see the cloud records and furthermore make the downloading.

Customer needs to transfer the record with some asked for traits with encryption key.

At that point customer needs to make the demand to the TPA and PROXY to acknowledge the download demand and demand for the mystery key which will be given by the TPA.

Subsequent to receiving the mystery key customer can make the downloading document.

PUBLIC CLOUD SERVER:

PCS is an element which is maintained by the cloud specialist co-op. PCS is the huge distributed storage space and calculation asset to maintain the customer's monstrous data.

PCS can see the all the customer's points of interest and transfer some document which is valuable for the customer and make the capacity for the customer transferred records.

Intermediary

Intermediary is a substance, which is approved to process the Original Client's data and transfer them, is chosen and approved by Original Client. At the point when Proxy fulfills the warrant mω which is marked and issued by Original Client, it can process and transfer the original customer's data; else, it can't play out the system.

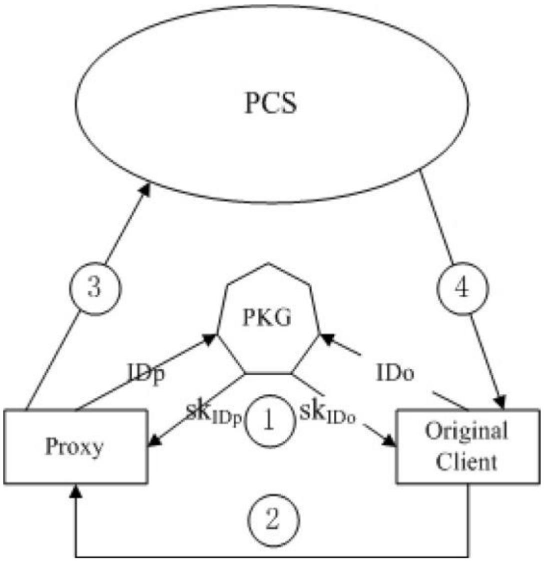
Just say implies: without the Knowledge of Proxy's validation and check and acknowledgment of intermediary customer can't download the record which is transferred by the Client.

KGC

KGC (Key Generation Center): a substance, while receiving an identity, it produces the private key which compares to the gotten identity.

Created Secret key is send to the customer who is make the demand for the mystery key by means of mail id which is given by the Client.

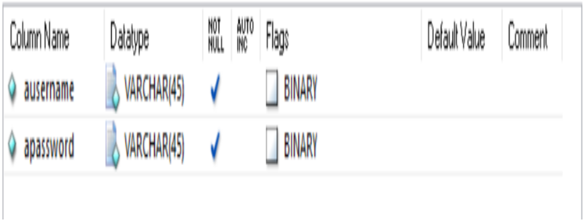
SYSTEM ARCHITECTURE:



4.9 Data Base Tables

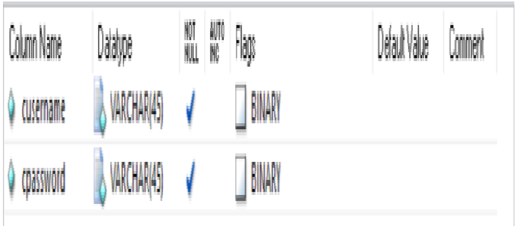
Data Base Tables

Auditor



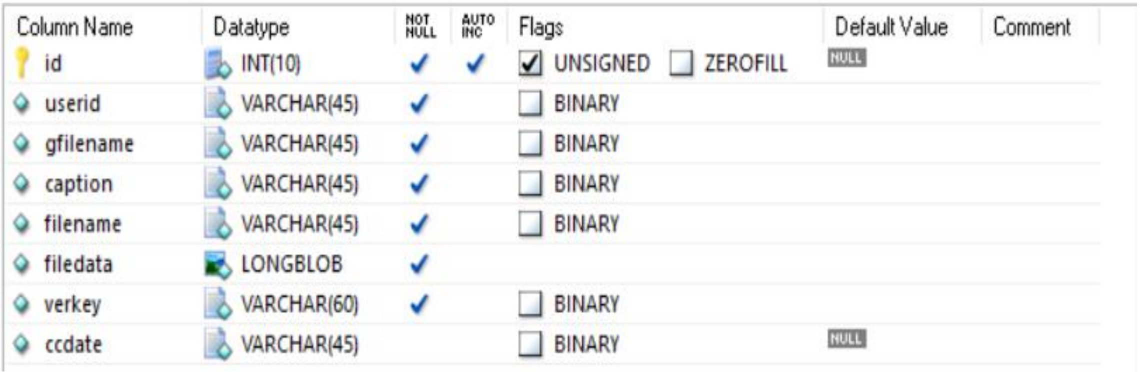
Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
ausername	VARCHAR(45)	✓		□ BINARY		
apassword	VARCHAR(45)	✓		□ BINARY		

CLOUD



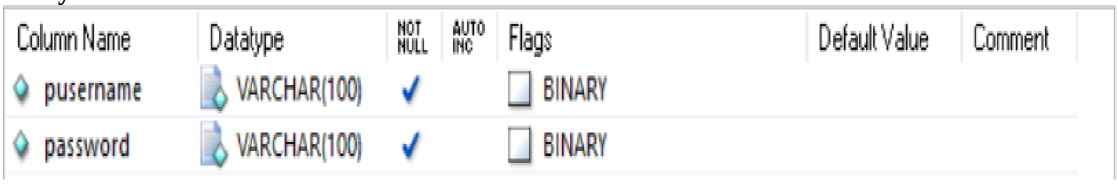
Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
cusername	VARCHAR(45)	✓		□ BINARY		
cpassword	VARCHAR(45)	✓		□ BINARY		

Cloud file upload



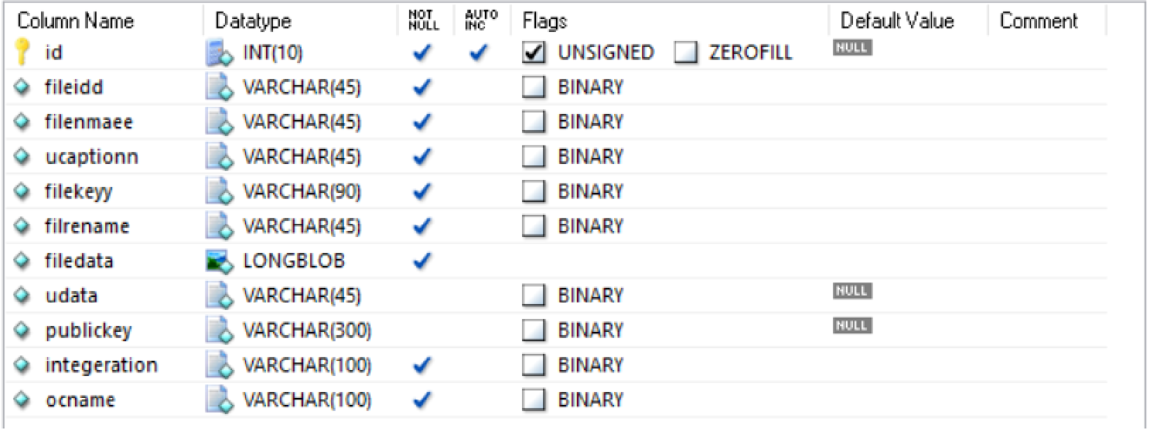
Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
id	INT(10)	✓	✓	☑ UNSIGNED □ ZEROFILL	NULL	
userid	VARCHAR(45)	✓		□ BINARY		
gfilename	VARCHAR(45)	✓		□ BINARY		
caption	VARCHAR(45)	✓		□ BINARY		
filename	VARCHAR(45)	✓		□ BINARY		
filedata	LONGBLOB	✓				
verkey	VARCHAR(60)	✓		□ BINARY		
ccdate	VARCHAR(45)			□ BINARY	NULL	

Proxy



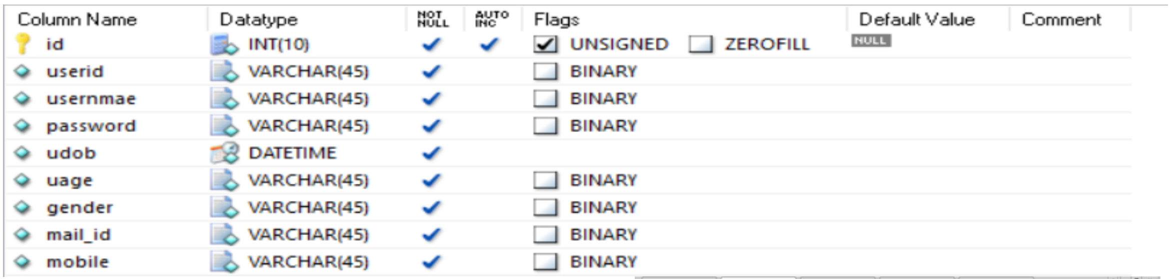
Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
pusername	VARCHAR(100)	✓		□ BINARY		
password	VARCHAR(100)	✓		□ BINARY		

User file upload



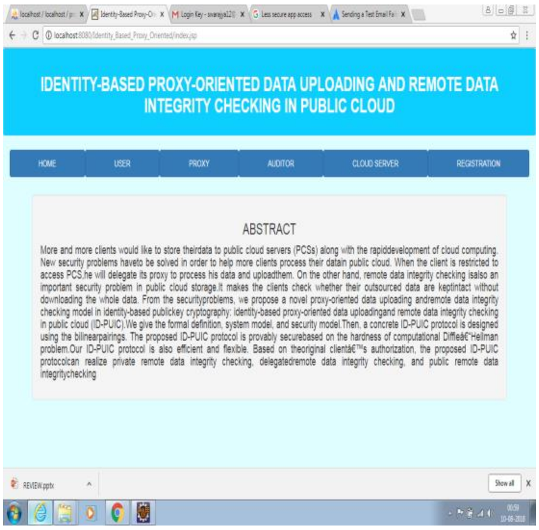
Column Name	Datatype	NOT NULL	AUTO INC	Flags	Default Value	Comment
id	INT(10)	✓	✓	☑ UNSIGNED □ ZEROFILL	NULL	
fileidd	VARCHAR(45)	✓		□ BINARY		
filenmaee	VARCHAR(45)	✓		□ BINARY		
ucaptionn	VARCHAR(45)	✓		□ BINARY		
filekeyy	VARCHAR(90)	✓		□ BINARY		
filrename	VARCHAR(45)	✓		□ BINARY		
filedata	LONGBLOB	✓				
udata	VARCHAR(45)			□ BINARY	NULL	
publickey	VARCHAR(300)			□ BINARY	NULL	
integeration	VARCHAR(100)	✓		□ BINARY		
ocname	VARCHAR(100)	✓		□ BINARY		

User reg



Column Name	Datatype	NOT NULL	AUTO INC	Flags		Default Value	Comment
id	INT(10)	✓	✓	☑ UNSIGNED	□ ZEROFILL	NULL	
userid	VARCHAR(45)	✓		□ BINARY			
usernmae	VARCHAR(45)	✓		□ BINARY			
password	VARCHAR(45)	✓		□ BINARY			
udob	DATETIME	✓					
uage	VARCHAR(45)	✓		□ BINARY			
gender	VARCHAR(45)	✓		□ BINARY			
mail_id	VARCHAR(45)	✓		□ BINARY			
mobile	VARCHAR(45)	✓		□ BINARY			

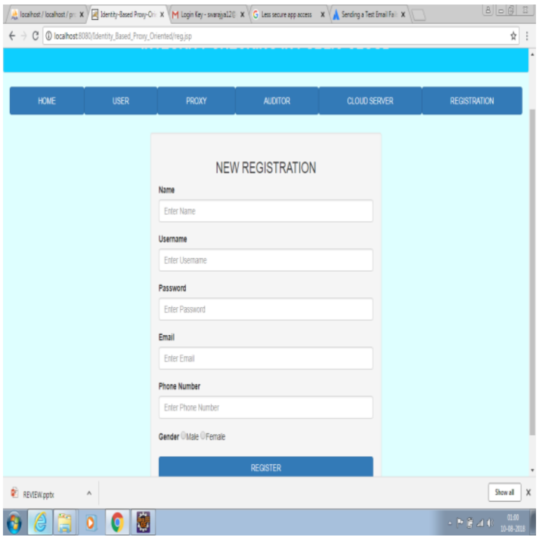
SCREENSHOTS



IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

ABSTRACT

More and more clients would like to store theirdata to public cloud servers (PCSs) along with the rapiddevelopment of cloud computing. New security problems haveto be solved in order to help more clients process their datain public cloud. When the client is restricted to access PCS,he will delegate its proxy to process his data and uploadthem. On the other hand, remote data integrity checking isalso an important security problem in public cloud storage.It makes the clients check whether their outsourced data are keptintact without downloading the whole data. From the securityproblems, we propose a novel proxy-oriented data uploading andremote data integrity checking model in identity-based publickey cryptography: identity-based proxy-oriented data uploadingand remote data integrity checking in public cloud (ID-PUIC).We give the formal definition, system model, and security model.Then, a concrete ID-PUIC protocol is designed using the bilinearpairings. The proposed ID-PUIC protocol is provably securebased on the hardness of computational Diffieâ€"Hellman problem.Our ID-PUIC protocol is also efficient and flexible. Based on theoriginal clientâ€™s authorization, the proposed ID-PUIC protocolcan realize private remote data integrity checking, delegatedremote data integrity checking, and public remote data integritychecking



NEW REGISTRATION

Name
Enter Name

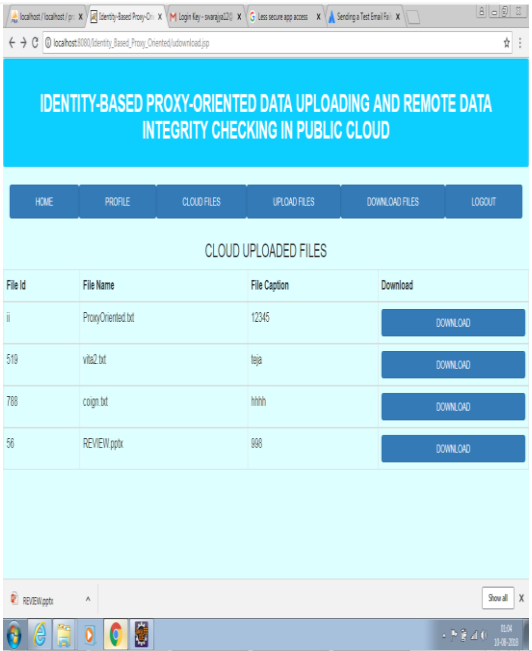
Username
Enter Username

Password
Enter Password

Email
Enter Email

Phone Number
Enter Phone Number

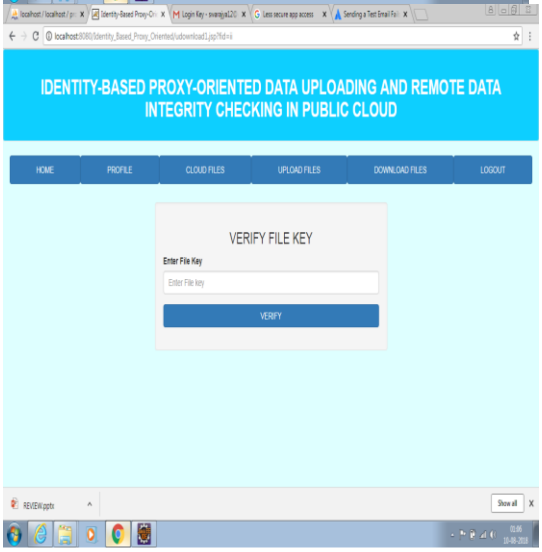
Gender ○Male ○Female



IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

CLOUD UPLOADED FILES

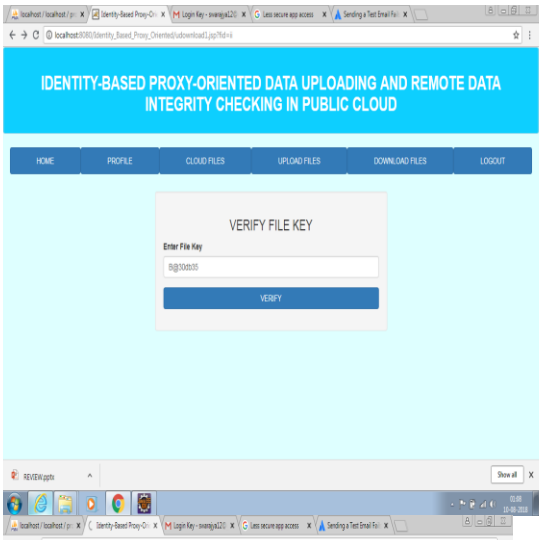
File Id	File Name	File Caption	Download
ii	ProxyOriented.txt	12345	DOWNLOAD
519	vita2.txt	teja	DOWNLOAD
788	coign.txt	hhhh	DOWNLOAD
56	REVIEW.pptx	998	DOWNLOAD



IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

VERIFY FILE KEY

Enter File Key
Enter File key

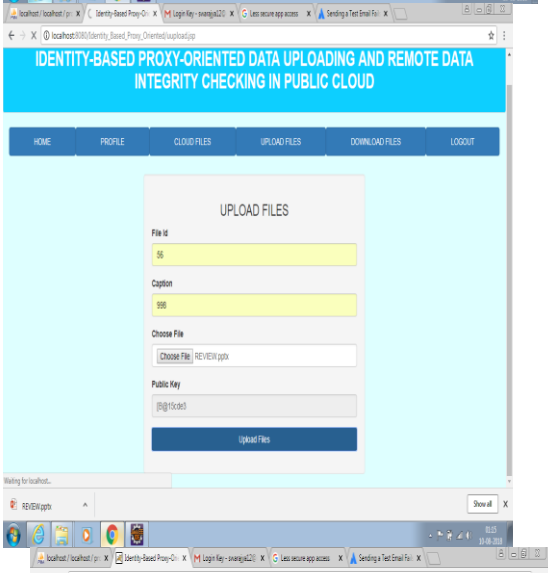


IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

VERIFY FILE KEY

Enter File Key: B@30db35

VERIFY



IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

UPLOAD FILES

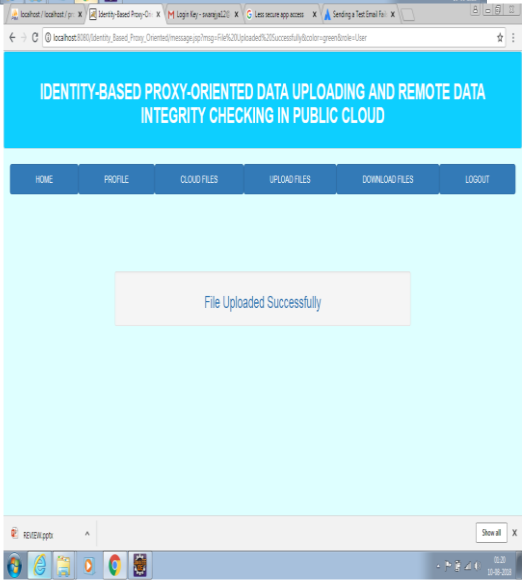
File Id: 56

Caption: 996

Choose File: Choose File REVIEW.pptx

Public Key: [B@15cde3

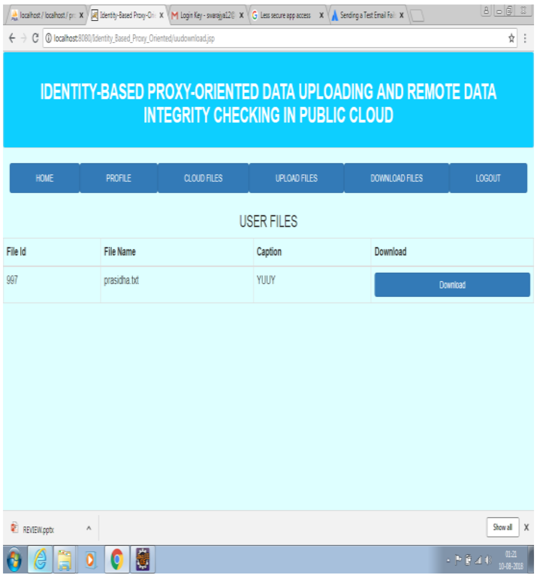
Upload Files


localhost:8080/Identity_Based_Proxy_Oriented/message.jsp?msg=File%20Uploaded%20Successfully&color=green&role=User
HOME
PROFILE
CLOUD FILES
UPLOAD FILES
DOWNLOAD FILES
LOGOUT
REVIEW.pptx
Show all

IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

File Uploaded Successfully

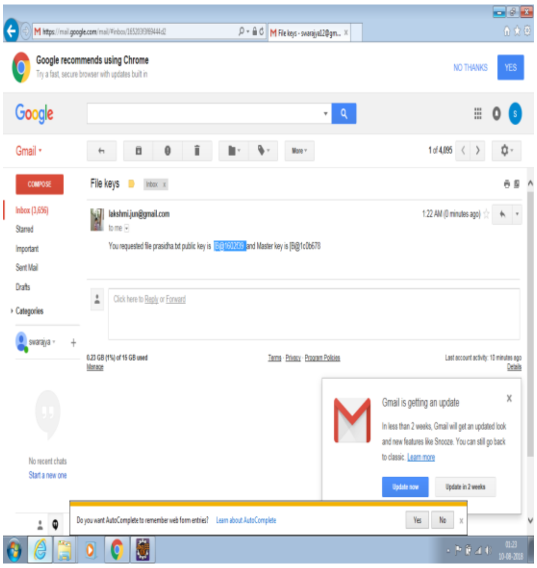
4.



IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

USER FILES

File Id	File Name	Caption	Download
997	prasidha.txt	YUUY	Download


5.

Google recommends using Chrome
Try a fast, secure browser with updates built in

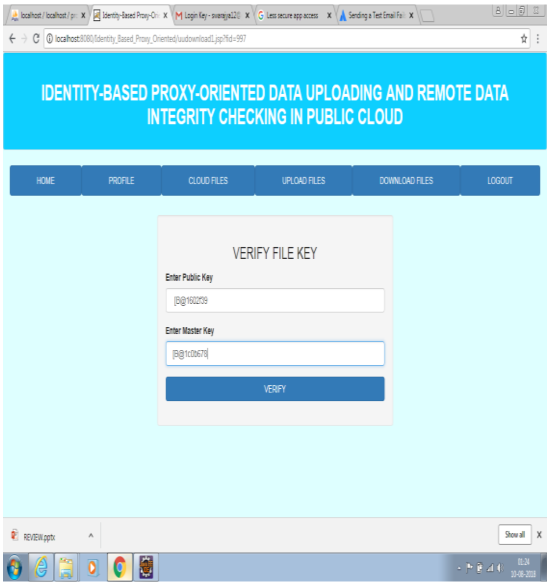
File keys

lakshmi.jun@gmail.com
to me

1:22 AM (0 minutes ago)

You requested file prasidha.txt public key is [B@1602f39 and Master key is [B@1c0b678

Gmail is getting an update
In less than 2 weeks, Gmail will get an updated look and new features like Snooze. You can still go back to classic. Learn more

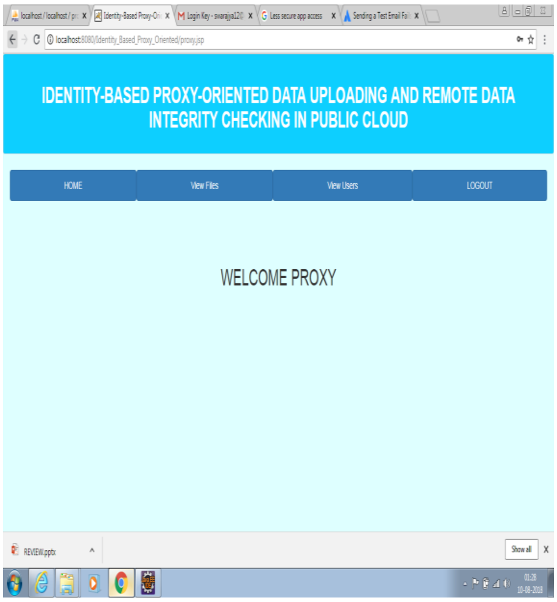

6.

IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

VERIFY FILE KEY

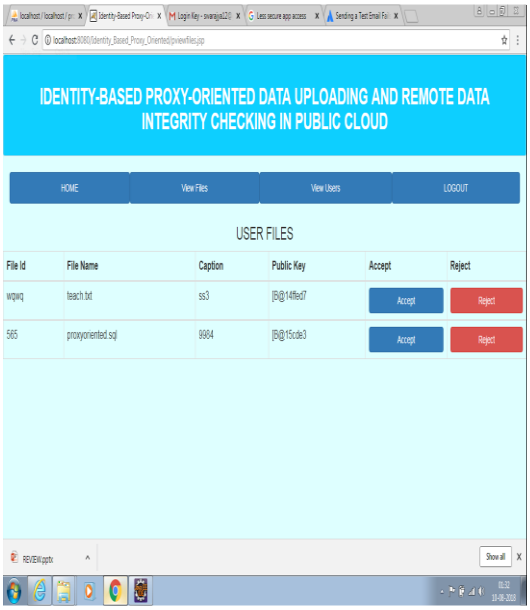
Enter Public Key: [B@1602f39

Enter Master Key: [B@1c0b678


7.

IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

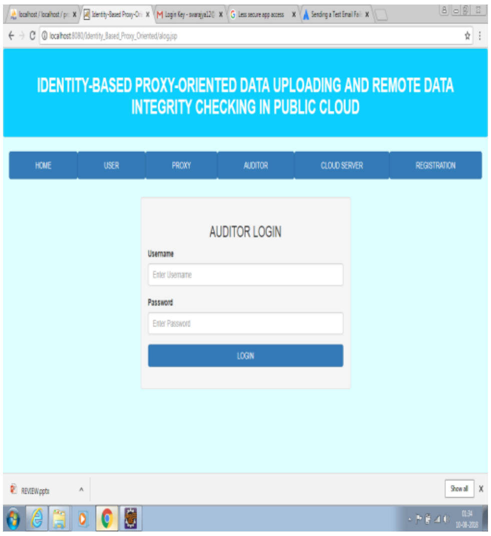
WELCOME PROXY



IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

USER FILES

File Id	File Name	Caption	Public Key	Accept	Reject
wqwq	teach.txt	ss3	[B@14ffed7	Accept	Reject
565	proxyoriented.sql	9984	[B@15cde3	Accept	Reject

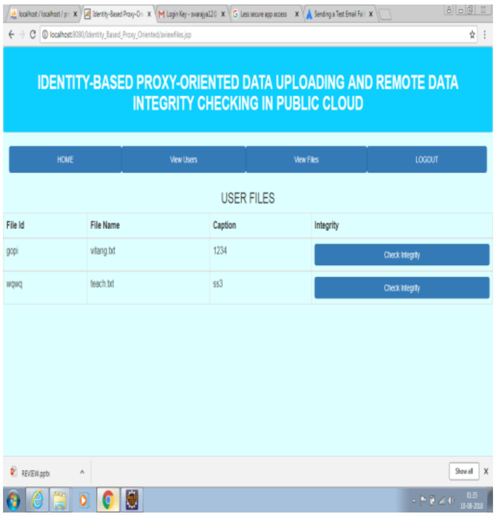


IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

AUDITOR LOGIN

Username: Enter Username

Password: Enter Password

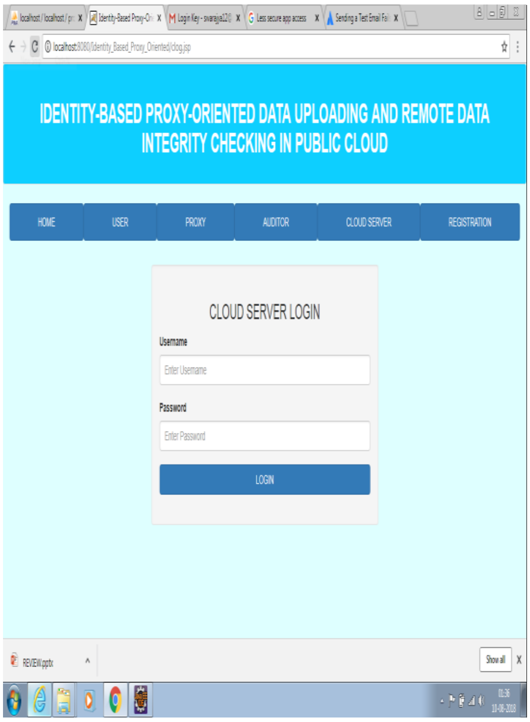


IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

USER FILES

File Id	File Name	Caption	Integrity
gopi	vitang.txt	1234	Check Integrity
wqwq	teach.txt	ss3	Check Integrity

8.

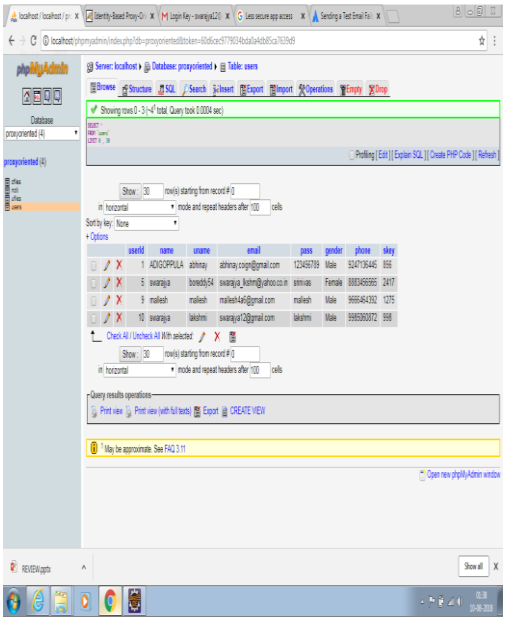


IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING AND REMOTE DATA INTEGRITY CHECKING IN PUBLIC CLOUD

CLOUD SERVER LOGIN

Username: Enter Username

Password: Enter Password



Server: localhost ▸ Database: proxyoriented ▸ Table: users

Showing rows 0 - 3 (~4 total, Query took 0.0004 sec)

SELECT *
FROM `users`
LIMIT 0 , 30

Show: 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None

userId	name	uname	email	pass	gender	phone	skey
1	ADIGOPPULA	abhinay	abhinay.coign@gmail.com	123456789	Male	9247136445	856
5	swarajya	boreddy54	swarajya_lkshm@yahoo.co.in	srinivas	Female	8883456565	2417
9	mallesh	mallesh	mallesh4a6@gmail.com	mallesh	Male	9666464392	1275
10	swarajya	lakshmi	swarajya12@gmail.com	lakshmi	Male	9985060872	998

Show: 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

phpMyAdmin
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Empty
Drop
Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]
+ Options
Check All / Uncheck All With selected:
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW
May be approximate. See FAQ 3.11
Open new phpMyAdmin window
REVIEW.pptx
Show all

CONCLUSION

Motivated by the application needs, this project proposes the novel security concept of ID-PUIC in public cloud. The project formalizes ID-PUIC's system model and security model. Then, the first concrete ID-PUIC protocol is designed by using the bilinear pairings technique. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis. On the other hand, the proposed ID-PUIC protocol can also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the original client's authorization

BIBLIOGRAPHY

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Trans. Commun.*, vol. E98-B, no. 1, pp. 190–200, 2015.

[2] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *J. Internet Technol.*, vol. 16, no. 2, pp. 317–323, 2015.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proc. CCS*, 1996, pp. 48–57.

[4] E.-J. Yoon, Y. Choi, and C. Kim, "New ID-based proxy signature scheme with message recovery," in *Grid and Pervasive Computing* (Lecture Notes in Computer Science), vol. 7861. Berlin, Germany: Springer- Verlag, 2013, pp. 945–951.

[5] B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from the weil pairing," *J. Supercomput.*, vol. 65, no. 2, pp. 496–506, 2013.

[6] X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing," in *Internet and Distributed Computing Systems* (Lecture Notes in Computer Science), vol. 8223. Berlin, Germany: Springer-Verlag, 2013, pp. 238–251.

[7] H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys," in *Cryptology and Network Security* (Lecture Notes in Computer Science), vol. 8813. Berlin, Germany: Springer-Verlag, 2014, pp. 20–33.

[8] E. Kirshanova, "Proxy re-encryption from lattices," in *Public-Key Cryptography* (Lecture Notes in Computer Science), vol. 8383. Berlin, Germany: Springer-Verlag, 2014, pp. 77–94.

[9] P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," *Chin. Sci. Bull.*, vol. 59, no. 32, pp. 4201–4209, 2014.

[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, "Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption," in *Proc. CT-RSA Conf.*, vol. 9048. 2015, pp. 410–428.

[11] G. Atenieseet *al.*, "Provable data possession at untrusted stores," in *Proc. CCS*, 2007, pp. 598–609.

[12] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proc. SecureComm*, 2008, Art. ID 9.

[13] C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. CCS*, 2009, pp. 213–222.

[14] E. Esiner, A. Küpçü, and Ö. Özkasap, "Analysis and optimization on FlexDPDP: A practical solution for dynamic provable

data possession," *Intelligent Cloud Computing* (Lecture Notes in Computer Science), vol. 8993. Berlin, Germany: Springer-Verlag, 2014, pp. 65–83.

[15] E. Zhou and Z. Li, "An improved remote data possession checking protocol in cloud storage," in *Algorithms and Architectures for Parallel Processing* (Lecture Notes in Computer Science), vol. 8631. Berlin, Germany: Springer-Verlag, 2014, pp. 611–617.

[16] H. Wang, "Proxy provable data possession in public clouds," *IEEE Trans. Services Comput.*, vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.

[17] H. Wang, "Identity-based distributed provable data possession in multicloud storage," *IEEE Trans. Services Comput.*, vol. 8, no. 2, pp. 328–340, Mar./Apr. 2015.

[18] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks," *J. Biomed. Inform.*, vol. 50, pp. 226–233, Aug. 2014.

[19] H. Wang, "Anonymous multi-receiver remote data retrieval for pay-TV in public clouds," *IET Inf. Secur.*, vol. 9, no. 2, pp. 108–118, Mar. 2015.

[20] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. ASIACRYPT*, vol. 5350. 2008, pp. 90–107.

[21] Q. Zheng and S. Xu, "Fair and dynamic proofs of retrievability," in *Proc. CODASPY*, 2011, pp. 237–248.

[22] D. Cash, A. Küpçü, and D. Wichs, "Dynamic proofs of retrievability via oblivious RAM," in *Proc. EUROCRYPT*, vol. 7881. 2013, pp. 279–295.

[23] J. Zhang, W. Tang, and J. Mao, "Efficient public verification proof of retrievability scheme in cloud," *Cluster Comput.*, vol. 17, no. 4, pp. 1401–1411, 2014.

[24] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.

[25] T. Ma *et al.*, "Social network and tag sources based augmenting collaborative recommender system," *IEICE Trans. Inf. Syst.*, vol. E98-D, no. 4, pp. 902–910, 2015.

[26] K. Huang, J. Liu, M. Xian, H. Wang, and S. Fu, "Enabling dynamic proof of retrievability in regenerating-coding-based cloud storage," in *Proc. IEEE ICC*, Jun. 2014, pp. 712–717.

[27] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[28] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.

[29] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Trans. Services Comput.*, vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.

[30] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds,"

IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.

[31] O. Goldreich, *Foundations of Cryptography: Basic Tools*. Beijing, China: Publishing House of Electronics Industry, 2003, pp. 194–195.

[32] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” in *Proc. ASIACRYPT*, vol. 2248. 2001, pp. 514–532.

[33] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Proc. CRYPTO*, vol. 2139. 2001, pp. 213–229.

[34] A. Miyaji, M. Nakabayashi, and S. Takano, “New explicit conditions of elliptic curve traces for FR-reduction,” *IEICE Trans. Fundam. Electron.,Commun. Comput. Sci.*, vol. E84-A, no. 5, pp. 1234–1243, 2001.

[35] C. Research. *SEC 2: Recommended Elliptic Curve Domain Parameters*. [Online]. Available: http://www.secg.org/SEC2-Ver-1.0.pdf, accessed 2015.

[36] *The GNU Multiple Precision Arithmetic Library (GMP)*. [Online]. Available: http://gmplib.org/, accessed 2015.

[37] *The Pairing-Based Cryptography Library (PBC)*. [Online]. Available: http://crypto.stanford.edu/pbc/howto.html, accessed 2015.

[38] B. Lynn, “On the implementation of pairing-based cryptosystems,” Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2008. [Online]. Available: http://crypto.stanford.edu/pbc/thesis.pdf