ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

Identity Based Cloud Storage Security System

Shaikh Nikkhatparvin[1], Karishma Maniyar[2], Snehal Tawhare[3], Prof. Gholap P. S[4]

B. E Student, Department of Computer Engineering, Dumbarwadi, Otur, Pune, India[1,2,3]

Assistant Professor, Department of Computer Engineering, Dumbarwadi, Otur, Pune, India [4]

ABSTRACT: Cloud storage system provides facilitative file storage and sharing services for distributed clients. To address integrity, controllable outsourcing, and origin auditing concerns on outsourced files, we propose an *identity-based data outsourcing* (IBDO) scheme equipped with desirable features advantageous over existing proposals in securing outsourced data. First, our IBDO scheme allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company's cloud account in a controlled way. The proxies are identified and authorized with their recognizable identities, which eliminates complicated certificate management in usual secure distributed computing systems. Second, our IBDO scheme facilitates comprehensive auditing, i.e., our scheme not only permits regular integrity auditing as in existing schemes for securing outsourced data, but also allows to audit the information on data origin, type, and consistence of outsourced files. Security analysis and experimental evaluation indicate that our IBDO scheme provides strong security with desirable efficiency.

KEYWORDS: Cloud storage, data outsourcing, proof of storage, remote integrity proof, public auditing**.**

I. INTRODUCTION

Cloud computing has been imagined as the following creation data innovation (IT) design for undertakings, because of its extensive rundown of unparalleled preferences in the IT history: on-request self-benefit, omnipresent system get to, area self-deciding asset pooling, fast asset versatility, utilization based estimating and transference of hazard.
As a disturbing innovation with significant ramifications, cloud computing is changing the very way of how organizations utilize data innovation. One essential part of this outlook changing is that information are being brought together or outsourced to the cloud. From clients' view, including together people and IT endeavors, putting away information remotely to the cloud in an adaptable on-request technique bring appealing advantages: arrival of the weight for storage room administration, boundless information access with place autonomy, and evasion of assets expenses on equipment, programming, and staff systems of support, and so on While cloud computing make these remuneration more engaging than any other time in recent memory, it additionally conveys new and testing security dangers to clients' outsourced information. As cloud administration suppliers (CSP) are part regulatory elements, information outsourcing is really surrendering client's last control more than the destiny of their information. As a matter of first importance, despite the fact that the frameworks beneath the cloud are significantly more effective and dependable than individual registering gadgets, they are still before the extensive variety of both inside and outside dangers for information respectability.

A. Paper Organization

We describe the IBDO system motivation in Section II. The framework of IBDO system and literature survey in Section III. A detailed IBDO system in Section IV. Finally, Section V concludes the paper.

II. MOTIVATION

Due to the complexity and volume, outsourcing ciphertexts to a cloud is deemed to be one of the most effective approaches for big data storage and access. Nevertheless, verifying the access legitimacy of a user and securely

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

updating a ciphertext in the cloud based on a new access policy designated by the data owner are two critical challenges to make cloud-based big data storage practical and effective. Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave
activities. In this paper, we propose a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds. We first propose a new NTRU decryption algorithm to overcome the decryption failures of the original NTRU, and then detail our scheme and analyze its correctness, security strengths, and computational efficiency.

III. LITERATURE SURVEY

In 2015 Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification in past years, the advancement of cloud storage administration makes it less demanding than at any other time for cloud clients to impart information to each other. To guarantee clients confidence of the honesty of their mutual information on cloud, various strategies have been proposed for information trustworthiness inspecting with centers around different commonsense highlights, e.g., the help of dynamic information, open uprightness evaluating, low correspondence/ computational review cost, and low stockpiling overhead. In any case, the greater part of these strategies consider that lone the first information proprietor can adjust the mutual information, which confines this system to customer read- just applications. As of late, a couple of endeavors began considering more practical situations by enabling numerous cloud clients to alter information with honesty confirmation. By and by, this endeavors are still a long way from pragmatic because of the gigantic computational cost on cloud clients, particularly when high mistake discovery likelihood is required by the framework. In this paper, we propose a novel trustworthiness evaluating plan for cloud information sharing administration portrayed by multiuser modification, open reviewing, high blunder location likelihood, efficient client repudiation and in addition useful computational/ correspondence inspecting execution. Our plan can oppose client pantomime assault, which isn't considering existing methods that help multiuser modification. Bunch evaluating of various errands is likewise efficiently bolstered in our plan. Broad analysis on Amazon EC2 cloud and distinctive customer gadgets (contemporary and cell phones) demonstrate that our outline enables the customer to review the respectability of mutual file with a steady computational cost of 340 ms likelihood with information defilement rate of 1%. In this paper, we propose a novel information uprightness evaluating plan that backings numerous journalists for cloud- based information sharing administration. our proposed conspire is highlighted by notable properties of open uprightness reviewing and steady computational cost on the client side. We accomplish this through our creative plan on polynomial- based verification labels which permits accumulation of labels of various information pieces. For framework versatility, we additionally engage the cloud with the capacity to total verification labels from various journalists into one when sending the honesty confirmation data to the verifier (who might be general cloud clients). Accordingly, only a consistent size of respectability confirmation data should be transmitted to the verifier regardless of what number of information squares are being checked and what number of journalists are related with the information pieces. Besides, our novel outline permits secure designation of client repudiation operations to the cloud with an efficient fundamental plan and a propelled outline with upgraded unwavering quality. To wrap things up, our proposed plot permits collection of honesty evaluating operation for different undertakings (files) through our clump trustworthiness inspecting method. We give functional application scenarios of proposed scheme. Extensive numerical examination and genuine tests approve the execution of our plan.

In 2015 Identity-Based encryption with outsourced revocation in cloud computing, identity based encryption (IBE) which simplifies the public and certificate management at public key infrastructure (PK) is a vital contrasting option to open key encryption. Be that as it may, one of the fundamental efficiency downsides of IBE is the overhead calculation at private key generator(PKG) amid client disavowal. Efficient repudiation has been all around considered in customary PKI setting, yet the un widely administration of certificates is a accurately the weight that IBE endeavors to reduce. In this paper, going for handling the basic issue of personality denial, we bring outsourcing calculation into IBE for the first time and propose a revocable IBE plot in the server aided setting, Our scheme off loads most of the key generation related operations during key- issuing and key-update processes to a key refresh cloud specialist organization, leaving

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

just a consistent number of basic operations for the PKG and clients to perform locally. This objective is accomplished by using a novel agreement safe system: We utilize a mixture private key for every client, in which an AND entry way is included to interface and bound the personality segment and the time part. Besides, we propose another development which is provable secure under the as of late formulized referred assignment of calculation show. At long last, we give broad trail result to show the efficiency of our proposed development. In this paper, focusing on the critical issue of identity repudiation, we bring out sourcing calculation into IBE and propose a revocable plan in which the renouncement operations are appointed to CSP. With the guide of KU-CSP, the proposed plot is fullhighlighted: It accomplishes steady efficiency for both calculation at PKG and private key size at client; Client needs not to contact with PKG amid key update, as such, PKG is permitted to be offline after sending the revocation list to KU-CSP;No secure channel or client verification is required amid key-refresh amongst client and KU-CSP. Further more, we consider to realize revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure under RDoC model, in which at least one of the KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs collude, it is unable to enable such client re-to get his/her decrypt ability. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed development.

A. 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. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. The manager will be restricted to access the network in order to guard against collusion. Here third party public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, if these data cannot be processed just in time, the manager will face the loss of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity.

- **Disadvantage of Existing System:**
- Data security protection cannot be directly user's control.
- Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.
- Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety,
- This is not just a third party data warehouse.

IV. SYSTEM ARCHITECTURE

The architecture of our IBDO system is shown in Fig. 1. An IBDO system consists of five types of entities, that is, fileowners, proxies, auditors, registry server, and storage server. Generally, the file-owners, proxies and auditors are cloud clients. The registry server is a trusted party responsible for setting up the system and responding to the clients' registration, and also allows the registered clients to store the public parameters of outsourced files. The cloud storage server provides storage services to the registered clients for storing outsourced files. In real-world applications, an organization buys storage services from some CSP, and the IT department of the organization can play the role of a registry server. In this way, the registered clients (employees) can take advantage of the storage services.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

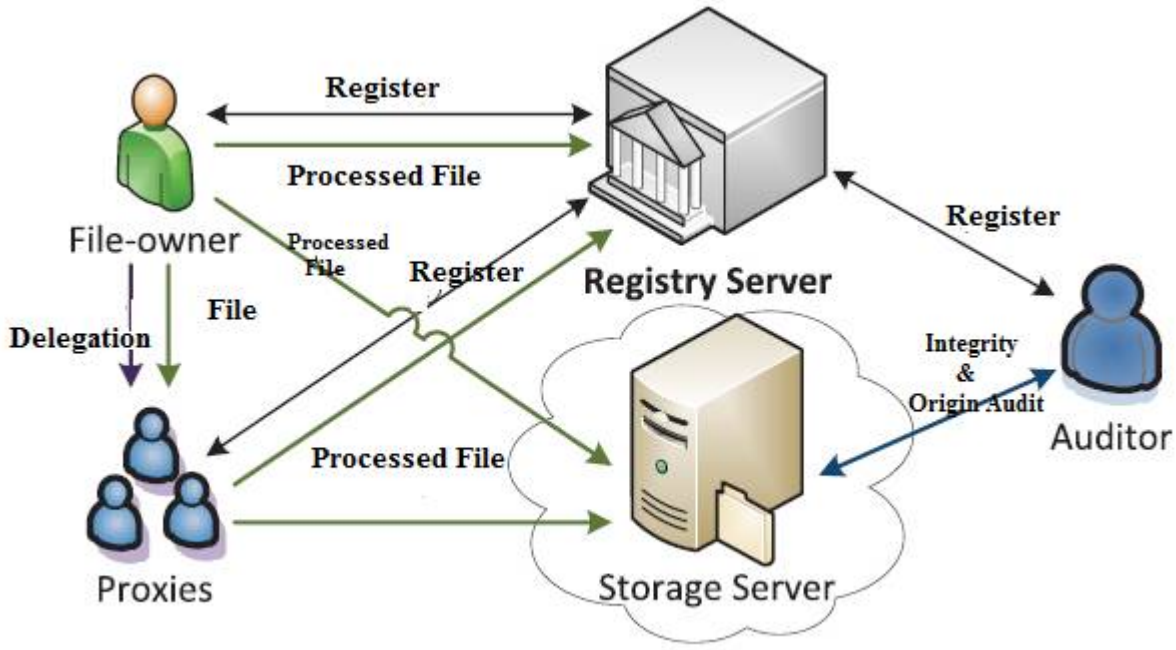

Fig 1. System Architecture

The file-owner and her authorized proxies can outsource files to the cloud server. Specifically, on behalf of the owner, the authorized proxy processes the file, sends the processed results to the storage server, and uploads the corresponding public parameters of the file to the registry server. Neither the file-owner nor the proxy is required to store the original file or the processed file locally. The duty of the auditor is to check the integrity of outsourced files and their origin-like general log information by interacting with the cloud storage server without retrieving the entire file.

A. Advantages of Proposed System

- Compared to a lot of its predecessors, which only provide binary results about the storage state across the cloud servers, the challenge-response protocol in our work more provides the localization of data error.
- Unlike most prior works used for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
- Extensive protection and act analysis demonstrate that the proposed scheme is extremely efficient and resilient beside Byzantine failure, malicious data modification attack, and even server colluding attacks.

V. CONCLUSION

In this system, we investigated proofs of storage in cloud in a multi-user setting. We introduced the notion of identitybased data outsourcing and proposed a secure IBDO scheme. It allows the file-owner to delegate her outsourcing capability to proxies. Only the authorized proxy can process and outsource the file on behalf of the file-owner. Both the file origin and file integrity can be verified by a public auditor. The identitybased feature and the comprehensive auditing feature make our scheme advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

REFERENCES

[1] Kan Yang and Xiaohua Jia" An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" IEEE TRANSACTIONS PARALLEL AND CLOUD SYSTEM, VOL. 24, NO. 9, SEPTEMBER 2013.
2] Byang Wang ,Baochun Li and Hui Li "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 1, JANUARY/ FEBRUARY 2015.
[3] Yong Yu, Member, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai "Attributer-Based Cloud Data Integrity Auditing for Secure Outsourced Storage" VOL. 14, NO. 8, AUGUST 2015.
[4] Jae Hong Seo and Keita Emura "Revocable Identity- Based Cryptosystem Revisited: Security Models and Constructions" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, JULY
2014.
[5] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, Senior Member " Identity - Based Encryption with Outsourced Revocation in Cloud Computing" IEEE TRANSACTIONS ON COMPUTERS
[6] Jia Yu, Kui Ren, Senior Member, IEEE, Cong Wang, Member, IEEE and Vijay Varadharajan, senior Memer, IEEE "Abstract- Cloud Storage Auditing with Key-Exposure Resistance" IEEE TRANSACTION ON INFORMATION FORENSICS AND SECURITY, VOL. No.,2014.
[7] Jiawei Yuan, Shucheng Yu, Member, IEEE, " Public Integrity Auditing for Dynamic data Sharing with Multi-User Modification" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
[8] H.Wang, "Identity - Based Cloud Provable Data Possession in Multi Cloud Storage," Service Computing IEEE TRANSACTIONS ON, VOL. 8, NO. 2, 328-340, MARCH 2015.
[9] T. Jiang, X.Chen, and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation, "IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 8,pp. 2363-2373, AUG 2016.
[10] Y. Yu, M. H. A. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity - Based Remote Data Integrity Checking with Perfect Data Preserving for Cloud Storage," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2016.
[11] K. Yang and X. Jia " Data Storage Auditing Service in Cloud Computing : Challenges, Methods and Opportunities," World Wide Web, VOL. 15, NO. 4, PP. 409-428, 2012.
[12] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud
Storage," Computers, IEEE TRANSACTIONS ON VOL. 62, NO. 2, PP. 362-275, 2013.
[13] Jianbing Ni, Yong Yu, YI Mu, Senior Member, IEEE, Qi Xia On the" Security of an Efficient Dynamic Auditing Protocol in Cloud Storage IEEE TRANSACTIONS ON PARALLEL AND CLOUD SYSTEM.
[14] Cong Wang, Member, IEEE, Scherman S.M. Chow, Quian Wang, Member, IEEE , Kui Ren, Senior Member, IEEE, and Wenjin Lou, Senior Member, IEEE "Privacy- Preserving Public Auditing for Secure Cloud Storage" IEEE, TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.
[15] Jia Yu, and Huaqun Wang "Strong Key- Exposure Resilient Auditing for Secure Cloud Storage" IEEE
TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOl., NO., 2016.
[16] Ziad Ismail, Christophe Kiennert, Jean leneutre, and Lin Chen "Auditing Cloud Provider's Compliance with Data Backup Requirements: A Game Theoretical Analysis" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.
[17] Jiangtao Li, Lei Zhang, Member, IEEE, Joseph K. Liu, Haifeng Qian and Zheming Dong "Privacy – Preserving Public Auditing Protocol for Low Performance End Devices in Cloud" IEEE TRANSACTIONS ON
INFORMATION FORENSICS AND SECURITY, VOL. 11, Issue: 11, Nov. 2016.
[18] Anmin Fu, Member, IEEE Shui Yu, Senior Member, IEEE, Yuquing Ahang, Huaqun Wang, and Chanying Huang "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" IEEE TRANSACTIONS ON BIG DATA, VOL., PP., Issue: 99, May 2017.