CLOUD-BASED DATA STORAGE THAT GUARANTEES CONFIDENTIALITY AND ANONYMITY

Abstract

There has been a rise in demand for public cloud storage (PCS) as a result of the proliferation of cloud computing. To facilitate more customers' data processing on the public cloud, new security issues must be resolved. If a client is unable to reach PCS directly, he may still process and submit data by using a proxy server. Remote data integrity verification, on the other hand, is a major issue for cloud security. It forces customers to verify the security of their outsourced data without requiring them to download the whole database. We propose a new way to use identity-based public key cryptography (ID-PUIC) in the public cloud for proxy-kind of data exporting and confidential data integrity is verifying. This will fix the current security problems. Formalization, system model, and security model are provided. The bilinear combinations are then used to develop a practical ID-PUIC technique. Because solving the computational Daffier-Hellman issue is very difficult, the suggested ID-PUIC protocol may be shown to be completely safe. The ID-PUIC technique we've developed is both practical and adaptable. The proposed ID-PUIC protocol allows for private, delegated, and public remote data integrity checking based on the permissions of the originating client.

Keywords: Security, Open Cloud Server, Proxy, Integrity Verifying, Exporting, Bilinear Pairs, Coherent and Pliant.

Authors

Dr. A.V.H. Sai Prasad
Associate Professor
Department of Information Technology
Malla Reddy College of
Engineering&Technology
Hyderabad, Telangana, India.
sai.alurip@gmail.com

Dr. K. Suresh
Associate Professor
Department of Information Technology
Malla Reddy College of
Engineering&Technology
Hyderabad, Telangana, India.
kurumallasuresh@gmail.com

K. Chandusha
Assistant Professor
Department of Computer Science and
Engineering
Malla Reddy College of Engineering
&Technology
Hyderabad, Telangana, India.
kandachandusha@gmail.com

I. INTRODUCTION

The rapid rise in data volume necessitates more processing power and storage space. Cloud computing has quickly grown in popularity as it has been able to meet the demands of many types of applications. In recent years, cloud computing has grown into a massive industry that dwarfs its predecessors [1]. When compared to older forms of computing, it offers a number of improvements. In addition, it offers a wide range of services for its customers. The cloud also offers storage as a service, among other features. Features include data protection, computer power, and storage space.

Using a public cloud platform and universal data to provide cross-regional access has reduced the administrative complexity of data storage. As a result, many customers choose to save their data on a distant cloud computing system and process it there. Rapid progress in computer and communication technologies has resulted in a vast amount of new information [2]. More powerful computing resources and more storage space are required to accommodate this massive volume of information. In recent years, the demand for loud computing has increased dramatically as it meets the needs of many applications. Information processing, including data storage, computation, knowledge security, etc., is outsourced and provided as a service. Customers are pampered by taking advantage of the public cloud. This means an increase in the number of customers eager to put their data into the "cloud" for storage and processing.

With public cloud computing, users have the option of storing their massive amounts of data on a network of faraway computers. Since the information is not under the control of the retailers, it presents security vulnerabilities related to privacy, reliability, and accessibility. Primitive methods like remote knowledge integrity checking might be used to assure cloud users that their data has not been compromised in any way [3]. When the data owner is unable to getting the open cloud server directly, they may turn to a proxy or another trusted third party to handle the data's processing and uploading on their behalf. However, the confidential data integrity verifying protocol has to be accurately so that it may be used by devices with limited storage space.

II. EXISTING METHODOLOGY

Most customers in a public cloud setting verify the security of their distant data over the web and upload it to PCS. Some logistical issues arise when the customer is the sole manager. Managers are subject to arrest and removal by law enforcement upon suspicion of involvement in commercial fraud. To prevent any possible cooperation, the manager's access to the network will be disabled throughout the inquiry. However, the manager's legal matters will continue as usual while the inquiry is underway [4]. Who can assist him in processing the data when it is produced in huge quantities? If these numbers aren't crunched in time, the manager stands to lose money. Managers may avoid this scenario by giving their secretaries, for instance, responsibility for processing the proxy's data. However, the management will not put their faith in subordinates to carry out the remote data integrity check.

Developed the Wein pairing into a proxy signature technique and a threshold proxy signature system some proxy re-encryption systems are presented, which combine proxy cryptography with the encryption method. Create the feature-based proxy signature in a formal setting. Demonstrated an interactive-free, chosen-plaintext-attack (CPA)-secure proxy re-encryption method that prevents forgery of re-encryption keys by groups.

1. Disadvantages of Existing System

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

III. PROPOSED METHODOLOGY

- This study examines the issues of distant data integrity verification and identity-based proxy-oriented data uploading in the public cloud.
- Our proposed ID-PUIC protocol is time-saving since it does away with the need for certificates and instead relies on recognized-based public-key cryptology. ID-open cloud is a revolutionary methodology for remote data integrity checking in the cloud that is proxy-based. We ensure the security design and formal system design of the ID-PUIC protocol. We then created the first practical ID-PUIC protocol using bilinear pairings.
- Our developed ID-PUIC protocol is probably safe in the random oracle paradigm. Our protocol enables Confidential checking, delegated checking, and public verifying based on authorization from the originating client [5].
  To address the security concerns associated with storing sensitive information in the cloud, we suggest an effective ID-PUIC protocol.
- Identity-based cryptography is now feasible thanks to the bilinear pairing method. Our approach relies on a system of bilinear pairs. Initially, we will go through the bilinear combinations.

1. Benefits of Proposed Model

- Reduced processing time for distant data integrity verification is a result of the protocol's use of identity-based public-key cryptography, which does away with certificates. In cloud-based settings, this efficiency may have a major influence on operating speed and resource consumption.
- With their innovative proxy-oriented method, ID-PUIC introduces a new standard for remote data integrity verification in the cloud. By improving security measures without sacrificing performance, this new approach completely transforms the way data integrity is handled in cloud settings.
- Providing a comprehensive security model and formal system model ensures building confidence and dependability in the protocol's application, enabling a clear knowledge of the protocol's workings.
- An ID-PUIC protocol that works with bilinear pairings demonstrates the practical application of theoretical ideas, making it workable and applicable in the real world.

IV. ENHANCED SYSTEM

The findings from studies on identity-based public key cryptography, confidential data reference checking, and proxy cryptography were used to write this article.

1. Modules

- Original Client
- Public Cloud Server
- Proxy
- KGC

- **Original Client:** For the most part, the original client will use remote control to verify the integrity of huge amounts of data that have been uploaded to the public cloud server (PCS) via the delegated proxy [6]. The client must follow these procedures for uploading and downloading data:

➢ The client has both read and writes access to the cloud storage.
➢ The client must upload the file, along with the desired properties and encryption key.
➢ After that, the client will need to ask the TPA and PROXY to approve the download and hand over the secret key.
➢ The client may access the file after obtaining the key.

- **Public Cloud Server:** The PCS is a separate entity managed by the cloud provider. The client's vast data requires a large amount of cloud storage space and compute resources, both of which are provided by PCS.PCS has access to the whole client profile, may provide helpful files for the client, and can even save such files for future reference.

- **Proxy:** A proxy is a third party that has permission to access and upload data on behalf of the originating client. The original customer made the decision and gave their approval. Proxy may only process and upload data belonging to the original client if it has the original client's signed and granted warrant, without which it cannot do so.The client cannot get the file it submitted without knowing the proxy's authentication, verification, and acceptance of the file.

- **KGC:** Upon receipt of an identification, a KGC (Key Generation Center) will provide the corresponding private key. When a customer requests a secret key, they provide their email address so that the created secret key may be supplied to them.

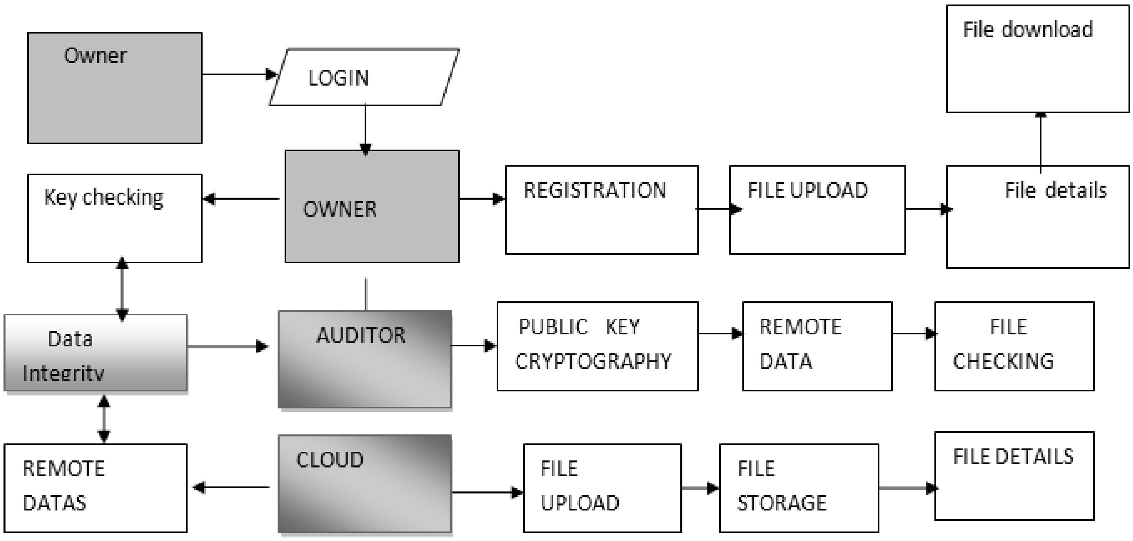

Figure 1: Data Flow of System

2. Discussion of Data Flow Diagram

- Security and control over data integrity verification are improved by the protocol's architecture, which allows for private checking, delegated checking, and public checking depending on permission from the originating client. This design caters to varied use cases and security needs.
- This protocol is relevant in protecting data from attacks or vulnerabilities that are unique to cloud storage settings because it aims to solve security concerns about storing sensitive information in the cloud.
- The use of the bilinear pairing approach paves the way for identity-based encryption, which may lead to easier key management and more secure data handling options.
- A solid mathematical basis is shown by the protocol's dependence on a system of bilinear pairings, which guarantees a solid cryptographic basis for its operations.

V. CONCLUSION

The needs of particular applications served as the inspiration for this work, which introduces the ground-breaking security concept of ID-Public cloud for use in the public cloud. The article outlines the security design and system model for ID-Public cloud in a formal way. The first practical ID-PUIC protocol is then developed utilizing bilinear pairing. Proof of security and accurate analysis are used to demonstrate the concrete ID-Public Cloud protocol's safety and effectiveness. On the other hand, depending on the permissions granted by the elder client, the proposed ID-PUIC protocol may potentially provide open remote data reference checking.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from the weil pairing," The Journal of. Supercomputing., vol. 65, no. 2, pp. 496–506, 2013.

[9] 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.

[10] 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.