e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707141 |

Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage

Shruti[1], Shweta Shri K[2]

Student, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: The cloud storage service allows people to efficiently share data within a group. Because the cloud server is untrustworthy, many remote data possession checking (RDPC) protocols have been proposed and are thought to be an effective way to ensure data integrity. However, the majority of RDPC protocols are based on the traditional public key infrastructure (PKI) mechanism, which has limitations. There is a clear security flaw, and certificate management is a significant burden. Identity-based cryptography (IBC) is being developed to address this shortcoming. RDPC is frequently chosen as the foundation. Unfortunately, key escrow is an inherent disadvantage of IBC. We use the to solve these issues.

I. INTRODUCTION

The CLOUD storage service provides users with an efficient way to share data and collaborate as a team. When one of the team members uploads a file to the server, the other members are notified. The use of a certificateless signature technique is used to present a new RDPC protocol for verifying the integrity of data shared among a group. The user's private key is made up of two parts: a partial key generated by the group manager and a secret value selected by herself/himself. To ensure that the correct public keys are selected during data integrity checking, each user's public key is associated with her unique ID. identity, such as a name or a phone number As a result, the certificate is no longer required, and the issue of key escrow is also resolved. Meanwhile, without downloading the entire dataset, the data integrity can still be audited by a public verifier. Furthermore, our plan includes allows for efficient user revocation from the group Our scheme's security is reduced to computational assumptions. CDH (Diffie-Hellman) and discrete logarithm (DL). Experiment results show that the new protocol is very efficient and effective.

II. LITERATURE SURVEY

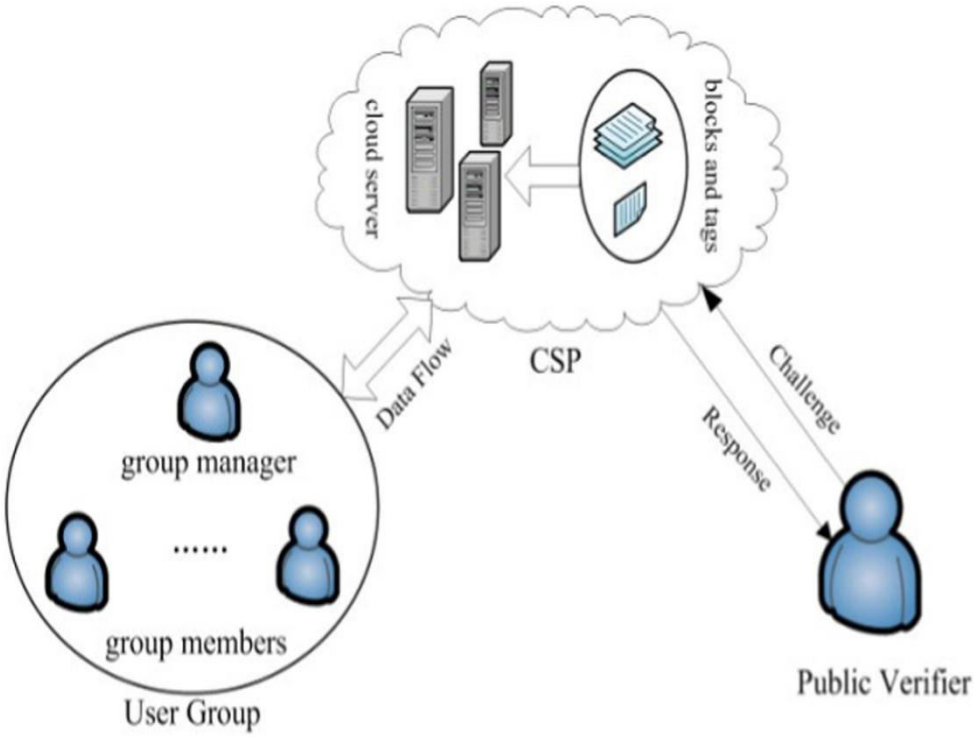
With the significant advances in Information and Communications Technology (ICT) over the last half century, there is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). This computing utility, like all other four existing utilities, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community. To deliver this vision, a number of computing paradigms have been proposed, of which the latest one is known as Cloud computing. Hence, in this paper, we define Cloud computing and provide the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs). We also provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation. In addition, we reveal our early thoughts on interconnecting Clouds for dynamically creating global Cloud exchanges and markets. Then, we present some representative Cloud platforms, especially those developed in industries, along with our current work towards realizing market-oriented resource allocation of Clouds as realized in Aneka enterprise Cloud technology.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707141 |

III. SYSTEM DESIGN



IV. RESULTS AND OUTCOMES

Dataset Collection and Preparation:

- Clearly define the objectives of the data collection, focusing on the parameters needed for certificateless public integrity checking.
- Identify relevant data sources such as cloud storage logs, user activity records, and shared file metadata.

Feature Selection and Engineering:

- **Enhanced Security Models**: Develop robust security models to handle advanced threats and attacks in certificateless public integrity checking schemes.
- **Scalability Solutions**: Focus on improving scalability to efficiently handle large volumes of data and a high number of users in group shared environments.

Outcome of the Detection:

- **Data Privacy**: These schemes ensure that data privacy is maintained while performing integrity checks. Data is not exposed during the verification process, protecting sensitive information from unauthorized access.
- **Scalability**: Certificateless integrity checking supports scalability, allowing large groups to share and verify data efficiently. This is crucial for cloud environments where data volume and user numbers can be substantial.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707141 |

Snapshots:

Figure 1: Group member login

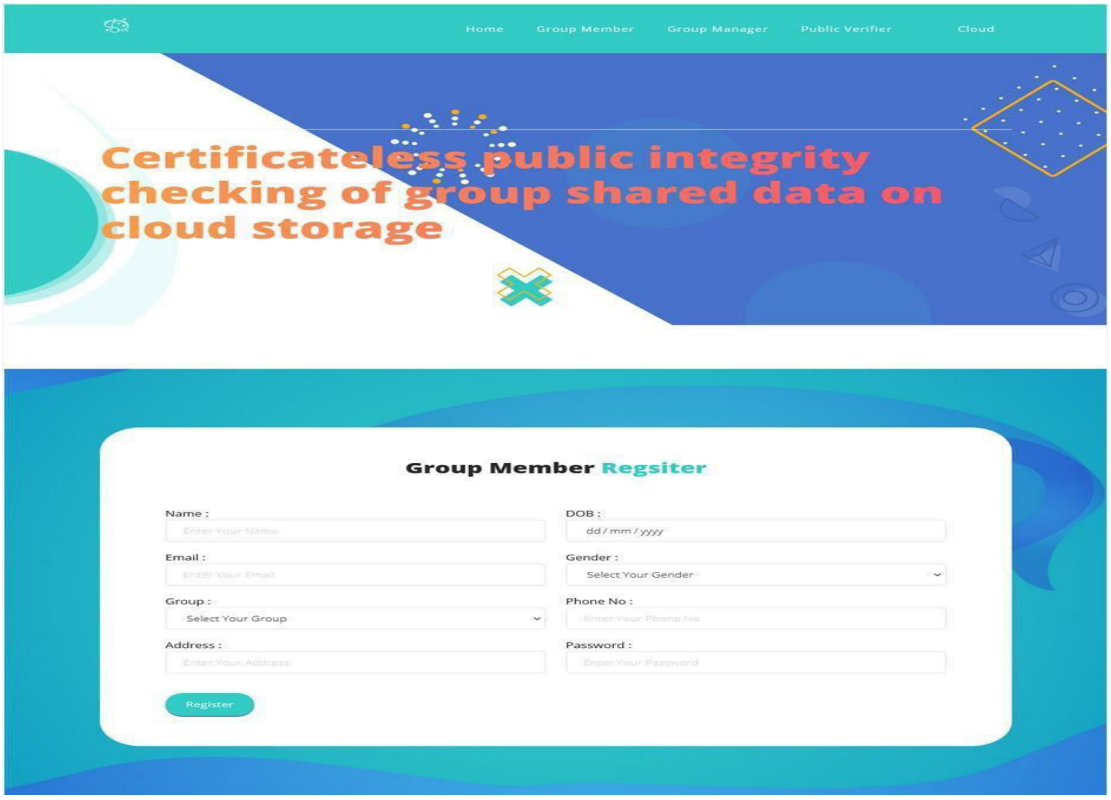


Figure 2: Group member register

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707141 |

Figure 3: public verifier login

Figure 4: cloud server login

V. CONCLUSION

In this article, we provide a unique RDPC scheme for information that has been examined again on a cloud server. Our strategy is to deal with the integrity verification for the information collection that is distributed across many clients of a group. For the production of all the block labels, we employ the potential of a certificateless mark. The Our method avoids the key escrow issue and the assertion that the PKI board doesn't exist because each group member possesses a fraction key and a secret value. Additionally, our plan supports public scrutiny, efficient client renunciation, and multiuser information modification. We describe the security model and framework model of our plan in detail. Finally, we show the security measures in light of the CDH and DL suspicion.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707141 |

REFERENCES

1. Dropbox for Business. [Online]. Accessible: https://www.dropbox.com/business, Accessed on: Sep. 16, 2016.
2. TortoiseSVN. [Online]. Accessible: https://tortoisesvn.net/,Accessed on: Sep. 16, 2016.
3. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Distributed computing and arising IT stages: Vision, publicity, and reality for conveying processing as the fifth utility," Future Gener. Comp. Syst., vol. 25, no. 6, pp. 599-616, 2009.
4. Y. Deswarte, J. J. Quisquater, and A. Saєıdane, "Distant honesty checking," in Proc. Sixth Working Conf. Integr. Inner Control Inf. Syst., 2003, pp. 1-11.
5. G. Ateniese, et al., "Provable information ownership at untrusted stores," in Proc. fourteenth ACM Conf. Comput. Commun. Security, 2007, pp. 598-609.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com