International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 4, July-Aug 2024

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

DATA STORING AND RETRIVAL IN CLOUD COMPUTING WITH HIGH SECURITY

G.Bharathikannan*, M.Atchiya **

*(Asst.Professor.CSE, Sembodai Rukmani Varatharajan Engineering College, Sembodai
Email: bharathi348@gmail.com)

** (PG Scholar CSE, Sembodai Rukmani Varatharajan Engineering College, Sembodai
Email: atchiya29052001@gmail.com)

----------**********----------

Abstract:

This addresses the cloud computing in critical issue of data security by accent the potential vulnerabilities that exist between users and cloud service providers, despite the security measures implemented by the latter. The conventional model, where cloud service providers (CSPs) possess both encryption and decryption keys, poses a significant threat to data security and user privacy, as data may be transmitted without user consent. To mitigate this threat, the study proposes the integration of a Third-Party Auditor (TPA) as an external entity responsible for managing and validating the security of cloud-stored data. In this proposed model, users encrypt their data before transmission, and the TPA conducts a thorough verification process before allowing the data to be stored in the cloud. This approach ensures that the data remains confidential and unchanged during both transit and storage. In conclusion, the study provides a practical and effective solution for users looking for robust data privacy and security in cloud computing environments, offering a structured and secured approach to data storing and retrieval.

Keywords — Cloud Service Providers, Third-Party Auditor.

----------**********----------

I. INTRODUCTION

In an era dominated by cloud computing, where vast amounts of sensitive data are transferred and stored remotely, the critical concern of ensuring robust data security has become paramount. Despite the implementation of security measures by cloud service providers (CSPs), a significant concern persists regarding potential vulnerabilities between users and these providers. The conventional model, wherein CSPs possess both encryption and decryption keys, poses a serious threat to data security and user privacy, as it may result in unauthorized data transmission.

Recognizing this challenge, this study proposes a solution that integrates a Third-Party Auditor (TPA) as an external entity to actively watch over and validate the security of data stored in the cloud. This novel approach involves users encrypting their data before transmission, and the TPA conducting a comprehensive verification process before permitting the data to be stored in the cloud. By doing so, the study aims to establish a more secure paradigm for data managing in cloud computing environments, where the confidentiality and integrity of data are protected throughout both transit and storage.

This introduction sets the stage for an in-depth discovery of the proposed methodology, emphasizing its practicality and effectiveness in addressing the upward concerns related to data privacy and security in cloud computing.

II. CLOUD COMPUTING

Cloud computing is a technology to store, handle, process, and access the data too much the internet instead of a local server or computer hard drives. Here, the term cloud is taken from the symbol of the internet users in the flowcharts. The inaccessible servers are used in cloud computing to store the data that can be accessed from wherever using the internet. With the help of cloud computing, an organization can save lots of cost of local data storage, maintenance of data, etc. The information over the cloud can be accessed by anybody, anywhere, and anytime, with the help of the internet. Using cloud computing as an alternative of traditional storage helps users with a lot of benefits such as speed, cost-effectiveness, security, worldwide access, etc.

III. RELATED WORKS

3.1 PRIVACY-PRESERVING AND REGULAR LANGUAGE SEARCH OVER ENCRYPTED CLOUD DATA[2021]

Kaitai Liang, Xinyi Huang, FuchunGuo, and Joseph K. Liu [3] discussed with using cloud-based storage service, users can re- motely store their data to clouds but also enjoy the high quality data retrieval services, without the tedious and cumbersome local data storage and maintenance. However, the sole storage service cannot satisfy all desirable requirements of users. Over the last decade, privacy-preserving search over encrypted cloud data has been a meaningful and practical research topic for outsourced data security.

The fact of remote cloud storage service that users cannot have full physical possession of their data makes the privacy data search a formidable mission. A naive solution is to delegate a trusted party to access the stored data and fulfill a search task. This, nevertheless, does not scale well in practice as the fully data access may easily yield harm for user privacy. To securely introduce an effective solution, we should guarantee the privacy of search contents, i.e. what a user wants to search, and return results, i.e. what a server returns to the user. Furthermore, we also need to guarantee privacy for the outsourced data, and bring no additional local search burden to user. In this paper, we design a novel privacy-preserving functional encryption based search mechanism over encrypted cloud data.

A major advantage of our new primitive compared to the existing public key based search systems is that it supports an extreme expressive search mode, regular language search.

3.2 EDGE-BASED DIFFERENITAL PRIVACY COMPUTING FOR SENSOR-CLOUD SYSTEMS[2019]

Tian Wang, YaxinMeia ,WeijiaJiab , Xi Zhengc , GuojunWangd , Mande Xi [19] discussed with in sensor-cloud systems, with more personal data being hosted in cloud, privacy leakage is becoming one of the most serious concerns. Privacy computing is emerging as a paradigm to systematically enhance privacy protection. In other words, the new paradigm requests us to improve the computing model to provide a general privacy protection service. In this paper, we propose an edge-based model for data collection, in which the raw data from wireless sensor networks (WSNs) is differentially processed by algorithms on edge servers for privacy computing.

A small quantity of the core data is stored on edge and local servers while the rest is transmitted to cloud for storage. In this way, the benefits are twofold. First, the data privacy is preserved since the original data cannot be retrieved even if the data stored in the cloud is leaked. Second, implemented by a differential storage method, compared to the state of the art, the edge-based model sends less data to the cloud and reduces the cost of communication and storage. Both theoretical analyses and extensive experiments validate our proposed method.

2.3 A CLOUD DATA DE-DUPLICATION SCHEME BASED ON CERTIFICATELESS PROXY RE-ENCRYPTION[2019]

XiaoyuZheng, Yuyang Zhou, Yalan Ye, Fagen Li [20] discussed with cloud data de-duplication removes redundant data blocks or files and keeps only one copy in the cloud storage server. In order to improve on security, we need to encrypt data files and blocks such that all same files and blocks are detectable based on cipher text for de-duplication.

So how to detect a cipher text to find the same files is a challenging problem. In this paper, we propose a cloud data de-duplication scheme based on certificateless proxy re-encryption.It contains certificateless proxy re-encryption (CL-PRE) and proof of ownership based on certificateless signature (PoW-CLS). Compared with the existing scheme, we use certificateless cryptography to solve the problem of key escrow and avoid the situation where a key generation center (KGC) impersonates a user to decrypt the cipher text. Our CL-PRE realizes data de-duplication across users and our PoW-CLS improves the efficiency of the proof of ownership (POW).

IV. PROPOSED METHODOLOGY

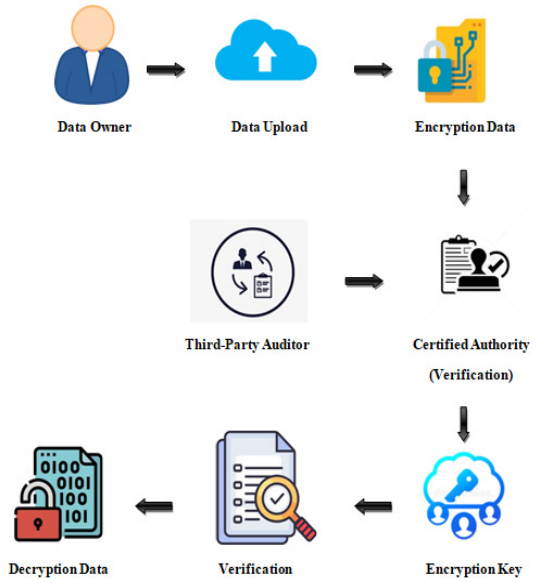

Fig. 1 System Architecture

A. Third-Party Algorithm

A third-party algorithm using the cloud typically involves leveraging algorithms or services provided by a company or entity other than the primary service or platform you're using, and executing these algorithms through cloud-based infrastructure.

Here's a breakdown:

1. **Third-Party Algorithm**: This refers to an algorithm created and maintained by an external entity. For instance, it could be a machine learning model for image recognition, language translation, data analysis, or any other specialized task developed by a different company.
2. **Cloud Infrastructure**: This includes services provided by cloud computing platforms like Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, etc. These platforms offer various resources such as computing power, storage, and services that can be accessed over the internet.

When you combine a third-party algorithm with cloud infrastructure, you're essentially using the capabilities of a service provider to execute the algorithm. Here's a step-by-step explanation of how it works:

- **Accessing the Algorithm**: You obtain access to the third-party algorithm. This might involve subscribing to their service, getting an API key, or some form of access that allows you to use their algorithm.
- **Integration with Cloud Services**: You then integrate this algorithm within your application, system, or workflow that is hosted on the cloud. This integration might involve using SDKs (Software Development Kits), APIs (Application Programming Interfaces), or other means provided by the

cloud platform to connect with the third-party algorithm.

- **Execution on Cloud Infrastructure**: When your application or system requires the functionality provided by the third-party algorithm, it sends a request to the cloud infrastructure. The cloud platform, through its computing resources, processes this request by utilizing the third-party algorithm.
- **Results Delivery**: The results generated by the third-party algorithm are then sent back to your application or system via the cloud infrastructure. These results can be in the form of analyzed data, predictions, classifications, translations, or any other output that the algorithm is designed to provide.

By utilizing the cloud to execute third-party algorithms, you gain scalability, flexibility, and potentially cost-efficiency since you pay for the resources used rather than maintaining dedicated hardware for running these algorithms. Additionally, it allows for easy integration of advanced functionalities without the need to build them from.

V. SYSTEM IMPLEMENTATION

A. *System Modules*

1. Encryption data
2. Cloud Storage
3. Data Transmission
4. Third-Party Auditor
5. User Authentication
6. Verification and decryption

B. *Module Description*

1. Encryption Data

The Encryption Data module focus on securing susceptible information by converting it into an illegible format before transmission. This ensure that even if unauthorized entrée occurs during data transmission or storage, the information remains confidential. Encryption algorithms and keys cooperate a crucial role in safeguarding the integrity and confidentiality of the data.

2. Cloud Storage

The Cloud Storage module involves the secure storage of data in cloud repositories. Cloud service providers (CSPs) host and handle these repositories, present scalable and reliable storage solutions. The module ensures that encrypted data is stored securely, preventing unauthorized access and given that users with a flexible and accessible storage environment.

3. Data Transmission

Data Transmission involves the secure transfer of information between the user and the cloud storage system. This module ensures the confidentiality and integrity of the data during transit. By incorporating encryption and secure communication protocols, the data transmission module minimizes the risk of interception or tampering during the exchange of information**.**

4. Third-Party Auditor

The Third-Party Auditor (TPA) module introduce an external entity responsible for validating and managing the security of the cloud-stored data. The TPA conducts thorough audits and verifications to ensure that the data complies with security standards. This adds an additional layer of assurance for users and helps prevent potential security breaches by providing an independent assessment.

5. User Authentication

User Authentication is a essential module that verifies the identity of users attempting to access the cloud-stored data. This process ensures that only authorized persons can recover or modify the information. User authentication methods may include passwords, multi-factor authentication, or biometric verification, enhancing the on the whole security of the system.

6. Verification and Decryption

The Verification and Decryption module comes into cooperate when a user requests access to the stored data. The user undergoes a verification process facilitate by the TPA to confirm their authority. Once authenticated, the data is decrypted

using the appropriate keys, allowing the user to access the original, impassive information. That only authorized users can retrieve and decrypt the stored data ensures in this module.

VI. CONCLUSIONS

This project describes the cloud data secure storage systems a feasible approach to solve the storage security problem, especially prevention from user data leakage at cloud storage layer. CSSM could also effectively protect cryptographic materials from storage perspective with improved data security. We can achieve the better cloud storage management protocol is implemented in this system for best cloud storage management. This proposed algorithm provide the better integrity of data storage management. CSSM adopted a combined approach of data dispersal and encryption technologies, which can improve the data security and prevent attackers from stealing user data. The experimental results show that CSSM can effectively prevent user data leakage at cloud storage layer. In terms of performance, the increased time overhead of CSSM is acceptable to users. This paper provides a feasible approach to solve the storage security problem, especially prevention from user data leakage at cloud storage layer. CSSM could also effectively protect cryptographic materials from storage perspective.

REFERENCES

[1] B. AlBelooshi, K. Salah, T. Martin, and E. Damiani, ‘‘Securing cryptographic keys in the IaaS cloud model,’’ in Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Compute. (UCC), Limassol, Cyprus, Dec. 2015, pp. 397–401.

[2] C.-Z. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, ‘‘Privacy-preserving naive bayes classifiers secure against the substitution-then-comparison attack,’’ Inf. Sci., vol. 444, pp. 72–88, May 2018.

[3] F. Guo, X. Huang, K. Liang, JK. Liu, “Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data “, IEEE Transactions, JAN 2016.

[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, ‘‘Secure attribute-based data sharing for resource-limited users in cloud computing,’’ Compute. Secure., vol. 72, pp. 1–12, Jan. 2018.

[5] J. Shao, R. Lu, and X. Lin, ‘‘Fine-grained data sharing in cloud computing for mobile devices,’’ in Proc. IEEE Conf. Compute. Common. (INFOCOM), Hong Kong, Apr. 2015, pp. 2677–2685.

[6] J. Zhou, H. Duan, K. Liang, Q. Yan, F. Chen, F. R. Yu, J. Wu, and J. Chen, ‘‘Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation,’’ Compute. J., vol. 60, no. 8, pp. 1210–1222, Feb. 2017.

[7] K.R. Ramesh Babu and K. P. Madhu, “Intelligent secure storage mechanism for big data”,Vol.18, pp. 246-261, 2021.

[8] Malik Mustafa , Marwan Alshare, Deepshikha Bhargava , Rahul Neware , Balbir Singh, and Peter Ngulube, “Perceived security risk based on moderating factors for block chain technology applications in cloud storage to achieve secure healthcare systems”, Jan 2022.

