IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Privacy Preservation and Data Leakage Detection in Cloud Computing

Dr. B.S Borkar[1], Ms. Neha Pawar[2], Ms. Rohini Nagare[3], Mr. Mayur Gosavi[4], Mr. Mahesh Gophane[5]
Professor, Department of IT, Amrutvahini College of Engineering, College, Maharashtra, India[1]
Student, Department of IT, Amrutvahini College of Engineering, College, Maharashtra, India[2,3,4,5]

Abstract: *With vast growing internet as giant, data through these nets needs to be private and secured. Cloud Servers act as major resource to store data. Thus, Cloud server need to be secured and cannot be exposed to the possibility of being misused for disclosure or theft by hackers. For this they need strategic schemes to ensure the security and privacy check of the data. The system proposed utilizes three schemes to ensure security of data. The schemes are encryption of data, distributing of data over multiple clouds and giving authenticity to share data through secret key only. First, system is designed for sharing of data through secure channel of encryption wherein Lightweight algorithm is used for encryption of data, then data is distributed over different clusters with help of DROP algorithm and data is replicated over clouds to contain any loss. Third only private key can give access to different segments of data to explicit people who need to know the information. Trapdoor is generated to detect any unethical request to share data, request is blocked and identity of the person is pursued for any data leakage.*

Keywords: Energy Efficient Algorithm; Manets; Total Transmission Energy; Maximum Number of Hops; Network Lifetime.

I. INTRODUCTION

Data is the main source of information, knowledge, and eventually the wisdom for correct decisions and actions. It might be helping to cure a disease, boost a company's revenue, make a building more efficient or be responsible for achieving the targets, and improving the performance. Furthermore, storage, analysis, and sharing of data are the essential services required by any organization to upgrade its performance. However, with the explosive evolution of data, enormous pressure emerges on the enterprises for storing the voluminous data locally. Also, it has become difficult to explore the data due to limited resources. Most businesses have shifted to the cloud for these services due to its several advantages such as on-demand service, scalability, reliability, elasticity, measured services, disaster recovery, accessibility, and many others.

Cloud computing is a paradigm that enables big reminiscence area and huge computation ability at a low fee. It allows user to get the services from multiple platform which are irrespective of location and time. For better cost saving and to enhanced productivity for project management is achieved by migrating local data management system into the cloud storage and by cloud-based services. Therefore, individuals and organizations are shifting increasingly to the cloud for their multiple services [8]. With the growing expansion of cloud computing technologies, it is not difficult to imagine that almost all the businesses will be switched to the cloud in the foreseeable future.

Cloud computing enables collaboration, verbal exchange, and essential online services for the duration of the COVID-19 crisis. Scientific collaborations executing such experiments have numerous wishes and undertake exceptional methods in developing the computing frameworks. Large facts may additionally exist in a big number of small documents, so substantial characteristic of the cloud facts warehouse is to ensure of the safety of confidential records that may be carried out via techniques of steganography and cryptography. There are troubles of security such as information loss, integrity, and botnet posing extreme threats to agencies' records and software. Security of sensitive records is a urgent want in cutting-edge communication, especially in cloud. Every day, the range of humans using cloud computing offerings increases, and masses of data had been stored in cloud computing environments. Cloud computing has giant benefits that consist of remote garage, mobility, information sharing, price financial savings in hardware and software program, and many others.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Facts leakage to cloud services is also increasing every year due to attackers who are constantly seeking to take advantage of the safety vulnerabilities of cloud. Engineers and researchers try to discover the feasible cloud threats and attacks to be able to implement better safety mechanisms to defend touchy statistics and cloud computing environments. These days, many facts cozy models over the cloud computing have been proposed. Transferring programs to the cloud and having access to the blessings is a manner of first evaluating unique records safety troubles and cloud protection troubles. When businesses circulate packages from on-premise to cloud-primarily based ones, traumatic conditions upward thrust up from facts residency, organization compliance requirements, and privacy and 1/3-celebration party responsibilities regarding the remedy of touchy statistics.

One component authentication is vulnerable to password guessing because of the fact that humans do now not regularly extrude their password. Therefore, protection of the cloud computing is important inside the cutting-edge-day world. Universal, art work offer enhancing protection for cloud computing, in addition to protection and protection for entire cloud-based computing shape. Open records sharing with others is viable with cloud.

II. RELATED WORK

Kao et al. [1] presented management scheme which named uCloud which is user-centric to protect the cloud. In uCloud, users' data indirectly encrypted by RSA by utilizing users' public keys. The private key of the user is stored on user's mobile device instead of users PCs. The two-dimensional (2D) barcode image used to express the private key of users and also further used for the decryption of data the users.

Al-Haj et al. [2] provided the two crypto-based algorithms to provide confidentiality, integrity, and authenticity to the data. The cryptographic function is introduced by using the hash code and to protect data symmetric key is there. The elliptic curve digital signature algorithm is applied for integrity and authenticity purpose. The Galois counter mode which is of advanced encryption standard is used with whirlpool hash function for the purpose authentication and confidentiality.

Liang et al. suggested a Attribute-Based Proxy Re-Encryption for secure sharing of cloud data [3]. An enhancement of re-encryption and re-encryption key generation phases is introduced by which we minimized the communication and better computational cost. A data owner is the authorized person in the scheme to which can give the rights of the encrypted data which is stored on a cloud system to others. Wang et al. Proposed report hierarchy attribute-primarily based encryption scheme [4] for securing the statistics within the cloud environment. The access structured layered model in used in this scheme to unravel issues of sharing hierarchical files.

Liu et al. [5] proposed a secure data access control scheme for cloud storage. The fair key reconstruction is performed in this scheme to resist the shared data access and no one can exchange theirs shares. A large number of fake keys are generated in the proposed scheme for obfuscating the decryption key of the shared data. The performance evaluation demonstrated that the communication costs are reduced and computational delay, but authentication is not efficient in this scheme.

Liu et al. proposed CP-ABBE scheme [6] to reduce the computation cost of heavy decryption at the user end which increases with respect to the complexity of access policy. This system facilitated revocation attributes, decryption outsourcing and policy updating while the user attributes are changed.

Li et al. [7] proposed a scheme for mobile cloud computing and name of that scheme is lightweight data sharing scheme (LDSS). LDSS enhanced the structure of the access control tree by adopting the scheme CP-ABE to stimulate the mechanism applicable for mobile cloud environments. A huge part of the computation is displaced to outside proxy servers from cell gadgets on this scheme. Zaghloul et al. Proposed a Privilege-primarily based Multilevel Organizational records-sharing (P-MOD) scheme in [8]. In P-MOD, by incorporating a privilege-based access structure the attribute-base encryption mechanism is get strengthened to operate the management of big data sets effectively.

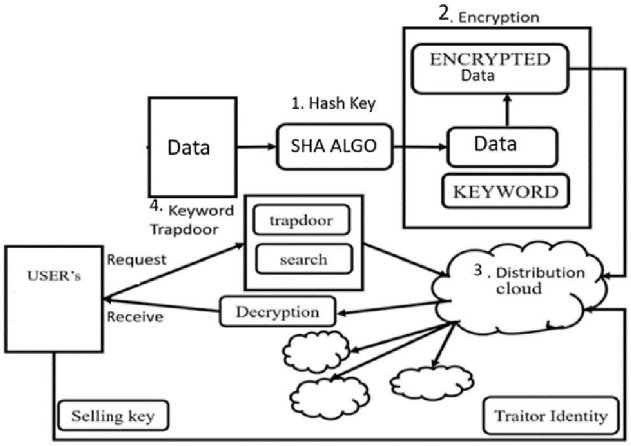
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Li et al. [9] presented a Linear Secret Sharing Scheme (LSSS) matrix access structure based an effectual CP-ABE scheme to update the file dynamically and improve the efficiency of the policy in the cloud environment. The goal of the scheme is to withstand the selected plaintext attacks (CPA), and reduce the storage consumption of the proxy cloud provider employer (PCSP), the communication fee, and the computing value of the information proprietor. The theoretical evaluation and experimental simulation of the proposed scheme confirmed that it has outperformed policy update CP-ABE in phrases of effective coping with of the coverage adjustments and report updates node.

III. PROPOSED SYSTEM

A) System Design

1. The system utilizes three techniques to ensure security of data.
2. The techniques are encryption of data, distributing of data over multiple clouds and giving authenticity to share data through secret key only.
3. First, system is designed for sharing of data through secure channel of encryption with hash key wherein AES algorithm is used for encryption of data.
4. Then the data is distributed over different clusters with the help of DROPS algorithm and data is replicated over clouds to avoid any loss.
5. If the User wants to access the data, he needs authorization using private key.
6. The private key can give access to different segments of data to explicit people who need to know the information.
7. Trapdoor is generated to detect any unethical request to share data, request is blocked and identity of the person is pursued for any data leakage.



B) Modules

1. Owner

Data is collected and then aggregated. The aggregated data isthen transmitted via a wireless interface, such as Bluetooth or WLAN. First, the record is scanned to extract the relevant keyword. Then, a specific access policy is determined, and the keyword along with the corresponding file are encrypted into a cipher text.

2. Data User

In this scenario, there are multiple users in a network, each with their own set of attributes including affiliation, department, and type of staff. These users are authorized to search for encrypted files based on their specific attributes. To conduct the search operation, the data users utilize resource-limited terminals to generate secret keys. These keys are then sent to the public cloud via a wireless channel, where the encrypted files are retrieved and returned. Finally, the data users decrypt the PHR files and verify the correctness of the decryption.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

3. Public Cloud

The proposed system utilizes a public cloud that has almost unlimited storage and computing power. This allows the cloud to handle the task of remote storage as well as respond to data retrieval requests. To improve performance, a lightweight test algorithm is designed and implemented in the system.

4. Key Generation Center(KGC)

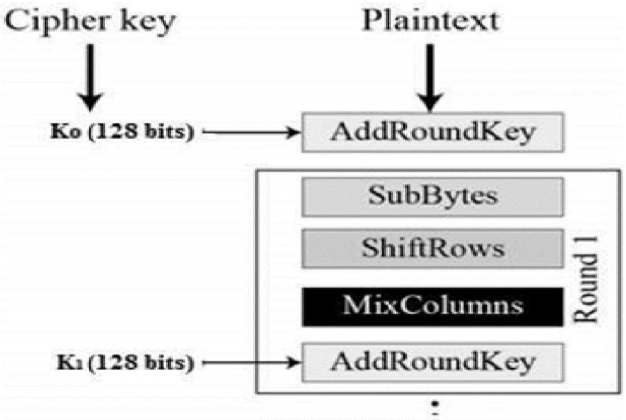
In this system, the Key Generation Center (KGC) is responsible for generating public parameters for the entire system and distributing secret keys to data users. Each data user's set of attributes is embedded in their secret key, allowing for access control. In the event that a user sells their secret key for financial gain, the KGC is able to trace the identity of the malicious user and revoke their secret key.

IV. ALGORITHM

Algorithm 1: Advanced Encryption Standard (AES)

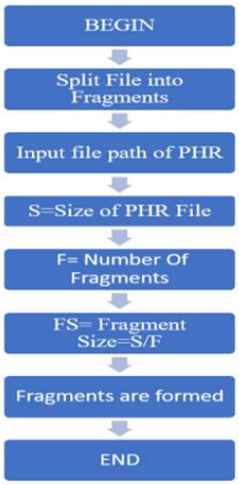
AES algorithm helps to encrypt the PHR. The algorithm uses 10 or 14 rounds for encryption with given key depending on 128 bytes or 256 bytes respectively. Each Round consist of 4 steps which includes SubByte where one each byte is substituted with another byte. The next is row shifting where whole row is shifted.

The next is mix column where columns are mixed and the last one is adding round key. One round is shown in Fig.



Algorithm 2: Data in the Cloud for Optimal Performance and Security (DROPS)

Drops Algorithm is used for the distributing of PHR data over multiple clouds. The uploaded file is divided in the number of fragments and replicated over number of clouds. The flow for division of file into the number of fragments is shown in below fig.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

V. EXPERIMENTAL RESULTS

Fig. 1 User Registration

Fig. 2 Login Page

Fig .3 OTP Verification

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

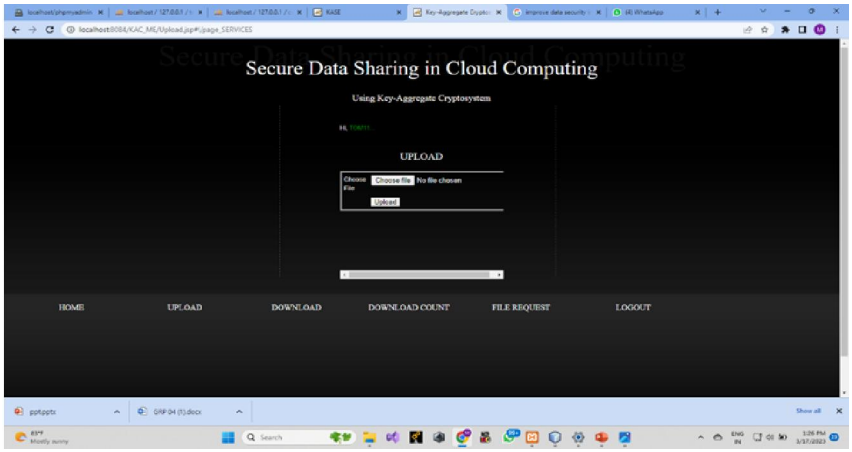


Fig. 4 File Upload

VI. CONCLUSION AND FUTURE WORK

Data protection is a challenging task in the field of cloud computing and information security. It is investigated that no technique alone is efficient in ensuring the absolute security of the data from every directly or indirectly engaged party in the system. The robust solution can be developed by integrating the techniques for providing complete security to the system in the sharing environment. Moreover, with the set of highlights of addressed remarkable solutions, it is deemed that the exposed analysis will act as a milestone for the potential researchers working in the area as well as other emerging applications demanding secure data storage and sharing for its protection.

REFERENCES

[1] Y. Kao, K. Huang, H. Gu and S. Yuan, "UCloud: A user-centric key management scheme for cloud data protection", IET Inf. Secur., vol. 7, no. 2, pp. 144-154, Jun. 2013.
[2] A. Al-Haj, G. Abandah and N. Hussein, "Crypto-based algorithms for secured medical image transmission", IET Inf. Secur., vol. 9, no. 6, pp. 365-373, Nov. 2015.
[3] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, et al., "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing", Future Generat. Comput. Syst., vol. 52, pp. 95-108, Nov. 2015.
[4] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing", IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.
[5] H. Liu, X. Li, M. Xu, R. Mo and J. Ma, "A fair data access control towards rational users in cloud storage", Inf. Sci., vol. 418, pp. 258-271, Dec. 2017.
[6] Z. Liu, Z. L. Jiang, X. Wang and S. M. Yiu, "Practical attribute-based encryption: Outsourcing decryption attribute revocation and policy updating", J. Network. Computer. Appl., vol. 108, pp. 112-123, Apr. 2018.
[7] R. Li, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing", IEEE Trans. Cloud Computer., vol. 6, no. 2, pp. 344-357, Apr. 2018.
[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, et al., "An efficient attribute-based encryption scheme with policy update and file update in cloud computing", IEEE Trans. Ind. Information., vol. 15, no. 12, pp. 6500-6509, Dec. 2019