IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

Integrating Multi-Cloud to Establish Cloud Security for Secured Cloud Transaction

Dr. Samydurai A[1], Achuthan R[2], Akash K[3], Eber Sheckel E[4]
Professor, Department of Computer Science and Engineering[1]
UG Scholar, Department of Computer Science and Engineering[2,3,4]
SRM Valliammai Engineering College, Chengalpattu, Tamil Nadu, India

Abstract: *Nowadays every possible transaction is occurring online so for all these transactions required security must be provided. It is not easy to produce such security since there will be a huge amount of data involved here as well as stored data must be kept confidential so to achieve these things we need to perform transactions through the cloud. Since technology has been developed the rate of the cloud being attacked is also increased so to prevent this integration two clouds must be used. The existing system does not apply cloud integration instead of that they use only data encryption for secure transactions. In the Proposed system of the project apart from data encryption cloud integration is also gets implemented here to establish transactions more securely. In this proposed system, we implement three levels of security which are low, medium, and high. Here We use only data encryption for low security level and in medium security level splitting of data occur along with data encryption to establish more secure transaction than low security level. Finally in order to produce a higher security level we use both cloud integration and splitting of data along with data encryption to produce transactions more securely than medium security level.*

Keywords: Three Levels of Security, Cloud Integration, and Data Encryption

I. INTRODUCTION

Cloud Security is the set of various methods and strategies to implement a mechanism that helps to protect the data in terms of not allowing any third parties to perform any modification in data as well as to provide data confidentiality. Day-to-day technology has been increasing faster so all the transactions including documents, payments, and other sensitive information, etc in various fields like education, finance, and health care are done online. The major risk in doing these transactions online is the interference of third parties who may be hackers or any person who manages to steal the data which includes payment details, user pieces of information, etc. This proposed system applies the integration of the two clouds to make it difficult for the hacker or any person who wants to perform any malicious activities in a cloud environment.

1.1. System Overview

This project aims to safeguard the user's data from any attacker by providing a secure cloud transaction through the integration of multiple clouds. This project provides more efficiency in providing a well-protected cloud environment for the users to use for transactions. This project uses the integration of multiple clouds the attacker may find it difficult to perform any malicious activities which may be data accessing and data modifications etc.

II. LITERATURE SURVEY

Qian Wang & et.al.(2020)[1]: Storage services allow data owners to store their huge amount of potentially sensitive data, such as audio, images, and videos, on remote cloud servers in encrypted form. To enable retrieval of encrypted files of interest, searchable symmetric encryption (SSE) schemes have been proposed. However, many schemes construct indexes based on keyword-file pairs and focus on Boolean expressions of exact keyword matches. Moreover, most dynamic SSE schemes cannot achieve forward privacy and reveal unnecessary information when updating the encrypted databases. We tackle the challenge of supporting large-scale similarity search over encrypted feature-rich multimedia data, by considering the search criteria as a high-dimensional feature vector instead of a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

keyword. Our solutions are built on carefully-designed fuzzy Bloom filters which utilize locality-sensitive hashing (LSH) to encode an index associating the file identifiers and feature vectors. Thus, The paper speaks only about the Data Retrieval system using Indexing methods via Bloom Filter. There is no Multi-User data Retrieval and Multi- Cloud Deployment

Yuan Li & et.al., (2021). [2] : With the widespread application of cloud computing technology, data privacy security problem becomes more serious. Recent studies related to searchable encryption (SE) areas have shown that data owners can share their private data with efficient search functions and high-strength security. However, the search method has yet to be perfected, compared with the plaintext search mechanism. In this paper, based LSSS matrix, we give a new searchable algorithm, which is suitable for many search methods, such as exact search, Boolean search, and range search. In order to improve the search efficiency, the 0, 1-coding theory is introduced in the process of ciphertext search. Meanwhile, it is shown that a multi-search mechanism can improve the efficiency of data sharing. Finally, the performance analysis is presented, which proves our scheme is secure, efficient, and human- friendly. Thus, The paper deals with the Best search algorithm and Multi-user search mechanism using ABE. There is no Multi-User data Retrieval and Multi-Cloud Deployment. There is no Security implemented apart from Encryption

Zheng Qin & et.al.,(2021). [3]**:** With the proliferation of cloud computing, data owners can outsource the spatial data from the Internet of Things devices to a cloud server to enjoy the pay-as-you-go storage resources and location- based services. However, the outsourced services may raise privacy concerns, since the cloud server may not be fully trusted by both data owners and search users. If the data owners and search users conventionally encrypt the spatial data and query requests, the efficiency and functionality of query processing are weakened. Most of the existing works only focus on spatial data search or keyword search and do not consider spatial keyword search over encrypted data. Thus, The paper deals with spatial keyword-based search with User defined access control. There is no Multi-User data Retrieval and Multi-Cloud Deployment. There is no Security implemented apart from Encryption

Yinbin Miao & et.al.,(2019). [4]**:** Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) schemes support both fine-grained access control and keyword-based ciphertext retrieval, which make these schemes attractive for resource-constrained users (i.e., mobile or wearable devices, sensor nodes, etc.) to store, share and search encrypted data in the public cloud. However, ciphertext length and decryption overhead in the existing CP-ABKS schemes grow with the complexity of access policies or the number of data users' attributes. Moreover, such schemes generally do not consider the practical multi-owner setting (e.g., each file needs to be signed by multiple data owners before being uploaded to the cloud server) or prevent malicious cloud servers from returning incorrect search results. To overcome these limitations, in this paper we first design an optimized Verifiable Fine-grained Keyword Search scheme in the static Multi-owner setting (termed as basic VFKSM), which achieves short ciphertext length, fast ciphertext transformation, accelerated search process, and authentic search result verification. Thus, The paper deals with effective data Retrieval using an optimized Verifiable Fine-grained Keyword Search scheme in the static Multi- owner setting. There is no Multi-User data Retrieval and Multi-Cloud Deployment. There is no Security implemented apart from Encryption

III. METHODOLOGY

The proposed system contains six modules that help to perform cloud integration to done transactions securely in the cloud environment. The behaviour and interaction of the above-mentioned modules are represented in the following figures.

3.1 User Interface

This module helps the user to interact with the system by displaying the dialog box for various activities that are done like user registrations, user login, file operations, and cloud connections, etc. With this module, users can know about any discrepancies occurring during each operation by proving a warning pop-up message. This module gets connected to the SQL server to maintain the records of all the registered users for authentication purposes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

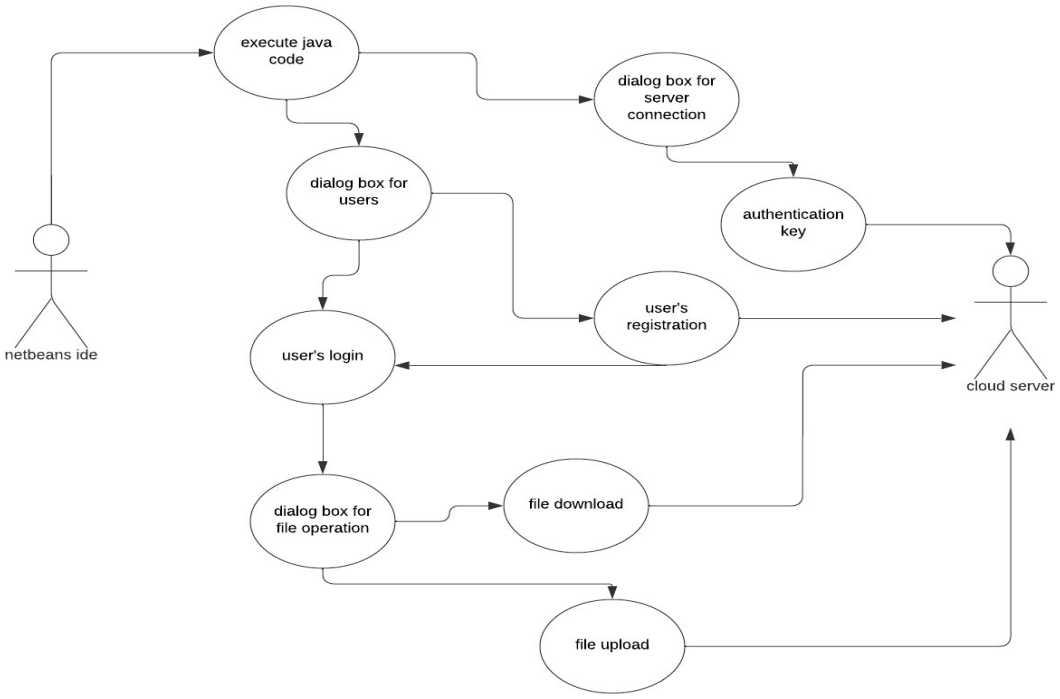

Fig. 1. User Interface

3.2 Cloud Server

In this module, Admin will use the newly generated access token to connect with Dropbox and use the authentication key to connect with google drive to perform any file operations like uploading and downloading the file, etc. After the successful connection of Dropbox and google d, rive this system can able to perform at both higher and medium security levels.

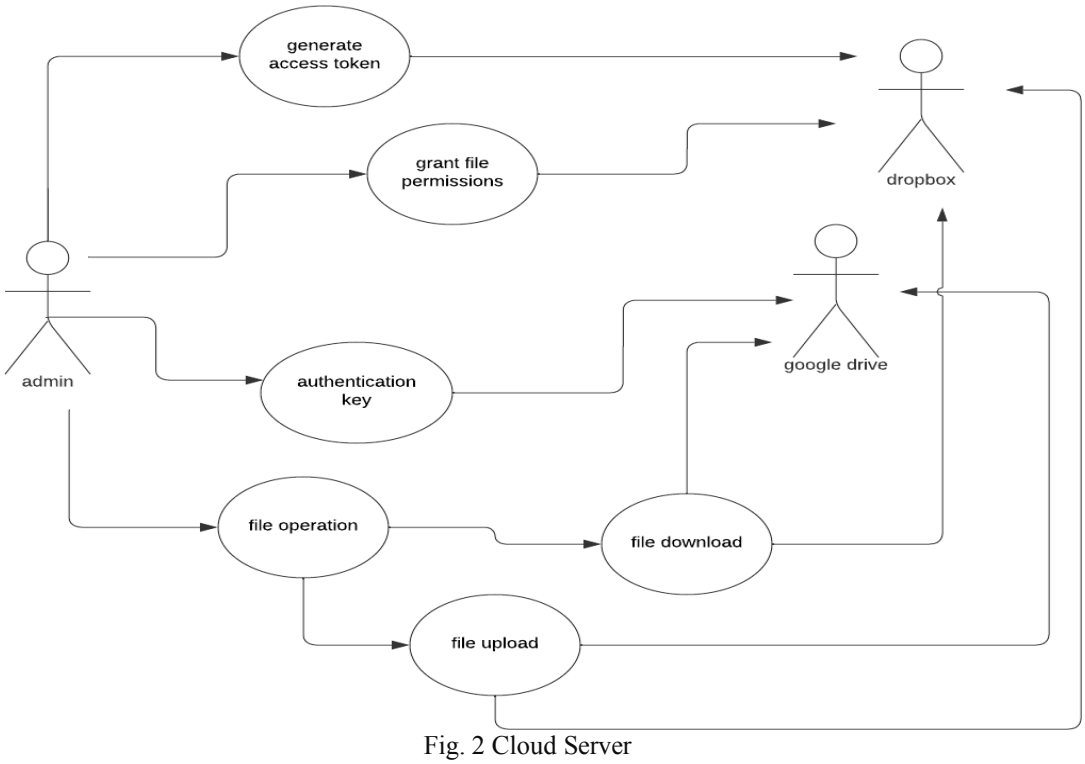

Fig. 2 Cloud Server

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

3.3 Data Encryption

In this module, the admin will upload the data and according to the user's profile, the level of security gets determined to perform data encryption. Thus if the security level has been determined as high and medium then data gets encrypted into byte format Still, if a low security level gets determined then a normal encryption process takes place.

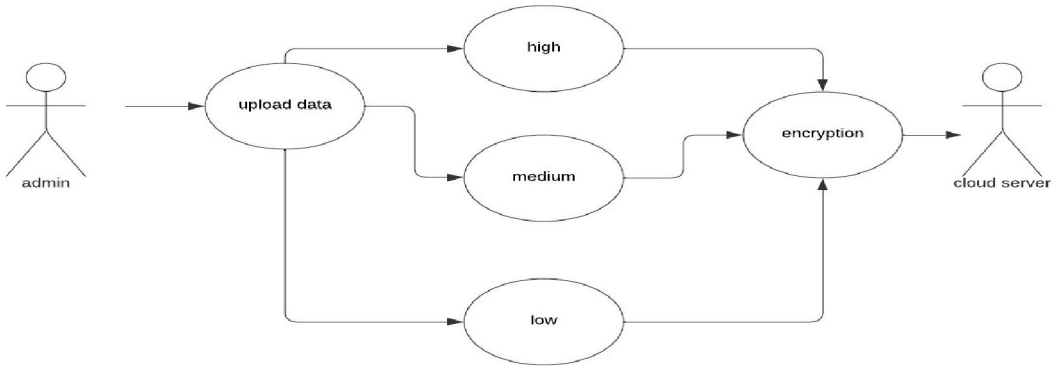

Fig. 3. Data Encryption

3.4 High Secure

In this module, The admin will upload the data and according to the user's profile if a higher security level gets determined then the data gets encrypted into byte format. Then the data chunking process occurs to divide this encrypted data into four types where two of them will be stored in Dropbox and the other two will be stored in google drive. Finally For the decryption process, all the divided data from Dropbox and google drive gets reconstructed into original encrypted data then this data gets decrypted to give the initially uploaded data to the respective user

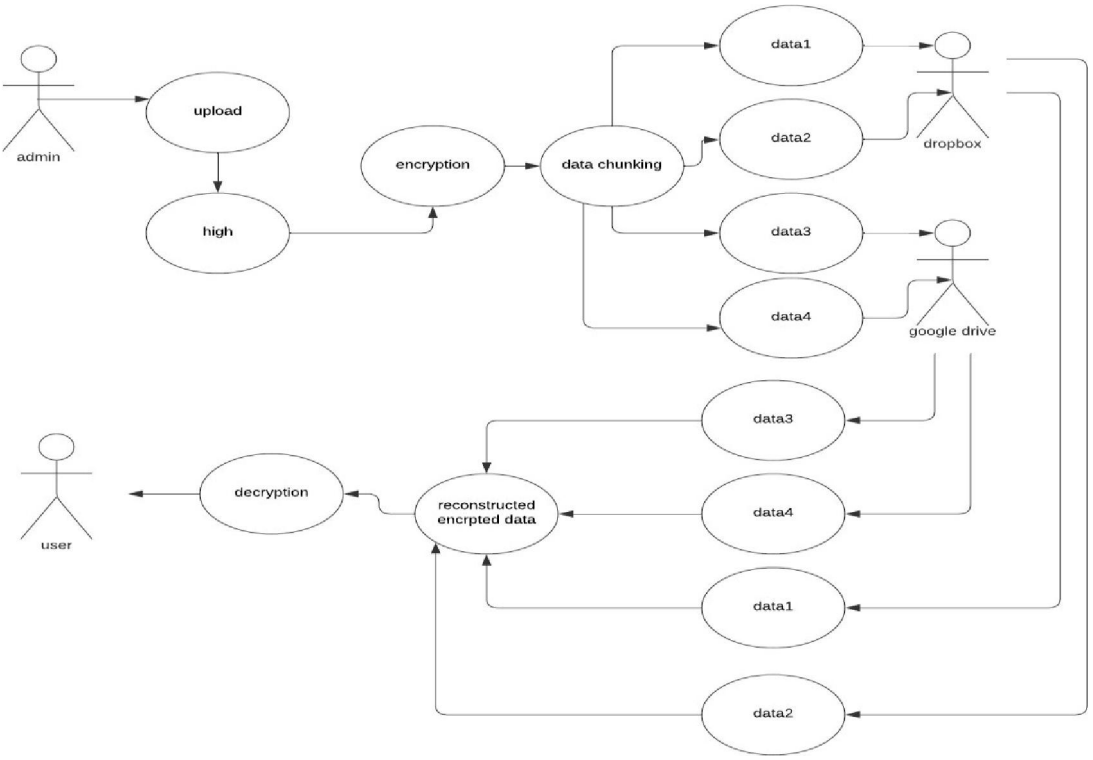

Fig.4. High Secure

3.5 Medium Secure

In this module, The admin will upload the data and according to the user's profile if a medium security level gets determined then the data gets encrypted into byte format. Then the data chunking process occurs using the Merkle hash algorithm to divide this encrypted data into four types where all of which will be stored in Dropbox. Finally, For the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

decryption process, all the divided data from Dropbox gets reconstructed into original encrypted data then this data gets decrypted to give the initially uploaded data to the respective user

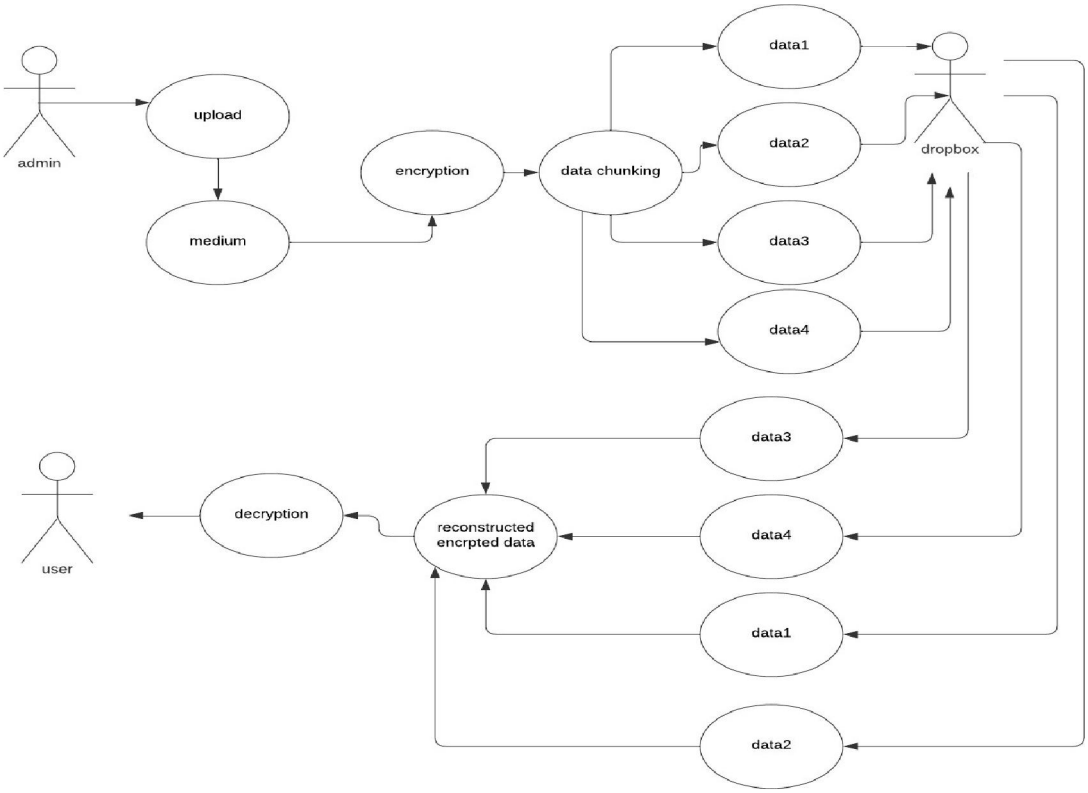

Fig.5. Medium Secure

3.6 Low Secure

In this module, The admin will upload the data according to the user's profile if a low security level gets determined then the uploaded data gets encrypted and will be stored in Dropbox which is used as a cloud service in this security level. Finally, for the decryption process, the encrypted data gets decrypted to give the initially uploaded data to the respective user

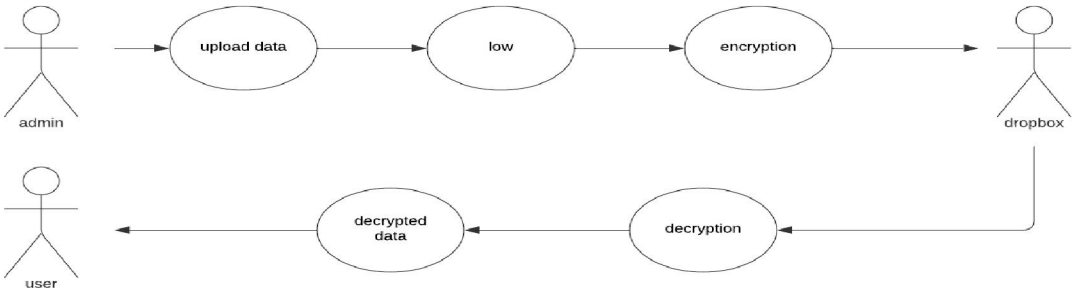

Fig.6. Low Secure

IV. EXISTING SYSTEM

The existing system uses only data encryption for the secure transaction so the attacker may be able to steal or gather information about any transaction that is made through the cloud environment. This system mostly focuses on keeping the confidentiality of the data using the keys which help to perform both encryption and decryption. The security mechanism that is used in this system is not able to compete with the attackers who are using advanced technology to perform any malicious activities. Thus this system has low efficiency in terms of protecting the user's sensitive information during the transactions that are performed in the cloud environment.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

V. PROPOSED SYSTEM

The proposed system helps to integrate two clouds to produce various levels of security such as medium and high to establish transactions securely. This system performs the data encryption using the AES algorithm to convert the data into byte format and then perform data chunking to divide the byte-formatted data into four types to maintain the data confidentiality of the users. The higher security in this system is produced by performing This proposed system also helps to maintain the information of the registered user using SQL Thus, this system focuses not only on cloud integration but also on data encryption and data chunking to make it difficult for the attackers to perform any malicious activities during the transaction.

VI. IMPLEMENTATION

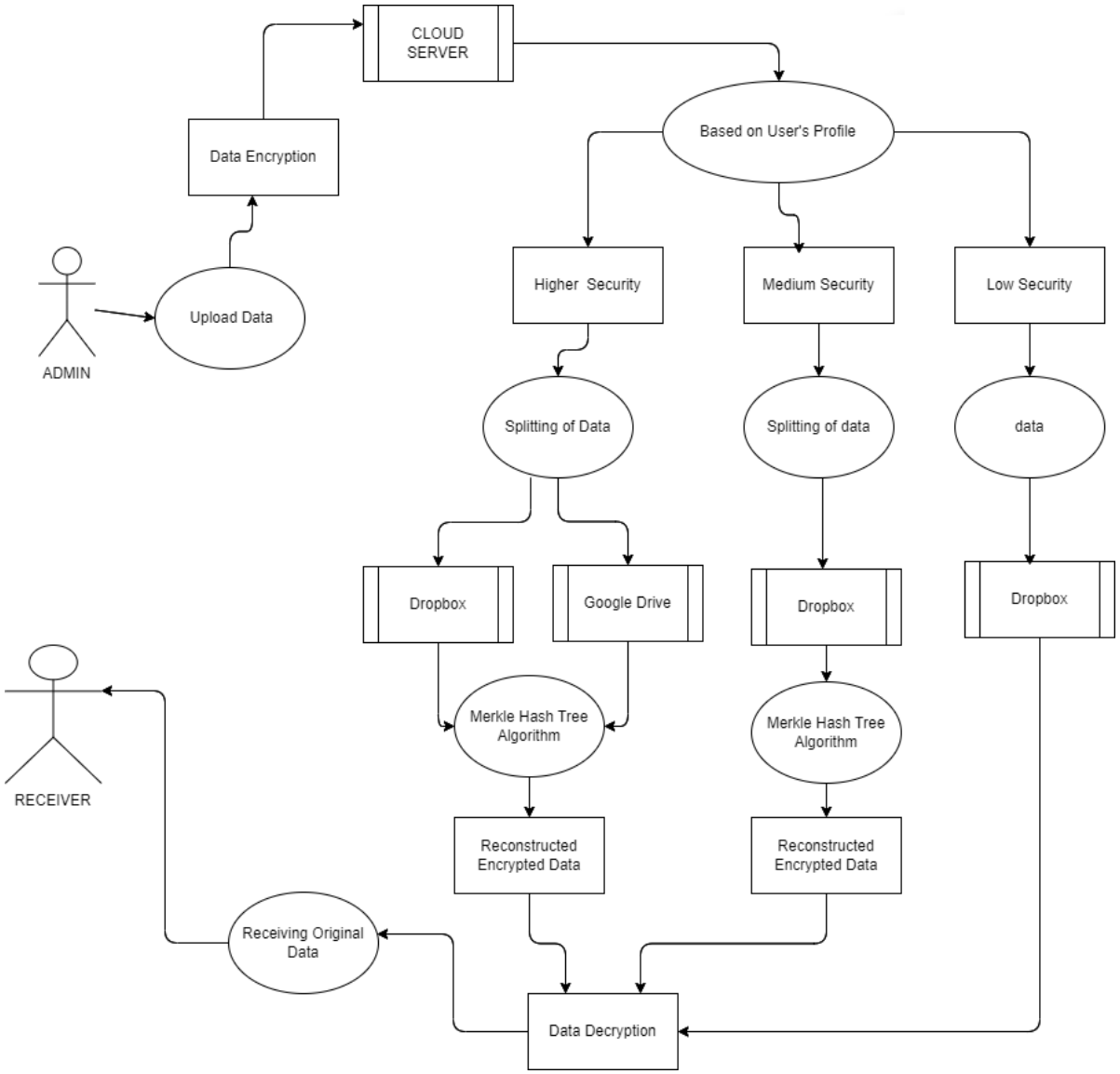

Fig 7. The Architecture Diagram for secured transaction using cloud integration

6.1 Data Encryption

At first, the admin will upload the data and the data gets encrypted using the AES(Advanced Encrypted Standard) Algorithm which will be stored in the cloud server After the encryption process, the user's profile which was given to the server by the user during the registration process will be analyzed to determine the level of security to be maintained to protect their data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

6.2 Three Levels of Security

If the user's profile has been classified as high profile, then a higher security level gets maintained where data gets split into two parts and each part gets stored in each cloud. If the user's profile has been classified as medium profile then medium security level gets maintained where data gets split into two parts and then both of the parts get stored in the same cloud. If the user's profile has been classified as low profile then a low-security level gets maintained where data just gets encrypted and stored in the cloud

6.3 Data Decryption

After the work is done by three security levels, the split data gets combined and reconstructed into the encrypted data by using the Merkle hash tree algorithm which will be the case for both higher and medium-level security. Then all the encrypted data from higher, medium, and low-security levels gets decrypted by using the key given to the respective receiver. Finally, the receiver will receive its transaction more securely without any interference from any unknown third parties who may be the hacker trying to gather this sensitive information for their purpose.

VII. CONCLUSION

Thus, the proposed system fulfills its main objective to improve the security for the various transactions that are done online by using the integration of the clouds. This system also helps to prevent any hacker or attacker from stealing the information of the transactions that are done in the cloud environment by enabling different levels of security like high, medium, and low according to the user profile and its priority level. Thus this system plays a vital role in maintaining the privacy of the data by not disclosing any important information involved during transactions to third parties except the required person which makes all the transactions that include documents in the form of the text file and images etc more secure than ever.

7.1 Future Scope

This system has a very high potential for future modifications and improvements. In the future, this system can be used to provide security for not only transactions related to documents but also for transactions involving money since there are lots of malicious activities occurring during any payment transaction which lead to huge losses in the user's money. This system uses data encryption along with data chunking to be able to provide even more security for transactions where money is involved. Thus by using this system users can tend to transfer amounts to any respective persons without any discrepancies occurring during transactions.

REFERENCES

[1]. P. Institute, "Sixth annual benchmark study on privacy and security of healthcare data," tech. rep., Ponemon Institute LLC, 2016.
[2]. R. Cohen, "The cloud hits the mainstream: More than half of U.S. businesses now use cloud computing." http://www.forbes.com, April 2013. Online; posted 10-January-2017.
[3]. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.
[4]. A. C. OConnor and R. J. Loomis, "2010 economic analysis of role-based access control," NIST, Gaithersburg, MD, vol. 20899, 2010.
[5]. Elliott and S. Knight, "Role explosion: Acknowledging the problem.," in Software Engineering Research and Practice, pp. 349–355, 2010.
[6]. E. Zaghloul, T. Li, and J. Ren, "An attribute-based distributed data sharing scheme," in IEEE Globeocm 2019, (Abu Dhabi, UAE.), 9-13 December 2018.
[7]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy (SP'07), pp. 321–334, IEEE, 2007.
[8]. Qian Wang & et., "Searchable Encryption over Feature-Rich Data," in 2020 IEEE EXPLORE
[9]. Yuan Li & et.al., "Attribute-Based Searchable Encryption Scheme Supporting Efficient Range Search in Cloud Computing," in 2021 IEEE EXPLORE

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

[10]. Zheng Qin & et.al., "Privacy-Preserving Keyword Similarity Search Over Encrypted Spatial Data in Cloud Computing," in 2021 IEEE EXPLORE

[11]. Yinbin Miao & et.al., "Optimized Verifiable Fine-Grained Keyword Search in Dynamic Multi-Owner Settings," in 2020 IEEE EXPLORE

[12]. G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Computers & Security, vol. 30, no. 5, pp. 320–331, 2011.

[13]. 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 Transactions on Information Forensics and Security, vol. 11, no. 6 pp. 1265– 1277, 2016.

[14]. M. Lichman, "UCI machine learning repository," 2013.

[15]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457–473, Springer, 2005.

[16]. D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in Theory of Cryptography Conference, pp. 253–273, Springer, 2011.

[17]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98, Acm, 2006.

[18]. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 456–465, ACM, 2007.