IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Special Issue 1, April 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

A Novel Model for Efficient Sharing and Storage of Data in Cloud Environment

Gunupati Venkateswarlu[1], Prashant Singh[2]

Research Scholar, Department of CSE, Shri Venkateswara University, Gajraula, Uttar Pradesh, India[1]

Research Guide, Department of CSE, Shri Venkateswara University, Gajraula, Uttar Pradesh, India[2]

Professor, Department of Computer Science & Engineering, Sunder Deep Engineering College, Ghaziabad, Uttar Pradesh, India[2]

ABSTRACT: One of the primary usage of cloud computing is data storage. Cloud provides enormous capacity of storage for cloud users. Secure data storage and retrieval of the relevant information from the in traditional as well as in cloud computing environment has always been a significant issue. Moreover, due to the loss of control over the cloud infrastructure, it is essential to demonstrate its security, increasing the trust and efficiency in cloud services. Numerous organizations are adopting cloud services because of the economy and technology changes. Over the past year, cloud computing has made life easier for other people or organizations by allowing people to have access to information from anywhere in the world through the internet. With the rapid growth of data sources, data sharing and security in Cloud is a big challenge. Different issues have ascended in the area of data security such as infrastructure security, data privacy, data management and data integrity. Currently, for sharing, processing, analytics and storage are secured using cryptography algorithms, which are not appropriate for data security over Cloud. Therefore, by this hybrid model (Attribute-Based Encryption (ABE) with Secure Data Sharing (SDS)) data will shared without leakage and stored without any hacking. Hence, a novel model for efficient sharing and storage of data in cloud environment shows better results interms of accuracy, efficiency and security.

KEYWORDS: cloud computing, data sharing, Attribute-Based Encryption (ABE), Secure Data Sharing (SDS), cryptography, Data Security, Cloud Users

I. INTRODUCTION

The cloud computing has revolutionized the information technology as well as business world for last several years. It has inimitable features like round the clock service availability at low cost, rapid elasticity, resilient computing, massive scale, ubiquity etc. The main idea in the cloud is to hiring a service rather owning it. There is a virtual world that provides the service in the cloud environment[1]. The cloud computing provides a model of its services which are managed and controlled by a third party.

The users who share their data over cloud have no control for its transmission and storage. Hence the cloud is an open and heterogeneous environment which makes it vulnerable for data security aspects. And it becomes important concern to develop a trust among cloud users that their data is safe and secure in the cloud [2]. As of now, an effective and efficient security model for cloud at various security levels like network, host, application and data is under research. Among all these cloud security aspects the data security in cloud becomes more important and essential. There is a scope and requirement of a dynamic and optimized data security model for cloud [3].

The term word Cloud Computing has emerged recently and is not is widespread . The several definitions which are available, one of the simplest is, “a network solution for providing inexpensive, reliable, easy and simple access to IT resources” [4]. Cloud Computing is not considered as application oriented but service oriented. This service oriented nature of Cloud Computing not only reduces the overhead of infrastructure and cost of ownership but also provides flexibility and improved performance to the end user [5]. A major concern in adaptation of cloud for data is security and privacy. It is very important for the cloud service to ensure the data integrity,

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data. One of the advantages of Cloud Computing is that data can be shared among various organizations. However, this advantage itself poses a risk to data.

In order to avoid potential risk to the data, it is necessary to protect data repositories. One of the key questions while using cloud for storing data is whether to use a third party cloud service or create an internal organizational cloud[6]. Sometimes, the data is too sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details etc. This type of data can be extremely sensitive and the consequences of exposing this data on a public cloud can be serious. In such cases, it is highly recommended to store data using internal organizational cloud. This method can help in securing data by enforcing on-premises data usage policy. However, it still does not ensure full data security and privacy, since many organizations are not qualified enough to add all layers of protection to the sensitive data[7].

Many organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere. From small to large enterprises affect towards cloud computing to increase their business and tie-ups with other enterprises Security and privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. Cloud computing has given a new dimension to the complete outsourcing arena (SaaS, PaaS and IaaS) and they provide ever cheaper powerful processor with these computing architecture The major thing that a computer does is to store in the available space and retrieve information whenever requested by the authenticated user. As simple solution encrypt the data before uploading it onto the cloud. This approach ensures that the data are not visible to external users and cloud administrators but has the limitation that plain text based searching algorithm are not applicable[8].

Cloud computing arises from the combination of the traditional computer technology and network technology, such as grid computing, distributed computing, parallel computing, utility computing, virtualization [9]. Cloud storage is a system that provides functions such as data storage and business access. It assembles a large number of different types of storage devices through the application software which are based on the functions of the cluster applications, grid techniques, distributed file systems, etc.

Users can use the powerful computing and processing function on clouds and they can order their service from the cloud according to their own needs. Cloud storage is essentially one of the simplest applications of cloud technology available. Google Drive, Microsoft OneDrive, Dropbox; all of these services are cloud storage services. They do one thing and one thing only: they allow you to store data on the cloud [10].

Meanwhile, a company like Google, Microsoft, Amazon, Dropbox, or one of the many other cloud service providers has much, much more money and resources at their disposal. They can provide petabytes of storage for near-trivial amounts of money, with redundancy and backups in case of hardware failure. All you need to do is pay to access it. In cloud storage, the user data stored on the server and storage devices, cloud storage service providers, these storage devices are no longer subject to regulation and control of direct users, equipment failure, administrator disoperation, internal leakage, the server was hacked and other reasons may lead to leakage of user, sensitive and important data loss or damage. On the one hand, users are concerned about the confidentiality of their data cannot be guaranteed. The weak point of confidentiality refers to the intruder cannot obtain the data stored in the cloud of meaningful information, confidentiality strong point refers to even cloud storage service providers are unable to obtain meaningful information of user data. Strong confidentiality is very necessary, because some special data such as the company's commercial secrets, the government's confidential information or other data related to the user's privacy needs to ensure that such strong confidentiality. On the other hand, users also worry about the availability of data, that is, cloud storage service providers can provide timely and correct data access services.

The remaining paper is organised as follows: section II provides a literature survey, section III presents a novel frame for efficient sharing and storage of data in cloud environment; section IV explains result analysis; section V concludes the paper VI references.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

II. LITERATURE SURVEY

D. Seethalakshmi, G. M. Nasira and P. Thangamani, et.al [11] inculcate a Cloud Storage Controller (CSC) that manages the allocation of group of data stored and it can only referenced and cannot download any database from cloud. The data will be blended together into one of two sets for example if two users storing data of 2 megabyte and 3 megabyte each then that will be merged together as two datasets with 1 megabyte of first user and 1 megabyte of second user. In the second data set it merges 1 megabyte of first user and 2 megabyte of second user using Fusing Data Technique (FDT). Every dataset will be bookmarked which symbolizes the user that dataset belongs to and that will be indexed in the Cloud Storage controller (CSC). It helps in fast and highly secured datasets storage management in cloud storage system. It achieves efficient database privacy and revokes user data swiftly and securely.

R. Banerjee, A. K. Chattopadhyay, A. Nag and K. Bose, et.al [12] propose a simple yet effective solution for enforcing the security of private data stored in some cloud storage for sharing. We consider an environment where even if the cloud service provider is not-reliable or is compromised, our data still remain secure. The data Owner encrypts the private files using a secret key, file identifier and hash function and then uploads the cipher text files to the cloud. When a Data user requests access to a file, the owner establishes a key with the user and creates a new key, which is sent to the user. The user can then extract the original key by using the mutually established secret key and use it to decrypt the encrypted file.

C. Jeyanthy, R. S. Shaji and J. P. Jayan, et.al [13] mobile cloud environment is used for storing and assessing data and thus it is needed to have an efficient cloud network that is a framework for communication and data authentication. For storage security it is vital to design a security framework for mobile cloud environment that ensures better storage of data in an encrypted way both in mobile devices and in the storage devices. We are proposing a new security framework for storage of data using the concept of Advance Encryption Standard (AES) that helps the data be much secured and can be used in cloud application.

K. Rani and R. K. Sagar, et.al [14] proposed the concept of cloud data storage security strategy capable to overcome the shortcomings of traditional data protection algorithms and improving security using steganography, encryption decryption techniques, compression and splitting technique adoptable to better security for the cloud. We have developed a desktop application through which user can share data. This paper enhanced advance security goal for cloud data storage.

Nelmiawati and W. Arifandi, et.al [15] Rabin's IDA and Shamir's SSA to implement a tool called dCloud for file protection stored in public cloud storage in a seamless way. It addresses data security by hiding its complexities when targeting ordinary non-technical users. The secret key is automatically generated by dCloud in a secure random way on Rabin's IDA. Shamir's SSA completes the process through dispersing the key into each of Rabin's IDA output files. Besides, the authentication key is used to communicate with all of the defined service providers during storage and reconstruction as well. It is stored into local secure key-store.

Q. Kang *et al*., [16] propose an approach to enable secure data processing on the Cloud with the data from different organizations. The approach consists of a data federation platform for secure data processing on the Cloud named FedCube and a greedy data placement algorithm that creates a plan to store data on the Cloud in order to achieve multiple objectives based on a cost model. The cost model is composed of two objectives, i.e., reducing both monetary cost and execution time. The experiments show that our proposed algorithm significantly reduce the total cost (up to 69.8%).

A. Santosh Pai Raiturkar, S. Fernandes and A. Pai, et.al [17] introduces a trusted third party as a Data Center to activate and deactivate a new user and to reveal the real identity of the user in case of any disputes and also Private Key Generator (PKG) that will responsible in generating the private keys that will be used by the members and Data Center.
L. Huang, G. Zhang and S. Yu, et.al [18] propose a data storage and sharing scheme for CPSS with the help of cloud storage service. Since data integrity assurance is an inevitable problem in cloud storage, we first design a secure and efficient data storage scheme based on the technology of public auditing and bilinear map, which also ensures the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

security of the verification. In order to meet the real-time and reliability requirements of the CPSS, the rewards of timeliness incentive and effectiveness incentive are considered in the scheme. we propose a lightweight access model for users to access the final data processed by cloud server.

Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan and G. Fortino, et.al [19] present an enhanced, secure, and convenient scheme for data access. Besides, in order to add the flexible distribution of data that is controlled by data-owner, our protocol provides proxy re-encryption in which the cloud server utilizes the proxy re-encryption key. Then, the data-owner generates the credential token during decryption for controlling user's accessibility. The security analysis determines that our proposed protocol resists numerous security attacks. Furthermore, performance analysis determines that our protocol has practical computation, communication, and storage costs as compared to various related protocols.

W. B. Chuan, S. Q. Ren, S. L. Keoh and K. M. Mi Aung, et.al [20] propose a secure de-duplication solution for enterprise tenants to leverage the benefits of cloud storage while reducing operation cost and protecting privacy. First, the solution uses a proxy to do flexible group access control which supports secure de-duplication within a group, Second, the solution supports scalable clustering of proxies to support large-scale data access, Third, the solution can be integrated with cloud storage seamlessly. We implemented and tested our solution by integrating it with Drop box. Secure de-duplication in a group is performed at low data transfer latency and small storage overhead as compared to de-duplication on plaintext.

T. E. Trueman and P. Narayanasamy, et.al [21] propose a novel method for ensuring privacy and data freshness of shared data in cloud using Homomorphic authenticable ring signature (HARS) scheme to preserve the user privacy and Overlay tree algorithm is used for ensuring that users the data with required level of freshness. Also Third Party Auditor (TPA) audits the data stored in the cloud. He should be able to verify the trustworthiness of the CSP without disclosing the identity of the users in the group.

B. S. Rawal and S. S. Vivek, et.al [22] a secure file sharing mechanism for the cloud with the Dis-Integration Protocol (DIP). The paper also introduces new contribution of seamless file sharing technique among different clouds without sharing an encryption key. Most of the security tools have a finite rate of failure, and intrusion comes with more complex and sophisticated techniques; the security failure rates are skyrocketing.

Y. Tao, P. Xu and H. Jin, et.al [23] propose a new secure data search and sharing scheme for CECS. Our scheme improves the existing secure CECS scheme in the following two ways. First, it enables users to generate a public-and-private key pair and manage private keys by themselves. In contrast, the existing solution requires edge servers to manage users' private keys. In terms of security, our scheme ensures the confidentiality of cloud data and secure data sharing and searching and avoids a single point of breakthrough. In terms of performance, the experimental results show that our scheme significantly reduces users' computing costs by delegating most of the cryptographic operations to edge servers.

S. J. Nadaf and R. Patil, et.al [24] proposes to build privacy into e-healthcare system with the help of private cloud. Privacy of the stored health data can be achieved by encrypting the data before storing it on cloud server. By doing this we can limit the user access for keyword search. Since one cannot perform plaintext search over encrypted content. But again it is necessary to provide keyword search mechanism to identify the encrypted source file. The salient features of the system are efficient key management, privacy preserving data storage and retrieval.

R. Rabaninejad, S. M. Sedaghat, M. Ahmadian Attari and M. R. Aref, et.al [25] propose an ID-Based public shared data integrity auditing scheme, in which all the group users are able to update, delete or insert new blocks into the shared data. Besides, the cloud server can revoke a misbehaving user with a minimum overhead. The scheme is secure against an untrusted cloud server and also preserves data privacy against the public verifier. Furthermore, overhead analysis shows the efficiency of proposed scheme in comparison to the existing well-known schemes.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

III. FRAMEWORK FOR A NOVEL FRAME FOR EFFICIENT SHARING AND STORAGE OF DATA IN CLOUD ENVIRONMENT

In this section, framework a novel model for efficient sharing and storage of data in cloud environment is observed in Figure 1.

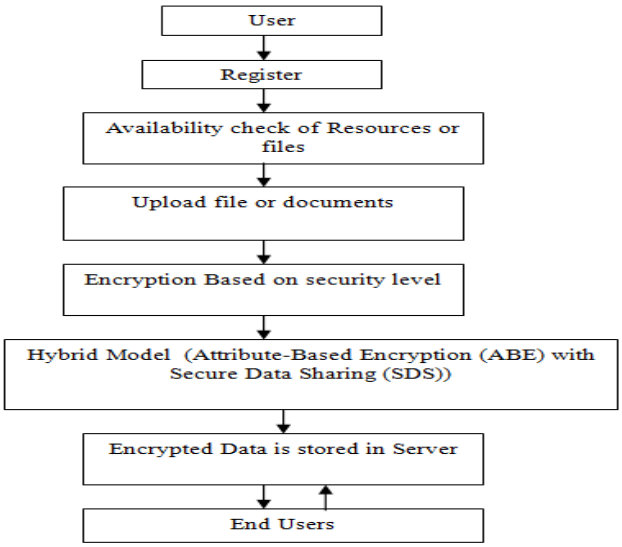

Figure 1: Framework a Novel Model for Efficient Sharing And Storage Of Data In Cloud Environment

Initially, users have to register with user id and password. After registration process, then it will check for availability for storing and sharing of data or files. Then, upload the file or document. After uploading, the data is encrypted based on its priority. Then apply, hybrid model algorithm to the data, finally the encrypted is stored in server with high security even at the time of sharing also it will share to the users who are having correct user id and password. Therefore, by using this algorithm hacking or losing of data will not happen.

A user is a person who utilizes a computer or network service. A user often has a user account and is identified to the system by a username. Some software products provide services to other systems and have no direct end users.

User registration is the process of creating an account or profile for a user on a system or platform. To register, a user usually provides credentials like a username, email address, and password to prove their identity. This process is also known as logging in. Resource availability in cloud computing is the stability and accessibility of resources, like storage and computing power, that are used to provision applications. It's an important aspect of cloud computing because it's critical to have access to the necessary resources and tools to succeed on a project.

Uploading a file or document to a cloud server is the process of transferring data from a local device to a remote server or storage system, usually over the internet. This allows users to share or store digital content, such as documents, images, and videos, with others.

Encryption is a form of data security in which information is converted to ciphertext. Only authorized people who have the key can decipher the code and access the original plaintext information. In even simpler terms, encryption is a way to render data unreadable to an unauthorized party. Attribute-based encryption (ABE) is a cryptographic technique that uses attributes to encrypt data and control access to it. ABE is a type of public key encryption that's well suited for cloud-based applications that require one-to-many encryption.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

The sharing of data securely in cloud computing is a very crucial method. The information is stored in cloud data centers. To access data from or store data into data centers through the internet, the intruders may attack our data.

Cloud encryption is a data security process in which plaintext data is encoded into unreadable ciphertext to help keep it secure in or between cloud environments. It is one of the most effective ways to uphold data privacy as well as protect cloud data in transit or at rest against cyberattacks.

IV. RESULT ANALYSIS

In this section, result analysis of a novel model for efficient sharing and storage of data in cloud environment is observed. In Table.1, performance comparison is observed between Dis-Integration Protocol (DIP) and hybrid model. The comparison parameters are interms of accuracy, efficiency and security.

Table.1: Performance Comparison

Parameters	Dis-Integration Protocol (DIP)	Hybrid Model
Accuracy	85.3	91.6
Efficiency	90.8	95.7
Security	79.1	93.4

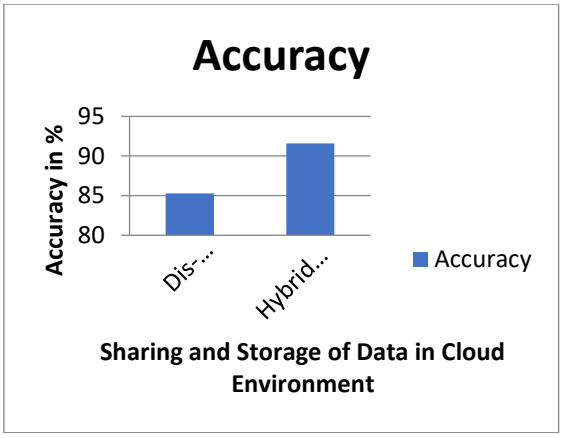

Figure.2: Accuracy Comparison Graph

In Figure 1, accuracy comparison graph is observed between Dis-Integration Protocol (DIP) and hybrid model. In this figure, X-axis demonstrates sharing and storage of data in cloud environment and Y-axis demonstrates accuracy. In this system, data is encrypted and stored in the cloud server. At the time of sharing the encrypted cannot be hacked by any attacker.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

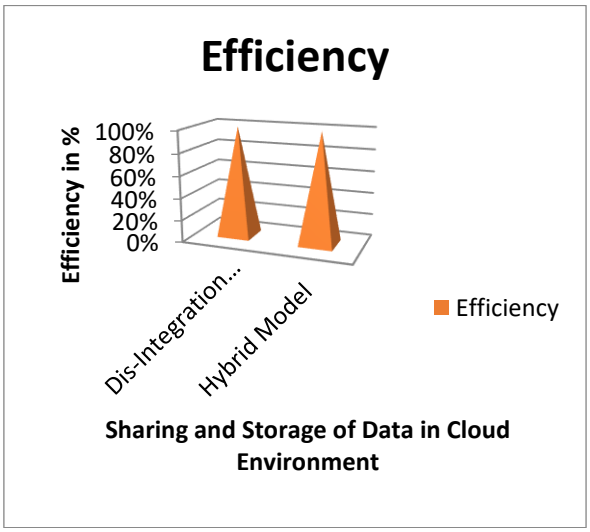

Figure.3: Efficiency Comparison Graph

In Figure 3, Hybrid model shows high efficiency when compared other model. In this hybrid model the data will store efficiently and even sharing of data to the other user or devices with secured password.

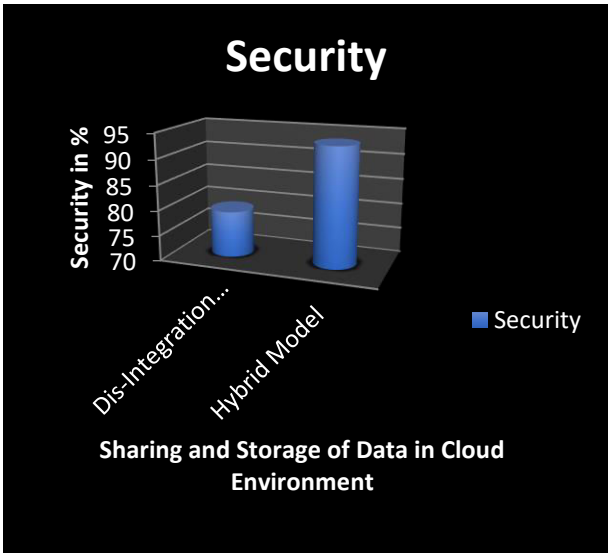

Figure.5: Security Comparison Graph

The graphical representation for security is observed in Figure 4. In this graphical representation, X-axis shows sharing and storage of data in cloud environment and Y-axis shows security. This technique is to secure more amount of information so that the hacker did not attack the data. This hybrid model can provide transparency to both the cloud user and the cloud service provider, which can help provides high security.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

V. CONCLUSION

Hence, in this section novel model for efficient sharing and storage of data in cloud environment is concluded. Today's, every organization is moving towards cloud environment to store their data, but data security is the principle issue in cloud. To share the personal file from one user to another user is most difficult using the cloud computing. To provide more secure to the data using different schemes. Therefore, in this hybrid model data sharing will highly secure. The data which is data stored in cloud server provides high security by using this model. Hence, this model achieves better results interms of accuracy, efficiency and security.

REFERENCES

[1] S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," *2017 IEEE International Conference on Circuits and Systems (ICCS)*, Thiruvananthapuram, India, 2017, pp. 76-81, doi: 10.1109/ICCS1.2017.8325966.
[2] A. Elghazi, M. Berrezzouq and Z. Abdelali, "New version of iSCSI protocol to secure Cloud data storage," *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, Marrakech, Morocco, 2016, pp. 141-145, doi: 10.1109/CloudTech.2016.7847690.
[3] R. Nivedhaa and J. J. Justus, "A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption," *2018 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India, 2018, pp. 0755-0759, doi: 10.1109/ICCSP.2018.8524257.
[4] J. Newport and B. von Solms, "A secure cloud storage system for small and medium enterprises," *2017 IST-Africa Week Conference (IST-Africa)*, Windhoek, Namibia, 2017, pp. 1-6, doi: 10.23919/ISTAFRICA.2017.8102293.
[5] R. V. Mante and N. R. Bajad, "A Study of Searchable and Auditable Attribute Based Encryption in Cloud," *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2020, pp. 1411-1415, doi: 10.1109/ICCES48766.2020.9137860.
[6] K. Kartheeban and A. D. Murugan, "Privacy preserving data storage technique in cloud computing," *2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Srivilliputtur, India, 2017, pp. 1-6, doi: 10.1109/ITCOSP.2017.8303136.
[7] A. Tripathi, M. Deep Khare and P. K. Singh, "A review of scalable data sharing techniques for secure cloud storage," *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, India, 2015, pp. 899-901, doi: 10.1109/ICACEA.2015.7164832.
[8] K. Rajkumar and V. Dhanakoti, "Methodological Survey to Improve the Secure Data Storage in Cloud Computing," *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, 2020, pp. 313-317, doi: 10.1109/ESCI48226.2020.9167677.
[9] C. Fu, J. Yang, Z. Liu and C. Jia, "A Secure Architecture for Data Storage in the Cloud Environments," *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Santa Catarina, Brazil, 2015, pp. 289-291, doi: 10.1109/IMIS.2015.45.
[10] D. Aarthi and N. Indira, "Enabling efficient and protected sharing of data in cloud computing," *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2016, pp. 1-5, doi: 10.1109/ICICES.2016.7518876.
[11] D. Seethalakshmi, G. M. Nasira and P. Thangamani, "Securing cloud database by Data Fusing Technique (DFT) using Cloud Storage Controller (CSC)," *2016 IEEE International Conference on Advances in Computer Applications (ICACA)*, Coimbatore, India, 2016, pp. 21-25, doi: 10.1109/ICACA.2016.7887917.
[12] R. Banerjee, A. K. Chattopadhyay, A. Nag and K. Bose, "A Nobel Cryptosystem for Group Data Sharing in Cloud Storage," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2019, pp. 0728-0731, doi: 10.1109/CCWC.2019.8666561.
[13] C. Jeyanthy, R. S. Shaji and J. P. Jayan, "Symmetric key based cryptic scheme for mobile cloud storage," *2015 Global Conference on Communication Technologies (GCCT)*, Thuckalay, India, 2015, pp. 571-575, doi: 10.1109/GCCT.2015.7342726.
[14] K. Rani and R. K. Sagar, "Enhanced data storage security in cloud environment using encryption, compression and splitting technique," *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, Noida, India, 2017, pp. 1-5, doi: 10.1109/TEL-NET.2017.8343557.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022

9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)

28 th -29 th April 2022

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

[15] Nelmiawati and W. Arifandi, "A Seamless Secret Sharing Scheme Implementation for Securing Data in Public Cloud Storage Service," *2018 International Conference on Applied Engineering (ICAE)*, Batam, Indonesia, 2018, pp. 1-5, doi: 10.1109/INCAE.2018.8579388.
[16] Q. Kang *et al*., "Quasi-optimal Data Placement for Secure Multi-tenant Data Federation on the Cloud," *2020 IEEE International Conference on Big Data (Big Data)*, Atlanta, GA, USA, 2020, pp. 1954-1963, doi: 10.1109/BigData50022.2020.9377953.
[17] A. Santosh Pai Raiturkar, S. Fernandes and A. Pai, "Efficient and Secure Cloud Data Distribution and Sharing Scheme in Groups," *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2018, pp. 157-161, doi: 10.1109/ICOEI.2018.8553711.
[18] L. Huang, G. Zhang and S. Yu, "A Data Storage and Sharing Scheme for Cyber-Physical-Social Systems," in *IEEE Access*, vol. 8, pp. 31471-31480, 2020, doi: 10.1109/ACCESS.2020.2973354.
[19] Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan and G. Fortino, "An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems," in *IEEE Access*, vol. 8, pp. 47144-47160, 2020, doi: 10.1109/ACCESS.2020.2977264.
[20] W. B. Chuan, S. Q. Ren, S. L. Keoh and K. M. Mi Aung, "Flexible Yet Secure De-duplication Service for Enterprise Data on Cloud Storage," *2015 International Conference on Cloud Computing Research and Innovation (ICCCRI)*, Singapore, 2015, pp. 37-44, doi: 10.1109/ICCCRI.2015.11.
[21] T. E. Trueman and P. Narayanasamy, "Ensuring Privacy and Data Freshness for Public Auditing of Shared Data in Cloud," *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Bangalore, India, 2015, pp. 22-27, doi: 10.1109/CCEM.2015.36.
[22] B. S. Rawal and S. S. Vivek, "Secure Cloud Storage and File Sharing," *2017 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, USA, 2017, pp. 78-83, doi: 10.1109/SmartCloud.2017.19.
[23] Y. Tao, P. Xu and H. Jin, "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage," in *IEEE Access*, vol. 8, pp. 15963-15972, 2020, doi: 10.1109/ACCESS.2019.2962600.
[24] S. J. Nadaf and R. Patil, "Cloud based privacy preserving secure health data storage and retrieval system," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 2016, pp. 1-6, doi: 10.1109/INVENTIVE.2016.7824831.
[25] R. Rabaninejad, S. M. Sedaghat, M. Ahmadian Attari and M. R. Aref, "An ID-Based Privacy-Preserving Integrity Verification of Shared Data Over Untrusted Cloud," *2020 25th International Computer Conference, Computer Society of Iran (CSICC)*, Tehran, Iran, 2020, pp. 1-6, doi: 10.1109/CSICC49403.2020.9050098.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details