International Journal of LNCT
Volume-6 Issue-28 February -2022
ISSN: (Online):2456-9895

# Design and Implementation Cloud Computing Data Using Light Weight Hybrid Encryption Scheme

**Author's Name**: [1] Ankit Bijoria, [2] Mrs. Bhawana Pillai

**Affiliation**: [1] *Student, Lakshmi Narain College of Technology and Science, Bhopal, India*

[2] *Professor of Lakshmi Narain College of Technology and Science, Bhopal, India*

**E-Mail**: ankitbijoria@gmail.com

## Abstract

***Cloud computing has a lot of advantages for those who use it, but it also has a lot of drawbacks and inefficiencies, the most important of which is security. In order to take use of a remote cloud-based infrastructure, a corporation must essentially hand up sensitive and proprietary data and information. To limit access to such sensitive and confidential data, secret sharing mechanisms are employed. The number of participants in the reconstruction phase is critical for recovering the secret in threshold secret sharing schemes. In this research, we introduce outsourced computation Design and Implementation Cloud Computing Data Using Light Weight Hybrid Encryption Scheme.***

**Keywords** *: Hybrid Encryption Scheme , Cloud Service Provider , Cloud Computing.*

## I. Introduction

Modern cloud computing, with its growing approach, delivers cost-saving computations and flexible services to both public and private companies through Cloud Service Providers (CSP)[1]. CSP must use a suitable access policy to maintain the confidentiality, security, and integrity of outsourced data storage. Cloud computing is a cutting-edge technology that allows users to pay for access to software and hardware resources. Virtualization is a critical strategy for serving multi-tenants in the usage of resources in order to conceal data movement from clients. Cloud computing is a hugely versatile information technology that allows you to supply services to external consumers using internet resources. Figure 1.1 depicts a common cloud computing concept that uses the internet to provide.

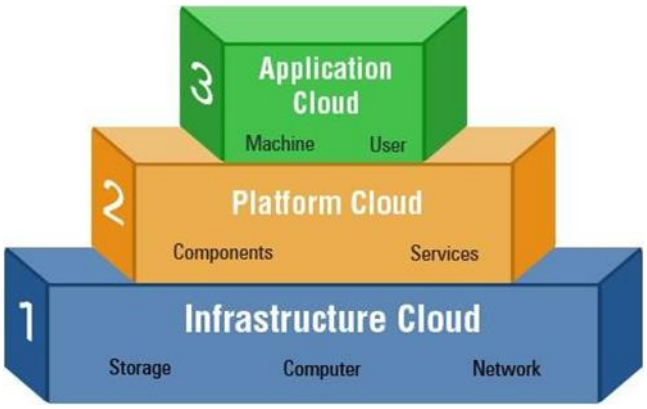


Figure 1: Cloud Computing Model

Increased adoption of cloud benefits, which are provided by the availability of resources, automated tools, and data configuration on demand, thereby displacing current traditional ways. On a rental basis, businesses can easily deploy and employ cloud services. It also delivers cost-effective network[2] connectivity with increased scalability. Additional benefits of cloud services include protection against network threats, security controls, and disaster recovery. However, as cloud use grows, the requirement for security and privacy in terms of multi-tenant, policy, access control, and confidentiality, as well as protecting sensitive information, is growing, as is the need to protect data from destruction.

Despite the numerous advantages of cloud computing, businesses are generally hesitant to use cloud-based components. Due to security concerns, privacy threats, and trust-based threats, the most essential issues when dealing with data in the cloud are its availability, privacy, protection, location, and secret transmission. These dangers arise when cloud data centres provide on-demand services over a traditional network.

Cloud security[3] is a subset of information security that discusses how to frame rules and controls, as well as how to use cryptography to safeguard data and cloud applications in off-site data centres. Many cloud clients use cloud storage services primarily for data recovery and backup purposes[4]. Not user data, however archives are commonly made. Computation and resources are metered at the start of the project and then turned off at the conclusion to save money.

## II. Related work

Z. H. Mahmood et al[5] The study provides an overview of cloud computing security challenges, and the use of completely homomorphic encryption has downsides such as huge key sizes and low calculation efficiency, making it impractical for secure cloud computing. We devise a hybrid homomorphic encryption technique based on the additively (single bit) homomorphic GM encryption algorithm and the multiplicative homomorphic RSA algorithm.

P. Kanchanadevi et al [6] In this study, we focus on data security in the Hybrid Cloud using an encryption approach. There are a variety of encryption systems available to us, but they all have data security concerns.

B. Deepthi et al [7] The system enhances data security for data that is outsourced. Honey encryption combined with hybrid cryptography allows only plausible-looking messages to be accessed by unauthorised individuals.

P. Kulkarni et al [8] Many classic security measures are presented to secure data exchange between users and the cloud. A hybrid encryption strategy is proposed in this research to safeguard the photos. The secret key is generated using Elliptic Curve Cryptography, which is then used in the DES and AES algorithms.

Z. Cao et al [9] The system is defective because: (1) its circuit access structure is unclear; (2) the cloud server is unable to execute the necessary computations; and (3) a group of users can collude to generate new decryption keys without the assistance of the key generation authority.

A. Chauhan et al [10] This study offers a new parallel cryptographic algorithm that improves security by combining and altering MD5 and Blowfish encryption algorithms. To overcome the shortcomings of symmetric block cryptography and hash function techniques, a hybrid MD5-Blowfish cryptographic calculation was developed.

K. A. Tayade et al [11] In order to ensure the confidentiality of sensitive personal data, de-duplication is supported. Before purchasing or deploying data from an outside agency, the convergent encryption technique is utilised to encrypt it.Proposed methodology

## III. Proposed Methodology

Cloud Security with a Cryptographic Approach recommended the usage of strict primary delegation and validation procedures to aid in the detection of rogue users. One of the representation models of the service level agreement (SLA) among end users and service providers is procedures for the protection of the company's significant assets. This introduces secrecy as well as the potential legal consequences that may be imposed if the service provider breaches the contract. Traits for SLA monitoring, execution, and validation are available in the Service Level Agreement description language. Furthermore, Circuitry monitoring should be general in nature in order to detect malicious packets, and the system's upgraded security devices should all be in place. In a cloud context, cataloguing distinct security provisions comes first, followed by providing an appropriate solution that eliminates these prospective alarms. This technique was proposed by a Trusted Third Party. The suggested explanation focuses on cryptography, as well as an independent Public Key Infrastructure that works in concert with SSO and LDAP to ensure authentication, integrity, and confidentiality for complex data[12] and communications. TTP is a cryptographic technique that aids in the establishment of stable communication between two parties who have faith in a third party. A TTP's scope is contained within an Information System, and it provides standard end-to-end scalable protection that is advantageous across multiple geographies, terrestrial areas, and specialist divisions.

A Trusted Third Party is an unbiased organisation that provides industry trust to a digital firm through economic and technological security qualities. Professional, licenced, commercial, and architectural means are used to administer and support its services. This feature makes use of digital licence acknowledgement and serves as a tool for matching these licences to their recognised source and destination locations on competing servers. Planning the notion of a Public Key Infrastructure (PKI) and it gives genuine and constitutionally permissible way to actualize [13] have reviewed six different symmetric key RSA data encryption algorithms under cloud settings to

provide a web of assurance. The main benefit of this strategy is the ability to handle two distinct storages for content and data security, which results in additional storage and computation overheads. The authors used a conjunctive approach to do a keyword search on the already encrypted data scheme. To mitigate keyword privacy violations, they have grouped the requested keywords into an index. However, this is impractical since the information master must compile all of the accessible keyword sequences into a single index. They've also added a constant keyword search for multi-user environments, allowing multiple users to explore an encrypted index using different private keys. In a cloud setting, a fuzzy keyword search across encrypted data systems has been advocated. When using specific keywords, they first created a wildcard keyword set that included all of the keyword's variations. They used edit measures to quantify the keyword association in the case of the trapdoor. This proposed keyword is counted as a keyword match if it is found inside the fuzzy keyword collection. The authors used the relevant processes to carry out various fuzzy keyword search plans by reducing the capacity of an index. For the secrecy-protecting cloud warehouse, a mechanism for ciphertext retrieval was implemented[3]. It also entails eliminating the obstacles encountered while working with encrypted data in order to reduce the amount of time spent on information management and supporting data content dissemination. We used interaction protocols, a key derivation technique, a combination of symmetric and asymmetric encryption, and bloom filters. Although it maintains scarcely owner-write-user-read and requires a process that supports text-based cypher computing, it can work on encrypted information to overcome the work pressure on preserving the space as well as communication and computation challenges. Proposed[4] a sufficient secrecy-protecting keyword exploration project in the cloud that provides a service. The effective privacy preserving keyword search technique allows the provider to participate in influenced decryption and authorises the exploration of keywords on encrypted documents (EPPKS). It protects the privacy of user data, encrypts searches, and aids keyword research on the encrypted file. It is thought to be useful, productive, and semantically and provably secure.

Secret key restoration in a cloud area is part of a categorization for strengthening user secrecy. It is recommended since it allows users to protect their data by encrypting their own records in the cloud storehouse. For securing data in encryption of client data content, a secret distribution technique based on AES is used. With the help of the ZIP algorithm, the uncertainty of the encryption key is removed, allowing data compression to be reduced. The related method, however, assigns a significant computation weight to the client, who must be concerned about the transfer rate. End-user key recovery is a difficulty since users are unable to search for information and are hampered by the diffusion of data[5]. For improving reliability in cloud ecosystems, the authors suggested a Hybrid Encryption algorithm based on RSA Small-e and Efficient RSA (HE-RSA)[14]. The number of key creation types in connection with the primary RSA has increased in the suggested design. To prevent repeated attacks on the RSA technique, a linked encryption method was used. For strengthening the security of the true RSA, HE-RSA has used a supplemental type. The third exponent was calculated using this method in relation to the RSA small-e, which was a short integer. According to the adjusted size of exponents, the relationship between main RSA and HE-RSA was encouraged. According to the results of the experiment, the encryption and decryption times in HE-RSA were reduced by 35%. Furthermore, the ratio of the initial RSA[15] and HE-RSA registers that the basic generation time has improved from the mid-40s to the mid-90s. Several algorithms, including as RSA, DES, AES, and Blowfish, have been proposed and examined in their study, and the results indicate that data content in the cloud is safe. Information is encrypted and decrypted using symmetric key methods such as DES, AES, and Blowfish. Their key sizes, which range from 56 to 1024 bits, are the most important distinction between them.

The RSA technique is mostly utilised in cloud environments to secure data. The entire message is mapped into an integer using Block Cipher. In most cloud environments, the public key is widely available, but the private key is very secure and only known by the user who handles the data at the outset. In most cases, the CSP is in charge[16] of encryption, while the cloud user or client is in control of decryption.

The symmetric AES block cypher provides an obvious answer to the application[17] and aids in rapid and efficient integration without requiring changes to the application[18][19]. A block cypher is the Data Encryption Standard (DES). It accommodates applications, and the key remains in place for an extended period of time without any essential changes.

Proposed Algorithm

Plain text message, proxy re encryption key as input

Expected cipher-text as output

Begin

Step 1: The data holder encrypts the data with the RSA method.

Step 2: Obtaining the CSP's public key. Data is encrypted again with ECC and sent to the CSP.

Step 3: Using the ECC private key, CSP decrypts the ciphertext and saves it in storage.

Step 4: CSP receives the re-encryption key and encrypts the data before sending it to the appropriate user.

Step 5: The original data can be decrypted using the end user's private key.

End

Results analysis

The experiment was carried out with the help of Python and Anaconda tools, as well as the NetBeans IDE and the CloudSim tool, which provides modelling, simulation, cloud infrastructures, and cloud services. Throughput and execution time of encryption and decryption actions are the performance metrics employed. Identity Based Encryption is compared to the proposed technique (IBE).

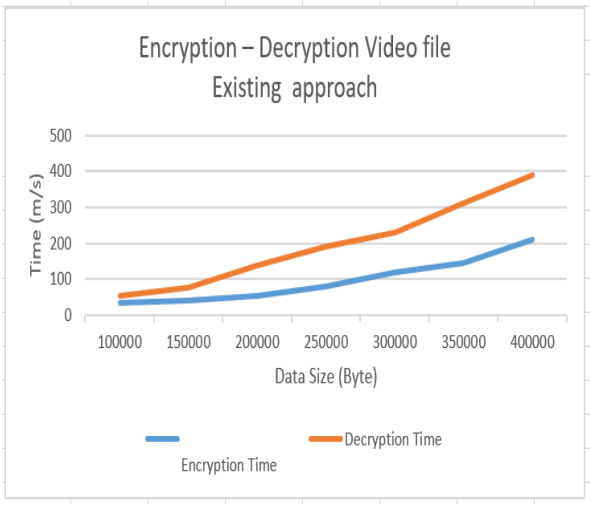


Figure 2: Encryption and decryption video file

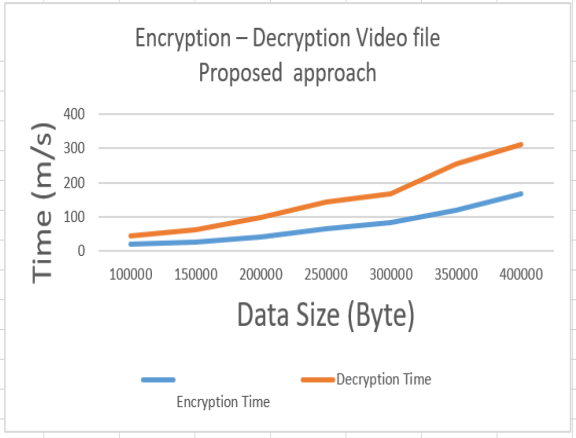


Figure 3: Encryption and decryption video file proposed approach.

### IV. Conclusion

The suggested hybrid RSA algorithm's goal is to provide security for cloud data that has been outsourced. The algorithm encrypts the data content before saving it in the storage so that the data owner has complete control over its security. The client sender who encrypts the information data content uses a mixed algorithm in this technique. Data security is the responsibility of both the sender and the CSP. In order to strengthen the information content of data security, sender encrypted data is mixed with proxy re-encryption technique and utilised for encrypting the data. Hybrid encryption and proxy re-encryption techniques are used to provide secure data transfer.

## Reference

[1]. I Z. H. Mahmood and M. K. Ibrahem, "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," 2018 1st Annual International Conference on Information and Sciences (AiCIS), 2018, pp. 182-186, doi: 10.1109/AiCIS.2018.00043.

[2]. P. Kanchanadevi, L. Raja, D. Selvapandian and R. Dhanapal, "An Attribute Based Encryption Scheme with Dynamic Attributes Supporting in the Hybrid Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 271-273, doi: 10.1109/I-SMAC49090.2020.9243370.

[3]. B. Deepthi, G. Ramani, R. Deepika and M. Shabbeer., "Hybrid Secure Cloud Storage data based on improved Encryption Scheme," 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), 2021, pp. 776-779, doi: 10.1109/ESCI50559.2021.9396842.

[4]. P. Kulkarni, R. Khanai and G. Bindagi, "A Hybrid Encryption Scheme for Securing Images in the Cloud," 2020 International Conference on Inventive Computation Technologies (ICICT), 2020, pp. 795-800, doi: 10.1109/ICICT48043.2020.9112499.

[5]. Z. Cao and O. Markowitch, "Comment on “Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption With Verifiable Delegation in Cloud Computing”," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 2, pp. 392-393, 1 Feb. 2021, doi: 10.1109/TPDS.2020.3021683.

[6]. A. Chauhan and J. Gupta, "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, pp. 349-355, doi: 10.1109/ISPCC.2017.8269702.

[7]. K. A. Tayade and G. S. Malande, "Survey paper on a secure and authorized de-duplication scheme using hybrid cloud approach for multimedia data," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 2966-2969, doi: 10.1109/ICECDS.2017.8389999.

[8]. H. Zhang, S. Zhao, Z. Guo, Q. Wen, W. Li and F. Gao, "Scalable Fuzzy Keyword Ranked Search over Encrypted Data on Hybrid Clouds," in IEEE Transactions on Cloud Computing, doi: 10.1109/TCC.2021.3092358.

[9]. Z. H. Mahmood and M. K. Ibrahem, "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," 2018 1st Annual International Conference on Information and Sciences (AiCIS), 2018, pp. 182-186, doi: 10.1109/AiCIS.2018.00043.

[10]. P. Kanchanadevi, L. Raja, D. Selvapandian and R. Dhanapal, "An Attribute Based Encryption Scheme with Dynamic Attributes Supporting in the Hybrid Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 271-273, doi: 10.1109/I-SMAC49090.2020.9243370.

[11]. B. Deepthi, G. Ramani, R. Deepika and M. Shabbeer., "Hybrid Secure Cloud Storage data based on improved Encryption Scheme," 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), 2021, pp. 776-779, doi: 10.1109/ESCI50559.2021.9396842.

[12]. P. Kulkarni, R. Khanai and G. Bindagi, "A Hybrid Encryption Scheme for Securing Images in the Cloud," 2020 International Conference on Inventive Computation Technologies (ICICT), 2020, pp. 795-800, doi: 10.1109/ICICT48043.2020.9112499.

[13]. H. Liu, X. Yao, T. Yang and H. Ning, "Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1352-1362, April 2019, doi: 10.1109/JIOT.2018.2843561.

[14]. Z. Lian, M. Su, A. Fu, H. Wang and C. Zhou, "Proxy Re-Encryption Scheme For Complicated Access Control Factors Description in Hybrid Cloud," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149306.

[15]. S. Kaushik and A. Patel, "Secure Cloud Data Using Hybrid Cryptographic Scheme," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777592.

[16]. D. K. Babu, P. V. Narasimha Rao and M. Rakesh, "PROTECTED STEADFAST DEDUPLICATION IN CROSSBREED CLOUD TECHNIQUE," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, 2018, pp. 542-546, doi: 10.1109/I-SMAC.2018.8653788.

[17]. K. S. Sankaran, N. Vasudevan, V. R. Prakash and P. Kumara Guru Diderot, "Access Control based Efficient Hybrid Security Mechanisms for Cloud Storage," 2019 International Conference on Communication and Signal Processing (ICCSP), 2019, pp. 0564-0567, doi: 10.1109/ICCSP.2019.8698037.

[18]. Rajawat A.S., Rawat R., Shaw R.N., Ghosh A. (2021) Cyber Physical System

Fraud Analysis by Mobile Robot. In: Bianchini M., Simic M., Ghosh A., Shaw R.N. (eds) Machine Learning for Robotics Applications. Studies in Computational Intelligence, vol 960. Springer, Singapore. https://doi.org/10.1007/978-981-16-0598-7_4

[19]. S. Rathod, S. A. Ubale and S. S. Apte, "Attribute-Based Encryption Along with Data Performance and Security on Cloud Storage," 2018 International Conference on Information , Communication, Engineering and Technology (ICICET), 2018, pp. 1-3, doi: 10.1109/ICICET.2018.8533815.

[20].Y. Yasumura, H. Imabayashi and H. Yamana, "Attribute-based proxy re-encryption method for revocation in cloud storage: Reduction of communication cost at re-encryption," 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA), 2018, pp. 312-318, doi: 10.1109/ICBDA.2018.8367699.

[21].B. PUSHPA, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 329334,doi:10.1109/ICCMC48092.2020.ICCMC-00062.

[22].S. Sharma and A. S. Rajawat, "A secure privacy preservation model for vertically partitioned distributed data," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016, pp. 1-6, doi: 10.1109/ICTBIG.2016.7892653.

[23].Y. Yasumura, H. Imabayashi and H. Yamana, "Attribute-based proxy re-encryption method for revocation in cloud storage: Reduction of communication cost at re-encryption," 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA), 2018, pp. 312-318, doi: 10.1109/ICBDA.2018.8367699.