International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

A Encryption Method for Transforming data on Cloud Securely

Mahendra Singh Panwar[1], Manoj Saini[2]

[1,2]*Department of Master of Computer Application, Compucom Institute of Information Technology and Mangement, Jaipur, India*

***Abstract*-- For those who use it, cloud computing offers many benefits, but it also has many disadvantages and inefficiencies, the most significant of which is security. A firm must effectively pass over sensitive and confidential data and information in order to use a remote cloud-based infrastructure. Secret sharing procedures are used to restrict access to such sensitive and private data.In threshold secret sharing schemes, the number of participants in the reconstruction phase is crucial for recovering the secret. In this study, we introduce the Lightweight Hybrid Encryption Scheme for Cloud Computing Data Design and Implementation Outsourced Computation.**

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

I. INTRODUCTION

Through Cloud Service Providers (CSP)[1, modern cloud computing offers flexible services and cost-effective computations to both public and commercial businesses. To preserve the confidentiality, security, and integrity of outsourced data storage, CSP must implement an appropriate access policy. Modern technology called cloud computing enables customers to purchase access to hardware and software resources.In order to hide data flow from clients, servicing many tenants with virtualization is a crucial resource management method. With the use of the internet and the incredibly flexible information technology known as cloud computing, you can offer services to customers outside your company. A typical cloud computing approach that makes use of the internet is shown in Figure 1.1.

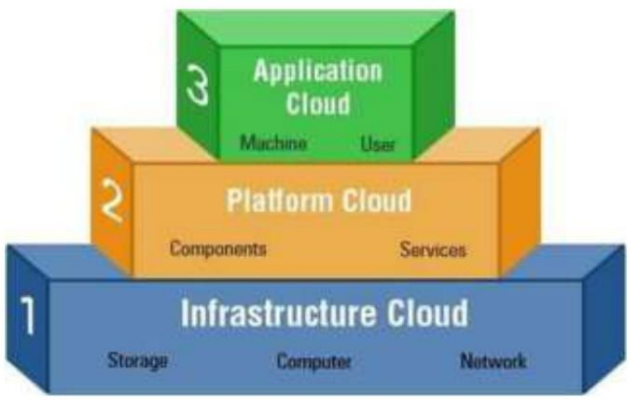

Figure1:Cloud Computing Model

Increased usage of cloud benefits, which replace present conventional methods by making resources, automated tools, and data configuration available when needed. Businesses can easily build and use cloud services on a rental basis. Additionally, it provides more scalable network[2] connectivity at a lower cost.Security measures, disaster recovery, and protection against network attacks are further advantages of cloud services. However, as the use of the cloud increases, so does the demand for security and privacy in terms of multi-tenant, policy, access control, and confidentiality, as well as the need to secure sensitive data and the need to prevent data loss.

Despite the fact that cloud computing has many benefits, companies are typically cautious to employ cloud-based components. The most crucial challenges when dealing with data in the cloud are its accessibility, privacy, protection, location, and secret transmission due to security worries, privacy threats, and trust-based dangers. When cloud data centres offer on-demand services across a conventional network, these risks materialise.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

Cloud security[3] is a subset of information security that covers how to create rules and controls, how to utilise cryptography to protect data, and how to protect cloud applications in off-site data centres. The primary uses of cloud storage for many clients are data backup and recovery[4]. Not user data, however archives are frequently created. To save money, computation and resources are metered at the beginning of the project and then shut off at the end. Related work

Z. H. Mahmood and others[5] According to the study's overview of cloud computing security issues, fully homomorphic encryption is not viable for secure cloud computing due to its disadvantages of having enormous key sizes and poor calculation performance. We create a hybrid homomorphic encryption method based on the multiplicative homomorphic RSA algorithm and the additively (single bit) homomorphic GM encryption algorithm.

Kanchanadevi, P., et al. We concentrate on data security in the Hybrid Cloud utilising an encryption technique in this work. We have access to several different encryption technologies, but they all have issues with data security.

B Deepthi and others [7] The system improves the security of outsourced data. Using honey encryption and hybrid cryptography, only messages that appear plausible can be viewed by unauthorised parties.

Kulkarni, P., et al. To safeguard data exchange between users and the cloud, many traditional security procedures are given. This study suggests a hybrid encryption method to protect the images. Elliptic curve cryptography is used to create the secret key, which is then utilised by the DES and AES algorithms.

Z. Cao and co. The system is flawed because (1) it lacks clarity regarding the circuit access structure, (2) the cloud server is unable to perform the required computations, and (3) a group of users can work together to generate new decryption keys without the help of the key generating authority.

Chauhan, A., et al. [10] The new parallel cryptographic technique presented in this paper combines and modifies the MD5 and Blowfish encryption algorithms to increase security. A hybrid MD5-Blowfish cryptographic calculation was created to fix the issues with symmetric block cryptography and hash function methods.

K. A. Tayde and others [11] De-duplication is supported in order to guarantee the confidentiality of sensitive personal data. The convergent encryption technique is used to encrypt the data before it is purchased or used by a third party. proposed approach

II. PROPOSED METHODOLOGY

To help in the identification of malicious users, Cloud Security with a Cryptographic Approach advised the adoption of stringent primary delegation and validation methods. Procedures for the protection of the company's important assets are one of the representation models of the service level agreement (SLA) between end users and service providers. This introduces confidentiality as well as the possibility of legal repercussions in the event that the service provider violates the contract.Service Level Agreement descriptive language features are available for SLA monitoring, execution, and validation. The system's improved security mechanisms should all be in place, and circuitry monitoring should be general in nature to detect malicious packets. In a cloud environment, cataloguing various security features comes first, then a suitable solution that disables these potential alerts. A Trusted Third Party suggested this method. In order to provide authenticity, integrity, and confidentiality for complex data[12] and communications, the suggested explanation concentrates on cryptography as well as a separate Public Key Infrastructure that functions in tandem with SSO and LDAP. TTP is a cryptographic method that helps two parties who trust one another establish stable communication.

An impartial organisation known as a Trusted Third Party establishes industry trust for a digital company through financial and technological security features. To administer and support its services, professional, licenced, commercial, and architectural methods are used. In order to match these licences to their recognised source and destination locations on competing servers, this feature uses digital licence acknowledgment. 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 algorithm sunder cloud settings to provide a web of assurance. The capacity to manage two different storages for content and data security, which results in more storage and compute overheads, is the key advantage of this system. The authors conducted a keyword search on the already encrypted data method using a conjunctive approach. They have compiled the specified keywords into an index in order to lessen keyword privacy infringement. The information master must combine all of the accessible keyword sequences into a single index, making this unfeasible. A constant keyword search for multi-user scenarios has also been implemented, enabling several users to browse an encrypted index using various private keys.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 01, January 2022)

A fuzzy keyword search across encrypted data systems has been recommended in a cloud environment.When employing particular keywords, they first generated a set of wildcard keywords that contained every possible version of the keyword. In the case of the trapdoor, they quantified the keyword association using edit metrics. If this suggested keyword is located in the fuzzy keyword collection, it is taken into account as a keyword match. By limiting the capacity of an index, the authors carried out numerous fuzzy keyword search plans using the appropriate techniques. A system for retrieving ciphertext was put into place for the cloud warehouse that protects confidentiality[3]. In order to shorten the time spent managing information and distributing data content, it also means removing the challenges that arise while working with encrypted data. In addition to symmetric and asymmetric encryption, we also used interaction protocols, a key derivation method, and bloom filters. It can work with encrypted information to get beyond the work pressure on conserving the space as well as communication and computation issues, even though it maintains hardly owner-write-user-read and requires a method that supports text-based cypher computing. An adequate secrecy-protecting cloud service that offers keyword exploration has been proposed[4]. By using an efficient privacy-preserving keyword search technique, the provider is able to take part in influenced decryption and is given permission to examine keywords on encrypted data (EPPKS). It safeguards.

Restoration of secret keys in a cloud environment is a category for enhancing user secrecy. It is advised since it enables users to secure their data by encrypting their own files in the cloud data centre.

For securing data in encryption of client data content, asecretd is tribution technique.

It is based on AES. Reduced data compression is possible thanks to the removal of encryption key uncertainty by the ZIP technique. The customer, who must be concerned about the transfer rate, is given a large computation weight in the linked technique, though. End-user key recovery is challenging since users can't look up information and are constrained by the spread of data[5]. The authors proposed a Hybrid Encryption algorithm based on RSA Small-e and Efficient RSA (HE-RSA)[14] to increase reliability in cloud ecosystems. In the suggested design, there are now more key creation kinds connected to the primary RSA.

The RSA approach was subjected to repeated attacks, hence a linked encryption method was employed. HE-RSA has utilised a supplementary type to increase the actual RSA's security. This approach was used to determine the third exponent with respect to the short integer RSA small-e. The link between main RSA and HE-RSA was fostered by the altered exponent size. The experiment's findings showed that HE-encryption RSA's and decryption times were cut by 35%. Additionally, the ratio of the.

To secure data, the RSA method is primarily used in cloud environments. Block Cipher is used to map the entire message into an integer. The private key is extremely safe and is only known by the user who handles the data initially in the majority of cloud environments, but the public key is typically freely accessible. The cloud user or client typically controls decryption, while the CSP typically controls encryption[16].

The symmetric AES block cypher helps with quick and efficient integration without necessitating changes to the application[17] and offers a clear solution to the problem[18][19]. The Data Encryption Standard is a block cypher (DES). Applications can be accommodated, and the key doesn't require any major adjustments for a long time.

Proposed Algorithm

Plain text message, proxy re encryption key
asinput

Expected cipher-text as

outputBegin

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 ciphertextandsavesitin 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 enduser'sprivate key.

End

III. Results Analysis

The experiment was carried out with the help of Pythonand Anaconda tools, as well as the Net Beans IDE and the Cloud Simtool, which providesmodelling, simulation, cloud infra structures, and cloud services. Throughput and executiontime of encryptionanddecryptionactionsaretheperformancemetricsemployed.IdentityBasedEncryptioniscomparedtotheproposedtechnique(IBE).

IV. Conclusion

The purpose of the proposed hybrid RSA method is to offer security for outsourced cloud data. Prior to being saved in the storage, the algorithm encrypts the data content to give the data owner full control over the security of the data. In this strategy, the client sender who encrypts the data content utilises a hybrid algorithm. Both the sender and the CSP are liable for data security. Sender encrypted data is combined with a proxy re-encryption technique and used to encrypt the data in order to increase the information content of data security. To enable safe data transfer, hybrid encryption and proxy re-encryption techniques are deployed.

REFERENCES

[1] IZ.H.MahmoodandM.K.Ibrahem,"NewFullyHomomorphicEncryptionSchemeBasedonMultistagePartialHomomorphicEncryptionAppliedinCloudComputing,"20181stAnnualInternationalConferenceonInformationand Sciences (AiCIS), 2018, pp. 182-186,doi:10.1109/AiCIS.2018.00043.

[2] P.Kanchanadevi,L.Raja,D.SelvapandianandR.Dhanapal,"AnAttribute Based Encryption Scheme withDynamicAttributesSupportingintheHybrid Cloud," 2020 Fourth InternationalConferenceonI-SMAC(IoTinSocial,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.,"HybridSecureCloudStoragedatabasedonimprovedEncryptionScheme,"2021InternationalConferenceonEmergingSmartComputing and Informatics (ESCI), 2021, pp. 776-779, doi: 10.1109/ESCI50559.2021.9396842.

[4] P. Kulkarni, R. Khanai and G. Bindagi, "AHybridEncryptionSchemeforSecuringImages in the Cloud," 2020 InternationalConferenceonInventiveComputationTechnologies (ICICT), 2020, pp. 795-800,doi:10.1109/ICICT48043.2020.9112499.

[5] Z. Cao and O. Markowitch, "Comment on"CircuitCiphertext-PolicyAttribute-Based Hybrid Encryption With VerifiableDelegationinCloudComputing","inIEEETransactionsonParallelandDistributedSystems,vol.32, no.2,pp.392-393,1Feb.2021,doi: 10.1109/TPDS.2020.3021683.

[6] A.ChauhanandJ.Gupta,"Anoveltechniqueofcloudsecuritybasedonhybrid encryption by Blowfish and MD5,"20174thInternationalConferenceonSignal Processing, Computing and Control(ISPCC),2017,pp.349-355,doi:10.1109/ISPCC.2017.8269702.

[7] K. A. Tayade and G. S. Malande, "Surveypaperonasecureandauthorizedde-duplicationschemeusinghybridcloudapproachformultimediadata,"2017InternationalConferenceonEnergy,Communication,DataAnalyticsandSoftComputing(ICECDS),2017, pp.2966-2969,doi:10.1109/ICECDS.2017.8389999.

[8] H. Zhang, S. Zhao, Z. Guo, Q. Wen, W. LiandF.Gao,"ScalableFuzzyKeywordRankedSearchoverEncryptedDataonHybrid Clouds," in IEEE Transactions onCloud Computing, doi:10.1109/TCC.2021.3092358.

[9] Z. H. Mahmood and M. K. Ibrahem, "NewFullyHomomorphicEncryptionSchemeBased on Multistage Partial HomomorphicEncryption Applied in Cloud Computing,"2018 1st Annual International ConferenceonInformationandSciences(AiCIS),2018, pp. 182-186, doi: 10.1109/AiCIS.2018.00043.

[10] P.Kanchanadevi,L.Raja,D.SelvapandianandR.Dhanapal,"AnAttribute Based EncryptionScheme withDynamicAttributesSupportingintheHybridCloud,"2020FourthInternational ConferenceonI-SMAC(IoTinSocial,Mobile, Analytics and Cloud) (I-SMAC),2020,pp.271-273,doi:10.1109/I-SMAC49090.2020.9243370.

[11] B.Deepthi,G.Ramani,R.Deepikaand M.Shabbeer., "HybridSecureCloudStorage data based on improved EncryptionScheme," 2021 International Conference onEmergingSmartComputingandInformatics (ESCI), 2021, pp. 776-779, doi:10.1109/ESCI50559.2021.9396842.

[12] P.Kulkarni,R.Khanai and G.Bindagi,"A Hybrid Encryption Scheme for SecuringImagesintheCloud,"2020InternationalConferenceonInventiveComputationTechnologies (ICICT), 2020, pp. 795-800,doi:10.1109/ICICT48043.2020.9112499.

[13] H.Liu,X.Yao,T.YangandH.Ning,"CooperativePrivacyPreservationforWearableDevicesinHybridComputing-Based Smart Health," in IEEE Internet ofThingsJournal,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 ForComplicatedAccessControlFactorsDescription in Hybrid Cloud," ICC 2020 - 2020IEEEInternationalConferenceonCommunications (ICC), 2020, pp. 1-6, doi:10.1109/ICC40277.2020.9149306.

[15] S. Kaushik and A. Patel, "Secure CloudDataUsingHybridCryptographicScheme,"20194thInternational Conference onInternet of Things: SmartInnovationandUsages(IoT-SIU),2019,pp.1-6,doi:10.1109/IoT-SIU.2019.8777592.

[16] D. K. Babu, P. V. Narasimha Rao and M.Rakesh,"PROTECTEDSTEADFASTDEDUPLICATIONINCROSSBREEDCLOUD TECHNIQUE," 2018 2nd International Conference on I-SMAC (IoTin Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC(IoTinSocial,Mobile,Analytics and Cloud) (I-SMAC), 2018 2ndInternationalConferenceon,2018,pp.542- 546, doi:10.1109/I-SMAC.2018.8653788.

[17] K.S.Sankaran,N.Vasudevan,V.R.PrakashandP.KumaraGuruDiderot," AccessControlbasedEfficientHybridSecurity Mechanisms for Cloud Storage,"2019InternationalConferenceonCommunicationandSignalProcessing(ICCSP),2019, pp.0564-0567, doi:10.1109/ICCSP.2019.8698037.

[18] RajawatA.S.,RawatR.,ShawR.N.,GhoshA.(2021)CyberPhysical System Fraud Analysis by Mobile Robot. In: BianchiniM.,SimicM.,GhoshA., Shaw R.N.(eds) Machine Learning for Robotics Applications. Studiesin Computational Intelligence,vol960.Springer,Singapore.https://doi.org/10.1007/978-981-16-0598-7_4

[19] S.Rathod, S. A. Ubale and S. S. Apte,"Attribute-BasedEncryptionAlongwithData Performance and Security onCloudStorage," 2018 International Conference onInformation , Communication, Engineeringand Technology (ICICET), 2018, pp. 1-3,doi:10.1109/ICICET.2018.8533815.

[20] Y.Yasumura, H.ImabayashiandH.Yamana,"Attribute-basedproxyre-encryption method for revocation in cloudstorage: Reduction of communication costatre-encryption,"2018IEEE3rdInternationalConferenceonBigDataAnalysis(ICBDA),2018,pp.312-318,doi:10.1109/ICBDA.2018.8367699.

[21] B.PUSHPA,"Hybrid DataEncryptionAlgorithmforSecureMedicalDataTransmission in Cloud Environment,"2020 Fourth International Conference onComputingMethodologies andCommunication(ICCMC),2020,pp. 329334,doi:10.1109/ICCMC48092.2020.ICCMC-00062.

[22] S. Sharma and A. S. Rajawat, "A secureprivacy preservationmodelforverticallypartitioneddistributeddata,"2016InternationalConferenceonICTinBusinessIndustry&Government(ICTBIG), 2016,pp.1-6,doi:10.1109/ICTBIG.2016.7892653.

[23] Y.Yasumura,H.ImabayashiandH.Yamana,"Attribute-basedproxyre-encryption method for revocation in cloudstorage: Reduction of communication costatre-encryption,"2018IEEE3rdInternationalConferenceonBigDataAnalysis(ICBDA),2018,pp.312-318,doi:10.1109/ICBDA.2018.8367699.