IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cryptographic Solutions For Secure Data SharingInCloudComputing:ASystematic Review

Dr.RAJEEVPANDEY,AssociateProfessor,DepartmentofComputerScience&Engg.,UIT RGPV BHOPAL (M.P.) India

Dr.SHIKHAAGRAWAL,AssociateProfessor,DepartmentofComputerScience&Engg.,UIT RGPV BHOPAL (M.P.)India

Author:RASHMIAHIRWAR,DepartmentofComputerScience&Engg.,UITRGPVBHOPAL (M.P.) India

Abstract–Thispaperexploresthecriticalissueofdatasharingsecurityincloudcomputing, drivenbythe increasing dependence on cloud-based infrastructures for data storage, processing, and management. It reviews the key challenges, strategies, and advancements in ensuring secure data exchange within cloud environments.Thestudyaddressesessentialconcernssuchasdataconfidentiality,integrity,accesscontrol, and privacy protection, while examining potential threats, including unauthorized access, data breaches, and insider attacks. Various cryptographic methods, secure access protocols, and emerging technologies like blockchain and homomorphic encryption are analyzed for their role in strengthening security. Additionally, the paper underscores the significance of legal and regulatory frameworks in enforcing securitymeasures and outlines future research directions to address existing gaps. This surveyserves as a valuable resource for researchers and professionals seeking to navigate and mitigate the complexities of secure data sharing in cloud computing.

Keywords-Security,Audit,CloudComputing,BackwardSecrecy;Forwardsecrecy;Regenerative coding

I. Introduction

Data sharing in cloud computing involves granting access to data for multiple users or systems through cloudplatformsovertheinternet.However,ensuringthesecurityof shareddataisasignificantchallenge, asitrequiressafeguardingsensitiveandconfidentialinformationfromunauthorizedaccess,databreaches, and corruption. Cloud environments are susceptible to various risks, including cyber threats and insider attacks, makingit crucial to implement robust securitymeasures. These includeencryption, secure access controls, multi-factor authentication, and continuous monitoring. Furthermore, privacy concerns emerge when third-party cloud providers handle data, necessitating compliance with industry regulations such as GDPR and HIPAA. Achieving secure data sharing in the cloud requires not only advanced technological protectionsbutalsowell-definedpoliciesandbestpracticestoupholdusertrustandregulatorycompliance [1].

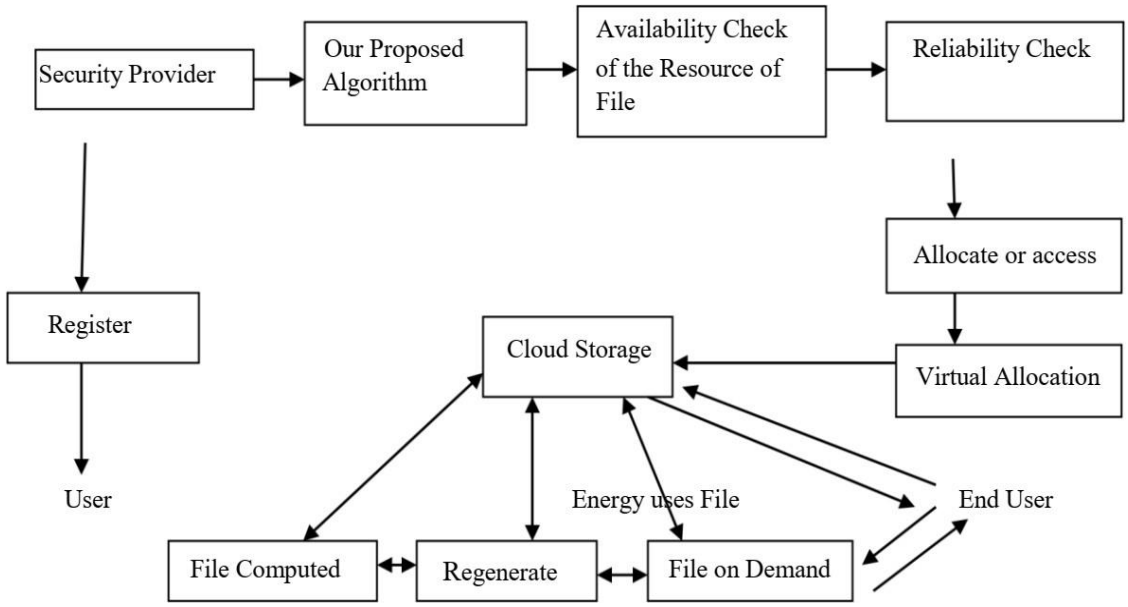

Fig.1. Securityof datasharingincloud computing

Data security is made more difficult by the dynamic nature of cloud computing, where resources are dispersed among several servers and locations. Because public cloud environments employ shared infrastructure, if security measures are not strictly followed, data may be accessed by unauthorized individuals. Because of this, it is increasingly crucial to encrypt data both in transit and at rest so that it cannot be decoded without the proper keys, even if it is intercepted. By putting access control measures like the least privilege principle into practice, you can ensure that only those with permission may access certain data [2] [1].

Technical safeguards and data interchange in cloud computing also require clear legal agreements and service-level agreements (SLAs) with cloud providers. These agreements outline both the supplier's and the customer's responsibilities, ensuring that security protocols and data protection safeguards are clear. Theshifttohybridandmulti-cloudsystemsaddsevenmorecomplexity,makingitnecessarytoseamlessly integratesecuritymeasuresacrossdifferentcloudplatforms.Manycompaniesaretacklingtheseproblems by putting in place state-of-the-art security frameworks, such as block chain for data integrity and AI-powered threat detection tools, to ensure the privacy, accessibility, and dependability of their data while utilizing the flexibility and capacity of the cloud.

To protect user data from new risks, cloud service providers need to implement strict security standards. Secure multi-party computing, attribute-based encryption, and homomorphism encryption are among methods that can improve secrecy while permitting regulated data access. Role-based access control, or RBAC,isanothertoolthatorganisationsshouldusetomakesurethatonlythosewithpermissionmaysee oraltersensitivedata.Furthermore,real-timemonitoring,intrusiondetectionsystems,androutinesecurity auditsaidinquicklydetectingandreducingthreats.Issuesincludingthird-partyintegrationvulnerabilities, misconfigurations,andinsiderthreatscontinuetoexist.Organisationsmustthustakeaproactivestanceby using artificial intelligence (AI) for threat detection and prevention, regularly updating security policies, and training staff on best security practices. Businesses may optimise cloud computing advantages and reducedatasharingrisksbyincludingstrongsecuritystandardsandcultivatingasecurity-consciousculture [3].

Because cloud computing facilitates easy cooperation and accessibility, data sharing has emerged as a crucialactivityforbothpeopleandenterprises.However,becauseofpossiblerisksincludingillegalaccess, databreaches,andcyberattacks,protectingshareddataincloudsettingsisacrucialtask.Strongencryption methods,accesscontrolsystems,andsecuredatatransportprotocolsarenecessarytoprotectsensitivedata.

Additionally, preserving data integrity and privacy depends heavily on adherence to legal and regulatory frameworks like GDPR and HIPAA. Implementingcutting-edge securitymethods, such as authentication usingmultiplefactorsandblockchaintechnology,mayimprovedataprotectionandfosteruserconfidence as cloud computing develops.

II. LiteratureSurvey

Because of possible risks including insider assaults, data breaches, and unauthorised access, cloud computingdatasharingsecurityisamajorconcern.Toprotectdatasecrecywhilepreservingaccesscontrol, a number of encryption strategies have been put forth, such as attribute-based encryption (ABE) and homomorphicencryption.Proxyre-encryption(PRE)andidentity-basedencryption(IBE),whichprovide fine-grained access control, further improve secure data sharing. Blockchain technology has also been investigated as a decentralised method to guarantee transparency and data integrity.

Xiuqing Lu et.al (2020) - The author suggests a safe and effective mobile data sharing system. Security andauthorisedaccessto sharedsensitivedataareguaranteedbythesystem.Inordertopreventinaccurate calculation, the method also does effective integrity check prior to DR sharing the data. Lastly, the plan makes it possible for mobile terminals on both the DO and DR sides to operate with little overhead [04].

SakshiChhabraet.al.(2020)-TheauthorsaresuggestingOneofthemainissuesforcloudusersthatface securitythreats is protecting data in dispersed cloud systems. Attackers frequentlyexploit data tampering orleakingtoobtainthepersonalinformationofotherusers whoexchangesensitivedataviavirtualization. The Secure Secret Sharing (SSS) strategy, which is acknowledged as one of the most effective ways to protect sensitivedata, is presentedin this study. Malicious checkersanalyzethecreatedsecret key, which is divided from several portions and supplied to qualified participants (Qn) exclusively. It exchanges encrypted data via the cloud. It confirms whether or not the clients are authorized participants bylooking attheirpriorperformances.Thecomputationofthekeyisassessed.Thesecretisreconstructedfromshares using Lagrange's interpolation approach. The experimental findings demonstrate that, in addition to offeringsuperiorsecurityandperformance,thesuggestedsecuredatasharingalgorithmoutperformsearlier countermeasuresintermsofkeymanagementanddatasecrecy.Securevirtualmachineplacementisused to increase security, and the effectiveness of our technique is assessed using time consumption and probability computation. Clouds is used to conduct experiments depending on the following parameters: encryption/decryption,responsetime,andkeygenerationcalculationtime.Theexperimentalfindingsshow thatthisapproachmaysuccessfullylowerriskswhileimprovingsecurityandtimeconsumptionby27.81% and 43.61%, respectively, compared to current techniques [05].

M Arumugam et.al (2021) - The RSA Algorithm provides the most secure data encryption method. Compared to other encryption technologies, it is extremely secure. One contemporary and evolving approachforon-demandcomputingiscloudcomputing.Therefore,thedatainoursuggestedworkisonly accessible to the authorized user. It is unable to decode the data and recover the original information becauseanunauthorizeduserorattackermaypurposefullyorunintentionallytakethedata.Itisnotpossible to obtain the data. Thus, data protection is provided by the RSA algorithm's implementation. When the business decides to switch to the cloud, the cloud loses power. As a result, the value of the data closely correlates with the level of security offered for data protection. Effective computing and encryption are essential for cloud security [06].

Amr M. Sauber et.al (2021) - The authors suggested that quick access to data without compromising its securityshouldbetheprimaryobjectiveofanycloud-baseddatastoragestrategy.Akeycomponentofany cloud data storage paradigm that ensures efficiency and safety is security. In this research, we provide a cloud-basedsafedataprotectionapproach.Thesuggestedapproachoffersaremedyforafewcloudsecurity problems,suchsafeguardingdatafrominfringementandpreventingauserwithafalseauthorisedidentity from negativelyimpacting cloud security. This document discusses a number of cloud computing-related problemsanddifficultiesthatcompromisedatasecurityandprivacy.Itoutlinesthedangersandassaults

that impact cloud-based data. Our suggested model delivers the benefits and efficacy of security in cloud computing such as strengthening of the encryption of data in the cloud. It offers cloud computing users data sharing scalability and security. Our methodology accomplishes cloud computing security features including encryption, authorisation, and identity and authentication. Additionally, this paradigm guards againstdangerousinformationenteredbyaphoneydataownerthatmightunderminetheprimaryobjective of cloud services. As a logging and uploading method, we created the one-time password (OTP) to shield users and data owners from any fraudulent unauthorised cloud access. Next Generation Secure Cloud Server(NG-Cloud)isamodelsimulationthatweusetoimplementourconcept.Theseoutcomesimprove themethodsforprotectingendusersanddataownersagainstfraudulentusersanddataownersinthecloud [07].

P. Ramesh Naiduet.al (2021) - In many organizations, the use of distributed computing has rapidly increased. There are several benefits to distributed computing in terms of information accessibility and convenience. Ensuring distributed computing security is crucial because customers frequently store sensitivedatawithcloudcapacityproviders,despitethepossibilitythattheseprovidersareunreliable.Due to the risks of administration accessibility

failure and the potential for retaliatory insiders in the single cloud, managing "single cloud" providers is expectedtobecomelesspopularwithcustomers.Recently,therehasbeenashifttowards"multi-mists,"or ultimately, "inter cloudsUsinganewcryptographicarchitecturecalled theHigh-Availabilityand Integrity Layer(HAIL),ateamofemployeesmayshowaclientthataputawayrecordisbothperfectandretrievable. HAIL strengthens, formally unifies, and smoothes out distinct techniques from the cryptography and distributed framework networks. Regardless of record size, workers may process evidence in HAIL with easeandsignificantlydecreaseittotensorevenhundredsofbytesonaregularbasis.Thecurrentanalysis analyses potential configurations and identifies single and multi-cloud security. It is found that the investigation into using several cloud providers to maintain security has received less attention from the examination network than has the use of single mists. Dueto its abilityto reduce securityrisks that affect the distributed computing client, this study aims to promote the adoption of multi-mists [08].

UmaNarayananet.al.(2022)-Bigdatasecurityinthecloudisamajorconcernduetothequickexpansion ofdatasources.Bigdatasecurityhasgivenrisetoanumberofproblems,includinginfrastructuresecurity, data privacy, data management, and data integrity. At the moment, cryptographic techniques are used to securebigdataprocessing,analytics,andstorage;however,thesealgorithmsarenotsuitableforprotecting big data over the cloud. In this article, we offer a solution to the primary problems with cloud-based big data security. We present the Secure Authentication and Data Sharing in Cloud (SADS-Cloud), a new system design. Big Data Outsourcing, Big Data Sharing, and Big Data Management are the three procedures that are covered in this study. The SHA-3 hashing method is used to register the data owners to a Trust Centre in big data outsourcing. The MapReduce architecture is used to split the input file into fixed-sizedatablocks,andtheSALSA20techniqueisusedtoencrypteachblock.Whentransferringdata, data users participate in a secure file retrieval procedure. The user's credentials (ID, password, secure ID, emailaddress,andcurrenttimestamp)arehashedandcomparedwiththosestoredinadatabasetoachieve this. Big data management uses three essential steps to organize data [09].

Mustafa Azeez AL Mayyahi et.al (2022) - Cloud computing plays a significant part in our daily lives. Demand-based resources are made available by the cloud computing concept. Because of its widespread use, affordability, and resilience, cloud computing has revolutionized how businesses manage their resources. Typically, a variety of techniques, including encryption, are used to provide data security. However,anothersignificantissuethatneedstobetakenintoaccountwhilemoving,storing,andanalyzing dataonthepubliccloudisdataprivacy.Thisworkproposesanovelapproachtomonitorhostileindividuals that decrypt datain asystem usingtheirprivatekey, shareit with others, and causesystem information to leak.Inordertoguaranteesystemsecurity,securitypoliciesarealsothoughttobelinkedwiththeencrypted messages.Forthisreason,thedatamustbeencryptedsothatitmaybesubjectedtooperationslikemax,

min, etc. before beingsent to the cloud. Order preservingsymmetric encryption (OPES), which is used in the suggested solution, eliminates the need for decryption or re-encryption for mathematical operations. Delayisgreatlyreducedasaresultofthisprocedure.Withouttheneedfordecryptionoperands,comparison operationscanbecarriedoutdirectlyonencrypteddatausingtheOPESmethod.Thefindingsclearlyshow that the suggested approach outperforms the base paper in terms of the system's capacity to identify the malevolent components that lead to the leakage issue and in terms of system security to stop privacy violations [10].

V. Rajkumar et.al (2022) –Data secrecy, authentication, authorisation, integrity, and safe data exchange withoutdoubleencryptionareallpossibleusingtheauthor'ssuggestedtechnique.Theprimarygoal ofthe suggested technique is to provide data access control in order to ward off malevolent intruders. Additionally, if the data is left unaltered, the SIPS technique guarantees its integrity. The key generator, which served as a reliable third party in the SIPS approach, assisted with the encryption and decryption procedures.Thesuggestedapproachmaybeusedtomobilecloudcomputingaswell.STPNandCodeDx were used to officially analyse how SIPS operated. Time consumption in three scenarios—key creation, uploading, and downloading data from the cloud—was used to assess performance. The findings suggest thatthesuggestedSIPSapproachmaybeusedforsafedataexchangeinthecloud.Thesuggestedparadigm maybeusedinreal-timeapplicationdomainsinthefuture.Additionally,themodelthathasbeenprovided may be expanded to incorporate lightweight cryptographic approaches [11]**.**

WenfangZhanget.al(2023)-ThesuggestedauthorsincludeTheextensiveuseofInternetofThings(IoT) technology, especiallyin manyindustrial domains, has fundamentallyaltered human civilisation. Despite the benefits that IoT services offer, it is important to recognise the underlying security risks. One of the many issues with cloud-based IoT data collecting is how to guarantee its integrity. Tian et al. have suggestedafog-to-cloudcomputing-basedpublicauditingsysteminIoTscenariostoaddressthisproblem. It offersatagtranslation approach and adata-privacyprotectingmechanism.However,bypresentingtwo attacks,wedemonstrateinthisstudythatTianetal.'sstrategyfallsshortofachievingsoundness,acrucial securitycriterion. The malicious cloud server can erase all of the data in the first attack and then trick the ThirdPartyAuditor(TPA)intothinkingthedataissafe.Themaliciouscloudservercanalterthedatathat is outsourced in the second assault, leading TPA to believe that all of the data is preserved. We also offer a straightforward yet powerful defence against the aforementioned attacks for Tian et al.'s plan. Additionally, security analysis and performance assessment are provided to show how reliable and effective the enhanced scheme is [12].

AwsHamedHamad et.al(2023)-TheauthorsofferavarietyofEM-CC systemsthathavebeendevised and executed by different research organisations. The frequent security issues with these techniques are compiled in this paper along with a well-known and simple remedy. In order to apply current EMCC solutions, this article first creates a common framework (cloud environment building, program segmentation, module assignment, module migration, program execution, and result return). The primary securitythreatsposedbyEMCCfromtheviewpointofmobiledeviceusersarethenexaminedandsummed up, including information flow hijacking and privacy leakage. It also makes note of the fact that risk management maybe employed to reduce the securitythreats posed bythe execution of EMCC programs. Quantifying the risks connected to each allocation system is essential to attaining risk management. In order to overcome this problem, we have created a risk quantification technique for assigning EMCC modules and resolved its primary challenge, which is identifying vulnerable modules. Future EMCC schemes can be designed using this framework as a guide [13]**.**

Haowen Tan et.al (2023) – The authors outline an IoT group association and updating concept based on edgecomputing.Withthehelpofneighbouringdevices,theout-of-rangeIoTdevicesmaybelinkedtothe edge network. While certain IoT devices' decryption information stays the same if they haven't been revoked,theEIsideofourarchitecture'sgroupkeyupdateprocessjustneedsminortweaks.Thesuggested method may accomplish the intended security characteristics, per the security evaluation [14].

Sijjad Ali et.al. (2024) - Safety and security of data are becoming more and more crucial as cloud computinggainspopularity.Ourresearchdemonstrateshowhomomorphismencryptionandcovertsharing techniques may be used to protect sensitive information in cloud computing settings. By employing this dual approach, we create a computer platform that is private, confidential, and safe. Our method involves spreadingdata over several servers while preservingdata security. This distribution lowers the possibility of single points of failure and raises the system's level of security. To ensure information confidentiality andsafety,dataencryptionrestrictsaccesstoonlyauthorisedusers.Toenableactivitiesonencrypteddata without having direct access to the originals, we employ homomorphism encryption as an additional feature.Byusingthisoption,sensitivedataisprotectedwhileprocessing.Asaresult,theoriginaldatamay remainsecretwhencomputingonencryptedshares.Severalperformancetestswereconductedtoshowthe feasibility and effectiveness of our strategy [15].

Tarek Ali et.al. (2024) - A well-liked technical advancement that offers centralised computer resources and services is cloud computing. It provides infrastructure, platform, and software in a variety of deployment models and modes, such as public, private, community, and hybrid. Cloud hosting offers benefitslikeminimumworkandflexibilityforexpansion,butitalsohasdrawbackslikelosingcontrolover data and infrastructure. Benefits of cloud computing include reduced expenses and time, enhanced reliability and performance, and on-demand access to limitless computing resources. But because cloud computingcomeswithproblemslikedatasecurityandprivacy,authentication,encryption,dataintegration, andaccessdifficulties,securityconcernsarestillveryreal.Astrongsecurityarchitecturethatcanadaptto theenvironment,usetherightresources,andefficientlymanagerisksisnecessaryforcriticalcloudhosting. The shift of enterprises' precious data assets to cloud-based infrastructure brings with it new dangers that necessitateacomprehensiveapproachtoriskmanagement,assessment,andgovernance.Thereareseveral approaches for managing and evaluating security risks in cloud-based systems [16].

Priya Singh et.al (2024) –A hybrid approach that uses AES, RSA, and the Diffie-Hellman algorithm to ensure security in sharing keys and data in cloud computing has been described. The authors discuss the security problem of sharing a symmetric key between the two parties for conducting AES encryption in sharing data. The suggested method is broken down into three stages: data transmission, login, and registration.Theuserwillregisterforthefirsttimewiththeproviderduringtheregistrationstep.Thiswill create a shared key for safe communication using Diffie-Hellman and RSA. The user will receive a user ID for future logins. An OTP will be created once the user enters their user ID during the login process. The hash of the created final password, which is equal to OTP + Key K, will be shared by the user. This will also beverifiedon theprovider's end. The usercan exchangedataduringthedatatransmission phase aftersuccessfullyloggingin.Theuserwillcreate astringandusetheotherparty'spublickeytoshareitin encrypted form. The shared key K will be added to the string to generate the final string. The symmetric key for AES encryption will be generated using the final string. Following its generation, the symmetric key is used to transmit encrypted data and decode it on the provider's end [17].

Rajesh Bingu et.al (2024) - The authors are introduced. Due to the enormous growth in the cloud computingenvironment,manycloudusers wanttosharetheirdatawithseverallusersandoutsourceittoa distant place. One popular method for organising data is the hierarchical model. When sensitive data is stored in this way, it is very difficult to ensure the data's integrity, privacy, and secrecy as well as the model's structure. The goal of this project is to provide a hierarchical approach for ensuring information security and privacy during data exchange. Over the rooted hierarchical graph structure, symmetric encryption is used using the constructive hierarchical data sharing (CHDS) technique. Incoming data characteristics are handled by the hierarchical graph model to ensure the model's confidentiality and legitimacy. The suggested CHDS is renowned for being open, safe, and self-assured in public settings basedonthisconcept.Performanceindicatorssuchasexecutiontime,predictionaccuracy,computational complexity,andkeygenerationareassessedhere.Whenthehierarchicalmodelexpandstoalargernumber

ofsiblings,edges,andvertices,theresultsofferthesecurityofthemulti-partyenvironmentwithout sacrificing reasonable resources [18].

Table-1CompressionTableofDifferentMethod

Name of Publisher	Year	Title	Algorithm	Result
Xiuqing Lu, ZhenkuanPan and Hequn	2020	Secure approach to sharing digitizedmedical data in a cloud environment	DataEnc,TagGen and In terEnc.	Theschemerealizesefficient integrity verification before DR shares the data to avoid incorrect computation.
Sakshi Chhabra, Ashutosh KumarSingh	December 2020	Security and privacy preservationusing constructive hierarchical data-sharing approach in cloud environment	Distribution Algorithm,Reconstruction Algorithm	The is introduced with theoretical models to more accurately quantify and explaintheproblemofsecret keysharing, especially when more participants are present in different locations with varied mechanisms of safeguards.
MArumugam, S Deepa , G Arun, P Sathishkumar4 andK Jeevanantham	2021	Cloudcomputing security issues and challenges	LDSS-RSA algorithm	Ourproposedmodelprovided the benefits and electiveness of security in cloud computing. The proposed model solves the issue ofbal-ancing between security and usability.
Amr M. Sauber, PassentM.El-Kafrawy,Amr F.Shawish, MohamedA. Amin, and IsmailM. Hagag	24 November 2021	Anefficientand secure data sharing scheme for mobile devicesincloud computing	AESalgorithmand asymmetric encryption (RSA algorithm).	The efficiency of this approach lies in its ability to seamlessly secure, manage, and optimize multicolor environments while ensuring consistent operations and communicationacrossdiverse infrastructures.
P.Ramesh Naidu, N.Guruprasad, Dankan Gowda. V3	2021	Security Enhancementin Cloud Environment using Secure Secret Key Sharing	SingletoMulti-Clouds	It can be observed that the proposed SADS-Cloud technique produces higher efficiencyamongtheother previous securityschemes.
Uma Narayana VarghesePaul	June2022	Securedata sharingformobile cloud	SHA3hashing algorithm	SHA-3hashingalgorithm provideshighefficiencywith strong security, resistance to

andShelbi Joseph		computingusing RSA		attacks, and fast cryptographicperformance.
Mustafa Azeez AL Mayyahi,Seyed Amin HosseiniSeno	5/12/2022	A New Secure Model for Data Protection over Cloud Computing	Attribute-based encryption(ABE) with step FCM-based algorithm	Developed the privacy-preservingcloudassisted mobilemultimedia(PPCMM) technique, which is a cloud-basedmobilemultimediadata access control scheme. This approach has also taken into account the privacy policy and efficiency of online encryption and decryption.
V. Rajkumar,, M.Prakash and V. Vennila	28 May 2022	A High-Availabilityand Integrity Layer for Cloud Storage, Cloud Computing Security: From SingletoMulti-Clouds	SIPSmethodology	The results infer that the proposedSIPSmethodology canbeimplementedincloud for secure data sharing. In future, the proposed model can be incorporated in real time application areas. Besides,thepresentedmodel canbeextendedtotheuseof light weight cryptographic techniques.
WenfangZhang,HengJiao, ZhuoqunYan, Xiaomin Wang, Muhammad KhurramKhan	February 2023	A novel system architecture for secure authenticationand data sharing in cloudenabledBig Data Environment	AESalgorithmand asymmetric encryption (RSA algorithm).	AES offers fast and secure dataencryption,whileRSA ensures reliable key exchange, creatinga strong andaccuratefoundationfor secure communication.
HaowenTan	2022	A Security and Privacy Aware Computing ApproachonData Sharing in Cloud Environment	Computing-based IoT	Insteadofsendingthekeying message to each device individually, EI sends out a single broadcast to all devices, making key distribution more efficient.
Tarek Ali, Mohammed AlKhalidi& Rabab Al-Zaidi	29 Mar 2024	Secure Data Sharing with Confidentiality, Integrity and AccessControlin Cloud Environment	AESalgorithm	The study highlights OCTAVEAllegroasthemost accurateandefficientsecurity risk assessment method for cloud computing, ensuring robust data protection with a systematic risk mitigation approach.

Y. Kiran Kuma, , R. Mahammad Shafi	2019	Security analysis andimprovement of a public auditing scheme for secure data storageinfog-to-cloud computing	RSA algorithm	TheModifiedRSA(MDSA) algorithm enhances security with higher key generation time, while maintaining comparable encryption efficiency at lower bit Lengths but increasing computationalcostathigher bit lengths.
A.Sahaiand B.Waters	2015	A secure sharing control framework supportingelastic mobile cloud computing	Fuzzy Identity BasedEncryption	Fuzzy Identity-Based Encryption achieves efficiencybyensuringthatthe number of group elements in public parameters, private keys, and ciphertexts grows linearly with the number of attributes, minimizing computational complexity.
K.Emura,A. Miyaji, A. Nomura, K. Omote, and M. Soshi,	2009	An efficient IoT groupassociation and data sharing mechanism in edge computing paradigm	Attribute-Based Encryption(ABE)	Theaccuracyoftheproposed CP ABE scheme with constant cipher text lengthand pairing computations can beevaluatedbythesuccessful decryptionrateofciphertexts corresponding to specific attributes and access structures.
Priya Singh, GauravTyagi	2024	Advancingcloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing	AES(advanced encryption standard)	The hybrid security approach enhances cloud data transmission by integrating AES encryption, RSA and Diffie-Hellmankeyexchange, and OTP for improved privacy, secure key sharing, and user authentication.

III. SecurityIssues &Risks of Cloud Computing

Organizations must handle the many security threats and concerns brought about by cloud computing in order to safeguard their systems and data. Data breaches are a significant worry as hackers may target privatedatakeptoncloudservers.Criticaldatamaypotentiallybeexposedbyunauthorizedaccessbrought onbyshoddyauthenticationorincorrectlyconfiguredcloudsettings.Furthermore,ransomwareandother assaults,devicemalfunctions,andinadvertentdeletionscanallresultindataloss.Lackofcontroloverdata isanotherissue,ascloudcompanieshandleinfrastructure,makingregulatorycompliancedifficult.Security flaws are exacerbated by insider threats, in which staff members or outside suppliers abuse their access.

Because several users use the same infrastructure, multi-tenancyin cloud settings increases the danger of cross-tenantattacksanddataleaks.Organizationsmustuserobustauthenticationmethodslikemulti-factor authentication (MFA) since inadequate identity and access management (IAM) might result in unwanted access. Because various nations have different data protection rules, there are additional compliance and legal difficulties that might emerge from keeping data on foreign cloud servers.

Sincecloudoutages,whetherbroughtonbycyberattacks,naturaldisasters,orproviderfailures,mayhave a major impact on corporate operations, data availability and dependability are also issues. Furthermore, insufficient software upgrades and security fixes might leave cloud services vulnerable, opening them up to hacker exploitation. Businesses should create strong incident response plans, carry out in-depth risk assessments, and collaborate closely with reliable cloud service providers to make sure security policies meet industry requirements in order to overcome these obstacles. Organizations may take advantage of cloud computing advantages while keeping a solid security posture by proactively addressing these concerns.

Securityissues andchallenges

Heightenedsecuritythreatsmustbeovercomeinordertobenefitfullyfromthisnewcomputingparadigm. Some security concerns are listed and discussed below [16]:

1) Security concern #1: Because the cloud model shares computer resources with other businesses, physical security is lost. neither awareness nor authority over the location of the resources..
2) Security concern #2: The business broke the law, which increases the possibility that the (foreign) government may seize its data.
3) Securityconcern#3:Ifacustomerchoosestoswitchbetweencloudproviders,storageservicesoffered byonemaynotbecompatiblewiththoseofferedbyanother(forexample,GoogleCloudandMicrosoft Cloud are incompatible).
4) Securityconcern#4:Whoisinchargeoftheencryptionanddecryptionkeys?Itshouldlogicallybethe client.
5) Security concern #5: Ensuring the integrity of data (transmission, storage, and retrieval) actually impliesthatonlyauthorisedtransactionscauseittochange.Thereisn'tcurrentlyastandardisedstandard to guarantee data integrity
6) Security concern #6: Security problem #6: Security managers and regulators must get data logs in accordance with the Payment Card Industry Data Security Standard (PCI DSS).
7) Securityconcern #7:Toensuretheirsafety, users need tobe informedabout application updates.
8) Security concern #8: Security risk #8: Certain banking authorities mandate that customers' financial information stayin their nation of residence, while other government rules place stringent restrictions on what information about their residents may be kept and for how long.
9) Security concern #9: Because virtual computers are dynamic and fluid, it will be challenging to maintain security consistency and guarantee record auditability.
10) Security concern #10: Security issue #10: If customers' privacy rights are infringed, they may be able to sue cloud service providers; also, the providers may suffer reputational harm. People become concernedwhentheydon'tunderstandwhytheirpersonalinformationisbeingaskedfororhowitwill be used or shared with other parties.

IV. AlgorithmsUsed

1. AES(AdvancedEncryptionStandard):Asymmetrickeyencryptionalgorithmknownforitsspeedand strong security. It uses a 256-bit key and a 16-byte initialization vector (IV) in this implementation. AES provides robust protection against brute force attacks and is widelyused for encryptingsensitive data.
2. Blowfish: A block cipher that operates on 64-bit blocks, using a variable-length key up to 448 bits. It is efficient and secure for various applications. In this project, Blowfish is paired with an 8-byte IV.
3. Triple DES (3DES): An enhanced version of the DES algorithm, applying encryption three times to each data block for improved security. It uses a 192-bit key and an 8-byte IV.
4. IDEA (International Data Encryption Algorithm): A symmetric key block cipher that operates on 64-bit blocks with a 128-bit key. Known for its simplicity and strong encryption, it provides secure data protection in this scheme.
5. Fernet:Ahigh-levelsymmetricencryptionsystem fromthecryptographylibrary,designedforease of use and strong encryption. It handles key management and encryption internally, ensuring reliable security.

By utilizing these algorithms in parallel, the system ensures that even if one algorithm were to be compromised, the remaining parts of the file would remain secure. This approach leverages the strengths of each algorithm, creating a layered security mechanism.

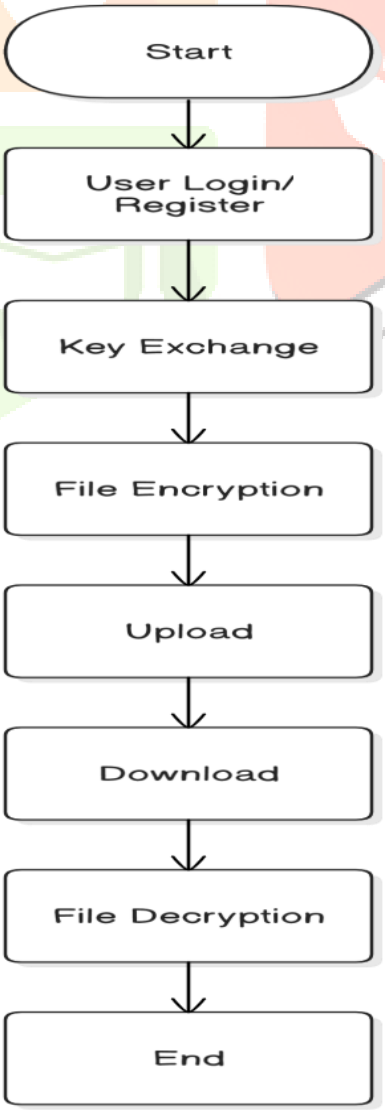

Fig2SecureFileSharing UsingCloud-FlowDiagram

V. CONCLUTION

Because of the dangers of illegal access, data breaches, and privacy violations, cloud computing data sharingsecuritycontinuestobeamajorconcern.Toimprovesecurity,anumberofcryptographicstrategies havebeeninvestigated,suchasblockchaintechnology,accesscontrolsystems,andencryption.However, maintaining safe and effective data exchange necessitates striking a balance between performance, usability, and security. Future studies should concentrate on creating stronger security frameworks, including AI to identify risks, and tackling new issues like the dangers posed by quantum computing. To establishtrustandguaranteetheconfidentiality,integrity,andavailabilityofshareddataincloudsettings, athoroughstrategyincorporatingcutting-edgesecuritymodels,regulatorycompliance,anduserawareness is necessary.

REFERENCES

[1] Kukatlapalli Pradeep,Kumar , Boppuru,Rudra Prathap , Michae,Moses Thiruthuvanathan , Hari Murthy,VinayJhaPillai“Secureapproachtosharingdigitizedmedicaldatainacloudenvironment” Volume 7, Issue 2, June 2024, Pages 108-118.

[2] Rajesh Bingu “Security and privacy preservation using constructive hierarchical data-sharing approachincloudenvironment”InformationSecurityJournal:AGlobalPerspectiveVolume33,2024 -Issue1,17Oct2024,https://doi.org/10.1080/19393555.2022.2128942.

[3] KrešimirPopović,ŽeljkoHocenski“Cloudcomputingsecurityissuesandchallenges”KnezaTrpimira 2b, Osijek, 31000, Croatia, June 2010, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/224162841.

[4] XiuqingLu,ZhenkuanPanandHequnXian“Anefficientandsecuredatasharingschemeformobile devices in cloudcomputing” 23 October 2020,number: 60 ,Journal of Cloud Computing Springer Open, https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-020-00207-5.

[5] Sakshi Chhabra,and Ashutosh Kumar Singh “Security Enhancement in Cloud Environmentusing Secure Secret Key Sharing” OurnalOf Communications Software And Systems, Vol. 16, No. 4, December 2020, (DOI): 10.24138/jcomss.v16i3.964.

[6] M Arumugam, S Deepa , G Arun, P Sathishkumar and K Jeevanantham “Secure data sharing for mobile cloud computing using RSA” IOP Conference Series: Materials Science and Engineering,l 2021 IOP Conf. Ser.: Mater. Sci. Eng. 1055 012108,doi:10.1088/1757-899X/1055/1/012108.

[7] AmrM.Sauber,PassentM.El-Kafrawy,AmrF.Shawish,MohamedA.Amin,andIsmailM.Hagag “A New Secure Model for Data Protection over Cloud Computing” Hindawi Computational Intelligence and Neuroscience Volume 2021, Article ID 8113253, 11 pages,24 November 2021.

[8] P.RameshNaidu,N.Guruprasad,DankanGowda.V3“AHigh-AvailabilityandIntegrityLayerfor CloudStorage, Cloud Computing Security: From Single toMulti-Clouds” Journal of Physics: Conference Series 1921 (2021) 012072,Journal of Physics: Conference Series ,ICASSCT 2021,doi:10.1088/1742-6596/1921/1/012072.

[9] Uma Narayanan ,Varghese Paul andShelbi Joseph “A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment” Journal of King Saud University – Computer and Information Sciences 34 (2022) 3121–3135 .Volume 34, Issue 6, Part B, June2022, Pages3121-3135, https://doi.org/10.1016/j.jksuci.2020.05.005.

[10] Mustafa Azeez ALMayyahi,Seyed Amin Hosseini Seno “A Securityand PrivacyAware Computing Approach on Data Sharing in Cloud Environment” 2022, 19(6): 1572-1580,Baghdad Science Journal,E-ISSN: 2411-7986,DOI: https://dx.doi.org/10.21123/bsj.2022.7077.

[11] V. Rajkumar,, M. Prakashand V. Vennila "Secure Data Sharing with Confidentiality, Integrity and AccessControl in Cloud Environment" Tech SciencePress,28 May 2022, Vol.40,No.2,2022, DOI:10.32604/csse. 2022.019622.

[12] Wenfang Zhang , HengJiao, Zhuoqun Yan , Xiaomin Wang,Muhammad Khurram Khan "Security analysis and improvement of a public auditing scheme for secure data storage in fog-to-cloud computing" Volume 125,103019,February 2023, ELSEVIER Journal

[13] Aws Hamed Hamad, Adnan Yousif Dawod, Mohammed Fakhrulddin Abdulqader, Israa Al_Barazanchi, Hassan Muwafaq Gheni "A secure sharing control framework supporting elastic mobilecloudcomputing"InternationalJournalofElectricalandComputerEngineering(IJECE)Vol. 13, No. 2, April 2023, pp. 2270~2277 ISSN: 2088-8708, DOI: 10.11591/ijece.v13i2.pp2270-2277.

[14] Haowen Tan "An efficient IoT group association and data sharing mechanism in edge computing paradigm" 5 July 2022 ,: http://www.keaipublishing.com/en/journals/cyber-security-and-applications,Cyber Security and Applications,https://doi.org/10.1016/j.csa.2022.100003.

[15] SijjadAli,ShuaibAhmedWadho,AunYichiet,MingLeeGan, ChenKangLee"Advancingcloud security:Unveilingtheprotectivepotentialofhomomorphicsecretsharinginsecurecloudcomputing" https://doi.org/10.1016/j.eij.2024.100519.

[16] TarekAli,MohammedAl-Khalidi&RababAl-Zaidi"InformationSecurityRiskAssessmentMethods in Cloud Computing" Journal of Computer Information Systems,: 29 Mar 2024, https://doi.org/10.1080/08874417.2024.2329985.

[17] Priya Singh, Gaurav Tyagi "A New Hybrid Approach For Key And Data Exchange In Cloud Computing"2024, 30(5), 11645-11650,Educational Administration: Theory and Practice,2024,Doi: 10.53555/kuey.v30i5.4989.

[18] Dr.NikhatAkhtar,Dr.BedineKerim,Dr.YusufPerwej,Dr.AnuragTiwari,Dr.SheebaPraveen"A ComprehensiveOverviewofPrivacyandDataSecurityforCloud Storage"Copyright: ©theauthor(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the termsof the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercialuse, distribution, and reproduction in any medium, provided the original work is properly cited International Journal of Scientific Research in Science, Engineering and Technology Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com) doi : https://doi.org/10.32628/IJSRSET21852.

[19] Hu, Y., Kumar, S. and Popa, R.A., 2020,Ghostor: Toward a secure data-sharing system fromdecentralized trust,in 17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20), pp. 851-877.

[20] Gutte,P.,Wankhade,J.V.andMote,S.,2020,KeyGeneration&AccessControlPolicyinCloudData Sharing, (No. 2562). EasyChair.

[21] Hidayat,T.andMahardiko,R.,2020.ASystematicLiteratureReviewMethodOnAESAlgorithmfor Data Sharing Encryption On Cloud Computing. International Journal of Artificial Intelligence Research, 4(1).

[22] Kumar, Y.K. and Shafi, R.M., 2020,An efficient and secure data storage in cloud computing using modifiedRSApublickeycryptosystem,InternationalJournalofElectricalandComputerEngineering, 10(1), p.530.

[23] P. P.Kumar, P. S.Kumar, and P. J. A. Alphonse, "Attribute based encryption in cloud computing:Asurvey, gap analysis, and future directions," J. Netw. Comput. Appl., vol. 108, pp. 37–52, 2018.

[24] A. Sahai and B. Waters, "Fuzzy identitybased encryption," in Proc. 24th Annu. Int. Conf. Theory Applications Cryptographic Techn., May 2005, vol. LNCS 3494, 2015, pp. 457–473.

[25] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. Inf. Security Practice Experience,Apr. 2009, pp. 13– 23.

[26] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[27] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1256–1277, Jun. 2016. [6] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. 30thAnnu.Int.Conf.TheoryAppl.CryptographicTechn.:AdvancesCryptology,May2011,pp.568– 588.

[28] B.Waters,"Dualsystemencryption:RealizingfullysecureIBEandHIBEundersimpleassumptions," in Proc. 29th Annu. Int. Cryptology Conf. Advances Cryptology, Aug. 2009, pp. 619– 636.

[29] T.Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partiallyhidden encryptor-specifiedaccessstructures,"inProc.Appl.Cryptogr.Netw.Security,Jun.2008,vol.LNCS5037,pp. 111–129.

[30] J. Lai, X. Zhou, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding CP-ABE," in Proc. 6th ACM Symp. Inf. Comput. Commun. Secur., 2011, pp. 24–39.