International Research Journal of Multidisciplinary Sciences ISSN:AWAITED
VOL-1 ISSUE-7 July 2025 PP:11-24

SeekDrive: Web-Based Security and Storage

[1]Bhawna Kaushik, [2]Yazdani Hasan
1.bhawna.kaushik@niu.edu.in, NoidaInternationalUniversity
2.yazhassid@gmail.com, NoidaInternationalUniversity

Abstract

MiniDrive is a web-based cloud storage application developed to provide a secure and user- friendly platform for managing personal files. The system, built using PHP and MySQL, incorporates file encryption and decryption features to enhance data confidentiality and protect user privacy. Key functionalities include user registration, secure authentication, encrypted file uploads,downloads,andfiledeletion,allmanagedthroughsessioncontrol.Thesystemwastested in a local XAMPP environment and is designed to be lightweight and easy to deploy for small- scale use. This project demonstrates the practical application of web development, cybersecurity principles, and database management to solve real-world data storage challenges. It also lays a foundation for future enhancements, such as cloud integration, advanced user roles, and scalable storage capabilities.

Keywords: *Secured Storage, Cloud Storage, Web Base Storage, Storage Application, Cloud Computing, Web Base Application*

1.0 Introduction

The rapid evolution of digital technology has precipitated an unprecedented demand for secure, efficient,andaffordabledatastoragesolutions.Traditionalstoragemethodsareincreasinglybeing supplanted by scalable, cloud-based alternatives that promise improved accessibility and managementcapabilities.However,thesesolutionsoftenharborsignificantsecurityvulnerabilities andincurrecurringsubscriptionfees,whichcanposeanongoingfinancialburdenonusers(Mann, 2022;Guoetal.,2018;Vengalaetal.,2021).Forexample,prominentplatformssuchasDropbox and Google Drive offer advantages in scalability and ease of use, but they simultaneously raise critical concerns about data privacy and usercontrol, particularly regarding sensitive information stored on their servers (Guo et al., 2018; Vengala et al., 2021).

In contrast, MiniDrive provides a compelling alternative by offering a secure, web-based file storageapplicationthatemphasizesusercontrolandprivacy.Byallowinguserstoupload,encrypt,

and store files locally without the need for monthly subscriptions, MiniDrive addresses the dual challenge of securing personal data while mitigating continuous expenses associated with traditional cloud services (Singh, 2024). The importance of encryption in safeguarding sensitive information is well-documented, with access control mechanisms employed on encrypted data to regulate who can view or manipulate stored files (Gupta et al., 2023). The Advanced Encryption Standard (AES), for instance, has emerged as a preferred encryption method due to its resilience against various attacks, including man-in-the-middle scenarios (Zainudin et al., 2022).

Moreover, emerging technologies are facilitating innovative storage solutions that harness distributedanddecentralizedstoragearchitectures.Researchindicatesthatblockchaintechnology cansignificantlyenhancedataintegrityandsecuritythroughitsimmutableandtransparentnature, effectively protecting against unauthorized access (Meng & Sun, 2022). Gupta et al. highlighted the role of decentralized systems in inherently reducing risks associated with centralized data storage, such as data breaches and loss (Gupta et al., 2023). This perspective aligns with the operational framework of MiniDrive, which emphasizes localized data storage to provide users with complete control over their files and minimize the risk of unauthorized third-party intervention (Vengala et al., 2021; Meng & Sun, 2022).

Theshifttowardscloudstoragesolutionsreflectsboththenecessityandthechallengesassociated withdatamanagementinthedigitalage.MiniDrive'smodel,combininglocalstoragewithrobust encryption protocols, serves as a promising alternative, ensuring that users maintain control over their sensitive information without the burdensome costs typically associated with commercial cloudservices.Theintegrationofadvancedencryptiontechniquesanddecentralizedarchitectures will further strengthen data security and user confidence in these emerging storage solutions.

Theproliferation ofdigital datahas necessitated thedevelopment ofsecure, user-friendly storage systems that prioritize data privacy and accessibility. This seeks to establish a localhost storage solution that emphasizes robust security measures, particularly through the use of symmetric encryption, while ensuring that users can manage their files easily. Encryption serves as the cornerstone of this project, safeguarding user data against unauthorized access. Symmetric encryption,whichinvolvesasinglekeyforbothencryptionanddecryption,hasgarneredattention foritsefficiencyandeffectivenessinprotectingsensitiveinformation(Gudimetla,2024;Dworkin, 2023). For instance, the Advanced Encryption Standard (AES) is a widely adopted symmetric algorithm recognized for its reliability in securing data against various types of cyberattacks (Dworkin, 2023).

Moreover, the project aims to offer a free storage alternative, liberating users from the recurrent coststypicallyassociatedwithcloudserviceswhileenhancingdataagency.Itiscriticaltointegrate HTTPS protocols into the system to fortify security during file transfers, thereby preventing eavesdropping and man-in-the-middle attacks, which are prevalent threats in data transmission (Wu,2023).Theemphasisonauser-friendlyinterfaceisequallyimportant,asitfacilitates

seamlessfilemanagementpractices,allowinguserstoupload,organize,andretrievefileswithout a steep learning curve. Effective user interfaces greatly enhance interaction with digital storage systems, thuspromotingboth accessibility and user satisfaction (Pijnenburg & Poettering, 2020).

Theincorporationofsymmetricencryptiontechniquesensuresthatdataremainsconfidentialatall junctures, addressing a significant concern for users who handle sensitive material. Additionally, the application of hashing methods, such as those illustrated by Lai and Heng, further bolsters security by verifying the integrity of data before and after the encryption process (Lai & Heng, 2022). This multi-faceted approach to data protection not only addresses concerns regarding unauthorized access but also enhances the overall robustness of the security framework by providing a layered defence against potential threats.

The objective of this localhost storage system is to establish a secure and accessible solution that leverages symmetric encryption for data protection, integrates HTTPS for secure transfers, and supportsanintuitiveuserinterfaceforeasyfilemanagement.Thisinitiativerepresentsasignificant step towards empowering users with control over their data in a cost-effective manner, ensuring privacy and security in an increasingly digital landscape.

2.0 LiteratureReview

ThedevelopmentofMiniDriveasasecureandcost-effectiveweb-basedcloudstorageapplication isinformedbyananalysisoftheexistingcloudstoragelandscape.Thisreviewdrawsuponvarious studies, industry reports, and assessments of popular platforms to identify user needs, technologicaltrends,andmarketopportunities.Keyfindingsindicatethatusersprioritizeattributes such as data security, system reliability, affordability, and user-friendliness.

Data security is a primary concern for users engaging with cloud storage solutions. As noted by Salam et al., the security of user data in cloud environments is critical, particularly given vulnerabilities associated with unauthorized access and data breaches Salam et al. (2015). Encryption techniques, including attribute-based encryption (ABE), are highlighted as effective strategiesforensuringdatasecurity,astheyofferfine-grainedaccesscontrol(Wangetal.,2018). Additionally,techniqueslikesearchablesymmetricencryption(SSE)facilitatesecurequeryingof encrypted data, balancing the need forprivacy with practical data retrieval (Alyousif et al., 2023; Poh et al., 2017).

Reliabilityisanothercriticalattributevaluedbyusers.Dutcheretal.discusshowtheevolutionof cloud storage capabilities has improved the resilience and efficiency of these systems, showing a positive trend in maintaining data integrity and availability even during service disruptions (Dutcher et al., 2024). A robust solutionlike MiniDrive aims to leverage this reliabilityto ensure consistent performance without risking user data.

Affordabilityisacrucialfactor,asmanyusersaredeterredbythesubscriptionfeesassociatedwith

commercialcloudservices.Providingafreeorlow-coststoragesolutionnotonlyattractsabroader userbase but also enhances accessibility forindividuals and organizations that maystrugglewith traditional cloud costs (Yang et al., 2020). Existing studies emphasize the need for creating cost-effective alternatives that maintain essential security features (Song & Zhou, 2025).

Moreover, user-friendliness is imperative for improving the overall user experience and ensuring thatindividualscaneasilymanagetheirfiles. Anintuitiveinterface cansignificantlyenhancefile management, allowing users to upload, organize, and retrieve their documents with minimal technical knowledge (Pijnenburg & Poettering, 2020). Research indicates that the efficiency of a cloud storage application often hinges on its ease of use, which directly influences user engagement and satisfaction (Liu et al., 2015).

TheEvolvingLandscapeofCloudStorage

The rapidly evolving landscape of cloud storage has been influenced significantly by the proliferation of cloud computing technologies. Major platforms such as Google Drive, Dropbox, and Microsoft OneDrive provide users with the convenience of storing, accessing, and sharing dataremotely,utilizingtheinfrastructureofthird-partyserviceproviders. Thisshiftencompasses a range of benefits, such as enhanced accessibility and flexibility, which enable users to manage dataacrossvariousdevicesseamlessly(Kusumawardhani&Masyithah,2019;Zhou,2024).Cloud storage is achieving ubiquity in modern data management, effectively reducing the constraints imposed by traditional local storage methods (Kusumawardhani & Masyithah, 2019).

However, this widespread adoption is concomitant with escalating concerns about data privacy andsecurity.Researchindicatesthatusersharborapprehensionsregardingthestorageofsensitive data on external servers run by third-party entities (Petrovčič et al., 2022; Shen et al., 2019). The inherent risks associated with such reliance are highlighted by the fact that many of these cloud servicesutilizeserver-sideencryption.Whilethisaddsalayerofsecurity,thecriticalissueremains that service providers typically hold encryption keys, thereby creating potential pathways for unauthorized access by employees, governmental agencies, or malicious actors (Mohammed & Abed, 2019; Aguru et al., 2024). As stated in several studies, this reliance on centralized control undermines users' trust, as they risk losing physical control over their data once uploaded to the cloud (Shen et al., 2019; Guo et al., 2023).

Furthermore, despite advancements in security measures, such as encryption and data integrity auditing, the lack of robust end-to-end encryption schemes represents a significant vulnerability (Li et al., 2019). In such frameworks, data is ideally encrypted at the user's device and remains encrypted throughout its transmission and while stored on the cloud; however, many existing services do not provide this assurance (Li et al., 2019). Consequently, the implementation of improvedsecurityprotocols,includingdecentralizedsolutionslikeblockchain,hasbeenproposed to enhance data governance and trustworthiness within the cloud storage landscape (Aguru et al., 2024;Guoetal.,2023;Reddy&Rao,2018).Notably,theintegrationofadvancedfeatureslike

identity-based auditing has emerged as a promising direction for fostering data security and integrity (Li et al., 2019; Shen et al., 2019).

SecurityasaPrimaryConcern:TheCaseforZero-Knowledge Encryption

The contemporary discourse on data privacy emphasizes the essential role of zero-knowledge encryption (ZKE) as a pivotal mechanism in cloud storage security. A systematic review of the literature reveals a compelling consensus on ZKE being an important method for safeguarding userdata.Thisencryptionparadigmensuresthatthecloudserviceproviderhas"zeroknowledge" oftheuser's data, as the processes for encryption and decryption occur exclusively on theclient's device. Such an approach fundamentally contrasts with prevailing practices in mainstream cloud storage solutions that commonly implement server-side encryption. In these systems, providers retain the ability to decrypt and access user data, raising significant privacy concerns (Maffei et al., 2015; Egorov & Wilkison, 2016).

ZKE guarantees that even the service provider, which is often a third-party entity, cannot access or view the files stored by users. This assurance addresses the critical trust gap that exists when users store sensitive or personal data in cloud environments (Hagen & Lucia, 2021). The architecture of platforms employing ZKE, such as ZeroDB, prioritizes security by employing client-side encryption. By doing this, they empower users with complete control over their data and directly confront the prevailing apprehensions regarding privacy in the digital marketplace (Egorov & Wilkison, 2016; Jeong et al., 2023).

Additionally,theliteratureemphasizesthatwhileserver-sideencryptioncanprovideameasureof security,itlacksthedepthofassurancefoundinZKEframeworks.Forinstance,recentdiscussions surroundingdecentralizedmodelsforsecuredatasharing, particularlyincontextssuchasvehicular networks, highlight ZKE’s potential role in facilitating security and scalability (Majigi et al., 2023). The application of ZKE within such frameworks not only fortifies data confidentiality but alsoensuresthatoperationalcorrectnesscanbeattestedwithoutexposingunderlyingdata,thereby reinforcing user privacy (Ma & Li, 2024).

Moreover, ZKE has also been highlighted in the context of emerging technologies, including its integration with blockchain systems where it serves to securely validate transactions and authenticate users while maintaining data confidentiality. Such developments illustrate the growing relevance and adaptability of zero-knowledge proofs across diverse applications within cloud storage and beyond (Jeong et al., 2023; Kumar & Goyal, 2024). As technology evolves, incorporating ZKE into data storage and management systems emerges as a crucial step in advancing the overall security landscape, allowing users to retain agency over their own data (Egorov & Wilkison, 2016; Li, 2022).

AddressingUsabilityandCost-Effectiveness

The discourse surrounding cloud storage increasingly recognizes that usability and cost-effectiveness are paramount considerations, alongside security. The literature emphasizes the advantages of modular architectures and decentralized systems in promoting flexible, scalable designs that can be easily updated and maintained. Such architectures typically contrast with the monolithic structures prevalent in many legacy systems, which can be cumbersome and less adaptabletouserneeds(Yadavetal.,2019;Wang,2024).Themodularityinherentindecentralized systems allowsfortailored solutions that can scaleefficiently as userdemands grow, leading to a better overall user experience.

User feedback consistently highlights that while many cloud storage services offer convenience and an array of features, the pricing structures can often be prohibitively expensive for both individualsandsmallbusinesses(Huangetal.,2022).Thisbecomesparticularlyproblematicwhen considering the cost-per-gigabyte, as many commercial providers charge rates for additional storage that do not reflect the actual cost of providing that capacity. Such pricing strategies can discourage users who require substantial data storage but are unwilling or unable to pay for enterprise-level features that they do not utilize (Huang et al., 2022; Cao et al., 2018).

In terms of usability, researchers have pointed out the importance of user-friendly interfaces and intuitive design in enhancing the overall user experience (Ramachandran et al., 2023). As cloud storage solutions evolve, providers must prioritize usability by ensuring that users can easily manage their data without needing extensive technical knowledge. Additionally, the introduction of more transparent pricing models, such as dynamic pricing that reflects actual usage levels not just fixed costs could improve accessibility for a broader range of users (Cao et al., 2018). By structuring pricing around resource consumption and user needs, cloud storage providers can create value for users while also enhancing their market competitiveness.

Furthermore, as various stakeholders, including businesses and individual users, seek ways to optimize their cloud expenditures against costs, flexible solutions become increasingly vital (Xu etal.,2022).Forinstance,heuristicalgorithmsthatprioritizecost-effectivenessinmulti-clouddata placementhighlighttheneedforstrategicapproachestomanageexpensesrelatedtocloudstorage, therebyfacilitatinggreateraccessibilityandoptimalresourceallocationforusers(Xuetal.,2022; Tricomi et al., 2020).

Addressing these elements is essential not only for maximizing the usability of cloud storage systems but also for ensuring that they remain economically viable options for all users. The balancebetweenusability,security,andcost-effectivenessiscriticalinshapingthefutureofcloud storage and determining how effectively it can serve diverse user needs.

AnalysisofExistingPlatforms:Gapsand Opportunities

A thorough analysis of leading cloud storage platforms, specifically Google Drive and Dropbox, hasidentifiedseveralcriticallimitationsthattheemergingMiniDriveaimstoaddress.Theexisting

solutionsexhibitsignificantgaps,particularlyintherealmofprivacy,cost-effectiveness,anduser interface intuitiveness.

One of the most notable deficiencies in mainstream platforms is the lack of true zero-knowledge encryption (ZKE). Despite robust security measures, both Google Drive and Dropbox do not defaulttoazero-knowledgeencryptionmodel,whichwouldensurethatonlyusershaveaccessto their encrypted data, thereby reducing the risk of provider access or data breaches Tian et al. (2019). This situation creates a substantial market opportunity for MiniDrive to attract privacy-conscious users who demand complete control over their data.

Highcostsassociatedwithdatastorageareanothercriticalfactorinfluencingusersatisfaction.The tiered pricing models employed by established providers can become expensive, especially for users requiring significant storage capacity without a corresponding need for the full suite of integrated services. Many individuals and smaller businesses find themselves deterred by the financialburdenimposedbyexistingmodels,whichdonotefficientlyaddresstheirstorageneeds (Abdoetal.,2024).MiniDriveaimstoprovideamoreaffordableandtransparentpricingstructure, catering specifically to this underserved demographic.

Another limitation is the cumbersome file-sharing models that existing services utilize. While sharingcapabilitiesareintegral,theyoftenlackfine-grainedcontrol,makingthemchallengingfor non-technicalusers who struggle with managing permissions and revoking access (Samy & Mary, 2022). This highlights yet another opportunity for MiniDrive to enhance user experience by streamlining sharing processes and providing intuitive tools for access management.

The architecture of MiniDrive is designed with these insights in mind. The system adopts a security-firstapproach,incorporatingmandatory client-sideencryption.Thisarchitectureensures that data is encrypted locally on the user's device before being uploaded to the server, which not only enhances security but also empowers users with greater control (Li, 2021). Additionally, MiniDriveseekstoincorporateahighlyadaptableanduser-friendlyinterface,addressingcommon usability problems found with current cloud platforms.

3.0 Methodology

The development of MiniDrive emphasizes the importance of implementing Agile methodology and a Prototyping model to ensure a structured, user-centered process. The Agile approach facilitates rapid prototyping and continuous user feedback, vital for adapting to user needs and expectationsthroughoutthedevelopmentcycleIvanovićetal.(2016).CoupledwithaPrototyping model, which enhances clarity surrounding user requirements at each development stage, MiniDrive ensures that both functional and non-functional requirements are met with precision.

FunctionalrequirementsforMiniDriveincludesecureuserlogin,fileuploads,fileencryption,and auser-friendlyinterface,whichare foundational forcreatingareliablecloud storagesolution. Non-

functionalrequirementscovercriticalaspectslikesecurity,usability,performance,compatibility, andmaintainability(Lietal.,2018).Aparticularfocusonsecurityisparamountgiventhesensitive nature of data being handled, making encryption an integral part of the architecture.

The system architecture of MiniDrive adheres to a client-server model. This model distinguishes between user interfaces tailored for end-users and administrators, enhancing the user experience byallowingsmoothnavigationandoperation(Contiuetal.,2018;Kundysetal.,2022).Tobolster security,filesareencryptedusingtheAdvancedEncryptionStandard(AES)algorithmbeforethey are stored on the server, which ensures that data remains protected from unauthorized access during transmission. Furthermore, all communications are secured using HTTPS protocols to provide a robust defense against data interception during uploads and downloads.

Moreover, this architecture considers scalability and maintainability, supporting the evolving needsofusers.Theclient-sideencryptionmodelcomplieswithbestpracticesfordatasecurityand enhances the user experience, allowing even non-technical users to easily navigate the platform and understand its functionalities (Chidambaram et al., 2020).

4.0 ResultsandAnalysis

A combination of quantitative and qualitative research was used to gather user feedback. A questionnaire was distributed to 11 respondents, revealing a high demand for a new, secure platform. Key findings from the quantitative analysis showed that most respondents consider affordability to be the most important factor in a cloud storage system. They also highlighted the importance of fast upload/download speeds and secure, password-protected file-sharing features.

Qualitative interviews provided deeper insights into user challenges. A professional user emphasized the critical need for role-based access control and file encryption for sensitive documents.Astudentuserhighlightedtheimportanceoffastuploadspeeds,cleaninterfaces,and mobile accessibility for academic purposes.

The system underwent unit and user acceptance testing. Unit testing was conducted to verify that each component, such as user login, file uploads, and downloads, functioned correctly. User acceptance testing confirmed that the system meets user expectations in terms of usability and functionality.

5.0 Conclusion

TheMiniDriveprojectaimstoaddressconcernsrelatedtodatasecurityandaffordabilityincloud storage by providing a viable alternative to existing platforms. This initiative is notable for implementing strong symmetric encryption alongside a user-friendly interface, which makes secure data management accessible for both individuals and small businesses (Xia, 2022; Yu et al.,2016).Theprojecthighlightsthepotentialtodeliverareliableandprivatestoragesolutionthat

alleviatestypicalconcernsassociatedwithconsumercloudservices.

One important feature of MiniDrive is its use of symmetric encryption, which enhances data securitywithoutsignificantlycompromisingperformance.Thisapproachiscrucialformaintaining the confidentiality of users' data while ensuring efficient access during file retrieval (Ma et al., 2016;Linetal.,2013).Byutilizingsuchencryptionmechanisms,MiniDriveaimstocomplywith rigorous security requirements and build trustamong users increasingly awareof the risks tied to cloud storage (Sheela, 2022; Liu et al., 2013).

Furthermore, affordability is a significant competitive advantage of MiniDrive. Given the high costsofmanycommercialcloudstoragesolutions,theprojectseekstocreateatransparentpricing model that is appealing to budget-conscious users. Existing platforms often adopt tiered pricing structures,whichcanbecomefinanciallyburdensome,particularlyforusersneedinglargerstorage capacities without requiring comprehensive services offered by largerproviders (Jegadeeswari et al., 2019; Yadav et al., 2019). MiniDrive's focus on delivering a cost-effective service could encourage adoption among individuals and small businesses looking for reliable storage without excess expenditures (Yadav et al., 2021).

Lookingahead,futureenhancementsforMiniDrivecouldgreatlyexpanditscapabilitiesandreach. Integration with scalable cloud infrastructure could enhance service availability and durability, ensuring users' data remains protected against outages and disruptions (Fu et al., 2014; Zhang et al., 2015). Additionally, developing cross-platform mobile applications may cater to users' growing preference for accessing data across devices a critical factor in today's mobile-oriented world(Sourietal.,2013;Tianetal.,2015).Anotherproposedadvancementincludesincorporating blockchain-based storage validation, which can further enhance data integrity through decentralized verification and bolster user confidence in the security of their stored information (Vimal, 2019).

References

Abdo, A., Karamany, T., & Yakoub, A. (2024). Enhanced data security and storage efficiency in cloud computing: a survey of data compression and encryption techniques. *FCIHIB*. https://doi.org/10.21608/fcihib.2024.263415.1107

Aguru, A., Mahadevan, R., Babu, E., Kaluri, R., Bashir, A., & Gadekallu, T. (2024). Scs: a secure cloud storageframeworkwithenhancedintegrityandauditabilityusingconsortiumblockchainsystem.*Research Square*. https://doi.org/10.21203/rs.3.rs-3926696/v1

Alyousif, A., Yassin, A., Abduljabbar, Z., & Xu, K. (2023). Improving the performance of searchable symmetric encryption by optimizing locality. *Basrah Researches Sciences*, 49(1), 102-113. https://doi.org/10.56714/bjrs.49.1.9

Cao,B., Wang, K., Xu, J.,Hou,C., Fan, J.,&Que,H.(2018). Dynamic pricing forresourceconsumption

in cloud service. *Wireless Communications and Mobile Computing*, 2018(1). https://doi.org/10.1155/2018/4263831

Chidambaram, N., Raj, P., Thenmozhi, K., & Amirtharajan, R. (2020). Advanced framework for highly secure and cloud-based storage of colour images. *Iet Image Processing*, 14(13), 3143-3153. https://doi.org/10.1049/iet-ipr.2018.5654

Contiu, S., Pires, R., Vaucher, S., Pasin, M., Felber, P., & Réveillère, L. (2018). Ibbe-sgx: cryptographic group access control using trusted execution environments., 207-218. *IEEE Xplore*. https://doi.org/10.1109/dsn.2018.00032

Dutcher, G., Azianyo, K., Dissanayake, T., & Mailewa, A. (2024). Secure cloud storage solution with "seafile" & "nextcloud": a resilient efficiency assessment. *Advances in Technology*. https://doi.org/10.31357/ait.v3i2.7341

Dworkin,M.(2023).Advancedencryptionstandard(aes).*FIPS*.https://doi.org/10.6028/nist.fips.197-upd1

Egorov, M. and Wilkison, M. (2016). Zerodb white paper. Arxiv. https://doi.org/10.48550/arxiv.1602.07168

Fu, Z., Cao, X., Wang, J., & Sun, X. (2014). Secure storage of data in cloud computing., 783-786. https://doi.org/10.1109/iih-msp.2014.199

Gudimetla, S.(2024). Data encryption in cloud storage. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/irjmets50637

Guo,x.,Xiong,z.,Chen,J.,&Chen,D.(2023).Asecure,blockchain-baseddatastorageschemeforcloud environments. https://doi.org/10.1117/12.2680904

Guo, Y., Liu, F., Cai, Z., Xiao, N., & Zhao, Z. (2018). Edge-based efficient search over encrypted data mobile cloud storage. *Sensors*, 18(4), 1189. https://doi.org/10.3390/s18041189

Gupta, R., Kanungo,P.,Dagdee, N.,Madhu, G., Sahoo, K., Jhanjhi, N.,… &AlZain,M.(2023). Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing. *Sensors*, 23(5), 2617. https://doi.org/10.3390/s23052617

Hagen, M. and Lucia, B. (2021). Practical encrypted computing for iot clients. *Arxiv*. https://doi.org/10.48550/arxiv.2103.06743

Huang, K., Zhang, X., Mu, Y., Rezaeibagha, F., Huang, X., & Gong, Y. (2022). Blockchain-based deduplication with arbitration and incentives. *Iet Information Security*, 16(6), 401-416. https://doi.org/10.1049/ise2.12066

Ivanović, M., Vidaković, M., Budimac, Z., & Mitrović, D. (2016). A scalable distributed architecture for client and server-side software agents. *Vietnam Journal of Computer Science*, 4(2), 127-137. https://doi.org/10.1007/s40595-016-0083-z

Jegadeeswari, S., Dinadayalan, P., & Gnanambigai, D. (2019). Efficient dynamic bloom filter hashing fragmentation for cloud data storage. *Cybernetics and Information Technologies*, 19(1), 53-72. https://doi.org/10.2478/cait-2019-0003

Jeong, G., Lee, N., Kim, J., & Oh, H. (2023). Azeroth: auditable zero-knowledge transactions in smart contracts. *Ieee Access*, 11, 56463-56480. https://doi.org/10.1109/access.2023.3279408

Kumar,S.andGoyal,M.(2024).Designofaniterativemethodfor blockchainoptimizationincorporating deepminer and anoblock. *Security and Privacy*, 8(1). https://doi.org/10.1002/spy2.492

Kundys, S., Havano, B., & Morozov, M. (2022). Software system for monitoring the situation in the settlement. Computer Systems and Network, 7(1), 38-45. https://doi.org/10.23939/acps2022.01.038

Kusumawardhani, D. and Masyithah, D. (2019). Security and privacy cloud storage as a personal digital archivestoragemedia.*RecordandLibraryJournal*,4(2),167.https://doi.org/10.20473/rlj.v4-i2.2018.167- 173

Lai,J.andHeng,S.(2022).Securefilestorageoncloudusinghybridcryptography.*JournalofInformatics and Web Engineering*, 1(2), 1-18. https://doi.org/10.33093/jiwe.2022.1.2.1

Li, J. (2021). Research on dynamic and secure storage of financial data based on cloud platform. *Web Intelligence*, 19(4), 263-274. https://doi.org/10.3233/web-210472

Li,J.,Wu,J.,Chen,L.,&Li,J.(2018).Deduplicationwithblockchainforsecurecloudstorage.,558-570. https://doi.org/10.1007/978-981-13-2922-7_36

Li,N.(2022).Combinationofblockchainandaiformusicintellectualpropertyprotection. *Computational Intelligence and Neuroscience*, 2022, 1-8. https://doi.org/10.1155/2022/4482217

Li,Y.,Yu,Y.,Min,G.,Susilo,W.,Ni,J.,&Choo,K.(2019).Fuzzyidentity-baseddataintegrityauditing forreliablecloudstoragesystems.*IeeeTransactionsonDependableandSecureComputing*,16(1),72-83. https://doi.org/10.1109/tdsc.2017.2662216

Lin, W., Lei, Z., Yang, J., He, G., Liu, J., & Fang, L. (2013). Secure cloud storage management method based on time stamp authority., 1-1. https://doi.org/10.1049/ic.2013.0198

Liu, H., Zhang, P.,& Liu, J. (2013). Public data integrity verification for secure cloud storage. *Journal of Networks*, 8(2). https://doi.org/10.4304/jnw.8.2.373-380

Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. (2015). A survey of security and privacy challenges incloudcomputing:solutionsandfuturedirections. *JournalofComputingScienceandEngineering*,9(3), 119-133. https://doi.org/10.5626/jcse.2015.9.3.119

Ma,H.,Gao,Z.,&Yao,N.(2016).Hierarchicalremotedatapossessioncheckingmethodbasedonmassive cloud files. *Journal of Algorithms & Computational Technology*, 11(2), 126-134. https://doi.org/10.1177/1748301816682243

Ma,J.andLi,F.(2024).Researchontransactionprivacyprotectionsolutionsforcross-border commerce. IetBlockchain,4(S1),586-595.https://doi.org/10.1049/blc2.12080

Maffei, M., Malavolta, G., Reinert, M., & Schröder, D. (2015). Privacy and access control for outsourced personal records., 341-358. https://doi.org/10.1109/sp.2015.28

Majigi, M., Idris, I., Abdulhamid, S., & Uduimoh, A. (2023). Blockchain-based zero knowledge proof modelforsecuredatasharingschemeinadistributedvehicularnetworks.*FudmaJournalofSciences*,7(3), 45-54. https://doi.org/10.33003/fjs-2023-0703-1786

Mann, S. (2022). A peer-to-peer file storage system using blockchain and interplanetary file system. *InternationalJournalofCurrentScienceResearchandReview*,05(02).https://doi.org/10.47191/ijcsrr/v5- i2-34

Meng, L. and Sun, B. (2022). Research on decentralized storage based on a blockchain. *Sustainability*, 14(20), 13060. https://doi.org/10.3390/su142013060

Mohammed, M. and Abed, F. (2019). An improved fully homomorphic encryption model based on n-primes. *Kurdistan Journal of Applied Research*, 4(2), 40-49. https://doi.org/10.24017/science.2019.2.4

Petrovčič, A., Reisdorf, B., Grošelj, D., & Prevodnik, K. (2022). A typology of aging internet users: exploringdigitalgradationsininternetskillsanduses.*SocialScienceComputerReview*,41(5),1921-1940. https://doi.org/10.1177/08944393221117753

Pijnenburg, J. and Poettering, B. (2020). Encrypt-to-self: securely outsourcing storage., 635-654. https://doi.org/10.1007/978-3-030-58951-6_31

Poh, G., Chin, J., Yau, W., Choo, K., & Mohamad, M. (2017). Searchable symmetric encryption. *Acm Computing Surveys*, 50(3), 1-37. https://doi.org/10.1145/3064005

Ramachandran, A., Ramadevi, P., Alkhayyat, A., & Yousif, Y. (2023). Blockchain and data integrity authentication technique for secure cloud environment. *Intelligent Automation & Soft Computing, 36(2),* 2055-2070. https://doi.org/10.32604/iasc.2023.032942

Reddy,B.andRao,M.(2018).Filterbaseddatadeduplicationincloudstorageusingdynamicperfecthash functions. *International Journal of Simulation Systems Science & Technology*. https://doi.org/10.5013/ijssst.a.19.04.08

Salam, I., Yau, W., Chin, J., Heng, S., Ling, H., Phan, R., … & Yap, W. (2015). Implementation of searchablesymmetricencryptionforprivacy-preservingkeywordsearchoncloudstorage.*Human-Centric Computing and Information Sciences*, 5(1). https://doi.org/10.1186/s13673-015-0039-9

Samy,I.andMary,M.(2022).Securedatatransmissionincloudcomputingusingstd-rsawitheslurnndata classification and blockchain based user authentication system. https://doi.org/10.21203/rs.3.rs-1724672/v1

Sheela, M. (2022). Robust key revelation of public auditing prototype for secure cloud storage. *Interantional Journal of Scientific Research in Engineering and Management*, 06(02). https://doi.org/10.55041/ijsrem11717

Shen, W., Qin, J., & Ma, J. (2019). A lightweight identity-based cloud storage auditing supporting proxy update and workload-based payment. *Security and Communication Networks*, 2019, 1-15. https://doi.org/10.1155/2019/8275074

Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2019). Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. *Ieee Transactions on Information Forensics and Security*, 14(2), 331-346. https://doi.org/10.1109/tifs.2018.2850312

Singh, J. (2024). Enhancing cloud data privacy with a scalable hybrid approach: he-dp-smc. *JES*, 19(4), 350-375. https://doi.org/10.52783/jes.643

Song, T. and Zhou, H. (2025). Design and construction of remote data disaster recovery center based on cloud storage., 81. https://doi.org/10.1117/12.3067950

Souri,A.,Salehpour,A.,&Pashazadeh,S.(2013).Anovelcloudstoragesystemwithsupportofsensitive data application. *International Journal of Mobile Network Communications & Telematics*, 3(5), 19-27. https://doi.org/10.5121/ijmnct.2013.3503

Tian,J., Guo, R., &Jing, X.(2019). Stern–brocot-basednon-repudiationdynamic provable data possession. *IeeeAccess*,7,96686-96694. https://doi.org/10.1109/access.2019.2916173

Tian, Y., Qin, X., & Jia, Y. (2015). Secure replica allocation in cloud storage systems with heterogeneous vulnerabilities., 205-214. *IEEE Xplore.* https://doi.org/10.1109/nas.2015.7255217

Tricomi, G., Merlino, G., Panarello, A., & Puliafito, A. (2020). Optimal selection techniques for cloud service providers. *IEEE Access*, 8, 203591-203618. https://doi.org/10.1109/access.2020.3035816

Vengala,D.,Kavitha,D.,&Kumar,A.(2021).Threefactorauthenticationsystemwithmodifiedeccbased secured data transfer: untrusted cloud environment. *Complex & Intelligent Systems*, 9(3), 2915-2928. https://doi.org/10.1007/s40747-021-00305-0

Vimal, V. (2019). An efficient and secure query processing and indexing model for secure dynamic cloud storage. *Turkish Journal of Computer and Mathematics Education (Turcomat)*, 10(2), 1043-1048. https://doi.org/10.17762/turcomat.v10i2.13623

Wang, S., Ye, J., & Zhang, Y. (2018). A keyword searchable attribute-based encryption scheme with attribute update for cloud storage. *Plos One*, 13(5), e0197318. https://doi.org/10.1371/journal.pone.0197318

Wang, X. (2024). Research on cloud storage data integrity verification protocol based on smart technologies., 39. https://doi.org/10.1117/12.3050931

Wu, H. (2023). Information encryption and data storage security. *Highlights in Science Engineering and Technology*, 57, 189-194. https://doi.org/10.54097/hset.v57i.10000

Xia,Z.(2022).Applicationofcloudcomputingtechnologyincomputernetworksecurestoragesystem., 83. https://doi.org/10.1117/12.2641080

Xu,K.,Chen,W.,&Zhang,Y.(2022).Aminimal-overheadmulti-clouddataplacementstrategybasedon heuristicalgorithm.*JournalofPhysicsConferenceSeries*,2170(1),012010.https://doi.org/10.1088/1742-6596/2170/1/012010

Yadav,A.,Ritika,R.,&Garg,M.(2019).Monitoringbasedsecurityapproachforcloudcomputing. *IngénierieDesSystèmesDInformation*,24(6),611-617.https://doi.org/10.18280/isi.240608

Yadav,A.,Ritika,R.,&Garg,M.(2021).Cryptographicsolutionforsecurityproblemincloudcomputing storageduringglobalpandemics.*InternationalJournalofSafetyandSecurityEngineering*,11(2),193-199. https://doi.org/10.18280/ijsse.110208

Yang,P.,Xiong,N.,&Ren,J.(2020).Datasecurityandprivacyprotectionforcloudstorage:asurvey. *IeeeAccess*,8,131723-131740. https://doi.org/10.1109/access.2020.3009876

Yu, H., Cai, Y., & Kong, S. (2016). An efficient public auditing scheme for cloud storage server. https://doi.org/10.2991/aest-16.2016.97

Zainudin, J., Puteri, F., Miserom, F., & Roslan, N. (2022). Securing academic student file using aes algorithm for cloud storage web-based system. https://doi.org/10.15405/epms.2022.10.26

Zhang, W., Ma, C., Sha, W., & Zhou, Q. (2015). Research of data security in cloud storage. https://doi.org/10.2991/iiicec-15.2015.192

Zhou,J.(2024).Comparisonofcloudstorageinthefieldofpersonaldataandbigdata. *HighlightsinScience Engineering and Technology*, 81, 547-552. https://doi.org/10.54097/wqsgs575