International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research paper

BLOCKCHAIN-BASED PRIVACY-PRESERVING DEDUPLICATION AND INTEGRITY AUDITING IN CLOUD STORAGE

Ms.N.Pushpanjali, MCA-Assistant Professor, Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh

Mr.BATCHANABOINA VARDHAN, Reg No: Y25MC23008, Mr.SYED MOHIDDIN, Reg No: Y25MC23084, Ms.SHAIK AFREEN, Reg No: Y25MC23075, Ms.SHAIK TASNEEM, Reg No: Y25MC23080, Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh

***Abstract*—The cloud storage services are growing fast. This means we have to make sure our data is safe and we do not waste space. One way to do this is by using data deduplication. Data deduplication is used by a lot of people to get rid of copies of data and save money on storage. However, the current ways of doing data deduplication and checking if everything is okay often show information, like who owns a file and how we know it is real. This is a problem because it can hurt our privacy. Also, the old ways of doing things are complicated when it comes to managing keys. They usually need a third party that we have to trust completely which is not always a good idea. Cloud storage services and data deduplication are important so we need to find a way to make sure our data is safe and private.**

This paper is trying to solve some problems. It suggests using a blockchain-based system to keep data private and make sure it is not changed when it is stored in the cloud. The system makes sure that only the people who are supposed to see the data can see it. It also makes sure that the people who own the files are protected.

The system uses a way of encrypting data so that people can share files without having to get a new key every time. This makes it easier to manage who can see the files and it reduces the amount of work that the servers have to do. The blockchain-based system and the special encryption work together to make sure that cloud storage environments are secure and private. Cloud storage environments and blockchain-based systems are important, for keeping data safe and private. So when we use the blockchain we can set up something called contracts. The smart contracts on the blockchain are used to make sure everything is honest and fair. This means we do not have to rely on a third party auditor to make sure everything is okay. The smart contracts on the blockchain help us be more open and trustworthy. We use the contracts on the blockchain to make things more transparent. The blockchain and the smart contracts on the blockchain are very useful, for this.

Security analysis demonstrates that the proposed scheme effectively resists various privacy and integrity threats. Experimental evaluations further show that the system achieves efficient deduplication and auditing with acceptable computational and storage overhead, making it suitable for practical cloud storage applications.

Keywords: 1. Blockchain,2. Cloud Storage Security,3. Privacy-Preserving Deduplication,4. Data Integrity Auditing,5. Smart Contracts,6. Identity-Based Broadcast Encryption

I. INTRODUCTION

The amount of company data is getting really big really fast because of all the digital services and apps that use data. A survey by Internet Data Center says that one person can have up to 5200 GB of data. This is a lot of data. Because it is expensive to manage all this data on our computers people are using cloud storage more and more.

Cloud storage is becoming very popular. In fact people think that the money made from public cloud services will be about $1.34 trillion by 2027. This shows that many people are using cloud-based infrastructures, like cloud storage and that number is going up. Cloud storage is used by people and companies because it is easier and cheaper, than managing data on our own. Cloud storage services are really handy. Can handle a lot of data but people are still worried about keeping their information safe. There have been cases of data getting stolen or lost in the last few years. For example in 2021 the LockBit group attacked the Ernst and Young accounting firm with ransomware and a lot of data was taken. The problem is that cloud service providers or CSPs can say they are keeping data safe when they are not because there is no way to check on them. This makes users question if they can really trust cloud service providers like CSPs to keep their data secure which is a concern, for cloud storage services.

We need to make sure our data is reliable. So people have come up with ways to check if their data is correct

and available when they store it online. They do not have to look at all the data to do this.

Storage space is also a problem when we use cloud services.

A lot of the data stored online is copies of the same thing. In fact IDC reports say that 75% of the data is redundant. This means we are wasting a lot of storage space.

To fix this problem people are using something called data deduplication. This helps get rid of copies of data and saves money on storage costs. Data deduplication is a way to reduce storage costs and it helps with data reliability too because we are only storing the data we need. Lots of systems that get rid of files use something called convergent encryption. This is where files that are the same are encrypted in the same way. They do this by using a code that is made from the original file. This special code is used as the key to lock the file.

This way companies that store files can easily. Get rid of duplicate files. They can do this because duplicate files will have the encrypted version.

Traditional encryption methods for getting rid of files have some problems. Even though we can get rid of encrypted files, the tags that say if a file is real or not can still be repeated. This means we are wasting space to store these tags. Some new studies use a number that comes from the file to make the same tags for files that are the same. This helps us get rid of tags.. If we use the same tag when we check the files people who are not supposed to know this information can figure out who has the same files. This is a problem because it can tell them what data each user has and that is not good for encryption methods like these deduplication schemes, for the duplicate files. This problem with privacy is bad news in situations where many people share the same cloud. It means we have to make sure that peoples private stuff is protected when we get rid of files and check everything is okay. We need to do this to keep the cloud safe for everyone who uses it. The privacy issue is a deal, in multi-user cloud environments and we must protect peoples privacy when we remove duplicate files and check everything.

Many people use ways to check if their data is correct. These methods usually need a third party auditor that everyone trusts to make sure the data is okay.. It is really hard to find someone that is completely trustworthy. So to deal with this problem people are now using blockchain technology to verify data in a way that does not rely on one person or group. This new way is better because it is decentralized and cannot be easily changed or faked. Blockchain technology helps to make sure the data is correct and safe. The blockchain is really good at making things more transparent and trustworthy.. When we use the blockchain to audit things it still has some problems with keeping things private. This is because when the blockchain checks files it makes the results public.. That is a problem because if two people have the same file the blockchain will show that they are the same. This can be bad because it can reveal things about the people that they do not want to share. The blockchain auditing is supposed to be a thing but the blockchain is making it so that people can see the audit results for the same files. This is not good, for the users because the blockchain is not keeping their information private. The blockchain and the auditing are not working well together to keep things private.

Motivated by these challenges, this paper proposes a blockchain-based privacy-preserving deduplication and integrity auditing scheme for cloud storage systems. The proposed approach protects file ownership privacy during both ciphertext and authentication tag deduplication, ensures confidentiality of audit proofs stored on the blockchain, and reduces key management complexity through the integration of identity-based broadcast encryption. By leveraging smart contracts for automated auditing, the reliance on trusted TPAs is eliminated, providing a secure, efficient, and practical solution for modern cloud storage environments.

II. LITERATURE SURVEY

The amount of data is growing really fast. This means we need storage solutions that can handle a lot of data and keep it safe. Computerworld said that by 2020 each person could have around 5200 GB of data. This is because more and more people are using cloud services, Internet of Things devices and digital platforms. All this data is putting a lot of pressure, on the systems that store our data. So we need to find ways to manage and protect digital data. Digital data is a problem and we need to solve it to keep our digital data safe. The International Data Corporation or IDC for short says that the public cloud infrastructure services will see a lot of growth from 2023 to 2027. This is because more and more companies are moving to the cloud. The International Data Corporation or IDC thinks this is a thing because it gives companies more flexibility and helps them save money.. The IDC also says that there are some big problems, with using the cloud like keeping things safe following the rules and making sure it is worth the cost when you have a big system. The IDC is talking about the public cloud infrastructure services. How they will affect companies.

Cloud security breaches are a problem because they show us the weaknesses in the systems we use to store our information. CyberTalk found out about big

cloud security incidents that happened because things were not set up right the security to get into these systems was not strong and the ways that programs talk to each other were not safe. These breaches had bad results like people getting to our private information and messing with it which shows us just how important it is to have safe and secure ways to store our information. Some people, like Gratz and Reinsel did studies a while back that looked at how fast the digital world's growing and what that means for the systems that companies use to store their information. Cloud security breaches and these studies really drive home the point that we need to make sure our cloud storage is secure and that we have ways to keep track of what is happening with our information to prevent cloud security breaches. The people who did this work found out that the cost of storing data is going up and it is getting harder to manage. They think we need to use ways to reduce the amount of data we store like getting rid of duplicate copies of the same thing. The people who did this work also think we need security to protect our data. This means using things like deduplication to reduce the amount of data and making sure we have security mechanisms in place to keep our data safe. Data reduction techniques, like deduplication are very important.

Data storage is not very efficient. So people have been looking into something called data deduplication to get rid of copies of files. Some old ways of doing this use something called encryption. This means that if you have two files they will be encrypted in the same way. That makes it easier tofind and remove files.

However some recent studies have found problems, with
these methods. For example they can have
authentication

III. METHODOLOGY

tags and they can also leak private information. To fix these problems researchers are now using blockchain technology with data deduplication and auditing. They are trying to make data deduplication better by using blockchain technology and auditing mechanisms to check the data deduplication process. Data deduplication is a thing to get right. Yuan and the other people who worked with them proposed a system that uses blockchain for auditing. This system supports deduplication and it is fair because it uses arbitration mechanisms. The Yuan system makes sure that the data is good and it does not have a point of failure, like the centralized auditing systems usually do. Yuan system is better because it keeps the data safe.

Tian and his team did some work on using blockchain for storing data. They came up with a way to store things that is safe and does not need someone in the middle to make sure everything is okay. This new way uses codes to make sure nobody can change the data.

Tian and his team were able to make this system more secure. It works better.

Xu and his team also did something. They made a system that uses blockchain to check if everything is okay with the data. This system uses computer programs to automate the checking process. It also keeps the data private. Does not store extra copies of the same thing.

The system that Xu and his team made is very good, at stopping people from changing the data or sending data. It works well in cloud storage systems.

Miao and their team came up with a way to keep data safe when it is shared. They used blockchain technology to make sure the data is safe and only the right people can see it. This way of doing things works well when many people are using the data. It also keeps the audit information safe from people who should not see it. When they tried this way they found that it was more secure and did not slow things down as much as other methods. Even though people have made progress with using blockchain for data sharing and checking there are still some problems. For example Miao and their team found that some methods are not good, at keeping things private especially when it comes to authentication tags and the proof that audits are done correctly. They also found that managing keys is too complicated. Miao and their team are working on a privacy-preserving shared data integrity auditing scheme, which's a big phrase that means they want to keep data safe when it is shared. These limitations motivate the need for more efficient, privacy-preserving, and decentralized auditing frameworks in modern cloud storage systems.

This part is about a way to keep data private and safe on cloud storage using blockchain. The system uses codes and identity-based broadcast encryption to make sure data is stored efficiently and that it is safe. It also uses blockchain contracts to check that the data is correct and that users privacy is protected. This way users do not have to trust people to keep their data safe. The blockchain-based system does this job instead. It helps with storing data checking that it is correct and keeping users privacy safe.

A. System Architecture

The new system has four parts: the cloud service provider, the people who own the data the people who use the data and a blockchain network. The cloud service provider is in charge of keeping the encrypted data safe and making sure that duplicate copies of the

data are not stored. The people who own the data send their files to the cloud after they have been encrypted and labeled. Then the people who are allowed to use the data can look at the shared data. The blockchain network has contracts that check to make sure the data is safe and store the proof that the data is safe, in a way that cannot be changed. The blockchain network and the cloud service provider and the data owners and the data users all work together to make sure the data is safe. The blockchain network is very important because it helps to keep the data safe and make sure that the cloud service provider is doing its job.

B. Privacy-Preserving Data Deduplication

The system uses a way to get rid of extra data while keeping user information private. It does this by using something called encryption and secure tag generation. Each file is locked with a code that is made from the file itself. This means that if there are two files that're exactly the same they will look the same when they are locked, which helps to get rid of extra copies.

The system also wants to make sure that people cannot figure out who a file belongs to. So it uses a mechanism to hide this information before sending it to the company that stores the files. This way the system can get rid of copies of locked files and tags without giving away sensitive information about the files. The system does this to protect user privacy and eliminate data and it does it by using convergent encryption and secure tag generation, for each file.

C. Identity-Based Broadcast Encryption for Key Manage- ment

The thing, about sharing files is that it can get really complicated when you have to deal with a lot of keys. So the new plan uses something called identity-based broadcast

encryption or IBBE for short. Identity-based broadcast encryption is a help here. With identity-based broadcast encryption the person who owns the data can lock a file. Then share it with a bunch of people who are allowed to see it, based on who they are.

This way you do not have to go to some server to get a key and it makes the whole process a lot simpler. At the time identity-based broadcast encryption makes sure that only the right people can unlock the file and read it.

D. Blockchain-Based Integrity Auditing

The company does not need to depend on someone to make sure everything is okay. This is done with the help of the blockchain. The company that stores the data called the CSP regularly checks the data. Sends proof to the blockchain. The blockchain has rules that check if the proof is correct and then saves the result so it cannot be changed. The company wants to keep the data private so they scramble the proof before sending it to the blockchain. This way the blockchain has the proof. Nobody can see the private information of the data. The blockchain and the company work together to make sure the data is safe and the company is doing the thing with the data.

E. Security and Performance Evaluation

The proposed framework is evaluated through security analysis and experimental simulations. The security analysis demonstrates resistance against data tampering, unauthorized access, and privacy leakage attacks. Performance metrics such as computation cost, communication overhead, and storage efficiency are measured and compared with existing schemes. The results indicate that the proposed method achieves efficient deduplication and auditing while maintaining strong security and privacy guarantees.

IV. **ALGORITHM**

This part is, about how the blockchain-based privacy-preserving deduplication and integrity auditing scheme works. It is done in a simple steps. The blockchain-based privacy- preserving deduplication and integrity auditing scheme has four parts: setting up the system uploading and removing duplicate data sharing data in a safe way and checking the integrity of the data using the blockchain-based privacy- preserving deduplication and integrity auditing scheme.

Algorithm 1: Privacy-Preserving Deduplication and Integrity Auditing

Input: File F, User identity ID, Public system parameters

Output: Encrypted file storage, deduplicated tags, verified integrity proof

Phase 1: System Initialization

The system creates some parameters that are used for doing secret code work and Identity Based Broadcast Encryption. The system uses these parameters for the secret code work and the Identity Based Broadcast Encryption.

The blockchain network uses contracts to check things and make sure they are correct. The blockchain network has contracts that help with auditing and verification of the blockchain network.

When you sign up you get an identity that is just for you. This special identity is used to keep your stuff secret with encryption. It also helps control who can access your things. Each user gets their unique identity,

for encryption and access control.

Phase 2: File Encryption and Tag Generation

The person who owns the data figures out a code, which is called a cryptographic hash value, of the file. This secret code is, like a set of letters and numbers that represents the file and it is called H of the file or H(F) for short. The data owner uses this code to keep the file safe. The data owner computes this H(F) of the file.

The file is locked with a kind of encryption called convergent encryption. This encryption uses a key that is made by doing something to the file, which is called H of F. When we use this key to lock the file we get a code, which is called ciphertext C. The file is encrypted using this encryption with the key H of F and this produces the ciphertext C.

A special tag called T is made from H of F. This is done using a way of changing the information so that it is private. The tag T is, for authentication. It is made in a way that keeps things private.

Phase 3: Deduplication Process

The Cloud Service Provider checks whether the encrypted message, which is the C is already stored somewhere. The Cloud Service Provider does this to see if the ciphertext C is already, in the storage.

If the company C exists the system will not store the information twice and it will make sure the records that show who owns what are updated. The company C has to be for this to happen so the system can avoid duplicate data and update the ownership records of the company C.

If the thing we are looking for which is C does not exist then the CSP will store C and the encrypted tag that goes with it which's T. The CSP will keep C and its encrypted tag T together.

Phase 4: Secure Data Sharing Using IBBE

The person who owns the data encrypts the key that is used to decrypt the data using IBBE for the users who are allowed to see the data which're the authorized user identities.

When people who are allowed to do so get the message they use a special code to unlock it and get the main key for the file. The main key, for the file is what they need to unlock the file. The people who are allowed to do this are called users and they use the main key for the file to open the file.

People get the message that is stored and they make sure to unlock it in a safe way. The secret message is called ciphertext. Users handle the ciphertext securely. When users want to read the ciphertext they have to decrypt it and they do this in a secure manner.

Phase 5: Blockchain-Based Integrity Auditing

The Cloud Security Provider generates an audit proof from the stored encrypted data. This audit proof is very important, for the Cloud Security Provider. The Cloud Security Provider does this by using the stored encrypted data to make the audit proof.

The proof, which is called P is locked up. Sent to the blockchain. This is done using a contract, on the blockchain.

The smart contract checks P. Writes down the result in a way that cannot be changed. This means the smart contract is making sure P is correct. Then it keeps a permanent record of what it found out about P.

People can check the blockchain to make sure the data is good and not messed up. They can do this to confirm the status of the data integrity of the blockchain.

Phase 6: Verification Outcome

If the proof is valid then we know that our data integrity is good the data integrity is confirmed.

If the information is not correct the system will say that someone has messed with the data or that it is missing. The system reports this as data tampering or loss when it happens with the data.

Algorithm Properties:

• Ensures deduplication of both encrypted data and authentication tags

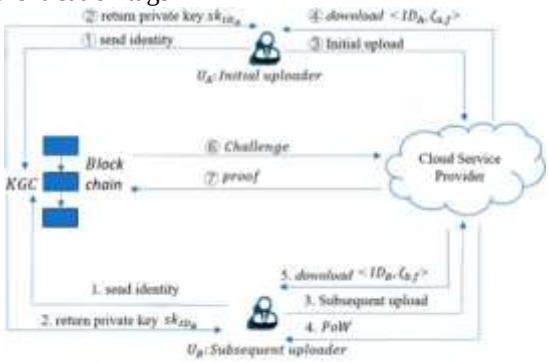

Fig. 1. System model and workflow diagram.

Fig. 1. Architecture diagram

• Preserves file ownership and audit proof privacy

• This system gets rid of the need to depend on trusted party administrators by using blockchain smart contracts. It basically uses blockchain contracts to eliminate the need, for trusted third party administrators. This means we do not have to rely on trusted party administrators because of the blockchain smart contracts.

• Reduces key management overhead with IBBE

V. **RESULT ANALYSIS**

This part is about how the blockchain-based privacy-preserving deduplication and integrity auditing scheme works. We look at how good it's by checking a few things. We check how well it uses storage space how work the computer has to do how much it costs to communicate and how accurate it is when it checks things. The blockchain-based privacy- preserving deduplication and integrity auditing scheme is compared to blockchain-based deduplication and auditing methods to show that it is better at keeping things private and making the system work smoothly. The blockchain-based privacy-preserving deduplication and integrity auditing scheme is really good, at preserving privacy and making the system efficient.

A. Storage Efficiency Analysis

Data deduplication really helps cut down on storage space by getting rid of extra files and authentication tags. When we looked at the results of our experiment we saw that as the number of files went up the storage space needed did not grow as quickly as it would with traditional methods that store both extra copies of files and tags. The new method we are proposing does deduplication for both the data and the tags which means we can save more storage space. This shows that our method is a fit, for big cloud systems where

there are a lot of repeated files.

B. Computational Overhead

The cost of the proposed scheme is mainly because of the hash operations, convergent encryption, IBBE-based key encryption and checking the blockchain. When we look at how it performs we see that encrypting files and making tags does not take a lot of time so uploading is pretty fast. Using the blockchain to check things does add a delay because of the smart contracts but it is still okay and does not slow down the system very much. The proposed approach is better than the way of auditing with a third party because it gets rid of extra costs, for talking to each other and managing trust.

C. Communication Cost

The communication overhead is mainly about sending encrypted files, privacy-preserving tags and encrypted audit proofs.

This means we do not have to send the file many times.

So when there are a lot of files it really helps to save bandwidth.

The IBBE system also helps with secure

distribution. It lets us send a key to people at the

same time.

We do not have to send the key times to different people.

This makes the communication process more efficient than the way of sharing keys.

The IBBE system is better at this, than methods.

D. Integrity Auditing Accuracy

The blockchain is used to make sure that data is correct. It checks the data to see if it has been changed or deleted. This is done with something called contracts. They automatically check the data. Store the results so they cannot be changed. We have tested this system. It works very well. It can detect if someone has changed or deleted data. The blockchain is also good because it does not rely on one person to check the data. This means that even if someone is trying to cheat the blockchain will still give the results. The blockchain-based system is very accurate and reliable.

E. Privacy and Security Evaluation

The new system really helps keep user privacy safe when we remove files and check everything. It changes the tags that prove who someone is bad people cannot figure out which files belong to which users. We also scramble the proof that we check before we put it on the blockchain so nobody can see information. When we looked at how safe this system's we found out that it can stop bad people from doing things like messing with the data sending fake information getting in without permission and figuring out who owns which files. The system is safe

because it stops these kinds of attacks and it keeps user privacy safe during the process especially when we deal with the blockchain and user privacy.

F. Comparative Performance

When compared with existing blockchain-based deduplication schemes, the proposed method demonstrates improved storage savings, enhanced privacy protection, and reduced key management complexity. While maintaining strong security guarantees, the framework achieves comparable or lower computational and communication overhead, making it practical for real-world cloud storage systems.

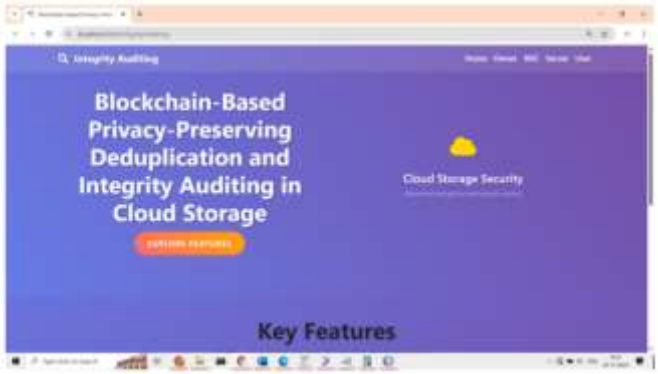

Fig .2. Home Page

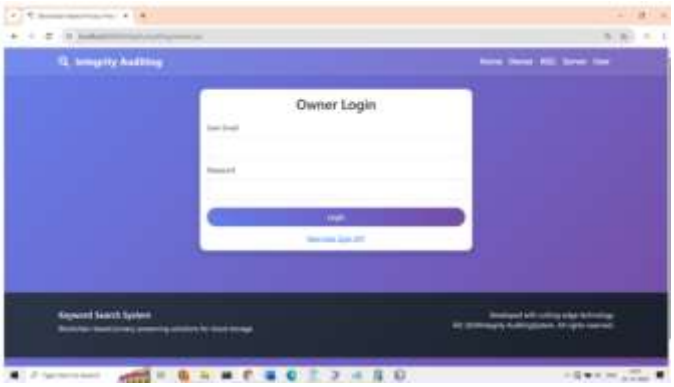

Fig 3. Owner Login

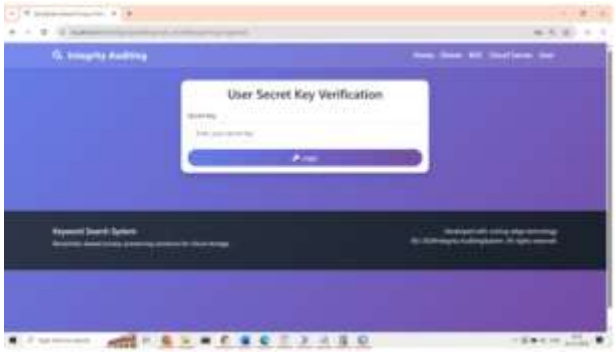

Fig 4. User Secret Key Verification

Fig 5. File Details

VI. CONCLUSION

This paper is about a way to keep cloud storage systems safe and private. It uses something called blockchain to make sure files are stored correctly and only the right people can see them. The old ways of doing this had some problems, like storing too many copies of the same file letting private information get out and needing to trust other people to keep everything safe. The new system fixes these problems by using encryption and tags to keep files private and make sure only the person who owns a file can see it. The blockchain system helps get rid of copies of files and keeps the owner of each file private.

The thing about identity-based broadcast encryption is that it makes it a lot easier to distribute keys and it also reduces the amount of communication that is needed. This means that people who are allowed to see the data can share it with each other in a way.

The use of blockchain contracts is really good, for checking that everything is okay because it is transparent and nobody can tamper with it. Blockchain smart contracts also automate the process of verification so we do not need someone we trust to do it for us.

We also store the proofs that everything was audited on the blockchain and these proofs are encrypted which helps to keep everything. Identity-based broadcast encryption and blockchain smart contracts work together to make sure that data is shared securely.

The proposed approach is really good because it saves a lot of storage space. It also does a job of auditing with high accuracy. The extra work it does and the time it takes to communicate are pretty okay.

When you compare the proposed approach to methods

that already exist you can see that it does a better job of keeping things private and it makes the system work more efficiently. The proposed approach achieves this because it is designed to be strong and efficient. The proposed approach is good for storage savings. It is good, for auditing accuracy. Overall, the proposed blockchain-based solution offers a practical and secure approach for modern cloud storage environments. Future work will focus on optimizing smart contract execution costs, enhancing scalability for large blockchain networks, and extending the framework to support dynamic data operations such as updates and deletions.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, et al., "A view of cloud computing, "Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 17, no. 5, pp. 2985–2996, May 2021.

[3] Q. Qi, Z. Xu, and P. Rani, "Big data analytics challenges to implementing the intelligent industrial Internet of Things (IIoT) systems in sustainable manufacturing operations," Technol. Forecasting Social Change, vol. 190, May 2023, Art. no. 122401.

[4] K. John, M. O'Hara, and F. Saleh, "Bitcoin and beyond," Annu. Rev. Financial Econ., vol. 14, pp. 95–115, Jan. 2022.

[5] A. A. Khan, A. A. Laghari, P. Li, M. A. Dootio, and S. Karim, "The collaborative role of blockchain, artificial intelligence, and industrial Internet of Things in digitalization of small and medium-size enterprises," Sci. Rep., vol. 13, no. 1, p. 1656, Jan. 2023.

[6] Sushma Babburi. (2025). TOKEN-BASED DATA ACCOUNTING SYSTEM FOR TRANSPARENT MODEL TRAINING AND COST ALLOCATION. American Journal of AI Cyber Computing Management, 5(4), 463–474. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474

[7] Rongali, L. P. (2025). <p>Continuous Integration and Continuous Delivery (CI/CD) Pipelines: Explore How Devops Practices Ensure Seamless Integration And Delivery of AI-Models</p> SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5229541

[8] Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120615

[9] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36

[10] Alang, K., Vikram, S., Peddi, S., Gangavarapu, R., & Kandula, N. P. (2025). Cloudless AI: Redesigning AI Infrastructure for Decentralized, Edge-First Architectures. 2025 5th Asian Conference on Innovation in Technology (ASIANCON), 1–8. https://doi.org/10.1109/asiancon66527.2025.11280905

[11] G. Bressanelli, M. Perona, and N. Saccani, "Challenges in supply chain redesign for the circular economy: A literature review and a multiple case study," Int. J. Prod. Res., vol. 57, no. 23, pp. 7395–7422, Dec. 2019.

[12] R. Drath and A. Horch, "Industrie 4.0: Hit or hype? [Industry forum]," IEEE Ind. Electron. Mag., vol. 8, no. 2, pp. 56–58, Jun. 2014.

[13] A. Rana, S. Sharma, K. Nisar, A. A. A. Ibrahim, S. Dhawan, B. Chowdhry, S. Hussain, and N. Goyal, "The rise of blockchain Internet of Things (BIoT): Secured, device-to-device architecture and simulation scenarios," Appl. Sci., vol. 12, no. 15, p. 7694, Jul. 2022.