AES Algorithm Based Data Possession in Cloud Using Blockchain

[1] Mariyam Farhana B,[2] Nithya S,[3] Reddy Prashanthi M and [4] Prathiksha M
[1,2,3,4]Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.
[1] farhanamariyam.11@gmail.com, [2] snithya722002@gmail.com, [3] prashanthi70.m@gmail.com,
[4] Prathiksha.mcsp@gmail.com

Article Info
A. Haldorai et al. (eds.), *2nd International Conference on Materials Science and Sustainable Manufacturing Technology,* Advances in Computational Intelligence in Materials Science.
Doi: https://doi.org/10.53759/acims/978-9914-9946-9-8_11

Abstract — Remote secure data storage is key importance in cloud computing. So, for checking remote data integrity, an important paradigm called PDP schemes is introduced. There are still PDP schemes which bilinear matching can be used. One huge file can be broken into various blocks. There is much computation cost and communication cost that arises due to inefficient PDP implementation. Anyway, this is not the right solution therefore, to solve this kind of problem, we propose a new one The PDP model: a blockchain-based private PDP. This new one the solution can be leveraged using blockchain which is vital role in cryptocurrency. For this new concept, paper formalizes its system model and security model. And then a specific blockchain-based private PDP scheme is created designed using blockchain and AES. It is very much safer and we also analyze its performance two different parts: theoretical analysis and implementation the prototype was our analyzes show that the proposed PDP the system is safe, efficient and practical.

Keyword — Provable Data Possession, Computation Cost, Cryptocurrency, Bilinear Matching, Scalability, Data Migration, Cloud Service Provider, Theoretical Analysis, Secure, Efficient.

I. INTRODUCTION

PDP provides a way for clients to ensure that their data is being stored securely and is accessible when needed. It is an important security measure for cloud storage and other remote data storage scenarios, as it enables clients to verify that their data has not been tampered with or lost without having to retrieve the entire dataset. Blockchain is a decentralized digital ledger that allows for secure, transparent, and tamper-proof recording and sharing of information. The concept was originally introduced in 2008 in a white paper by an unknown individual or group of individuals using the pseudonym Satoshi Nakamoto, as the underlying technology behind Bitcoin, the world's first decentralized digital currency. [1] At its core, a block-chain is a continuously growing chain of blocks that contain a series of transactions or pieces of information. Each block is cryptographically linked to the previous block, forming an immutable chain. [2] This means that once a block is added to the block-chain, it cannot be altered or deleted without the consensus of the network. [3] Blockchain technology has evolved beyond just the realm of cryptocurrency and has numerous applications in various industries such as finance, supply chain management, healthcare, and more. It allows for secure and transparent record-keeping and enables trust between parties without the need for intermediaries such as banks or third-party verifiers.

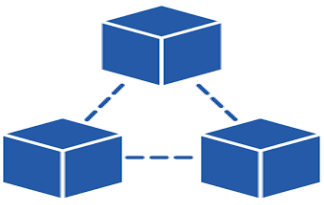

Fig 1. Diagram of Blockchain

Fig 1 shows Cloud computing offers solutions for data storage irrespective of local infrastructure limitations as well as equips the users with a platform to process their information. The main focus of this technology is to widen the efficacy of shared resources available in the cloud and also to reallocate them dynamically if needed. Blockchain is a chain of blocks, where each block contains a set of transactions [4]. These transactions are recorded in a chronological order and are linked to the previous block in the chain. This linking of blocks creates an immutable chain, which ensures

that once a transaction has been recorded, it cannot be altered or deleted without the consensus of the network. One of the key features of block-chain is its ability to maintain transparency and security. The decentralized nature of block-chain means that there is no central authority controlling the network, which prevents any single entity from altering or manipulating the data. In addition, the use of cryptography ensures that the data stored in the block-chain is secure and can only be accessed by authorized parties. This paper is organized by the following topics: Section I. Literature Survey, Section 2. Proposed Work, Section 3. Methodology, Section 4. Results, Section 5. Conclusion and Future Work.

II. LITERATURE SURVEY

For cloud storage, the security of remote data is a critical problem. In response to the flaws in the existing PDP schemes, we propose the blockchain-based private PDP scheme. This paper formalizes the system paradigm and security concept of our blockchain-based private PDP. Then, we propose the first real private PDP scheme based on blockchain. We also assess its effectiveness in terms of the execution of the prototype and theory. In addition to the traits described above, we also discuss its anonymity. According to the debate of client anonymity, our plan can also provide such confidentiality.

In [5] has proposed in this paper. By streamlined access to the data and the removal of device compatibility restrictions, cloud computing makes doing business easier by storing a sizable amount of data in the cloud and then delivering it via the internet. A man-in-the-middle attack, a known plain text attack, a chosen cypher text attack, a related key attack, or a pollution attack, on the other hand, could intercept data that is in transit. As a result, there is a chance that uploading data to a single cloud will make the secret data more likely to be harmed. For large-scale data processing on Hadoop and related frameworks, the Hadoop Distributed File System (HDFS) is a well-liked option among distributed file systems.

The [6] have proposed in this paper. a multi-cloud storage system with an effective Blockchain-based data integrity verification method. We create two methods for ensuring data integrity: global verification and local verification. In the overall verification, Pedersen commitment technology is used to construct the aggregated commitment for the data in different CSPs, and Musing technology is used to sign the aggregated commitment. This technique can withstand a Rough Key attack and validate the data integrity of several CSPs. Local verification can identify the precise CSP where the integrity of the data has been compromised. Additionally, the data verification procedure is set up specifically for public execution in the blockchain, offering data integrity verification services without the use of any third-party platforms and eliminating security issues brought on by unreliable TPA. In the future, we'll think about optimizing the plan. In the coming work, we'll think about upgrading the scheme's security and resistance to replay attacks.

The [7] proposed in this paper. The integrity of remote data is a crucial security concern for cloud storage. We suggest the blockchain-based private PDP scheme in response to the drawbacks of the current PDP schemes. The system paradigm and security model of our blockchain-based private PDP are formalized in this work. The first actual blockchain-based private PDP scheme is what we then suggest. We also evaluate its effectiveness in terms of theory and prototype execution. Together with the aforementioned qualities, we also talk about its anonymity. Our plan can also achieve the anonymity of the Client, as discussed in the anonymity discussion.

In this profession, there are a lot of prerequisites as well. It is also vital to get rid of the certificate verification process in order to increase efficiency even more.

In [8] has proposed in this paper. We first integrate the cuckoo filter into the fast corrupted data locating proven data possession (PDP) technique. We also mix the Reed-Solomon codes with PDP to achieve the data recovery objective. We provide a public proven data possession protocol for fault-tolerant cloud storage systems based on the two methods. Our plan is secure and effective, according to the performance assessment and security analysis. We will create a brand-new data structure for data dynamics in the future to complement our current system. We compare the effectiveness of corrupted data location between our cuckoo filter and earlier systems' verification of each individual block. In more detail, we model the discovery of 50–500 faulty blocks among 20000 data blocks. Verifying each data block takes far longer to locate than applying the cuckoo filter does. Also, when more data blocks become corrupted, the time difference between the two methods gets larger. This is due to the fact that computing hashes, which takes far less time than computing the verification equation, is the primary time-consuming task when utilizing the cuckoo filter. The experiment's findings thus demonstrate that our method is more effective at discovering faulty data. Huaqun Wang has proposed in this paper. The integrity of remote data is a crucial security concern for cloud storage. We suggest the blockchain-based private PDP scheme in response to the drawbacks of the current PDP schemes. The system paradigm and security model of our blockchain-based private PDP are formalized in this work. The first actual blockchain-based private PDP scheme is what we then suggest [9]. We also evaluate its effectiveness in terms of theory and prototype execution. Together with the aforementioned qualities, we also talk about its anonymity. Our plan can also achieve the anonymity of the Client, as discussed in the anonymity discussion.

In this profession, there are a lot of prerequisites as well. It is also vital to get rid of the certificate verification process in order to increase efficiency even more

III. PROPOSED WORK

To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Provable Data Possession and Proofs of Retrievability. In [10] first proposed the PDP model for

ensuring possession of files on untrusted storages and provided an RSA-based scheme for a static case that achieves the communication cost. They also proposed a publicly verifiable version, which allows anyone, not just the owner, to challenge the server for data possession. They proposed a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption, but the servers can deceive the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere [11]. Implementation is the stage in the project where the theoretical design is turned into a working system. The most crucial stage is achieving a successful new system and giving a user confidence in that the new system will work efficiently and effectively in the implementation stage. In implementation part first we have a login page with valid credential.

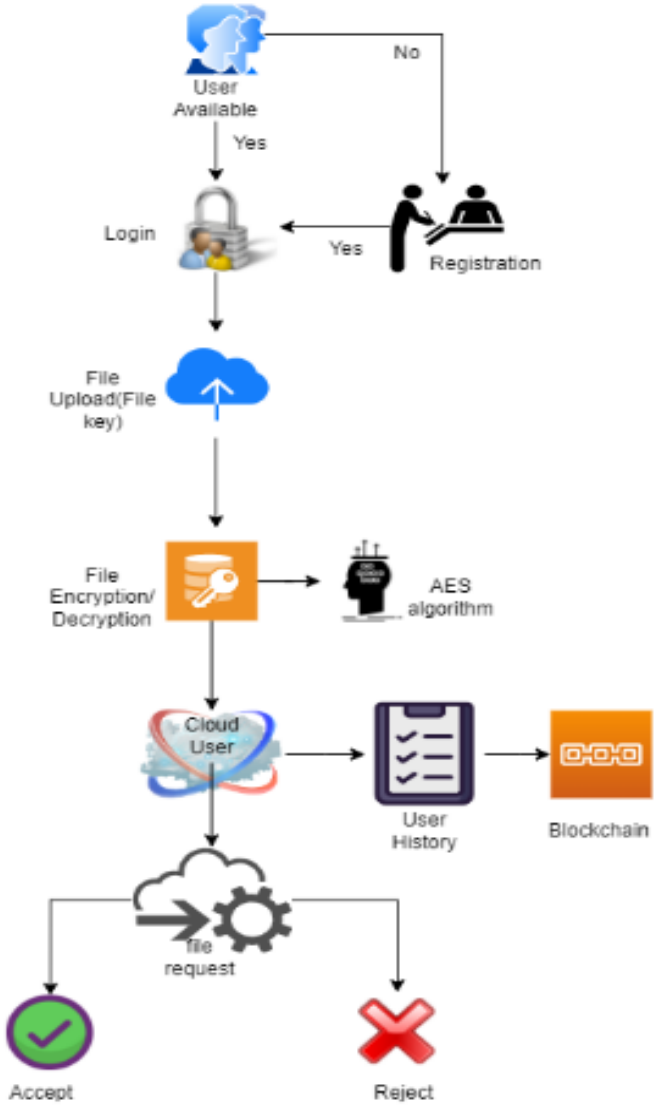

Fig 2. Implementation Flow

Fig 2 shows Main advantages of this system are that allows a data owner to verify that their data is being stored and maintained as intended by a remote storage provider, without having to retrieve the entire data set PDP allows data owners to verify that their data is being stored as intended without having to retrieve the entire data set, which can help reduce storage costs. PDP can help improve the efficiency of data retrieval and verification, as it eliminates the need for the data owner to retrieve the entire data set to verify its integrity. There are several main reasons why someone might choose provable data possession (PDP) as their main method for verifying the integrity and security of stored data: PDP provides a high level of security for stored data, as it allows data owners to verify that their data is being stored as intended and has not been tampered with. This is particularly important for sensitive data, such as financial or personal

information. PDP allows for more efficient data retrieval and verification, as it eliminates the need for the data owner to retrieve the entire data set to verify its integrity. This can save time and resources, particularly for large data sets. PDP provides a way to hold storage providers accountable for maintaining the integrity of stored data, as they are required to provide proof of possession when requested by the data owner. This can help ensure that storage providers are meeting their obligations and providing a high level of service. While PDP has many advantages, it also has some disadvantages. PDP requires additional computation to be performed by both the client and the server, which can increase the processing time and resource requirements of both parties. PDP requires additional complexity to be introduced into the data storage and retrieval process, which can make the system more difficult to design, implement, and maintain. PDP is not always applicable to all scenarios. For example, it may not be suitable for systems with large amounts of data or for systems that require low-latency access to the data.

IV. METHODOLOGY

The implementation phase is less creative than system design. A system design may be dropped at any time prior to implementation, although it becomes more difficult when it goes to the design phase. The final report of the implementation phase includes procedural flowcharts, record layouts, and a workable plan for implementing the candidate system design into a operational design. Mainly we used AES algorithm for our implementation method. Here we used AES (Advanced Encryption Standard) for Encrption of text document. AES uses a symmetric key encryption model, which means that the same key is used for both encryption and decryption of data. The text documents are stored in 6 different blocks. The algorithm works by dividing the data to be encrypted into blocks, and then applying a series of mathematical operations on each block using the encryption key. The output of these operations is the encrypted data. One of the key advantages of AES is its speed and efficiency, which makes it suitable for encrypting large amounts of data in real-time. Another advantage is its resistance to attacks, as AES has proven to be highly secure and resilient against various types of attacks. AES algorithm is best in Security, Speed, Standardization, Flexibility, compatibility.

V. RESULTS

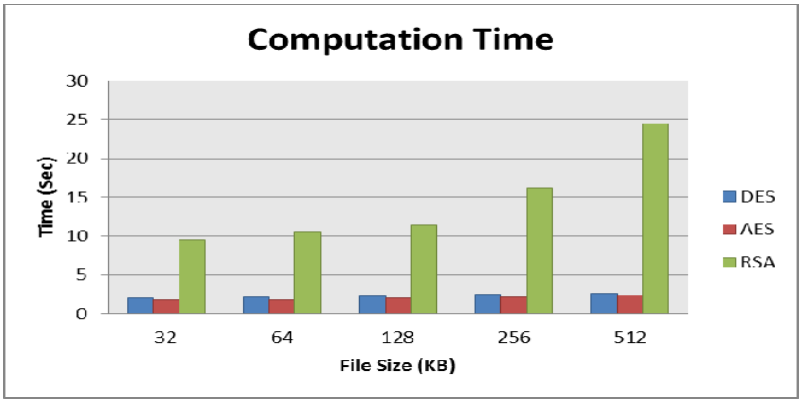

Fig 3. Comparison of Computation Time among AES, DES and RSA

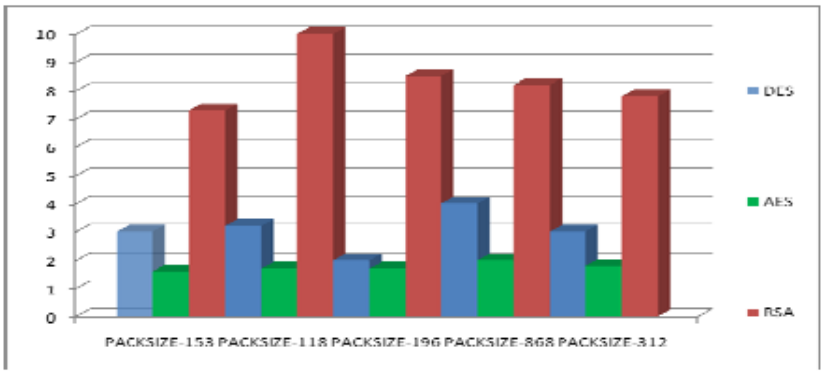

Fig 4. Comparative Status of Encryption Time among DES, AES and RSA

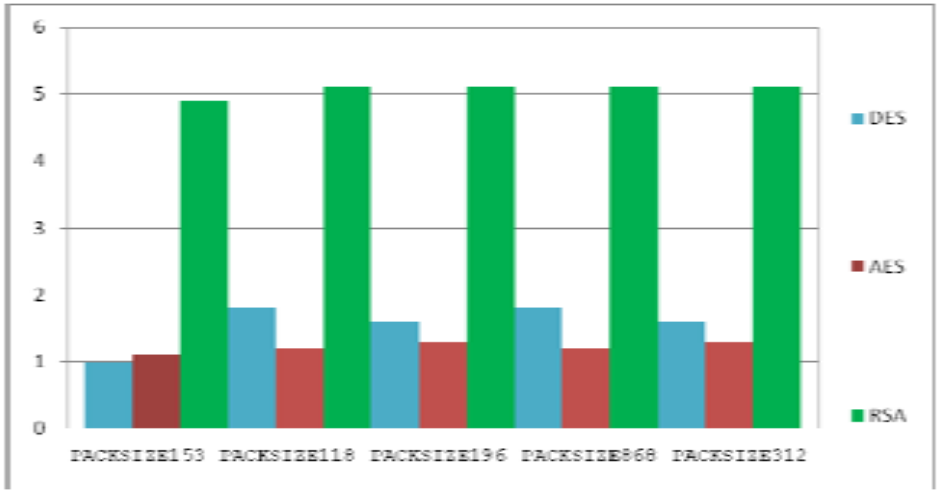

Fig 5. Comparative Status of Decryption Time among DES, AES and RSA

By analyzing **Fig 3, 4** and **5** which shows time taken for encryption and decryption on various size of file by three algorithms. RSA algorithm takes much longer time compare to time taken by AES and DES algorithm. AES and DES algorithm show very minor difference in time taken for encryption and decryption process.

VI. CONCLUSION AND FUTURE WORK

With the help of encryption, a company can scramble data into "cypher text," which is unintelligible. It safeguards the privacy of data that is kept on a company's computer systems or sent over the internet between its personnel and clients. Any substantial collaboration in which many different individual owners of personal computers permit some of their computers' processing time to be placed to the service of a significant challenge is referred to as distributed computing. Each cloud administrator in our system is made up of data blocks. Data is uploaded to many clouds by the cloud user. The architecture and protocols used to create cloud computing environments are open and have the capacity to combine numerous internal and/or external cloud services to offer high interoperability. We refer to such a distributed cloud system as multi-cloud. Through the interface, the multi-cloud allows clients to quickly access its resources remotely. As part of future work, we would extend our work to explore more effective CPDP constructions. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such a issue to provide the support of variable-length block verification.

References

[1]. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/access.2016.2566339.
[2]. H. Wang, Q. Wang, and D. He, “Blockchain-Based Private Provable Data Possession,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2019, doi: 10.1109/tdsc.2019.2949809.
[3]. C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, “A Blockchain-Based Multi-Cloud Storage Data Auditing Scheme to Locate Faults,” IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2252–2263, Oct. 2022, doi: 10.1109/tcc.2021.3057771.
[4]. R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, “An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain,” IEEE Access, vol. 9, pp. 69513–69526, 2021, doi: 10.1109/access.2021.3077123.
[5]. Y. Qi, Z. Yang, Y. Luo, Y. Huang, and X. Li, “Blockchain-Based Light-Weighted Provable Data Possession for Low Performance Devices,” Computers, Materials & Continua, vol. 73, no. 2, pp. 2205–2221, 2022, doi: 10.32604/cmc.2022.027939.
[6]. Y. Ren, H. Guan, Q. Zhao, and Z. Yi, “Blockchain-Based Proof of Retrievability Scheme,” Security and Communication Networks, vol. 2022, pp. 1–8, Feb. 2022, doi: 10.1155/2022/3186112.
[7]. R. Chen, Y. Li, Y. Yu, H. Li, X. Chen, and W. Susilo, “Blockchain-Based Dynamic Provable Data Possession for Smart Cities,” IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4143–4154, May 2020, doi: 10.1109/jiot.2019.2963789.
[8]. H. Yuan, X. Chen, J. Wang, J. Yuan, H. Yan, and W. Susilo, “Blockchain-based public auditing and secure deduplication with fair arbitration,” Information Sciences, vol. 541, pp. 409–425, Dec. 2020, doi: 10.1016/j.ins.2020.07.005.
[9]. Z. Li, Y. Xin, D. Zhao, and Y. Yang, “A Noninteractive Multireplica Provable Data Possession Scheme Based on Smart Contract,” Security and Communication Networks, vol. 2022, pp. 1–14, Apr. 2022, doi: 10.1155/2022/6268449.
[10]. H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, “A blockchain-based scheme for privacy-preserving and secure sharing of medical data,” Computers & Security, vol. 99, p. 102010, Dec. 2020, doi: 10.1016/j.cose.2020.102010.
[11]. F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, “A Blockchain-Based Flexible Data Auditing Scheme for the Cloud Service,” Chinese Journal of Electronics, vol. 30, no. 6, pp. 1159–1166, Nov. 2021, doi: 10.1049/cje.2021.08.011.