PRIVACY PRESERVING PUBLIC AUDITING FOR SHARED CLOUD DATA

Uthkam Sriveni,

Scholar,Department of MCA,

Vaageswari College Of Engineering, Karimnagar

P. Sathish,

Supervisor, Department of MCA,

Vaageswari College Of Engineering, Karimnagar

Dr. V. Bapuji,

Professor & Head,

Department of MCA,

Vaageswari College Of Engineering, Karimnagar

ABSTRACT: People have long desired for computers to function as utilities, and cloud computing enables this by allowing users to transfer data to the cloud from a remote location.People who outsource their data are relieved of the burden of managing and securing it. When it comes to outsourcing data protection, our focus is mostly on achieving the fundamental standards and bringing in a reliable third-party monitor who can obtain the data fast. We created a homomorphic, authenticable ring signature system that allows anyone to verify the integrity of cloud-based sharing data. TPA should be able to conduct a thorough analysis of cloud data storage and require a significant amount of online labor from the cloud user. Our technology makes it simple and flexible to audit data in the cloud, allowing external auditors to examine data that users have saved in the cloud. The TPA allows us to perform auditing work for several people at the same time. We are making our consumers safer by increasing the level of security we provide.Users utilize third-party auditors (TPA) to ensure and check the accuracy of their data. It promotes data privacy by allowing you to track and verify data. The proposed method will complete audits swiftly and effectively for a large number of users.

Keywords: Privacy preserving, HARS, Data storage

1. INTRODUCTION

Cloud computing Cloud computing refers to the usage of computer resources, such as tools and software, that are made available as a service across a network, typically the Internet. This expression refers to the popular use of a cloud-shaped icon in system diagrams to demonstrate the intricate design. When a person utilizes cloud computing, their data, software, and computer power are transferred to remote servers. Cloud computing refers to the availability of hardware and software tools via the internet as managed third-party services. Users can typically connect to cutting-edge server networks and software packages using these services.

Structure of cloud computing

Characteristics and Services Models: The National Institute of Standards and Technology (NIST) lists these as the most important aspects of cloud computing:

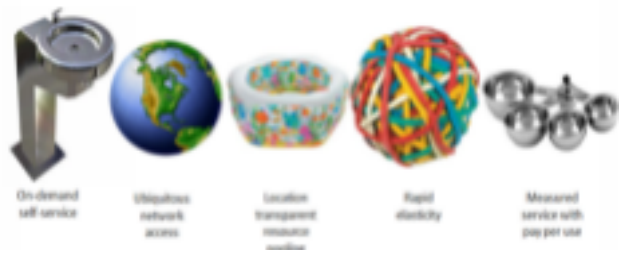
On-demand self-service: A client can set up computer resources such as server time and network storage on their own, without having to meet with each service provider individually. This process occurs spontaneously, depending on the customer's preferences.

Broad network access: Traditional techniques for accessing network capabilities can be used on a variety of client systems, including PDAs, laptops, and cell phones.

Resource pooling: To share computer resources with multiple clients, the service provider employs a multi-tenant model. This entails shifting and assigning various physical and virtual resources based on customer requirements. The customer can select a location at a higher level, such as a country, state, or data center,but they often have no influence over or knowledge of where the resources are situated. In the eyes of the customer, this suggests that the firm is not strictly positioned. Resources include servers, memory, computing power, storage space, network speed, and virtual machines.

Rapid elasticity: Capabilities can be swiftly assigned (and sometimes automatically assigned) for efficient expansion and returned for efficient shrinkage. The customer appears to have access to a limitless number of service skills that can be purchased at any time.

Measured service: Cloud systems automatically control and optimize resource usage by applying metering at the appropriate abstraction level for each service type, such as storage, processing, bandwidth, and live user accounts. Both the service provider and the user can provide transparency by monitoring, managing, and reporting on resource usage.



Characteristics of cloud computing

2. LITERATURE SURVEY

M. Rabin. “Efficient dispersal of information for security, load balancing, and fault tolerance” The length of the file F is shown by 1 F⌐. The data is divided into n parts, Fi, with l ≤ i ≤ n and 1Fi⌐ = L/m for each component. An Information Dispersal Algorithm (IDA) is used to split the file into m fragments, each of which is required to completely recreate F. When it comes to computing, both reconstruction and distribution strategies are quite effective. The sum of the lengths 1Fi⌐ equals (n/m)•L. You can choose an n-to-m ratio close to l to have the IDA approach take up little space. The Information Dispersal Algorithm (IDA) can be utilized for a variety of purposes. For example, it can ensure that information is transmitted rapidly and

reliably across networks, make it easier for processors in parallel computers to communicate with one another, and keep data secure on disks and in computer networks. For the aforementioned situation, it is possible to offer extremely reliable and verifiably time-efficient routing on the n-cube using only fixed-size buffers.

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. "Provable data possession at untrusted stores" We offer a system for verifiable data possession (VDP) that allows a client to verify that an untrusted server has the original data without needing to obtain the data itself. The method generates probabilistic proofs of ownership by randomly picking blocks from the server, significantly lowering input and output (I/O) costs. The consumer is constantly monitoring and verifying the authenticity of materials. The challenge/response protocol transmits a modest, homogeneous quantity of data across the network, minimizing network interaction. The PDP paradigm enables remote data checking in distributed storage systems with large data volumes.

It is clear that our two PDP systems are safer than previous methods, even when contrasted to methods with fewer guarantees. To be more exact, the amount of extra work that must be done on the computer does not increase or decrease with the size of the data; it remains constant or just slightly increases. There is evidence that PDP is feasible, and experiments with our version suggest that its speed is restricted by disk I/O rather than cryptographic processing.

A. Juels and B. S. Kaliski. "Pors: Proofs of retrievability for large files" The primary purpose of this work is to define and investigate proofs of retrievability (PORs). Using the evidence of Retrievability (POR) approach, an archive or backup service provider can create a concise evidence that a verifier can use to retrieve a specific file F. This means that the archive stores and transfers the necessary file data securely and rapidly, allowing the user to fully recover F. In cryptography, a proof of retrievability (POR) is a specific method for dealing with a large file or bitstring F. We investigate Proof of Retrievability (POR) protocols that maintain the length of F constant regardless of how much it costs to communicate, how many times the prover uses memory, or how much space the user (verifier) requires. We develop novel and useful POR constructs while also investigating implementation issues and ways to improve existing schemes that have been investigated. A Proof of Retrievability (POR), unlike a Proof of Knowledge (POK), does not require that either the prover or the checker fully comprehend F. As a result of our research, we have developed a novel and unorthodox approach to the security issues created by PORs.

We believe that PORs are a vital tool for online archives that can be only partially trusted. Existing encryption solutions can protect the privacy and security of downloaded files. Similarly, users frequently want to ensure that archives do not delete or change data before it can be recovered. The primary goal of a POR is to do these checks without requiring users to download the files one by one. Proof of Retrievability (POR) can also demonstrate that a file can be accessed in a specific length of time, as well as service quality guarantees.

C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia. "Dynamic provable data possession" We investigate how to quickly verify the accuracy of data stored on servers that are not always available. According to the proved data possession (PDP) model, the client retains certain meta-data while preparing the data for transmission to a server that it does not trust to store it. Following that, the client requests that the server confirm that the stored data has not been modified or erased, but does not download it. In contrast, the initial PDP system could only handle static (or append-only) files.

We introduce a novel concept called dynamic provable data possession (DPDP) and demonstrate how it may be applied effectively. DPDP updates the PDP model with modifications that can be validated against saved data. We employ up-to-date, validated definitions derived from ranking data. Changing a file with n blocks requires O(logn) (or O(nμlogn)) time, resulting in a worse performance than O(1). However, the likelihood of detecting bad activity remains the same or may even improve. In truth, the lag is

minimal, as demonstrated by our tests, which included a proof size of 415KB and a processing time of 30ms for a 1GB file. In addition, we demonstrate how our DPDP approach may be used to distant file systems and version control systems such as CVS.

C. Wang, Q. Wang, K. Ren, and W. Lou. "Privacy-preserving public auditing for data storage security in cloud computing" Cloud computing is the concept that allows individuals to store their data in a centralized location and access high-quality apps and services anytime they want. These tools can be shared by anyone, and their usage is easily customizable. Users can avoid managing and storing their data on their own devices by sending it to third-party sources.

It can be difficult to keep data secure in the cloud, especially for those without advanced computing abilities or equipment. This is because users do not have direct access to the massive volumes of data that have been transmitted to other companies. For this reason, it is critical to make cloud data storage publicly auditable so that customers can seek assistance from an outside audit party to ensure the accuracy of data they have outsourced if necessary.

To securely and successfully bring in a third-party auditor (TPA), two key prerequisites must be met: 1) TPA should be able to conduct effective audits of cloud data storage without requiring a local copy of the data and without making it more difficult for cloud users to do their tasks online. 2) The third-party auditing method should not create any new privacy gaps that users may fall into. This study demonstrates how to audit data in public clouds while protecting privacy.

To achieve the requirements specified, the system effectively combines a public key-based homomorphic authenticator and random masking. We dive deeper into the concept of bilinear aggregate signatures before applying our main discovery to a scenario with numerous users and a Trusted Public Auditor (TPA) who can do several auditing jobs at the same time. This idea contributes to the effective management of various accounting activities. Following a thorough examination of their security and performance, the suggested approaches were found to be highly effective and safe.

3. SYSTEM ANALYSIS

EXISTING SYSTEM:

Companies and academics are both interested in ZCash because it is a relatively young and well-known technology that is constantly improving. Satoshi Nakamoto first proposed the concept of blockchain as a form of digital cash. This new technology is also significant in fields other than finance, such as public services, identity management, decentralized storage systems, the internet of things (IoT), and vehicle ad hoc networks (VANETS).

The Ethereum network supports decentralized apps (dApps) and smart contracts, making it more than merely a payment system. This money, like Bitcoin, can only be used in digital payment systems that rely on a stack-based scripting language to complete transactions. On the Ethereum platform, on the other hand, any program can be created and executed at the same rate. Ethereum is a programmable digital currency, similar to Bitcoin. Both Ethereum and Bitcoin use the proof-of-work (PoW) consensus method. However, Ethereum 2.0, which represents a significant step forward for Ethereum, intends to transition to the proof-of-stake (PoS) technique by 2022. The purpose of this update is to improve scaling and simplify things for users. Fraud, service disruptions, censorship, and outside intervention are impossible on the Ethereum network.

Disadvantages of existing system:

The system does not have the ATTRIBUTE-BASED ACCESS CONTROL POLICY enabled.

It is now impossible to properly apply the IOTCHAIN SCHEME CHARACTERIZATION.

PROPOSED SYSTEM:

By storing Internet of Things data in an autonomous storage system called IPFS integrated within the Ethereum blockchain, this technique eliminates the requirement for traditional cloud or third-party storage.

Set up a strong access control system to prevent unauthorized users from accessing or modifying data. To ensure data security and privacy, we deploy attribute-based access control (A-BAC) and AES-128 encryption. Before sending the IoT stream to IPFS, these methods will encrypt it.

In addition, the Ethereum smart contract contains encrypted hashes. As part of our key management strategy, we also use the elliptic curve Diffie-Hellman key exchange protocol to securely share the secret key. This eliminates the necessity for a reliable private key maker. If a data user loses their private key, the only way to recover it is to retrieve transaction information from the Ethereum blockchain.

For example, IoTChain employs a reward-driven approach. As a reward, the nodes that store the information will receive digital currency. IPFS established a sort of digital cash known as Filecoin. It will be distributed as a reward for using storage nodes. Smart contracts on the Ethereum blockchain are utilized to do private keyword searches within the IPFS.

In the IoTChain architecture, the proof-of-authority (PoA) consensus mechanism replaces the proof-of-work (PoW) approach to reduce transaction costs and accelerate the system. Furthermore, the smart contracts will operate in a logical and ethical manner.

To replicate our strategy, we used the official Ethereum test network Rinkeby and assessed transaction costs and speed.

Advantages of proposed system:

The proposed system incorporates key aspects of blockchain technology, such as its distributed and immutable nature, resilience, use of cryptography to safeguard data, decentralized governance, and ability to execute smart contracts.

The proposed solution employs blockchain technology to facilitate the sharing of medical records. Additional research has been conducted to determine the best strategies to keep medical records secure and organized. To maintain electronic medical records (EMRs) for patients, it is best to employ a decentralized record management system in conjunction with a blockchain-based data exchange technique.

4. IMPLEMENTATION

MODULES:

Cloud server

Group of users

Public verifier

Auditing Module

MODULES DESCRIPTION:

Cloud server

In the first module, we create our system around a cloud server, which securely saves data on a global scale. Our device, Oruta, should include the following features:

A public auditor can use public auditing to verify the accuracy of shared data with others without having to get all of the data from the cloud.

Accuracy: A public checker can quickly ensure that shared data is accurate.

Unforgeability implies that only someone in a group can provide genuine proof of ownership information, such as signatures, for shared data.

Name Privacy: During the auditing process for each block of shared data, the public verifier is not given the signer's name.

Group of users

A group contains two sorts of users: the original user and several group users. Initially, one person creates shared data on the cloud and delivers it to the other members of the group. Everyone in the group is a member, including the person who started it. Everyone in the group has access to and the ability to update information shared among them. The cloud server stores both the data set and the verification information (signature-based data). A public validator can ensure the accuracy of shared data stored on a cloud server for anyone to see. Public verifiers include third-party auditors who provide professional data monitoring services, as well as outside data users who wish to use shared data.

Owner Registration: In this module, the owner must complete the registration process before sending files to a cloud server. They are the only people who can accomplish it. To proceed, he must complete the registration form with all of the requested information. This precise info is stored in a database.

Proof of Identity for Owners: To access this part, owners must provide their email address and password.

User Registration: Before users can access their data from the cloud, they must first provide their personal information. This precise info is stored in a database.

Users who have been granted permission to view the file can do so by logging in with the file ID generated by the data owner during the upload procedure.

Public verifier

A public verifier sends an auditing job to the cloud server to ensure that the shared data is authentic. In response to an auditing challenge, the Cloud server provides the public verifier with confirmation that the shared data is held by different people.

Following that, the public validator ensures that all of the data is correct by verifying the auditing evidence. Public reporting is carried out using a challenge-response mechanism between a public verifier and a cloud server.

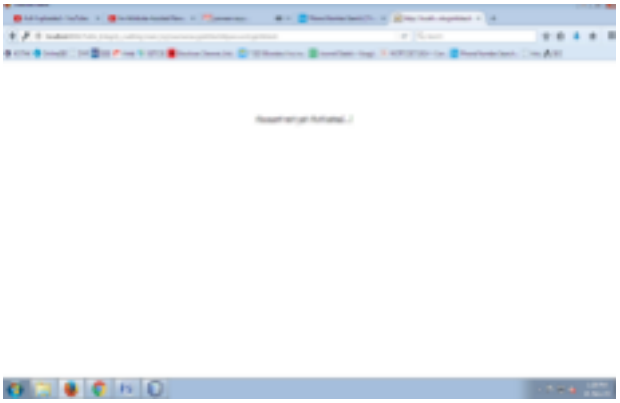
Auditing Module

This module asks if a TPA (cloud maintainer) or a third-party inspector should be registered first. Only cloud service providers can utilize this strategy. When a third-party inspector logs in, they can view how many data owners have uploaded files to the cloud. Here, we provide Third-Party Administration (TPA) services to keep cloud systems operational.

We exclusively consider methods for verifying the accuracy of shared data in cloud systems that use static groups. This line implies that the group is formed ahead of time, before any data is shared in the cloud, and that the members of the group remain constant while data is shared.

Before transmitting data to the cloud, the primary user is responsible for ensuring that only authorized users can access it. Another attractive difficulty is ensuring that shared data on the cloud is secure, particularly in groups that are constantly changing and where people can be added or withdrawn at any time while keeping their identities hidden.

5. RESULTS



6. CONCLUSION

As the number of IoT devices grows, data safety, accessibility, storage management, and transparency become increasingly crucial. Natural calamities, single points of failure, and

devised methods to employ multi-signature conditional provenance, faster and more secure authentication, and privacy protection to rapidly regulate and limit data on the Ethereum blockchain. Our research results demonstrated that our solution provides robust, comprehensive, and indestructible data management services. The simulations suggest that changing from a proof-of-authority (POA) agreement method to a proof-of-work (POW) mechanism reduces gas consumption by 20-25%. Furthermore, out of numerous cryptographic algorithms, AES-128 was the fastest encryption method, topping the others by 65% while keeping the maximum level of security. Based on our review of the study, the concept makes sense and is feasible.

governmental censorship can all render traditional data storage methods inaccessible. So we developed a new way for the Internet of Things (IoT) to share information based on blockchain technology. It has been given the moniker IOT Chain. It enables the secure storage of large amounts of Internet of Things data, allowing only authorized users to access it. Furthermore, it has advantages over a centralized system, such as faster data processing and lower expenses. This study focuses on the issues that arise when attempting to share and preserve information over the Internet of Things (IoT). Our idea makes use of the Ethereum blockchain, the AES encryption method, gas-efficient consensus, and an IPFS-based distributed storage system. There is no requirement for a reliable PKG. We invented an off-chain solution that uses blockchain technology to store genuine Internet of Things (IoT) data. We 103164

REFERENCES

1. M. A. Ferrag and L. Shu, ``The performance evs for the Internet of Things: A tutorial," IEEE Internet Things J., vol. 8, no. 24, pp. 17236_17260, Dec. 2021. aluation of blockchainbased security and privacy system

2. M.Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, ``A systematic review of IoT in healthcare: Applications, techniques, and trends," J. Netw. Comput. Appl., vol. 192, Oct. 2021, Art. no.
3. Sathish Polu and Dr. V. Bapuji. “Analysis of DDOS Attack Detection in Cloud Computing Using Machine Learning Algorithm”, Tuijin Jishu/Journal of Propulsion Technology, Vol. 44, No.5, Pages:2410-2418, ISSN:1001-4055, December2023.

https://www.propulsiontechjournal.com/index.php/journal/article/view/2978

4. V. Hemamalini, G. Zayaraz, and V. Vijayalakshmi, ``BSPC: Blockchainaided secure process control for improving the ef_ciency of industrial Internet of Things," *J. Ambient Intell. Hum. Comput.*, pp. 1_14,Jan. 2022.
5. Sathish Polu and Dr. V. Bapuji, "Distributed Denial of Service (DDOS) Attack Detection in Cloud Environments Using Machine Learning Algorithms", International Journal of Innovative Research in Technology, (IJIRT), Volume 9, Issue7, ISSN:2349-6002.December 2022, (UGC CARE LIST – I).
6. R. Gür_dan and M. Ersoy, ``A new approach with blockchain based for safe communication in IoT ecosystem," *J. Data, Inf. Manage.*, pp. 1_8, Feb. 2022.
7. P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. Moscholiosb, ``Securing the Internet of Things: Challenges, threats and solutions," *Internet Things*, vol. 5, pp. 41_70, Mar. 2019.
8. Sathish Polu and Dr. V. Bapuji," "Mitigating Ddos Attacks in Cloud Computing Using Machine Learning Algorithms", The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA. (CNPJ 32.432.868/0001-57) Vol.No.10, Pages:340-354January2024. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/66109
9. G. Wood. Ethereum: A Secure DecentralisedGeneralised Transaction Ledger. Byzantium Version. [Online].
10. Y. Zhou, J. Wu, and S. Zhang, ``Anonymity analysis of bitcoin, zcash and ethereum," in Proc. IEEE 2nd Int. Conf. Big Data, Artif. Intell. InternetThings Eng. (ICBAIE), Mar. 2021, pp. 45_48.