International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Ensuring Distributed Accountability for Data Sharing in the Cloud

Angelin Rosy M[1], Bakiyalakshmi S[2]

[1]Assistant Professor, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur
[2]II MCA, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur

Abstract:
With the help of abstract computing, companies can now quickly access more or less computing power from the Internet. Even though cloud services help businesses save money, grow easily and be more comfortable, they also raise issues about private data and managing it. Many businesses find it risky that cloud computing users aren't always aware where their information is held or the work happening on other servers. When information involving money or health is not made transparent, customers are more cautious about using cloud services which may stop many from trying them. In this report, we propose a design for a decentralized information accountability framework to watch over and track how users' data is handled by cloud service providers.

Keywords: cloud computing, storage security, public auditability,data integrity,data dynamic.

INTRODUCTION

Using cloud computing, users can get their hands on storage, computer power and software over the internet, immediately and with little to no upfront expense. Because it scales, flexes and always remains available, it is often chosen both by individuals and enterprises. Yet, using cloud computing is convenient, but it can be tricky to keep data safe and secure, since the data is stored remotely by third-party firms. Although these providers handle all the infrastructure required, users might not see or control exactly how their data is being used.

What matters most is that companies like Amazon, Google and Microsoft hide the technology details from anyone using their cloud services. For this reason, users might be unclear about the safety of their data which can lead to worry about unauthorized use, theft or abuse. Many people avoid using cloud services because the sensitive information they keep such as health, finances and personal identity, isn't always handled securely.

Also, using this approach improves the reputation of cloud service providers since it ensures they follow privacy regulations. Because privacy is becoming a bigger concern, organizations must have an accountability system to win their customers' trust and follow the rules. Wider adoption of cloud services can only happen if decentralized accountability is integrated to address concerns about privacy.

Industry experts consider decentralization an effective way for users to manage their data, even as it allows them to use the helpful features and scaling options of the cloud.

With this technique, access to data is checked and recorded independently of the cloud provider, making

it possible for users to monitor and control their data human resource consulting services, without only using the cloud provider's internal tools.

PROPOSED WORK

1. The system suggests a new way of doing cloud computing, concentrating on clearer ownership and understanding of data.
2. Using blockchain and other distributed ledger technologies, the system guarantees that all data access and use is seen and audited by others.
3. Because data is decentralized, users now have more power to protect their personal information.
4. As a further feature, the system supports real-time monitoring and auditing, enabling users to see exactly when and by whom their data was accessed.
5. Share files are to have Case Sensitive names.

MODULES

User Registration

You need to register your user id and password before you can view the home page. This is so we can identify our users and make sure they belong to our Community. The user needs to pick the constant factor and every user is given a special random salt. At registration, the user must opt for the random function to be used for the future.

Login

In this stage of code, a user selects a digit from his password and this is a, the same with a digit chosen from his random salts password—b. Finally, they add the constant value from before. At last, use the a, b and constant values with the function chosen by the user. If the result found by the system is the same as the user's password, the system allows the user to proceed with login.

File Download

Some Content is available to download from the Cloud. These files are put up online by the data owner. If user have the necessary all rights, then they can download the files. Individuals whose download rights are missing are only able to view cloud files online. Here we play a role in managing user accounts. There are people in organizations who have all of the rights. Specific rights are available to else.

Admin Module:

1. We are needing specific information from users to register them in the system. The admin can also see, edit and remove user details when needed.
2. To upload files for use on a network from your PC, you need to be logged in via a personal computer.
3. Copying in such a way means downloading files. That way admin can download files he added.
4. In cloud, cloud users use the approach by being swift, firm and respectful when people misbehave within that environment.
5. The server looks at the token and ensures it is similar to the record it holds.

SOFTWARE DESCRIPTION

Back in 1995, a self-employed software developer named Rasmus Lerdorf wrote a Perl/CGI script that let him check how many people were reading his online résumé. With the script, the Web page involved logging new visitors and immediately showing how many guests were currently there. Since the Web was just starting back then, these types of tools didn't exist yet and they led many people to write to Jack asking

about both of his scripts. As soon as someone visits your PHP web page, the web server will process its PHP code for you. After that, it figures out what users see (that is, content and images) and what they do not (files and calculations) and it changes your PHP code into HTML. When it is translated into HTML, your visitor's browser is sent the webpage file.

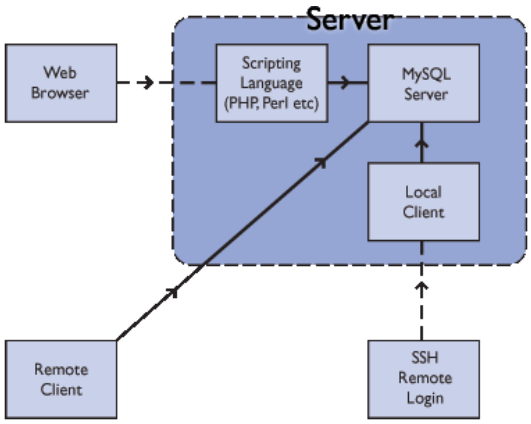


Figure 1: System architecture

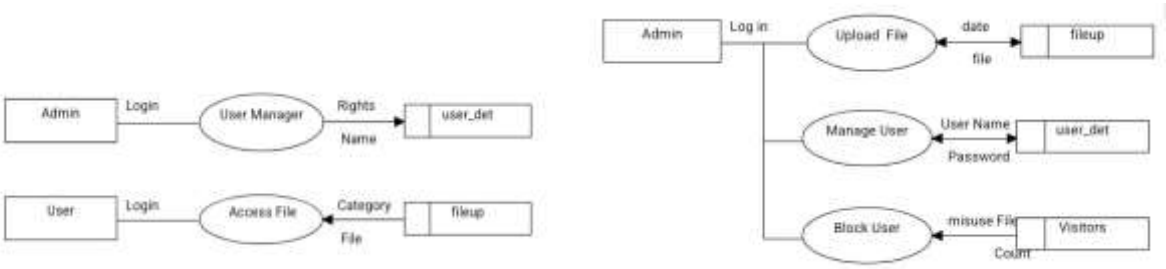
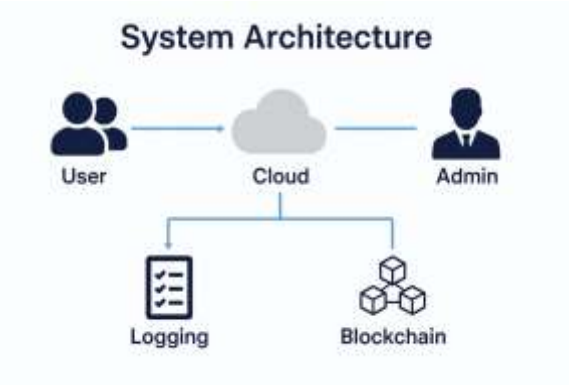


Figure 2: Data architecture



Usage of PHP

How you use PHP As of 2000, there were hardly any PHP web sites being developed. In 2007, there were over 2, 00, 00, 000 of these cushions and their numbers continue to rise. It is currently PHP that enables the creation of the world's most visited sites.

PHP Security

All discovered vulnerabilities in computer software are listed in the National Vulnerability Database. At the time, the amount of PHP-related vulnerabilities included in the database was: 20% in 2004, 28% in

2005, 43% in 2006, 36% in 2007 and 35% in 2008. Most of these issues can be exploited from anywhere: they give hackers access to your data on web servers, allow them to send spam and spread malware and make it possible for them to cause a DOS attack.

Data types

On each operating system, PHP has its own limit for storing whole numbers. Typically, the range is for 32-bit signed integers. Sometimes, unsigned integers are seen as signed values which is not usual in other programming languages.

Integer variables are able to be set using decimal, octal and hexadecimal forms. Floating point numbers follow different storage ranges according to the system they are used on.

Functions

PHP includes hundreds of standard functions, plus thousands more from extensions.

All of this information can be found on the PHP site, but the built-in library has a number of differences in function names.

Platforms and interfaces

Tools and means of communication MySQL is programmed using C and C++. MySQL was designed to function on many systems, including: AIX, BSDi, FreeBSD, HP-UX, i5/OS, Linux, Mac OS X, NetBSD, Novell NetWare, OpenBSD, Open Solaris, eComStation, OS/2 Warp, QNX, IRIX, Solaris, Symbian, SunOS, SCO Open Server, SCO UnixWare, Sanos, Tru64 and Microsoft Windows. A port of MySQL is available for use on OpenVMS. Storage engines are a feature of MySQL. MySQL is unique among many database servers since it gives users a wide range of features and options based on their specific situation. From a server's perspective, its default settings work fine across many different hardware systems. Various data types are available when you design tables to hold your data during application development. What's different here is that you can select the type of table that stores your records.

MySQL storage engines

Thinking about storage engines and their benefits for MySQL will be easier if you clearly picture where they are enlisted. The illustration in Figure 2-1 gives a logical picture of MySQL. It doesn't always capture the detailed way things are built which is usually more complex and not always clear. Even so, it helps you understand the role of storage engines within MySQL. Just before this book was created, MySQL got the NDB storage engine. Be on the lookout for an update to this book in the second edition.)

MySQL Architecture

Phishing attacks are detected right away and special authentication methods are provided for users who take part in approval procedures. Using this process, the system can easily integrate future security methods thanks to incorporating biometric or blockchain technologies.

RESULTS

The system operates effectively to detect phishing attacks immediately and creates secure visual authentication procedures for users during approval processes. The system creates a reliable platform for future security integration by enabling biometric or blockchain technologies since both are depicted in Figs.

CONCLUSION

The development and implementation of this system have been a comprehensive journey, from the initial design to its successful deployment. The integration of blockchain for decentralized tracking, along with a robust user authentication system, ensures that both security and transparency are at the forefront of the system's architecture.

The file management module, combined with role-based access control, guarantees that users can manage their files effectively while ensuring that unauthorized access is prevented. The inclusion of detailed logging and auditing capabilities not only enhances security but also provides valuable insights into system usage and potential issues, further strengthening its reliability.

The system uses visual cryptography mechanics that split user-based images into shares alongside time-sensitive OTPs to minimize unauthorized access attempts.

The preprocessing procedures simultaneously boost system accuracy while protecting against conventional phishing attempts which makes the model appropriate for real-world deployment while ensuring security.

File Analysis: One potential enhancement for the system would be the integration of machine learning algorithms to analyze the content of the uploaded files.

Enhanced User Role Management: This would provide greater flexibility in managing different user groups and could be particularly beneficial in large organizations.

AI-Based File Security Scanning: Leveraging AI and machine learning, the system could scan files for potential security threats such as viruses, malware, or ransomware before they are uploaded.

Multi-Factor Authentication: To further enhance security, implementing multi-factor authentication (MFA) for both users and administrators could be a valuable future enhancement.

REFERENCES

1. In 2022, Smith and Chen conducted this research. The use of blockchain to protect data in the cloud setting is discussed in the topic. International Journal of Cloud Computing and Services, issue 15.3: 234-245. In 2020, Stojanovic and Fisher published their work on this subject. Blockchain as a Technology for Cloud Computing. Springer.
2. Williams, H. & Zhang, F. published in 2021. Enhancements in Decentralized Cloud Storage and Security Protocols." Find the article in the Journal of Computing and Information Technology at 27(1), pp. 112-124. In 2021, Kumar, P. and Gupta, R., authored the report.
3. The report was written by A. Garcia and S. Li in 2020. Use of Machine Learning for Grouping Files and Manage Content in the Cloud. Published in Journal of Cloud Computing and AI, Vol 9 No 2, pages 56-67.
4. O'Conner and Patel wrote the article in 2021. "A Detailed Look at Using Blockchain in Cloud Storage." The article was published in International Journal of Blockchain Technology, Volume 13, Issue 4, pages 478-491.
5. In 2020, Lee, D. and Park, Y., completed the study. How Can Blockchain Improve Security in Cloud Storage. The Journal of Information Security and Privacy, vol 15, no 5, pp 202-213.
6. Recent research by Jones and Kumar was done in 2022. Managing Access to Files Using Roles in the Cloud. The article appeared in the Journal of Network Security and Privacy 10(3) pages 157-168.
7. Lopez, C. and Torres, M., published their paper in 2019 Addressing Security Issues in Cloud Data Access Control: Discussion of Obstacles and Possible Solutions. Cloud Computing Security Journal, volume 5, issue 6, pages 34-45.
8. L. Zhang and Z. Yang collaborated in writing this (2021). Managing data in the cloud with secure and transparent decentralized technology. International Journal of Data Science and Security, 11(1), pages 102 to 115.