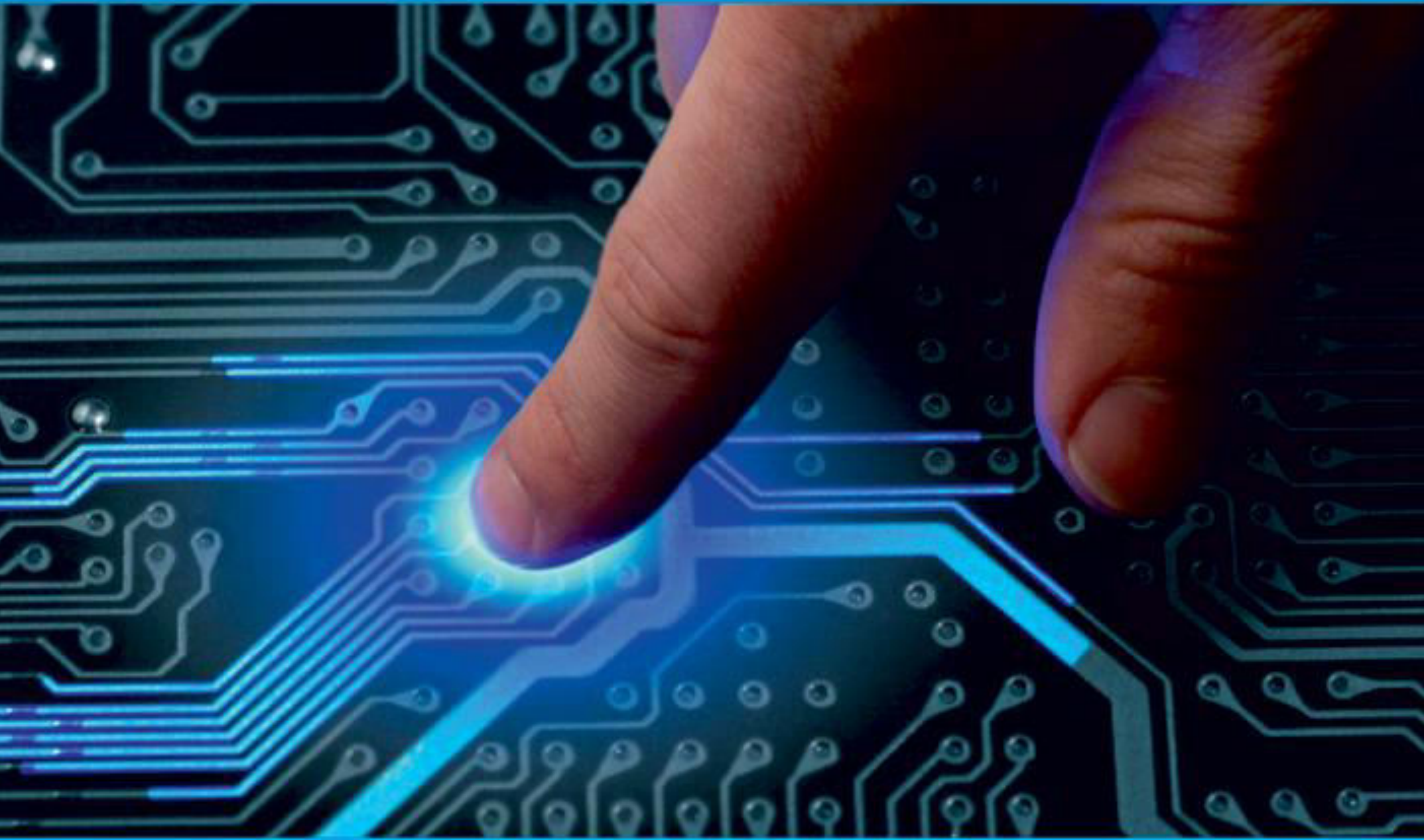
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103103 |

Blockchain Based Cloud File Sharing System

Durairam.R,Nandhasriram.P, Madhan.M, Ramu.A, Yuvaraj.A

Department of Computer Science and Engineering, Mahindra Institute of Technology, Namakkal, India

ABSTRACT: As cloud services greatly facilitate file sharing online, there's been a growing awareness of the security challenges brought by outsourcing data to a third party. Traditionally, the centralized management of cloud service provider brings about safety issues because the third party is only semi-trusted by clients. Besides, it causes trouble for sharing online data conveniently. In this paper, the blockchaintechnology is utilized for decentralized safety administration and provide more user-friendly service. Apart from that, Ciphertext-Policy Attribute Based Encryption is introduced as an effective tool to realize fine-grained data access control of the stored files. Meanwhile, the security analysis proves the confidentiality and integrity of the data stored in the cloud server. Finally, we evaluate the performance of computation overhead of our system.

I. INTRODUCTION

Nowadays, the problem faced by various organizations is storing an enormous amount of data. To address this issue, organizations have adopted cloud storage as an option to store data. Due to this in the last few years, cloud-based services have increased. These services facilitate remote storage of user data on the cloud as well as properties like sharing and transferring of data. Organizations need not maintain in-house storage because services are available irrespective of time and location across multiple platforms. Despite the mentioned benefits, there are various problems associated with cloud storage. They are maintaining the confidentiality and integrity of data. Data stored on the cloud may contain sensitive information. However, here copyright issues come into the picture. As we are uploading data on the external environment, anyone other than the owner can access data. Security is the most crucial parameter that should be taken into consideration while storing data on the cloud. But, loud service providers don't ensure a high level of security. Currently, there are very few options available to guarantee the security of data on cloud servers.

With the rapid development of mobile computing, wearable technology and wireless sensing, people have been using different types of mobile and wearable devices, such as smartphone, smart watch, smart band and smart glasses etc., to realise various health-related applications, such as remote diagnosis [1], disease monitoring [2] and elderly people caring [3]. Large amount of personal health data are produced by these devices and these data are valuable resources for healthcare research and commercial applications. Properly sharing personal health data will benefit all related stakeholders including the device users, patients, researchers, companies and even the whole public healthcare system. As personal asset, the health data should be owned and controlled by the respective users themselves, while in reality they are usually controlled by different service providers, device manufactures or scattered in different healthcare systems [4], [5]. In general, it brings barriers for the data sharing and puts data security and privacy at risk as these centralised data stores and authority providers are attractive targets for cyber-attacks [6]. The blockchain technology has gained substantial popularity in recent years, primarily in financial field, due to the cryptocurrencies.

II. LITERATURE SURVEY

1. Decentralized File Storing and Sharing System using Blockchain and IPFS
Author - MihirNevpurkar, ChetanBandgar, RanjeetDeshmukh
Year - 2022

Data is considered asthe basic building block for any system. If data is not handled in secured way then this insecurity may lead to many threats for existing system. It is necessary to provide a system which can overcome security loopholes of current systems being used so that those systems will be able to store and share most valuable data of the users in a secured way. In the proposed methodology,the design and implementation of a decentralized file storage and sharing system is carried out using Blockchain and IPFS technologies. Various principles of smart contracts, decentralized storage, cryptographic hashing algorithms, peer to peer networking are taken into consideration while developing system using blockchain and IPFS. The web application is designed such that any person can store and send their data in secured way. The aim of this system is to develop a web application which ensures security, authenticity and integrity of data.

2. Blockchain based Cloud Data Storage System
Author - AishwaryaPatil, SwapnajitPatil, Sachin Rokade, Vijay Sharma
Year - 2020
In today's world, the simplest way to share data is through the internet. Cloud computing is a technology provided by the internet, which is dependent on large storage providers. These storage providers act as untrusted third parties who manage enormous data stored on the cloud. This data may contain sensitive information that belongs to multiple individuals or organizations. Such types of models may involve security issues like privacy and integrity. In this paper, we introduce a prototype of a multi-user system for access control to documents that use the blockchain technology for securing shared data storage. The data owner is allowed to upload the documents on the cloud using Web Portal and the user will request an access link of the document from the owner. Whenever the user tries to access the document using the provided link, a smart contract will be triggered which will send a notification to the owner. The owner will receive the notification to grant permission to the user. The user who has the permission to access a particular document stored on the cloud can only access it. The above operation on the document will be recorded on the blockchain. Owner can always see the logs to find any suspicious operation on the documents. Therefore, the privacy of data is ensured using the smart contracts, immutability property and ledger of blockchain.

3. Blockchain-based Personal Health Data Sharing System Using Cloud Storage
Author - XiaochenZheng, Raghava Rao Mukkamala, Ravi Vatrapu
Year - 2018
With the advent of rapid development of wearable technology and mobile computing, huge amount of personal health-related data is being generated and accumulated on continuous basis at every moment. These personal datasets contain valuable information and they belong to and asset of the individual users, hence should be owned and controlled by themselves. Currently most of such datasets are stored and controlled by different service providers and this centralised data storage brings challenges of data security and hinders the data sharing. These personal health data are valuable resources for healthcare research and commercial projects. In this research work, we propose a conceptual design for sharing personal continuousdynamic health data using blockchain technology supplemented by cloud storage to share the health-related information in a secure and transparent manner. Besides, we also introduce a data quality inspection module based on machine learning techniques to have control over data quality. The primary goal of the proposed system is to enable users to own, control and share their personal health data securely, in a General Data Protection Regulation (GDPR) compliant way to get benefit from their personal datasets. It also provides an efficient way for researchers and commercial data consumers to collect high quality personal health data for research and commercial purposes.

4. Towards Blockchain-based Scalable and Trustworthy File Sharing
Author - Shujie Cui, Muhammad RizwanAsghar, and Giovanni Russello
Year - 2021
In blockchain-based systems, malicious behaviour can be detected using auditable information in transactions managed by distributed ledgers. Besides cryptocurrency, blockchain technology has recently been used for other applications, such as file storage. However, most of existing blockchain-based file storage systems can not revoke a user efficiently when multiple users have access to the same file that is encrypted. Actually, they need to update file encryption keys and distribute new keys to remaining users, which significantly increases computation and bandwidth overheads. In this work, we propose a blockchain and proxy re-encryption based design for encrypted file sharing that brings a distributed access control and data management. By combining blockchain with proxy re-encryption, our approach not only ensures confidentiality and integrity of files, but also provides a scalable key management mechanism for file sharing among multiple users. Moreover, by storing encrypted files and related keys in a distributed way, our method can resist collusion attacks between revoked users and distributed proxies.

III. EXISTING SYSTEM

The research about using personal data generated by mobile and wearable devices to improve the quality of healthcare service has been popular for decades. One of the most challenging tasks during these studies is data acquisition, which is usually costly and time consuming. Most people believe that their medical and other health-related data is private and not willing to share it due to the concerns about data security and privacy. The success of blockchain technology in the financial field demonstrated that, trusted and auditable computing is possible using a decentralized network of peers accompanied by a public ledger. There have been many studies about applying blockchain technology to other fields beside financial recently. In 2015, the study in used blockchain to protect the privacy of personal data.

DISADVANTAGE

- Health data can be divided into continuous data and instant data.
- The instant data are obtained in one single measurement.
- The data reflecting the same health indicator may belong to different categories.

IV. PROPOSED SYSTEM

As mentioned above, our study only focused on the continuous-dynamic data. These data are usually generated by standard sensors. The information of the sensor is accessible through the APIs of the devices. Moreover, the pattern of the collected data can be evaluated using advanced machine learning techniques to make sure that the data is valid according to certain validation patterns or checks. It enables us to validate the quality of the data from both hardware and software aspects. Take the above-mentioned acceleration data as an example and imagine that a user’s acceleration data are collected by a smart watch during 24 hours. The quality validation algorithms will be able to distinguish sleep from other daily activities. The data corresponding to the sleep period could be classified as high-quality data or noise depending on if the user want to share sleep related data or only other daily activities.

ADVANTAGE

- Hardware aspect
- Data sharing transaction validation
- Cloud storage
- Data encryption
- Crypto token

MODULES DESCRIPTION

Blockchain based Cloud File Sharing System

A cloud file system is a storage system that allows for shared access to file data. Users have the ability to create, delete, modify, read, and write files. Cloud file sharing is a service that allows multiple users to access a common set of file data. Cloud file sharing security is managed through user and group permissions, allowing the admin to tightly control access to shared file data.

Authorization Or Access Control Policies

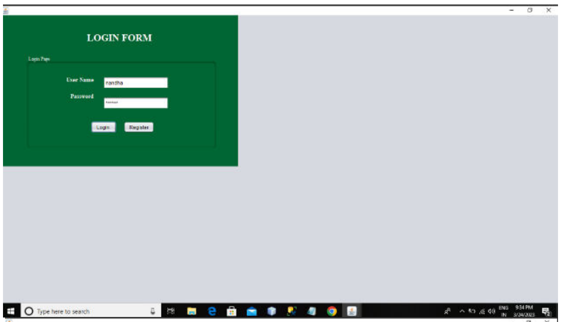
Users can easily share files with one another by using our blockchain-based application and the cloud-based file sharing method. As a result, this system enables users to easily and effectively store and share files via cloud networks. When we upload data to the cloud, we typically lose control of it, introducing new security risks to the integrity and confidentiality of our data. For sensitive and private data, security is a major concern. The user can specify who has access to which resources based on certain attributes or roles using authorization or access control policies.

Third Party Organisations

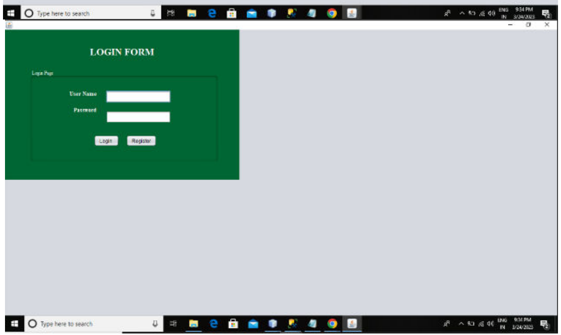
Third party organisations usually access documents through a shared link given by the owner with proper access rights. There seems no significant problem there. Stil as a measure of precaution, the organisation will need permission granted from the owner. In the worst case, we could imagine a situation in which the organisation passes on the shared link to the next organisation. In that case this system is helpful because of the second step of permission grant.

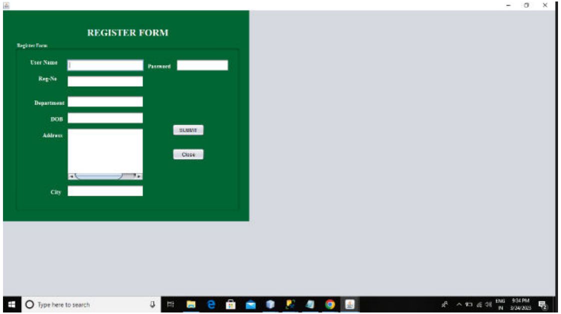
Secure File Sharing

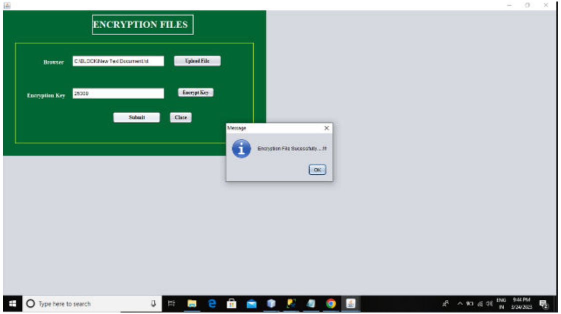
Cloud computing is a relatively new technological advancement that has steadily increased market share over the last three years. In this paper, we will present a new methodology for securely sharing files via the cloud, combining block chain for secure transactions and viewing the shared files. Many individuals utilise file shredding software. Some people utilise these apps to make money by sharing their work in the form of files. We've all heard of Chegg, Scribd, and other similar services that provide a platform for students , researchers, freelancers to publish their work. However, in order to use these programmes, we must have a membership. Even if a user wants to access the files, he or she must pay a fee to the application rather than the author.



User Name nandha



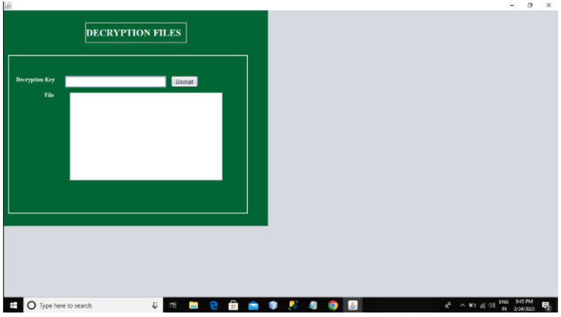




Browser C:\BLOCK\New Text Document.txt

Encryption Key 25320

Encryption File Successfully ....!!!



V. CONCLUSION

In this paper we proposed a personal health data sharing system based on blockchain, cloud storage and machine learning techniques. It enables users to own, control and share their personal health data easily and securely, and get benefits during this process. In this work, first, we classified personal health data into different categories according to data characters (dynamic and static data), and the data acquisition methods (continuous and instant data) in the context of health related data from wearables and mobile devices. We proposed to use different solutions to share the large size continuousdynamic data using hash pointers to the storage location.

REFFERENCES

[1] D. Son, J. Lee, S. Qiao, R. Ghaffari, J. Kim, J. E. Lee, C. Song, S. J. Kim, D. J. Lee, S. W. Jun et al., “Multifunctional wearable devices for diagnosis and therapy of movement disorders,” Nature nanotechnology, vol. 9, no. 5, p. 397, 2014.

[2] X. Zheng, A. Vieira Campos, J. Ordieres-Mere, J. Balseiro, ´ S. Labrador Marcos, and Y. Aladro, “Continuous monitoring of essential tremor using a portable system based on smartwatch,” Frontiers in neurology, vol. 8, p. 96, 2017.

[3] Y. Gao, H. Li, and Y. Luo, “An empirical study of wearable technology acceptance in healthcare,” Industrial Management & Data Systems, vol. 115, no. 9, pp. 1704–1723, 2015.

[4] U. Varshney, “Pervasive healthcare and wireless health monitoring,” Mobile Networks and Applications, vol. 12, no. 2-3, pp. 113–127, 2007.

[5] J. Zhang, N. Xue, and X. Huang, “A secure system for pervasive social network-based healthcare,” IEEE Access, vol. 4, pp. 9239–9250, 2016.

[6] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A blockchainbased approach to health information exchange networks,” in Proc. NIST Workshop Blockchain Healthcare, vol. 1, 2016, pp. 1–10.

[7] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[8] S. T. Ali, D. Clarke, and P. McCorry, “Bitcoin: Perils of an unregulated global p2p currency,” in Cambridge International Workshop on Security Protocols. Springer, 2015.

[9] R. Bohme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, ¨ technology, and governance,” The Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–238, 2015.

[10] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. R. Mukkamala, and R. Vatrapu, “Breaking bad: De-anonymising entity types on the bitcoinblockchain using supervised machine learning,” in Proceedings of the 51st Hawaii International Conference on System Sciences, 01 2018.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING