GLOBUS PUBLICATION

Cosmos Journal of Engineering & Technology
A Refereed Research Journal
Vol 13 / No 1 / Jan-Jun 2023 ISSN: 2231-4210

SECURING DATA COMMUNICATION USING BLOCKCHAIN

[*] Balakrishna Nayudori
[**] Raju Kummari
[***] Venu Kunareddy
[****] Naveen Kumar Vunnam

Paper Received: 17.02.2023 / **Paper Accepted**: 25.03.2023 / **Paper Published**: 26.03.2023
Corresponding Author: Naveen Kumar Vunnam; Email: naveennavy219@gmail.com; doi:10.46360/cosmos.et.620231009

Abstract

In the digital era, data has become so important. So has the responsibility to protect it from unauthorized access. Digital data certified bya reputable organization are valuable digital data that can be stored or shared on the internet. However, the problems of ensuring the anonymity of organizations on issued certificates, verifying thereliability of shared data while still ensuring the confidentiality of its content still exist. This paper presents the methods to ensure the security of data while storing and sharing. In the data-producing schema, an organization in the group generates valuable digital data from raw data sent from a data owner and then issues a certificate on the ciphertext of this digital data. In the data storing schema, the data owner uploads his/her data to the public Inter Planetary File System network and then stores the access address of the stored data and the corresponding certificate on the blockchain ledger. In the data sharing schema, everyone on thesystem could verify the reliability of shared data before sending a data sharing request to the data owner. The schemas of data storing and sharing and sharing guarantee security propertiesincluding confidentiality, integrity, privacy, and anonymity.

Keywords: Blockchain, Data Encryption, Data Decryption, Data Producing, IPFS, Data Storing, Data Sharing.

Introduction

There has been exponential data growth in the world, and trusted data are considered one of the most valuable assets of individuals and organizations. The amount of data created and stored globally is predicted to create about 175 zettabytes by 2025. Consequently, the demand for valuable data storing and sharing is tremendous, which also poses challenges related to data is tremendous, which also poses challenges related to data security in the processes of data storing and sharing. Currently, there are two main architectures used for data storing and sharing, centralized and decentralized architectures. For the centralized architecture, organizations can store data on their data center system. However, these systems have high operating costs and are limited in scalability. Using cloud storage services can reduce costs and can be flexible in system expansion. However, the centralized architecture has two limitations including. Data security, stored data could be accessed, modified, or removed illegally by system administrators or attackers who compromised the system. Availability when the centralized systems are crashed due to system overload, denial-of-service or distributed denial-of-service or distributed denial-of-service (Dos/DDoS) attacks, or system errors, the services are not available for users .For decentralized architecture, most solutions use blockchain (BC) technology as the main component in the systems because of its properties such as anonymity, transparency decentralization, and auditability. However, current solutions do not provide features for verifying the accuracy and the reliability of the shared data on the BC network.

Specifically, data verified and certified by a reputable organization (RO) are considered meaningful data (MD). For instance, in the medical field, a diagnostic result of an electronic medical record is published by a reputable medical organization with highly skilled doctors, which is MD. MD needs to be securely stored on the system, besides a data owner (DO) can completely share or commercialize his/her MD to other people or organizations on the network. Data sharing methods must ensure that requesters can verify the reliability and accuracy of shared data before deciding to perform a data-sharing contract.

Literature Survey

It presents a survey of the current state of-the-art in data center networks virtualization, and provide a detailedcomparison of the surveyed proposals. We discuss the key research challenges for future research and point out somepotential directions for tackling the problems related to data center design [1]. A data storage framework not only enabling efficient storing of massive IoT data, but also integrating both structured and unstructured data.

*–**** *Department of CSE, Sree Vidyanikethan Engineering College, Tirupati, India.*

This data storage framework is able to combine and extend multiple databases and Hadoop to store and manage diverse types of data collected by sensors and RFID readers.

In addition, some components are developed to extend the Hadoop to realize a distributed file repository, which is able to process massive unstructured files efficiently [2]. The proposed solution includes strategies for expressing common IoT datain the form of key-value pairs, as well as a data pre-processing and sharing mechanism to build a Web of Things connecting HTTP-enabled smart devices such as sensors and actuators with virtual "things" such as services, social networks, and APIs. Its multi-layer architecture was claimed to reduce the amount of data to be processed at the cloud management layer. Besides, the work also provided several experiments that showed a promising performancewhen storing and querying a huge volume of data [3]. The survey on emerging technologies toward the real-timeutilization of IoT data streams in terms of networking,processing, and content curation and clarify the open issues. Then we propose a new framework for IoT data streams called the Information Flow of Things (IFoT) that processes, analyzes, and curates massive IoT streams in real-timebased on distributed processing among IoT devices [4]. This solution assumes the existence of multiple distributed cloud data centers, called mini-Clouds, among which data can be replicated model our problem comprehensively based on various parameters such as effective bandwidth of the IoT network, available number and size of data items at eachmini-Cloud, and we present our problem as a collection of various sub-problems based on subsets of these parameters [5].

Objective

The objective of this paper is to provide a solution to secure data producing, data storing, and data sharing with confidentiality, integrity, privacy and anonymity. Existing System provides the data sharing and data producing but there are no capabilities for validating the accuracy and reliability of shared data on the BC network inthe solutions. Meaningful data is defined as data that has been validated and approved by a reputable organisation (RO) (MD). Data storing and sharing for certified digital data are very necessary, which requires data storage and sharing.

Proposed System

Our proposed scheme for data production, data storage and information sharing We use a group authentication protocol in the data generating structure for a team of reputable companies that provide the identical sort of service. One of the organizations in the group produces valuable online information from raw data sent by a data owner and then concerns a certificate based on the encrypted message of this digital information.

Limitations

- Blockchain can slow down when there are manyusers on the network.
- Blockchain implementation is a costly process.

Methodology

Blockchain technology is a decentralized ledger recording all confirmed transactions and is also considered as a linked list of blocks, in which each block is pointed to its previous block via a hash pointer containing a hash valueof the predecessor at a fixed time. The first block of the chain is called the genesis block which has no parent block, so the previous hash value field of the block is initialized bythe BC network builder. The general structure of each blockconsists of a block header and a block body, where a blockheader contains management information of block as well aschain such as block id, version, previous hash, timestamp, while a block body stores a list of transactions There are twotypes of nodes on a BC network. User nodes which only perform transactions and do not hold the ledger. And miner nodes which are responsible for verifying transactions, creating new blocks, and holding a ledger. The ledgercontains blocks that reached the consensus from honest miners, and data in the ledger is immutable. A miner node can also perform transactions as a user node. Each node owns a public/private key pair where the private key is used to sign transactions, while the public key is as the Blockchain address of the node. In general, there are three types of Blockchain networks: Public Blockchain, private Blockchain, and consortium Blockchain. Nodes in aBlockchain network communicate directly with each other through a peer-to-peer network. Therefore, to synchronizedata on the ledger of miners, one of the consensus protocols can be deployed in a Blockchain system.

Conclusion and Future Work

In this paper, we propose three schemes: data producing, data storing, and data sharing. In the data producing scheme,we consider RO as DP, a group manager sets up a group ofDPs providing the same type of services. DP can generateMD from RD sent from DO, and then issues a certificate on EMD. In the data storing scheme, we provide not only the confidentiality and integrity of the stored data but also the anonymity of DP and the privacy of DO which have not been fulfilled in the existing solutions. In the data sharing scheme, everyone on the system can verify the reliability of shared data before submitting a sharing request to DO. Notethat everyone can only verify the reliability of the

shared data but cannot read its contents. This property could not be fulfilled by existing solutions. In addition, the data sharingprocess is done directly between DO and DU without depending on any intermediaries. The results of the security analysis show that the proposed schemes meet the security properties including confidentiality, integrity, privacy, non-repudiation, and anonymity.

In the future work, we will apply the proposed system to specific applications such as IoT, electronic medical records. We will then evaluate and optimize the schemes.

Conflict of Interest

There is no conflict of interest between the authors in this manuscript.

References

1. Bari, M. F., Boutaba, R., Esteves, R., Granville, L. Z., Podlesny, M., Rabbani, M. G., Zhang, Q. and Zhani, M. F. (2013). Data center network virtualization: A survey. EEE Commun. Surveys Tuts., 15(2), 909-928, 2nd Quart.
2. Jiang, L., Xu, L. D., Cai, H., Jiang, Z., Bu, F. and Xu, B. (2014). An IoT-oriented data storage framework in cloud computing platform. IEEE Trans. Ind. Informat., 10(2), 1443-1451.
3. Phan, T. A., Nurminen, J. K. and Francesco, M. Di (2014). Cloud databases for Internet-of-Things data. In Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. SocialComput. (CPSCom), 117-124.
4. Yasumoto, K., Yamaguchi, H. and Shigeno, H. (2016). Survey of real-time processing technologies of IoT data streams. J. Inf. Process., 24(2), 195-202.
5. Kumar, A., Narendra, N.C. and Bellur, U. (2016). Uploading and replicating Internet of Things (IoT) data on distributed cloud storage. In Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD), 670-677.