


Chapter 11

A Study on Data Sharing Using Blockchain System and Its Challenges and Applications

Santosh Kumar Smmarwar

National Institute of Technology, Raipur, India

Govind P. Gupta

 <https://orcid.org/0000-0002-0456-1572>

National Institute of Technology, Raipur, India

Sanjay Kumar

National Institute of Technology, Raipur, India

ABSTRACT

Blockchain since 2009 has been gaining more popularity in various fields to use in numerous applications to overcome the security issues such as privacy, transparency, and mutability of data in the process of data sharing. Process of data sharing has many addressed and unaddressed challenges such as information encryption and decryption, data authentication, storage security, latency time, transfer speed of data, detecting malicious nodes, prevent the computer system from attacks, trust in the sharing process. In this chapter, the authors have reviewed the data sharing paper based on blockchain technology and presented the analysis of various techniques used in the information sharing process. The comprehensive analysis is categorizing in the following areas like incentive mechanism-based work, IoT-based data sharing, healthcare data sharing, and internet of vehicle data sharing using blockchain.

INTRODUCTION

In the recent era of Big Data development with the advancement in information and communication technology the rate of growing data and digital resources has been grown exponentially. Storing these data has become important for customer and business organizations (Feng et al., 2019). One of the ways to control the growth rate of data to reduce the same information creation is through the data sharing

DOI: 10.4018/978-1-7998-7789-9.ch011

process in various organizations such as health care, academic, financial sector, etc. Data sharing has many uses in various fields such as healthcare, the internet of things, smart devices, and internet of vehicles, supply chains, and logistic networks. In data sharing, secure data sharing is necessary to achieve security goals like confidentiality, integrity, availability, authentication, transparency, and privacy of the data. These problems can be overcome by using blockchain technology in making data sharing transparent, immutable, decentralized storage, integrity protected, and confidentiality. The feature of transparency and immutability of blockchain made it most popular to deploy or integrate into secure data sharing. Blockchain technology is based on the three pillars that are distributed ledger, peer-to-peer communication, and consensus protocol. These are the core of this technology that makes it more secure and transparent (McGhin et al., 2019). In this survey study, we have reviewed the blockchain used data sharing papers and analyses various methods used by the early researcher for secure data sharing to resolve the privacy concern by using some cryptographic techniques.

OUR CONTRIBUTION

In this research paper we have reviewed the work of data sharing using blockchain technology, to get a research trends of various security mechanism used in blockchain for information sharing. We found that in our study most of the author described comprehensive overview of secure data sharing by proposed method such as incentive mechanism, privacy preserving scheme, dynamic data access control policy, secret sharing schemes and some attribute based encryption technique. In this paper we demonstrated the summary of existing work and methods used in blockchain to secure data sharing. Shown existing work, pros and cons of early research work in areas of healthcare data sharing and IoT device-based data sharing, incentive-based data sharing and various industrial application.

MOTIVATION

As mentioned above security challenges faced by centralized authority such as single point of failure may lead to the collapse of all data, high sharing cost, reduce manual verification (Goyal et al., 2018), reduce wastage of time, brings transparency and immutability in the system encourage us to work on secure data sharing among the peer to peer or decentralize environment by integrating blockchain technology and smart contract functionality (Mohanta et al., 2019). Since the inception of blockchain technology came into existence these have brought some potential solutions that may be overcome by using blockchain in various emerging fields of information technology.

OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain is distributed ledger technology initially developed for cryptocurrency purposes like bitcoin by an unknown person named Satoshi Nakamoto in 2009 (Feng et al., 2019), (McGhin et al., 2019). It is a decentralized system of digital ledger stored the synchronized copy of data. The blockchain system is based on asymmetric cryptography where two keys, a public key for device identification and a private key for signing transactions used (Goyal et al., 2018). Blockchain is a chain of the block, each block

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/a-study-on-data-sharing-using-blockchain-system-and-its-challenges-and-applications/292238

Related Content

Security Issues for Cloud Computing

Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham (2010). *International Journal of Information Security and Privacy* (pp. 36-48).

www.irma-international.org/article/security-issues-cloud-computing/46102

Blockchain-Based Data Market (BCBDM) Framework for Security and Privacy: An Analysis

Shailesh Pancham Khapre, Chandramohan Dhasarathan, Puviyarasi T. and Sam Goundar (2023).

Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 162-180).

www.irma-international.org/chapter/blockchain-based-data-market-bcbdm-framework-for-security-and-privacy/310446

Access Control, Authentication, and Authorization

Joseph Kizza and Florence Migga Kizza (2008). *Securing the Information Infrastructure* (pp. 180-208).

www.irma-international.org/chapter/access-control-authentication-authorization/28504

The Advancing Cybersecurity Ecosystem of Israel: An Overview of Current Challenges and Opportunities in the Early 2020s

Szabolcs Szolnoki and Árpád Ferenc Papp-Váry (2021). *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 37-60).

www.irma-international.org/chapter/the-advancing-cybersecurity-ecosystem-of-israel/284145

A Secure Cluster Head Selection Mechanism Based on Node's Features and Behavior in Wireless Sensor Networks

Deepika Agrawal, Sudhakar Pandey and Veena Anand (2019). *International Journal of Information Security and Privacy* (pp. 74-90).

www.irma-international.org/article/a-secure-cluster-head-selection-mechanism-based-on-nodes-features-and-behavior-in-wireless-sensor-networks/232670