International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 2, Mar-Apr-2022, ISSN (Online): 2395-566X

Using Blockchains for Security and an Algorithm for Cloud Computing

Divya Asritha Somisetty, Mohammad Tajammul
School of Computer Science and IT,
Jain (Deemed-to-be University),
Bangalore, Karnataka, India
divyasomisetty666@gmail.com

Abstract- Blockchain is a completely new approach for the development of Internet technology due to its distributed mechanism, decentralized mechanism, password mechanism, and scripted mechanism. As a result of Blockchain technology, storing and spreading information in a network has been redefined. There is no need for participants to know each other, nor is it a requirement for third-party certification bodies. An asymmetric cryptographic algorithm ensures that data cannot be tampered with and forged while recording, transmitting and storing transfer activities of the information value. The exchange of blockchain data information enables all participants to reach consensus. Moreover, the current industry research on blockchain explains the applications of the technology in identity authentication, data protection, and network security. This new technology will lead to a major shift in information.

Keywords- Big Data, Hadoop, HDFS, MapReduce, YARN, Python.

I. INTRODUCTION

Throughout the entire process of national informatization, information security touches all aspects of social life. This is the focal point of the national informatization process and involves practical interests of the vast majority of citizens. Social problems related to information security have caused severe concerns from related departments, and security technologies, such as system security, network security, and data security, have received more attention in recent years.

Using blockchain technology is essential to building Bitcoin data structures and encrypting transaction information. Supporting the operation and development of bitcoin, it is also pushing a revolution in information security technology. As a key component of identity and certification, prevention of DDoS attacks, and ensuring data integrity and credibility, Blockchain technology will actively promote the development of national information security.

II. SURVEY MOTIVATION AND METHODS

There is no generally agreed upon logical or specialized definition of distributed computing. Many traffic redundancy elimination methods are ushering in a period of distributed computing, an Internet-based advancement and utilisation of PC innovation.Together with the ever-cheaper and more capable processors, Software as a Service (SaaS) pioneering engineering is transforming server farms into large amounts of figuring management. In light of the increasing speed of data transfer and the availability of reliable yet adaptable system connections, clients can now subscribe to top-notch administrations from information and software which lives on remote server farms.

When you use cloud services, your data is much safer and more convenient to store. Your data is protected by a solid fence, and no unauthorized person will have access to it. By sharing the relevant links, you can share your data without worrying about hackers or any other unwanted intrusion. In this way, your data will not be compromised by malware, and anyone can't access your privacy lounge without your permission.

III. SURVEY OUTCOMES

Since clients no longer have to worry about direct equipment administration, moving information into the cloud is a wonderful accommodation for them. In the history of distributed computing, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well-known examples. Despite the fact that these services do provide a lot of storage space and powerful processing abilities, this shift from a physical to an online platform also wipes out the obligation of maintaining local machines.

Consequently, as clients we are helpless before our cloud service providers (CSP) when it comes to access and reliability of their information, despite the fact that the cloud frameworks are more capable and robust than individual computers and are more flexible. Clients may get to and change the cloud information that they put away, which includes addition, cancellation, adjustment, adding, and so forth. Cloud computing offers two great benefits: ease of use and a lower cost. However, transferring critical applications and sensitive data to public and shared cloud environments has significant security concerns.

IV. CONCLUSION

Blockchain technology is the foundation for the construction of Bitcoin data structure and transaction information encrypted transmission.

It is a security framework that protects the network and communication in MANETs. The primary focus is to secure access to a virtually closed network (VCN) that allows expedient, reliable communication with confidentiality, integrity and authenticity services.

REFERENCES

[1] P. S. Kiran, “Protocol architecture for mobile ad hoc networks,” 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.
[2] A. Chandra, “Ontology for manet security threats,” PROC. NCON, Krishnankoil, Tamil Nadu, pp. 171–17, 2005.
[3] K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.
[4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, “A cluster- based approach to consensus based distributed task allocation,” in Parallel, Distributed and NetworkBased Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.
[5] D. Chakeres and E. M. Belding-Royer, “Aodv routing protocol implementation design,” in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE, 2004, pp. 698–703.
[6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot et al., “Optimized link state routing protocol (olsr),” 2003.
[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, “Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.
[8] Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, “Performance analysis of mesh routing protocols for uav swarming applications,” in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp. 317–321.
[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38– 47, 2004.
[10] N. Garg and R. Mahapatra, “Manet security issues,” IJCSNS, vol. 9, no. 8, p. 241, 2009.