iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XI **Month of publication:** November 2020

DOI: https://doi.org/10.22214/ijraset.2020.32242

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

Blockchain - An Advance Security System

Rahul Avdhesh Yadav
Research Student Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous) Kalyan, Thane, India.

Abstract: ***Blockchain may be a decentralized technology. Blockchain has slowly become one among the foremost frequently discussed methods for securing data storage and transfer through decentralized, trust less, peer-to-peer systems. This timely systematic review also sheds light on future directions of research, education and practices within the blockchain and cyber security space, like security of blockchain in IoT, security of blockchain for AI data, and sidechain security. We also review the safety enhancement solutions for blockchain, which might be utilized within the event of varied blockchain systems, and suggest some future directions to stir research efforts into this area. Blockchain has attracted tremendous attention because of its immutable nature and thus the associated security and privacy benefits. BC has the potential to beat security and privacy challenges of the web of Things.***
Keywords: blockchain, security, cryptocurrency, decentralization, smart contracts, security.

I. INTRODUCTION

There is no doubt that the popularity of blockchain has increased worldwide. More than simply becoming popular, it has made a lasting impact on the world. Blockchain is a new technology that offers the possibility to create a distributed database that is maintained by thousands of nodes. These nodes all make sure that the data in the blockchain is safe and that the data will be stored forever. Blockchain technology has huge potential with a variety of applications and provides wide opportunities for various infrastructure. This technology encourages resource management and makes communications secure and easy to manage.

II. OBJECTIVES

A. To understand that blockchain security is the safe in future.
B. To analyse that blockchain security is trustable or not in security.

We can use this objectives by checking through the survey analysis. We find the following
1) Hypothesis : "After this security system technology greatly reduces the risk of malicious intervention."
.

III. LITERATUREE REVIEW

A Survey in the Security of Blockchain Systems by Xiaoqi Lia et all. [1] The article conclude that in future we summarize blockchain security enhancements and suggest a few future directions in this area. For each risk or vulnerability, we analyies its causes and possible consequence by Peng Jianga et all.[2] Blockchain will give Better security during transaction of any value. This technology is mainly proposed to handling bitcoin transaction. Smart contract, Ethereum and distributed ledger are some applications of blockchain, This will also give more security by Remya Stephen et all. [3] This research has identified available recent research on how blockchain solutions can contribute to cyber security problems. The initial keyword searches for this research and current media reports [43] highlight blockchain as a standalone technology that brings with it an exorbitant array of possible solutions for finance, logistics, healthcare and cyber security by Paul J. Taylor et all. **[4]** In this paper, we adopt the Pow consensus mechanism. A consensus of all mining vehicles in the blockchain network can be established to generate a new block that can be used as a ground truth for the next block. The evaluation and analysis show that our proposed local blockchain scheme can be used efficiently in the VANET without storage overhead by Rakesh Shrestha et all. [5] we proposed a novel automotive security architecture based on blockchain (BC). Due to its distributed nature, the proposed architecture eliminates the need for a centralized control and allows novel automotive services. The privacy of the users is ensured by using changeable Public Keys (PK). The security of our architecture is largely inherited from the strong security properties of the underlying BC technology Marco Steger et all. [6] In this paper, we argued that although Blockchain (BC) is an effective technology for providing security and privacy in IoT, its application in the IoT context presents several significant challenges including: complexity, bandwidth and latency overheads and scalability by Salil et all. [7] This paper presents a comprehensive survey of the existing blockchain protocols for the Internet of Things (IoT) networks.

©IJRASET: All Rights are Reserved

We start by describing the blockchains and summarizing the existing surveys that deal with blockchain technologies by Mohamed Amine et all.[8] In the aera of big data, large volumes of heterogeneous data are generated from different sources allowing big data management to play a pivotal role in the success and viability of any businesses by Sara Hosseinzadeh et all. [9] In this paper, we presented a comprehensive survey on the utilization of the blockchain technology in providing distributed security services. These services include entity authentication, confidentiality, privacy, provenance, and integrity assurances. The entity authentication and the confidentiality can be achieved by the public key cryptography using encryption and the signature schemes by Tara Salman et all.[10] In this paper, a blockchain-based privacy-preserving data sharing system for EMRs is proposed, named BPDS. In BPDS, EMRs are stored in the cloud and the indexes are recorded in a tamper-proof consortium blockchain, which solves the potential security risks of data centralized storage. The joint-design of the CP-ABE-based access control mechanism and the content extraction signature scheme provides strong privacy preservation in data sharing by Jingwei Liu et all.

IV. METHODOLOGY

We took an online survey with help of Google Form. The link of the form was circulated in social media platform. The questionnaires in the form were designed to test the proposed hypothesis and result.

A. Participants

To test the proposed hypothesis, this study used two conditions i.e.

1) Blockchain security will secure or trustable for people.

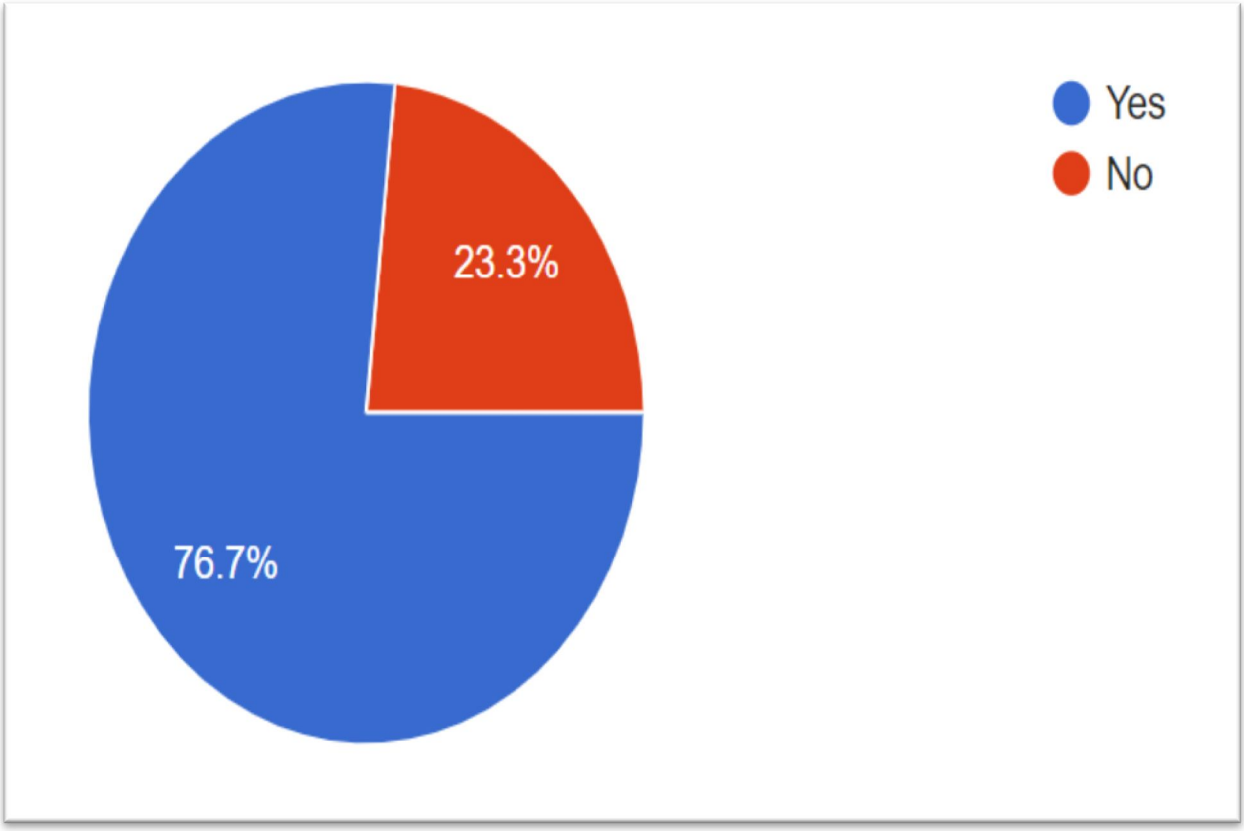
2) Blockchain security will be add extra security for people.

Total of 32 participants data was collected from different city. All the 32 participants in which 55% male and 45% female.

B. Measures

Participants were asked to indicate their agreement on a two scale (1= YES, 0= NO).

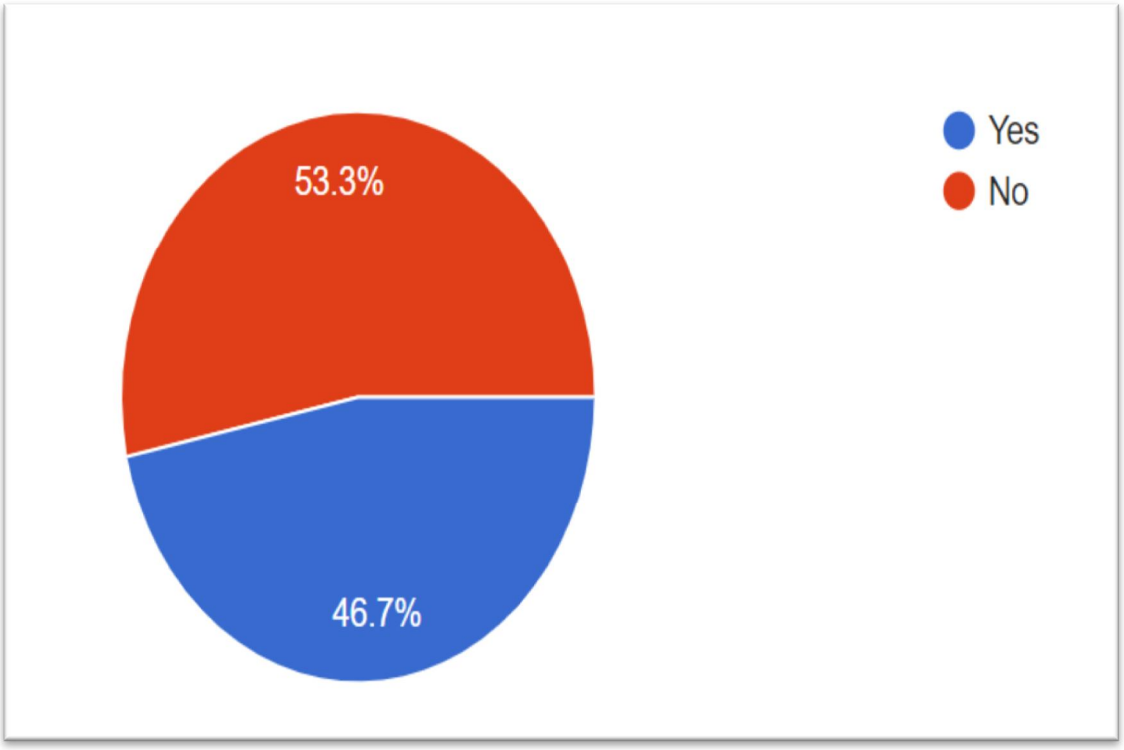
Male reply on the blockchain security is the secure or not secure in the future?



©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

Female reply on the blockchain security is the secure or not secure in the future?



V. EXPERIMENT

A. Calculated by Chi-Square test with two scales (YES/NO).

B. After performing the chi-square test got x^2 tabulated=0.054 and x^2 calculated= 10.851 at the significant level of 95%.

C. Here x^2 tabulated< x^2 calculated therefore we accept the hypothesis i.e. Students are interested to learn with blockchain security that will positively increase their number.

VI. RESULT

There is little question that the recognition of blockchain has increased worldwide. More than simply becoming popular, it has made a lasting impact on the world. Blockchain is a new technology that offers the possibility to create a distributed database that is maintained by thousands of nodes. These nodes all confirm that the info within the blockchain is safe which the info are going to be stored forever. Blockchain technology has huge potential with a spread of applications and provides wide opportunities for various infrastructure. This technology encourages resource management and makes communications secure and easy to manage.5

VII. CONCLUSION

A blockchain, originally block chain, could also be a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. the research concerning IoT security using blockchain applications often made comments on network latency and power consumption to take care of the distributed network. For the aim of this paper, it had been impossible to quantify such data thanks to the variability in solutions employed by each group of researchers. Future work could include an assessment of network latency, power consumption and data packet flows of blockchain-based IoT networks, and standardization of knowledge presented within the primary studies. This research has identified available recent research on how blockchain solutions can contribute to cyber security problems.

VIII. ACKNOWLEDGEMENT

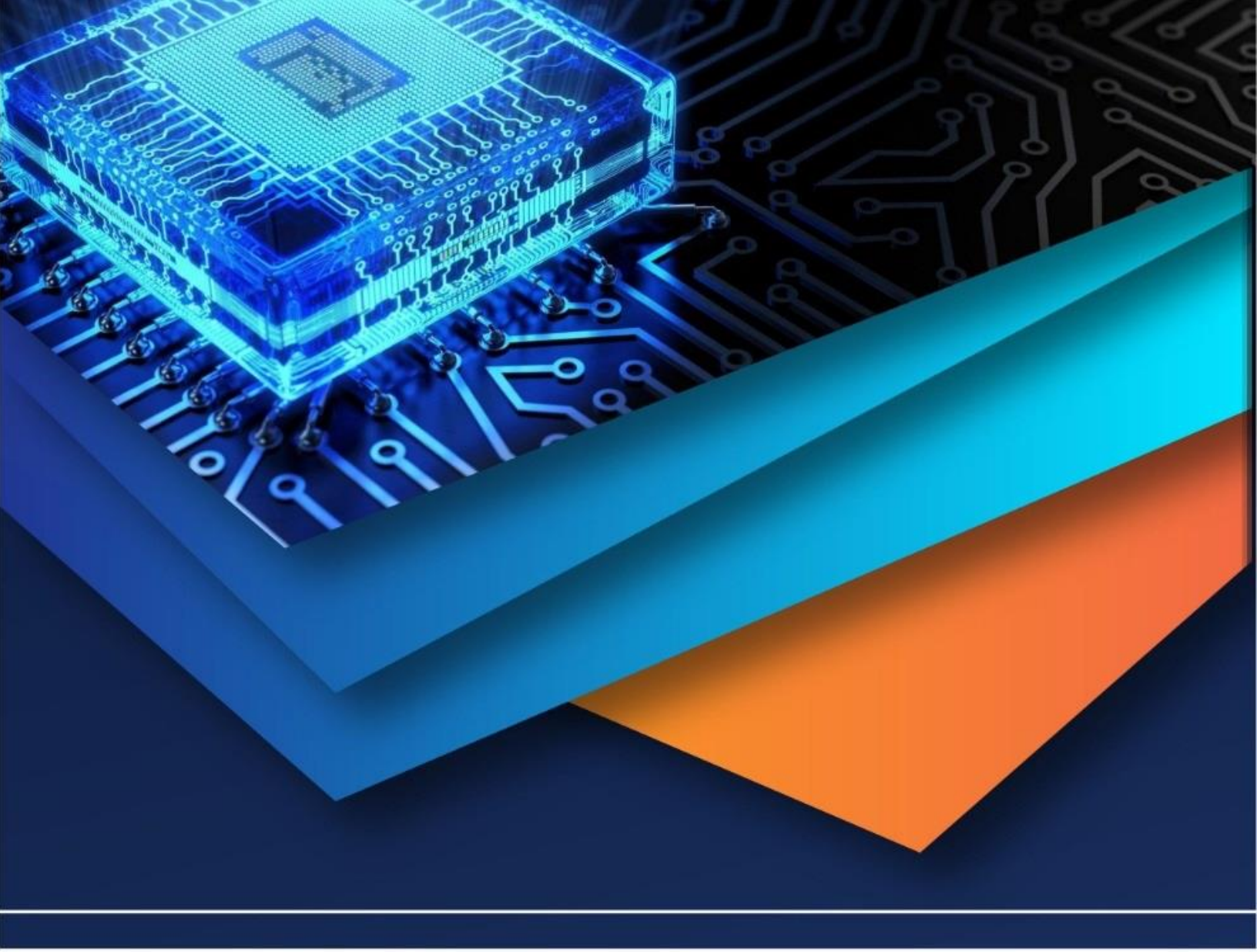
A special gratitude is conveyed to our Prof. Swapna Augustine Nikale, Department of Information Technology of B.K. Birla College of Arts, Science and Commerce (Autonomous) Kalyan, Thane. Also, thanks to the participants who responded to the survey.

©IJRASET: All Rights are Reserved

REFERENCE

[1] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. ACM Comput. Surv. 1, 1, Article 1 (January 2019), 35 pages. https://doi.org/10.1145/3316481
[2] Ali Dorri, Salil S Kanhere, Raja Jurdak, Praveen Gauravaram Journal of Parallel and Distributed Computing 134, 180-197, 2019 https://doi.org/10.1016/j.jpdc.2019.08.005
[3] Ali Dorri, Salil S Kanhere, Raja Jurdak, Praveen Gauravaram Journal of Parallel and Distributed Computing 134, 180-197, 2019
[4] Li, X., Jinang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survay on the security of blockchain system, 10.1016/j.future.2017.08.020
[5] Park, J. H., & Park, J. H. (2017). Block chain security in cloud computing use cases, challenges and solutions.
[6] Angelis, S. D., Zanfino, G., Aniello, L., Lombardi, F., & Sassone, V. (2019). Block chain and cyber security a taxonomic approach. University of Southampton.
[7] Mosalheil, J. H. (2018). security threats classification in block chain. St.cloud state University, 5, https://repository.stcloudstate.edu/msia_etds
[8] Bult, T. (2019). Security analysis of blockchain technology. Business information technology oulu University of Applied sciences, 1-41.
[9] Harry Halpin, Marta Piekarska. Introduction to Security and Privacy on the Blockchain. EuroS&P 2017 - 2nd IEEE European Symposium on Security and Privacy, Workshops, Apr 2017, Paris, France. IEEE, Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on, pp.1-3, 2017, ff10.1109/EuroSPW.2017.43ff. ffhal-01673293f
[10] Lin, I. C., & Liao, T. C. (2017). A survay of blockchain security issues and challenges. Department of Photonics and Communication Engineering, 19(5), 653-659. 10.6633/IJNS.201709.19(5).01)
[11] Mathew, A. R. (2019). Cyber security through block chain technology. International Journal of Engineering and Advanced Technology (IJEAT), 9(1), 2249-8958.
[12] Gervais, A., Karame, G. O., Wust, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2019). On the security and performance of poor of work block chain. ETH Zurich Switzerland, 1-13.
[13] Faizullah, S., Khan, M., Alzahrani, A., & Khan, I. (2020). Permissioned block chain based security for SDN in IOT cloud networks. Department of computer science, Islamic University, 1-6. arXiv:2002.00456v1
[14] Z. Liu, N. C. Luong and et al., "A Survey on Applications of Game Theory in Blockchain", retrieved from https://arxiv.org/abs/1902.10865, 2019.
[15] Hamoliak, I., Venugopalan, S., Hum, Q., & Szalachowski, P. (2019). A security reference architecture fot block chain. Singapore University of technology and design, 1-11. arXiv:1904.06898v1
[16] Kim, S. K. (2018). The trailer of blockchain governance game series
[17] Remya Stephen and Aneena Alex 2018 IOP Conf. Ser.: Mater. Sci. Eng. 396 012030 https://doi.org/10.1088/1757-899X/396/1/012030
[18] Arquam, M., Singh, A., & Sharma, R. (2018). A blockchain based Secure and Trusted framework for Information Propagation on Online Social Networks. Computer Science and Engineering National Institute of Technology Delhi New Delhi, India, 1-6. arXiv:1812.10508v1
[19] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizan, M. (2018). BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records. †School of Computer Science and Engineering, Harbin Institute of Technology, Harbin, 150001, China., 1-6. http://arxiv.org/abs/1811.03223v1
[20] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security Services Using Blockchains: A State of the Art Survey1. IEEE Communications Surveys & Tutorial, 1-131. DOI 10.1109/COMST.2018.2863956
[21] Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2017). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. IEEE, 1-14. arXiv:1806.09099v1
[22] Ugobame, U., Kassani, S. H., & Deters, R. (2018). Blockchain access control Ecosystem for Big Data security. Department of Computer Science University of Saskatchewan Saskatoon, Canada, 1-6.
[23] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy. 95-116. http:// arXiv.org/abs/1712.02969v1
[24] Farhad Daneshgar, Omid Ameri Sianaki, Prabhat Guruwacharya Workshops of the International Conference on Advanced Information Networking and Applications, 966-974, 2019
[25] Donghang Lu, Pedro Moreno-Sanchez, Amanuel Zeryihun, Shivam Bajpayi, Sihao Yin, Ken Feldman, Jason Kosofsky, Pramita Mitra, Aniket Kate 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), 39-48, 2019

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)