iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.38816

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 9 Issue XI Nov 2021- Available at www.ijraset.com

Adoption of Blockchain Based Smart Application in Machine Learning

Vijaya Ravindra Wankhade[1], Prof. Mayur S. Bhurange[2]
[1, 2]*Computer Science and Engineering, P.R Pote(patil) college of Engineering and Management*

Abstract: ***In recent years, the emergence of blockchain technology (BT) has become a novel, most disruptive, and trending technology. The redistributed database in BT emphasizes data security and privacy. Also, the consensus mechanism makes positive that data is secured and bonafide. Still, it raises new security issues like majority attacks and double-spending. To handle the said problems, data analytics is required on blockchain-based secure knowledge. Analytics on these data raises the importance of arising technology Machine Learning (ML). ml involves the rational quantity of data to create precise selections. data reliability and its sharing are terribly crucial in ml to enhance the accuracy of results. the combination of those two technologies (ML and BT) provide give highly precise results. in this paper, present gift a detailed study on ml adoption we BT-based present applications additional resilient against attacks. There area unit varied ancient ML techniques, for example, Support Vector Machines (SVM), clustering, bagging, and Deep Learning (DL) algorithms like Convolutional Neural Network (CNN) and Long STM (LSTM) are often used to analyze the attacks on a blockchain-based network. Further, we tend to embody however each the technologies are often applied in many sensible applications like unmanned Aerial Vehicle (UAV), sensible Grid (SG), healthcare, and sensible cities. Then, future analysis problems and challenges are explored. At last, a case study is presented with a conclusion.***

Keywords: Blockchain, machine learning, smart grid, data security and privacy, data analytics, smart applications.

I. INTRODUCTION

From the past few decades, data has become a necessary source of intelligence and carries new opportunities to the real-life problems such as wireless communications, bioinformatics [1], agriculture [2], and finance [3] through smart applications. These applications square measure data-driven and incorporate unjust insights into user expertise, that permits individuals to complete the required task additional expeditiously. It operationalizes insights, personalizes the customer experience, optimizes customer interactions, improves operational efficiency, and enables a new business model. There are various smart applications such as SG, UAV, Smart Cities, which make the life of an individual easier. These applications generate a huge amount of data and storage of this ever-evolving data in databases is a problem, and its communication also raises security concerns. To handle these issues, BT can be used, which has a distributed database network. It was coined by Satoshi Nakamoto in the year 2008 and contained a time-stamped series of tamper-proof records, which are managed by a cluster of distributed computers. It comprises of a chain of blocks that are connected using cryptographic primitives. The three mainstays of BT are immutability, decentralization, and transparency. These three characteristics opened its door for a wide variety of applications, for example, digital currency existence (currency with no physical existence) and analysis on its suitability in smart applications [4]. though BT ensures security and privacy problems, some vulnerabilities conjointly started showing when its implementation. as an example, the character of attacks began to be more and more subtle like majority attacks (51% attack) that management selection, Sybil attacks for pretend identity generation to regulate the agreement [5]. To handle the said issue, a sturdy Intrusion Detection System (IDS) is needed in situ as a result of the normal ways use a signature-based approach to sight specific patterns. But, to sight intrusions and attack patterns, one among the rising technology called cubic centimeter are often accustomed analyze the information traffic.

In a communication network of blockchain-based good applications, there's layer-wise handling of security problems. Some security problems area unit handled at the network layer, such as malicious packets, and a few at the application layer like malware [6]. At the network layer, malicious packets will be used to impose the network to determine fraudulent agreement. A naive answer to the current drawback will be to use a firewall to ensure that packets meet pre-defined security criteria [7]. Though, the attacks are getting a lot of refined with unseen patterns to bypass a firewall. To stop this issue, packets header data will be analyzed mistreatment ml models [8] in real-time mistreatment historical knowledge. This analysis helps to discover new and ever-changing patterns. Similarly, ml techniques will be accustomed classify malware to end-point like servers, mobile, or workstations.

Further, many blockchain-based smart applications like UAV [9], data trading [10], SG builds trust between data exchangers [11]. it's terribly crucial in any good application at an equivalent time; data ought to be secure. BT ensures data security however builds confidence, and ml techniques area unit accustomed predict untrustworthy nodes based on past patterns. Similarly, UAVs have considerably different network topology compared to the traditional blockchain network topology [9]. It includes communication using satellites and varied ground stations. For UAV, BT is used to securely store coordinates and different relevant data to maintaining graph integrity for the vehicles. In ensuant sections, we have a tendency to explore the recent analysis work on ml adoption in the blockchain-based good application.

II. LITERATURE SURVEY

The proposed architecture[1] can pave the way for full duplex communications in 5G spectrum. authors illustrate the same for a healthcare unit. The idea of a node-pair formation is specifically advantageous as it helps set the premise for directed communication. The node-pairs allow us to determine the direction of communication and thus facilitate full duplex communication. In absence of such an arrangement, it would be impossible for nodes to transmit and receive on the same channel simultaneously, as a node would not be able to single out the original signal. The case for static nodes is appealing, but mobile nodes are closer to reality. Unless bedridden, chances for a patient to remain static are low. Thus, if the delay in node formation can be reduced, they can realize a feasible architecture for mobile communication in the 5G spectrum.

Precision irrigation (PI) is one of the most prominent issues where most of the research organizations, government or private industries, agricultural and farm based institutions or universities are showing their interest keenly. Hence, utilization of latest technologies like, WSN and CC can meet out the exact requirement of farmers to increase the crop fertility. In the paper of Sudhanshu Tyagi, Mohammad S. Obaidat, Sudeep Tanwar‡, Neeraj Kumar, and Mohan Lal[2], they propose “PI-Cloud,” which is a sensor-cloud based M2M system. The system includes cluster based hierarchical architecture of sensor-cloud, where sensors are dynamic in nature and can be recharged as per the requirements. This architecture measures the real these time values of moisture level of soil and compares these with standard stored data within cloud. Based on the comparison, respective CAM has been prepared and directly transferred to M2M system for final control action. Simulation results obtained under different chosen parameters show success of PI-cloud for the sensing of moisture level of soil in real time. Moreover, the energy harvesting to the CHs reduces the requirement of replacement of sensors.

The authors Umesh Bodkhe, Pronaya Bhattacharya, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar,[3] discusses helpful insights to the readers concerning the importance of blockchain technology in touristry and hospitality, wherever security remains a dominant issue. In their paper, they planned a framework named as BloHosT (Blockchain Enabled good touristry and hospitality Management) for registration of the traveler user through one unified cryptocurrecy enabled application. Then, the touristry stakeholders also registers themselves through a similar application and executes good contracts for ability. BloHosT used varied levels of good contracts those are applicable within the good contract layer. Then, a TeDL style framework is additionally planned to come up with a rating scores for future travelers across the world by running LSTM over previous saved traveled itinerary. Finally, 3 case studies are bestowed to predict the suitableness of the planned BloHosT framework in touristry sector.

MOHAMED RAHOUTI, KAIQI XIONG AND NASIR GHANI[5] said that, blockchain has demonstrated its potential to transform and mutate classical financial and transactional market models with its key distinctive features, including decentralization, anonymity, and auditability. Hence, in their survey paper, they presented an intensive and comprehensive discussion overviewing Bitcoin and blockchain infrastructures along with relevant key components.

This paper of A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso[6] reviews the foundational information of malware and anti-malware systems. We presented summaries of works found in literature about malware evolution, malware analysis techniques, malware evasion techniques and existing malware detection methods. they then review literature of recent research approaches to malware analysis and detection. their work was done as foundation for malware detection frameworks that have been developed.

III.BACKGROUND

A. Machine Learning

ML is that the field of study that focuses on building applications that learn through expertise. it's the power to show a computer while not programming it expressly [18]. ml encompasses its work from a various set of disciplines, together with philosophy, information theory, probability and statistics, control theory, psychology and neurobiology, computational complexity, and artificial intelligence [19]. ml algorithms are utilized in several applications and benefited it as listed below:

1) In data mining, massive databases contain completely different patterns that may be discovered mechanically by victimisation ml techniques to research outcomes, as an example, medical treatments of a patient from health record databases or to identify the trustworthiness of someone from financial databases.
2) ml applies in areas wherever a settled algorithmic program is not promising, like human face recognition from images.
3) Application domains wherever the flexible programming is needed, as an example, dominant producing processes as per the demand of the customer and adapting to the variable reading interests of readers.

ML algorithms are application specific and depends on the output needed by the system. There area unit many ml algorithms, like supervised ml, Semi-Supervised metric capacity unit, and unsupervised ml.

a) Supervised ml uses statistical models to predict output in numerical information and classify the correct label [20]. Here, the most commonly known algorithms embrace the regression approach and decision trees.
b) Unsupervised ml doesn't have label data. Here, data samples area unit grouped into clusters looking on their similarity or difference [21] using a different approach. For example, K means that clustering and association rules algorithms.
c) Semi-Supervised ml is also a category of interest [22]. It involves a mixture of supervised and unsupervised ML techniques. Unsupervised learning may be applied to discover the structure of input variables, following which it is used to make best guess predictions for the unlabeled data. It feeds that predicted data back into the supervised ML algorithm as training data and use the model to make predictions on unseen data.

B. Blockhain

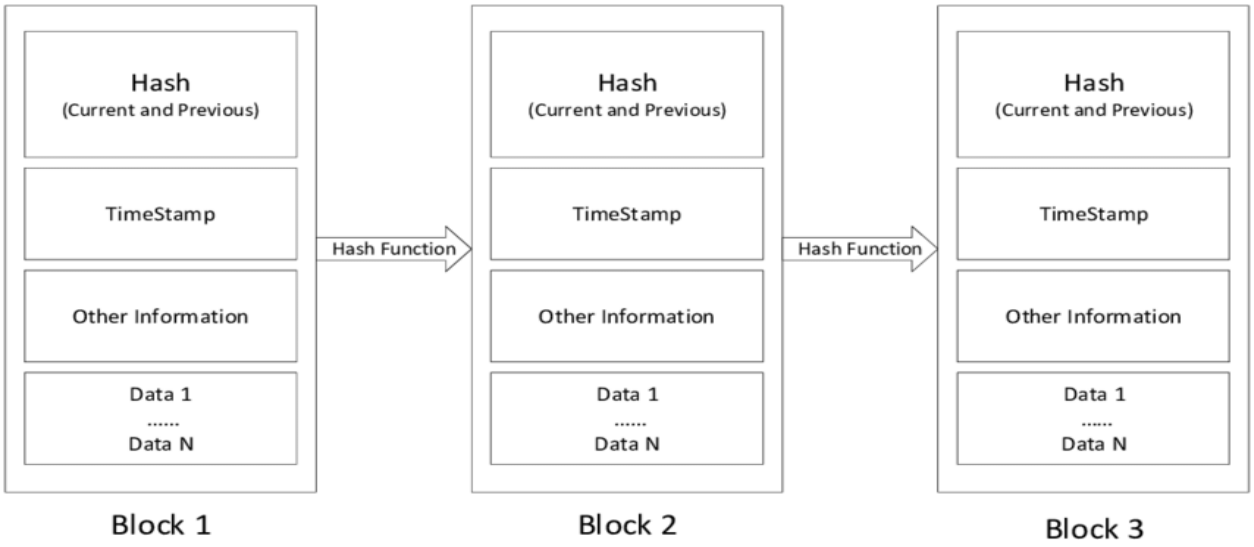


Fig. 1 Block chain Structure

Blockchains are an immutable set of records that are cryptographically connected along for audit [23]. it's kind of like an accounting ledger. Here, previous records within the accounting ledger can not be modified, and new records have to be compelled to be verified by a trusted party. the sole distinction between these 2 is that new blocks (set of records) are checked by a decentralized structure of nodes that have a replica of the ledger. There is no centralized party to verify the records. Blockchain is formed by linking valid blocks together; this block contains the hash of the previous block, and so on, as shown in FIGURE 1. This makes blockchain traceable and immune to change [24]. Older blocks can not be changed, just in case they're changed in any way; their hash would amendment. This stress to link hash all told consequent blocks to create the blockchain network valid once more. a replica of the blockchain is on the market with each individual among the network; henceforward, any changes is cross verified by the opposite users. These copies of the blockchain are updated with the addition of a brand new block. Then, everybody will see the block, depending on the permissions assigned by the administrator. BT uses a cryptographic secure hash algorithmic program (SHA) like SHA-256 and SHA-512 to keep up the data integrity among the block. Each block incorporates a distinctive hash price. for example, Ethereum uses Keccak-256 and Keccak-512, whereas Bitcoin uses double SHA-256. This SHA may be a collision-resistant algorithmic program, whereno 2 completely different input data may turn out constant output (hash value). henceforth SHA is wont to check if the data is that the same or not. There are numerous SHA algorithms.

C. Integration Of Machine Learning In Blockchain-Based Applications

The learning capabilities of ml will be applied to blockchain-based applications to create them smarter. By victimization ml security of the distributed ledger could also be improved. ML may also be wont to enhance the time taken to achieve agreement by building better information sharing routes. Further, it creates an opportunity to make higher models by taking advantage of the decentralized design of BT. we have a tendency to planned design for ml adoption in BT-based good application, as shown in Figure a pair of. Here, the good application collects data from totally different information sources like sensors, good devices, and Intenet of Things (IoT) devices. data collected from these devices get processed as an good applications. The blockchain work as associate integral a part of these good applications. Then, ML will be applied to those application's data for analysis(Data analytics and period of time analytics) and prediction. The data sets employed by ml models may be keep on a blockchain network. This reduces errors within the data like duplication, missing data worth, errors, and noise. Blockchains ar targeted learning capabilities of ml which will be applied to blockchain-based applications to create them smarter. By victimization ml security of the distributed ledger could also be improved. ML may also be wont to enhance the time taken to achieve agreement by building higher data sharing routes. Further, it creates associate opportunity to make higher models by taking advantage of the decentralized design of BT. we have a tendency to planned design for millilitre adoption in BT-based good application, as shown in Figure a pair of. Here, the good application collects data from totally different data sources like sensors, good devices, and Intenet of Things (IoT) devices. data collected from these devices get processed as a part of good applications. The blockchain work as an integral a part of these good applications. Then, ML will be applied to those application's data for analysis(Data analytics and period of time analytics) and prediction. The data sets employed by ml models may be keep on a blockchain network. This reduces errors within the data like duplication, missing data worth, errors, and noise.

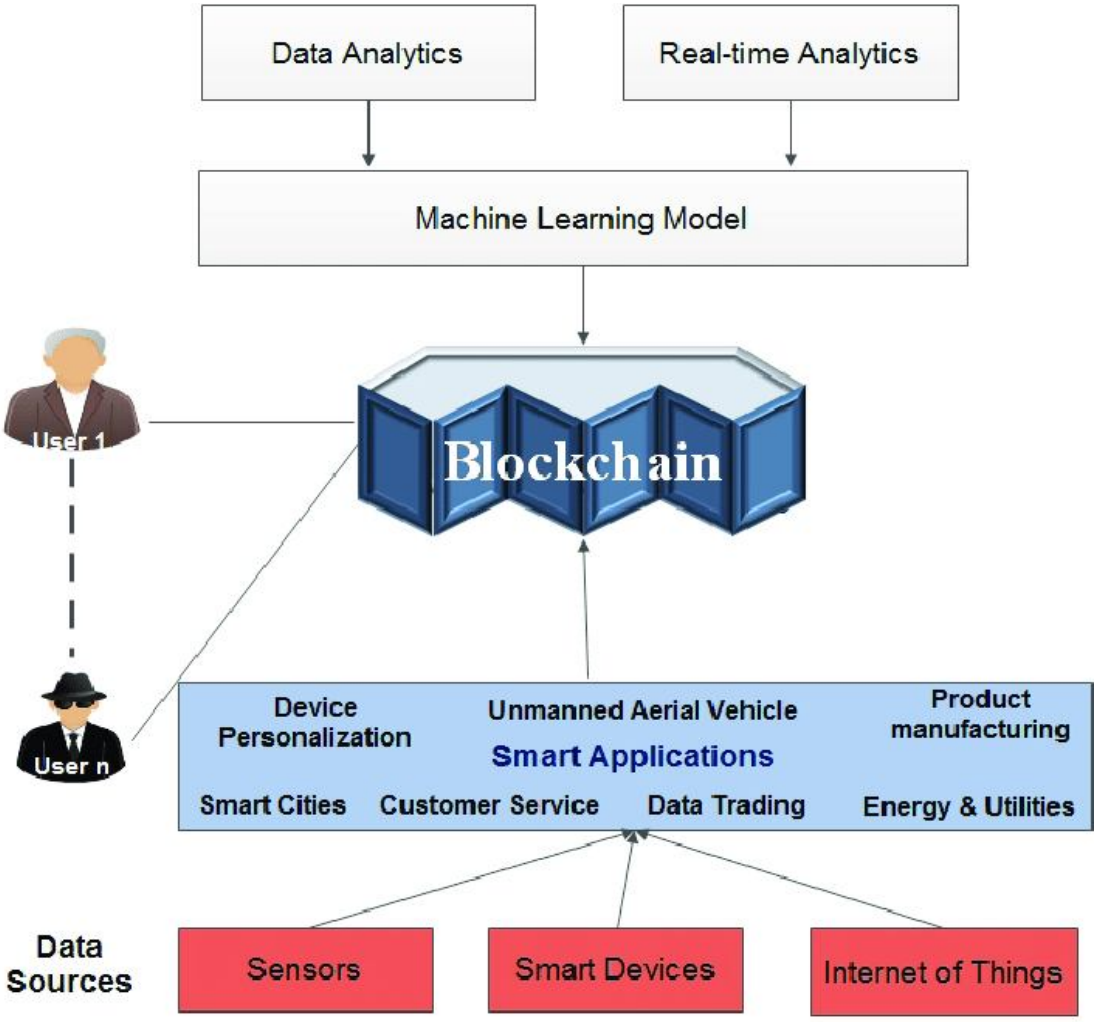


Fig. 2 Architecture for Machine Learning adoption in Blockchain-based applications.

Blockchains are targeted on the information, and thus data-related problems in ml models may be eliminated. ml models will be supported specific segments of the chain instead of the complete data set. This could offer custom models for various applications, such as fraud detection and fraud detection. many of the advantages are listed beneath when ml is applied:

1) User authentication as a legitimate user for requesting or performing any transaction in the blockchain network.
2) BT provides a high level of security and trust.
3) Blockchain integrates public ML models into smart contracts to ensure that the conditions and terms which were previously agreed are sustained.
4) BT helps in the reliable implementation of an incentivebased system; thus, it encourages users/customers to contribute data. This huge data will help to improve ML model performance.
5) ML models can be updated on-chain environment of BT with a small fee and off-chain, locally on an individual's device without any costs
6) Good data contributions can happen from users/ customers, these data consistently computed, and rewards can be given to the users.

IV. CONCLUSION

The recent advancements in Blockchain and ML have made them path-breaking technologies. The distributed ledger has the possibility to work as the backbone of various smart applications such as smart cities, UAV, SG, data trading. In this paper, we have presented detailed information on BT and ML, along with their usages in smart applications and proposed an ML-BT based architecture. This architecture can be used to design and deploy an ML-BT based data analysis system.

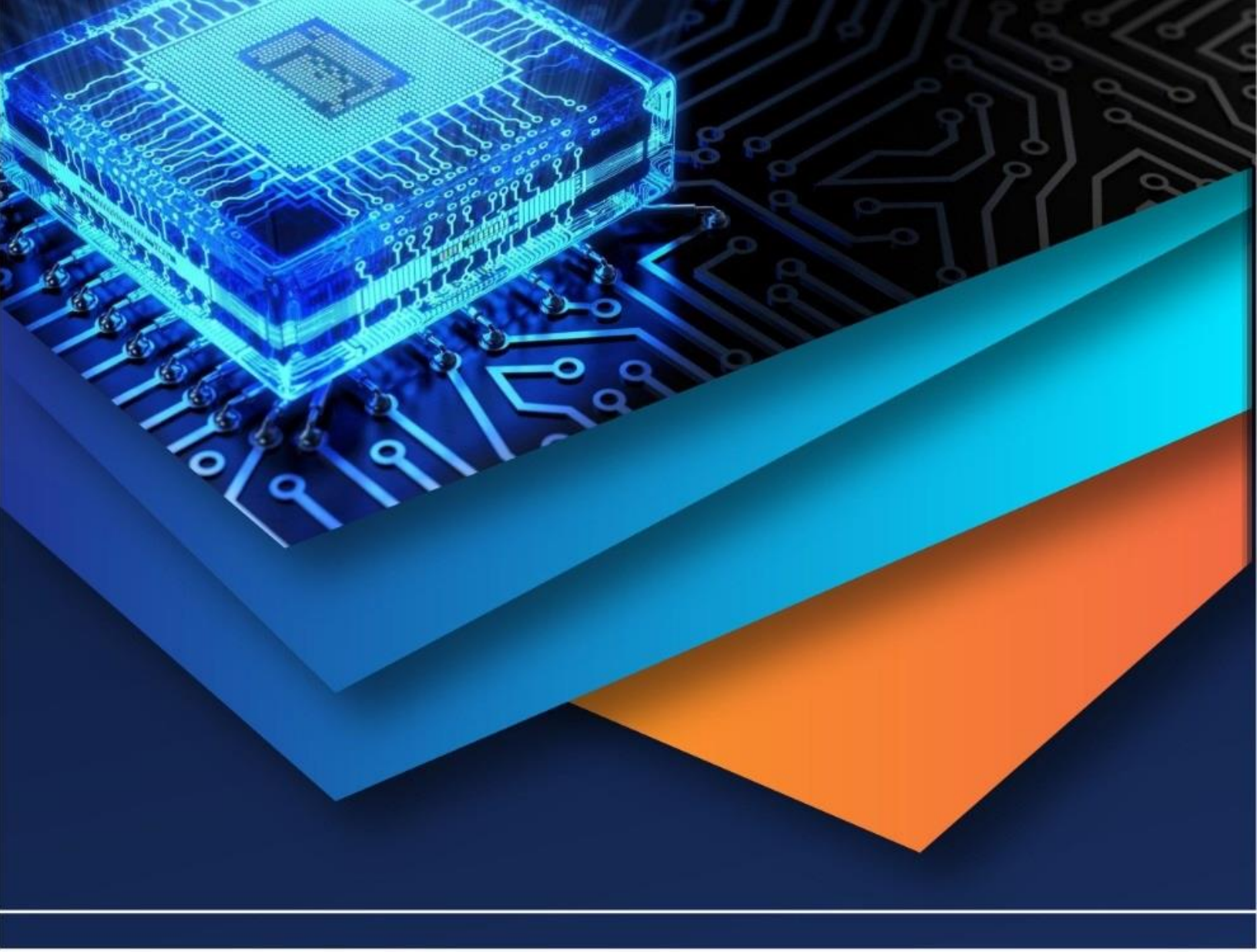
V. ACKNOWLEDGMENT

It is our proud privilege to release the feelings of our gratitude to every person who helped us directly or indirectly to conduct this research work. we express our heart full indebtness and owe a deep sense of gratitude to our colleagues from P.R Pote(patil) college of Engineering and Management for their sincere guidance and inspiration for completing this paper.

REFERENCES

[1] S. Kaneriya, J. Vora, S. Tanwar, and S. Tyagi, ''Standardising the use of duplex channels in 5G-WiFi networking for ambient assisted living,'' in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), May 2019, pp. 1–6.
[2] S. Tyagi, M. S. Obaidat, S. Tanwar, N. Kumar, and M. Lal, ''Sensor cloud based measurement to management system for precise irrigation,'' in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2017, pp. 1–6.
[3] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, ''Blohost: Blockchain enabled smart tourism and hospitality management,'' in Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS), Aug. 2019, pp. 1–5.
[4] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. [Online]. Available: https://bitcoin.org/en/bitcoin-paper
[5] M. Rahouti, K. Xiong, and N. Ghani, ''Bitcoin concepts, threats, and machine-learning security solutions,'' IEEE Access, vol. 6, pp. 67189–67205, 2018.
[6] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso, ''The world of malware: An overview,'' in Proc. IEEE 6th Int. Conf. Future Internet Things Cloud (FiCloud), Aug. 2018, pp. 420–427.
[7] S. Krit and E. Haimoud, ''Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically,'' in Proc. Int. Conf. Eng. MIS (ICEMIS), May 2017, pp. 1–7.
[8] G. Betarte, E. Gimenez, R. Martinez, and A. Pardo, ''Improving Web application firewalls through anomaly detection,'' in Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA), Dec. 2018, pp. 779–784.
[9] A. Kuzmin and E. Znak, ''Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles,'' in Proc. IEEE Int. Conf. Service Oper. Logistics, Informat. (SOLI), Jul. 2018, pp. 32–37.
[10] Y. Zhao, Y. Yu, Y. Li, G. Han, and X. Du, ''Machine learning based privacy-preserving fair data trading in big data market,'' Inf. Sci., vol. 478, pp. 449–460, Apr. 2019.
[11] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, ''Blockchain based decentralized management of demand response programs in smart energy grids,'' Sensors, vol. 18, no. 1, p. 162, Jan. 2018.
[12] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ''When intrusion detection meets blockchain technology: A review,'' IEEE Access, vol. 6, pp. 10179–10188, 2018.
[13] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, ''A survey on security and privacy issues of bitcoin,'' IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
[14] D. Ucci, L. Aniello, and R. Baldoni, ''Survey of machine learning techniques for malware analysis,'' Comput. Secur., vol. 81, pp. 123–147, Mar. 2019.
[15] K. Salah, M. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ''Blockchain for AI: Review and open research challenges,'' IEEE Access, vol. 7, pp. 10127–10149, 2019.
[16] F. Casino, T. Dasaklis, and C. Patsakis, ''A systematic literature review of blockchain-based applications: Current status, classification and open issues,'' Telematics Inform., vol. 36, pp. 55–81, Mar. 2018.
[17] W. Xiong and L. Xiong, ''Smart contract based data trading mode using blockchain and machine learning,'' IEEE Access, vol. 7, pp. 102331–102344, 2019.
[18] T. M. Mitchell, Machine Learning, 1 ed. New York, NY, USA: McGraw-Hill, 1997.

[19] P. Louridas and C. Ebert, ‘‘Machine learning,’’ IEEE Softw., vol. 33, no. 5, pp. 110–115, May 2016.
[20] R. Saravanan and P. Sujatha, ‘‘A state of art techniques on machine learning algorithms: A perspective of supervised learning approaches in data classification,’’ in Proc. 2nd Int. Conf. Intell. Comput. Control Syst. (ICICCS), Jun. 2018, pp. 945–949.
[21] V. Vats, L. Zhang, S. Chatterjee, S. Ahmed, E. Enziama, and K. Tepe, ‘‘A comparative analysis of unsupervised machine techniques for liver disease prediction,’’ in Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (ISSPIT), Dec. 2018, pp. 486–489.
[22] C. Liu, X. Xu, and D. Hu, ‘‘Multiobjective reinforcement learning: A comprehensive overview,’’ IEEE Trans. Syst., Man, Cybern, Syst., vol. 45, no. 3, pp. 385–398, Mar. 2015.
[23] Z. Zheng, S. Xie, H. Dai, and H. Wang, ‘‘An overview of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data, Big Data Congr., Jun. 2017, pp. 557–564.
[24] G. B. Mermer, E. Zeydan, and S. S. Arslan, ‘‘An overview of blockchain technologies: Principles, opportunities and challenges,’’ in Proc. 26th Signal Process. Commun. Appl. Conf. (SIU), May 2018, pp. 1–4.
[25] W. Penard and T. van Werkhoven, ‘‘On the secure hash algorithm family,’’ Cryptogr. Context, pp. 1–18, 2008.
[26] M. Vukolić, ‘‘The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication,’’ in Open Problems in Network Security, J. Camenisch and D. Kesdogan, Eds. Cham, Switzerland: Springer, 2016, pp. 112–125.
[27] S. Thompson, P. L. Seijas, and D. Adams, ‘‘Scripting smart contracts for distributed ledger technology,’’ Tech. Rep., Dec. 2016. [Online]. Available: https://kar.kent.ac.uk/61162/
[28] K. Christidis and M. Devetsikiotis, ‘‘Blockchains and smart contracts for the Internet of Things,’’ IEEE Access, vol. 4, pp. 2292–2303, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY