Grenze International Journal of Engineering and Technology, June Issue

Empirical Analysis of Blockchain and Machine Learning Models for QoS Aware Security Architectures in Wireless Networks

Abhijit Maidamwar[1] and Vivek Kapur[2]
[1,2]G H Raisoni Institute of Engineering & Management Nagpur India
Email: {abhijit.maidamwar@gmail.com, vivek.kapur@raisoni.net}

***Abstract*— Providing node and network level security in wireless environments requires implementation of highly complex algorithms. These algorithms include encryption models, privacy preservation models, secret sharing models, hashing algorithms, etc. Implementation and deployment of these models requires additional computational power, which results in increased end-to-end delay, increased energy consumption, reduced throughput, and increased routing load. Due to which overall Quality of Service (QoS) of the network is impacted. To improve the QoS, machine learning optimization models are implemented. These models aim at reducing redundancies during network communications, thereby assisting the network to have better QoS performance. It has been observed that blockchain-based networks tend to have better security performance than their non-blockchain counterparts. Thus, in this text an in-depth survey of such blockchain based networks is done, wherein each network is compared in terms of security and QoS performance. Due to a wide variety of applications for these networks, it is necessary for researchers and network designers to select the most optimum blockchain implementation for their network. This text will assist such network designers to select application specific blockchain models for high security and QoS performance. Along with this, the underlying text also compares various machine learning models and evaluates them in terms of computational complexity & QoS performance. Finally, this text recommends the best combination of blockchain & machine learning models that can be combined in order to improve overall system performance. By referring this text, system designers will be able to improve their network performance by integrating blockchain & machine learning optimized solutions to their networks.**

***Index Terms*—Security, QoS, machine learning, blockchain, wireless.**

I. INTRODUCTION

Enhancing wireless network security is a multi-domain task, which requires in-depth analysis of node vulnerabilities, network vulnerabilities, network infrastructure, node computational limitations, etc. A wide variety of algorithms are available for improving network security, which work at data level, node level, route level or network levels. Data level algorithms include encryption & hashing mechanisms, wherein the data is converted from one form to another in order to transmit it over the network. Node level algorithms allow for better authentication, node registration, node-policy updates, etc. These algorithms aim at securing healthy nodes from malicious nodes via rule enforcement and outlier detection mechanisms.

Grenze ID: 01.GIJET.11.2.99_20

These algorithms are also applied to route level security, wherein apart from scanning for node's authenticity; its historical performance is also analysed. This analysis allows the network to improve its internal routing mechanisms, thereby assisting in providing a secure route for data communication. Apart from this, anonymity algorithms are also used by networks which aim at transforming the routing information in such a way that it cannot be decoded by malicious entities. Finally, network level security algorithms aim primarily at traffic analysis in order to improve trust levels in the network. Thereby allowing for benign traffic packets to pass through the network. It is observed that blockchain-based solutions can perform all these tasks with utmost efficiency, because they allow for node level, network level, route level and data level security mechanisms. But a wide variety of blockchain models are available for network security, which raises ambiguity in model selection during deployment. In order to reduce this ambiguity, the next section describes various blockchain models and compares their performance in terms of security and QoS metrics.

II. Literature Review

Generally, securing wireless networks requires the inclusion of rule-based algorithms such as authentication, authorization, access control, and data privacy mechanisms. Researchers have proposed various system models to address these requirements effectively. For instance, the work in [1] introduces a blockchain-based IoT model that uses chain splitting and multiple agents to enhance trust and Quality of Service (QoS) parameters in process. The system ensures that the main blockchain is divided into smaller sidechains managed through practical Byzantine Fault Tolerance. This ensures that the system achieves high security as well as efficient mining processes. Although it has the capability of mitigating Distributed Denial of Service and blackhole attacks, scalability issues persist with sidechain management. To mitigate this, [2] presents a dual fog layer architecture in which requests are categorized into three types: real-time, non-real-time, and delay-tolerant blockchain types to optimize the distribution of computational load. While improving throughput and end-to-end delay, the dual fog network suffers from high deployment costs, which may be mitigated by substituting the secondary fog node with machine learning models for dynamic blockchain mining process.

Other works have explored machine learning and deep learning frameworks for scalability and QoS improvements. The work of [3] uses service-oriented permissioned blockchains with QoS-driven consensus protocols, such as PBFT, Zyzzyva, and Quorum, chosen dynamically based on deep Q-learning networks. While this provides enhanced security and delay control, a high delay in training limits real-time adaptability. Also, [4] proposes an optimization of the consensus protocol selection based on a deep reinforcement learning model using Paxos and Spinning techniques to boast the quality of services, but continuous changes in the network call for intense training, thereby increasing computational costs. The effort in [5] moves computational overhead to public clouds, and with the Ethereum blockchain, using data compression makes it cost-efficient but still limits the utility to financial transactions.

In further utilization of blockchain, [6-8] show 5G network integration and vehicular ad-hoc network traffic control. Random forest and kMeans clustering methods are applied to off-chain and on-chain request resolution, respectively. Despite these advantages, deployment in massive networks is highly constrained for such models, making it recommendable to integrate decentralized mechanisms and adaptive learning-based frameworks for resource allocation as in [10] and [11] in process.

Recent developments aim at decentralized caching, incentivized blockchain mechanisms, and context-aware consensus models. In [12], an edge caching framework combining contract management and trading market data aims at improving QoS and security. The healthcare application-oriented deployments [13], vehicular networks [8], and economic models [17] exemplify blockchain's diversity in use but indicate a design need to tailor blockchain systems according to specific cases. Comparative analyses of mining delay, computational complexity, and scalability performance among these models, as presented in [29-30], provide essential benchmarks for researchers and network designers to balance cost and QoS in blockchain-enabled wireless networks.

III. Empirical Analysis of Different Blockchain Architectures

From the review, it is observed that blockchain models have high security, and can be used to trace and mitigate attacks like DDoS, Sybil, Masquerading, blackhole, wormhole, etc. with high efficiency. This is possible due to the traceability, immutability, distributed computation, and cryptographic capabilities inherent to blockchain deployment models. But these modes have specific design and resource constraints, due to which their QoS performance in terms of block mining & verification delay (D), computational complexity (CC), scalability performance (S), and cost of deployment (CD) varies w.r.t. the algorithm used. In order to evaluate this performance, this section categorizes each of these values into low (L), medium (M), high (H), and very high (VH) fuzzy ranges. This categorization is done via estimating average values for each of the parameters, and normalizing them w.r.t. the blockchain deployment with minimum (L) & maximum (VH) parametric value. In order to reduce the complexity of algorithm selection, this section evaluates each of these algorithms in terms of application (A) of deployment, and tabulates these observations in table 1, wherein fuzzy values of the compared parameters can be observed.

TABLE I: EMPIRICAL ANALYSIS OF DIFFERENT BLOCKCHAIN DEPLOYMENTS

Method	D	CC	S	CD	Application
Federated side chain [1]	M	H	H	H	IoT
Dual Fog [2]	L	VH	H	VH	IoT
QoS aware consensus [3]	L	M	M	M	IoT
Deep re-enforcement learning [4]	H	H	VH	VH	Gen. N/W
Public fog nodes [5]	M	H	H	H	Gen. N/W
Stackelberg game theory [6]	H	M	M	M	Femto-cell N/W
Deep learning for security [7]	H	VH	L	H	Gen. N/W
BCOOL [8]	M	H	H	VH	Veh. N/W
BMEC [10]	L	H	H	H	Gen. N/W
Deep Re-enforcement learning [11]	H	VH	VH	VH	Gen. N/W
De-centralized caching [12]	M	H	H	VH	Gen. N/W
ssHealth [13]	L	VH	H	VH	Health-care N/W
MDEO [14]	H	H	VH	H	Gen. N/W
WPEG [15]	M	H	M	VH	IoT
DMIIoT [16]	L	VH	VH	VH	IoT
AI & blockchain [17]	M	VH	H	VH	EV
Routing Chain [18]	L	M	M	H	Gen. N/W
Incentive blockchain [20]	M	M	L	M	Gen. N/W
MVNOs [21]	M	M	M	H	Gen. N/W
Deep Re-enforcement learning [22]	H	VH	H	VH	Gen. N/W
IoT Chain [23]	M	H	M	H	IoT
Edge to cloud blockchain [24]	L	H	M	VH	Gen. N/W
GA with SFLA [25]	M	L	M	M	IoT

Each of these deployments are divided into general purpose networks, and IoT networks for the purpose of comparison. This is done mainly because IoT networks are resource constraint networks, while general purpose networks do not have that limitation for the process.

IV. CONCLUSION

From the comprehensive review, it can be observed that delay performance of Dual Fog [2], QoS aware consensus [3], DMIIoT [16], Federated side chain [1], WPEG [15], and IoT Chain [23] is better for IoT blockchain deployments. Similarly, GA with SFLA [25], QoS aware consensus [3], Federated side chain [1], WPEG [15], and IoT Chain [23] have low computational complexity, while, DMIIoT [16], Federated side chain [1], Dual Fog [2], and Reputation based coalition formation [26] outperform in case of scalability performance. Finally, the best deployment cost is obtained when GA with SFLA [25], QoS aware consensus [3], Federated side chain [1], Transaction validation [27], and IoT Chain [23] are used in process.Similarly, for general purpose wireless networks, BMEC [10], Routing Chain [18], Edge to cloud blockchain [24], ssHealth [13], AI & blockchain [17], Public fog nodes [5], De-centralized caching [12], and Incentive blockchain [20] outperform other models in terms of delay performance.

While, Routing Chain [18], Skychain [30], Incentive blockchain [20], MVNOs [21], Stackelberg game theory [6], ELM for storage [28], BMEC [10], and Edge to cloud blockchain [24] have lower computational complexity. Similarly Deep re-enforcement learning [4], MDEO [14], Deep Re-enforcement learning [11], BMEC [10], Public fog nodes [5], De-centralized caching [12], BCOOL [8], ssHealth [13], AI & blockchain [17] and Deep Re-enforcement learning [22] have better scalability sets. Finally, Stackelberg game theory [6], Incentive blockchain [20], MDEO [14], BMEC [10], Public fog nodes [5], Routing Chain [18], MVNOs [21], and Deep learning for security [7] outperform other models in terms of deployment cost, and thus must be considered while deploying general purpose wireless networks.

In future, it is recommended that hybrid combination of these models must be used for better deployment performance of domain specific blockchain networks.

REFERENCES

[1] W. Viriyasitavat, L. D. Xu, Z. Bi, D. Hoonsopon and N. Charoenruk, "Managing QoS of Internet-of-Things Services Using Blockchain," in IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1357-1368, Dec. 2019, doi: 10.1109/TCSS.2019.2919667.

[2] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan and J. Ahmed, "DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things," in IEEE Access, vol. 7, pp. 169073-169093, 2019, doi: 10.1109/ACCESS.2019.2952472.

[3] C. Qiu, H. Yao, F. R. Yu, C. Jiang and S. Guo, "A Service-Oriented Permissioned Blockchain for the Internet of Things," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 203-215, 1 March-April 2020, doi: 10.1109/TSC.2019.2948870.

[4] C. Qiu, X. Ren, Y. Cao and T. Mai, "Deep Reinforcement Learning Empowered Adaptivity for Future Blockchain Networks," in IEEE Open Journal of the Computer Society, vol. 2, pp. 99-105, 2021, doi: 10.1109/OJCS.2020.3010987.

[5] M. Debe, K. Salah, M. H. Ur Rehman and D. Svetinovic, "Monetization of Services Provided by Public Fog Nodes Using Blockchain and Smart Contracts," in IEEE Access, vol. 8, pp. 20118-20128, 2020, doi: 10.1109/ACCESS.2020.2968573.

[6] Z. Liu, L. Gao, Y. Liu, X. Guan, K. Ma and Y. Wang, "Efficient QoS Support for Robust Resource Allocation in Blockchain-Based Femtocell Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 11, pp. 7070-7080, Nov. 2020, doi: 10.1109/TII.2019.2939146.

[7] S. Rathore, J. H. Park and H. Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," in IEEE Access, vol. 9, pp. 90075-90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[8] S. Maaroufi and S. Pierre, "BCOOL: A Novel Blockchain Congestion Control Architecture Using Dynamic Service Function Chaining and Machine Learning for Next Generation Vehicular Networks," in IEEE Access, vol. 9, pp. 53096-53122, 2021, doi: 10.1109/ACCESS.2021.3070023.

[9] W. Viriyasitavat, L. D. Xu and Z. Bi, "Specification Patterns of Service-Based Applications Using Blockchain Technology," in IEEE Transactions on Computational Social Systems, vol. 7, no. 4, pp. 886-896, Aug. 2020, doi: 10.1109/TCSS.2020.2999574.

[10] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu and V. C. M. Leung, "Adaptive Resource Allocation in Future Wireless Networks With Blockchain and Mobile Edge Computing," in IEEE Transactions on Wireless Communications, vol. 19, no. 3, pp. 1689-1703, March 2020, doi: 10.1109/TWC.2019.2956519.

[11] M. Liu, Y. Teng, F. R. Yu, V. C. M. Leung and M. Song, "A Deep Reinforcement Learning-Based Transcoder Selection Framework for Blockchain-Enabled Wireless D2D Transcoding," in IEEE Transactions on Communications, vol. 68, no. 6, pp. 3426-3439, June 2020, doi: 10.1109/TCOMM.2020.2974738.

[12] J. Liu, S. Guo, Y. Shi, L. Feng and C. Wang, "Decentralized Caching Framework Toward Edge Network Based on Blockchain," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 9158-9174, Sept. 2020, doi: 10.1109/JIOT.2020.3003700.

[13] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini and A. Refaey, "ssHealth: Toward Secure, Blockchain-Enabled Healthcare Systems," in IEEE Network, vol. 34, no. 4, pp. 312-319, July/August 2020, doi: 10.1109/MNET.011.1900553.

[14] V. K. Rathi et al., "A Blockchain-Enabled Multi Domain Edge Computing Orchestrator," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 30-36, June 2020, doi: 10.1109/IOTM.0001.1900089.

[15] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang and J. Piran, "Blockchain-Based Incentive Energy-Knowledge Trading in IoT: Joint Power Transfer and AI Design," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3024246.

[16] A. Kumari, S. Tanwar, S. Tyagi and N. Kumar, "Blockchain-Based Massive Data Dissemination Handling in IIoT Environment," in IEEE Network, vol. 35, no. 1, pp. 318-325, January/February 2021, doi: 10.1109/MNET.011.2000355.

[17] H. ElHusseini, C. Assi, B. Moussa, R. Attallah and A. Ghrayeb, "Blockchain, AI and Smart Grids: The Three Musketeers to a Decentralized EV Charging Infrastructure," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 24-29, June 2020, doi: 10.1109/IOTM.0001.1900081.

[18] M. Karakus and E. Guler, "RoutingChain: A Proof-of-Concept Model for a Blockchain-Enabled QoS-Based Inter-AS Routing in SDN," 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2020, pp. 1-6, doi: 10.1109/BlackSeaCom48709.2020.9235021.

[19] H. Lee, K. Sung, K. Lee, J. Lee and S. Min, "Economic Analysis of Blockchain Technology on Digital Platform Market," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), 2018, pp. 94-103, doi: 10.1109/PRDC.2018.00020.

[20] J. Zheng, X. Dong, Q. Liu, X. Zhu and W. Tong, "Blockchain-based secure digital asset exchange scheme with QoS-aware incentive mechanism," 2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR), 2019, pp. 1-6, doi: 10.1109/HPSR.2019.8808111.

[21] D. B. Rawat and A. Alshaikhi, "Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints," 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 332-336, doi: 10.1109/ICCNC.2018.8390344.

[22] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, "Deep Reinforcement Learning (DRL)-Based Transcoder Selection for Blockchain-Enabled Video Streaming," 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644290.
[23] Sodhro, A.H., Pirbhulal, S., Muzammal, M. et al. Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications. J Grid Computing 18, 615–628 (2020). https://doi.org/10.1007/s10723-020-09527-x
[24] Kochovski, P., Stankovski, V., Gec, S. et al. Smart Contracts for Service-Level Agreements in Edge-to-Cloud Computing. J Grid Computing 18, 673–690 (2020). https://doi.org/10.1007/s10723-020-09534-y
[25] Asghari, P., Rahmani, A.M. & Javadi, H.H.S. Privacy-aware cloud service composition based on QoS optimization in Internet of Things. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-01723-7
[26] A. Asheralieva and D. Niyato, "Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in IoT Blockchains With Mobile-Edge Computing," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11830-11850, Dec. 2020, doi: 10.1109/JIOT.2020.3002969.
[27] A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.
[28] D. Jia, J. Xin, Z. Wang and G. Wang, "Optimized Data Storage Method for Sharding-Based Blockchain," in IEEE Access, vol. 9, pp. 67890-67900, 2021, doi: 10.1109/ACCESS.2021.3077650.
[29] N. Sohrabi and Z. Tari, "ZyConChain: A Scalable Blockchain for General Applications," in IEEE Access, vol. 8, pp. 158893-158910, 2020, doi: 10.1109/ACCESS.2020.3020319.
[30] A. Mizrahi and O. Rottenstreich, "State Sharding with Space-aware Representations," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-9, doi: 10.1109/ICBC48266.2020.