International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 11, No. 2, 2024, pp. 28-32.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Blockchain-SDN Framework for Secure and Reliable 5G Massive IoT Networks Utilizing Deep Learning for Bandwidth Estimation

Neeraj Chauhana [a], Aishwarya Iqbal [b]

[a] *Energy-Efficient Systems Lab, Solapur Engineering and Computing School, India*.
[b] *Energy-Efficient Systems Lab, Solapur Engineering and Computing School, India*.

Abstract

The emerging 5G wireless network will offer new opportunities for resolving the networking problems of the Internet of Things (IoT) because it is expected to support the massive 5G-IoT (5G-MaIoT) architecture. 5G technologies are expected to allow light, large-scale IoT devices to be dormant for long periods and have them switch on to 'sleep mode,' significantly lowering power consumption while still providing high data output through a low-latency mobile data interface. IoT systems, on the other hand, have several safety and confidentiality problems; attempting to mitigate unauthorized access to IoT nodes is required. In this work, the research proposes the BC-SDN framework for Secure and Reliable 5G Massive IoT Networks (5G-MaNet) using Software Defined Networks (SDN) Blockchain, which uses Deep Learning for Bandwidth Estimation (DL-BE) to estimate bandwidth. The proposed architecture instantiates the SDN concept of network control as the division of information and command planes, with BC providing additional control over maintaining security and secrecy. Thus, BC-SDN-5G-MaNet can protect sensitive information without compromising reliable data transfer within and outside the layers of 5G network architecture. Also, an SDN controller is designed with a DL-BE module to estimate network capacity and assist the manager in selecting the optimal configuration that fulfills the BE in the network.

The efficiency of the "BC-SDN-5G-MaNet" architecture has been executed via a simulation setting, demonstrating the impact of the suggested solution relative to standard IoT architectures.

Keywords: Blockchain, Software Defined Networks, 5G, IoT, Deep Learning, Bandwidth Estimation, Security.

DOI: 10.71086/IAJSE/V11I2/IAJSE1146
Received: 21 April 2024/Revised: 13 May 2024/Accepted: 23 June 2024/Published: 30 July 2024

Outline of the Research

The burgeoning 5G mobile internet greatly enhances IoT connection. Numerous battery-operated IoT devices, intelligent cameras, environmental detectors, and electronic meters are utilized across various contexts such as intelligent towns, self-sustaining agriculture, and intelligent production; these kinds of tasks necessitate the transmission of substantial data through minimal latency mobile communication protocols (Rahman et al., 2024).

Nonetheless, 5G-enabled enormous IoT has several concerns about privacy and security, which impede the dependability of the associated devices. Contemporary 5G security frameworks that bolster IoT devices use the characteristics of the radio channel to improve communication safety via suitable encoding and signal processing methods (Hakiri & Dezfouli, 2021; Turner et al., 2023). An infected IoT device may be susceptible to Distributed Denial-of-Service (DDoS) assaults, inundating the IoT network with harmful data. Hostile IoT nodes may infiltrate the extensive IoT network at any moment, inundating its assets with harmful traffic to render their services inaccessible.

BC has created several opportunities for the IoT age by handling data from multiple devices and offering a safe communication framework across critical situations (Rahman et al., 2021). BC establishes a distributed security framework to mitigate DDoS assaults and eradicate the vulnerabilities associated with dependence on a single point of breakdown. Notwithstanding its potential, BC may prove economically unfeasible for extensive IoT applications.

SDN has a lot of promise in helping IoT systems handle their high demands by shifting computing to FC designs close to edge devices and allowing for more IoT capabilities through on-demand management and control. SDN makes monitoring communication lines in big IoT systems easier, enabling them to split up information streams and handle errors better for important data (Das et al., 2023; Choudhary & Dorle, 2022). If a server or link fails, SDN guarantees that flows satisfy Quality of Service (QoS) criteria and helps reroute and balance IoT streams.

Combining BC with SDN, according to researchers, enables better analysis of IoT activity and more private and secure information from the worldwide knowledge of SDN managers, thereby helping to keep traffic flowing more smoothly during attacks (Al Ghamdi, 2022). This approach uses SDN and BC technologies to develop trust and thereby strengthen the resilience of large-scale IoT networks, hence improving their efficiency and effectiveness.

SDN management can communicate IoT and BC security guidelines to the network nodes and routers. Furthermore, remote controllers set trust and protection between IoT nodes and area sensors (Gao et al., 2019). Eliminating the need for deep packet analysis of IoT data enables the BC-enabled framework to create new trust-less links, enhancing IoT capabilities and increasing its accountability and efficiency.

Proposed Method

This section introduces the proposed "BC-SDN-5G-MaNet" robust architecture for 5G networks. Fig. 1 illustrates that "BC-SDN-5G-MaNet" amalgamates SDN, BC, and DL technologies inside the 5G network, facilitating communication for various IoT sensors, including intelligent automobile systems and smart homes. The continuous allocation of bandwidth is facilitated by several SDN controls, which improve the scalability and adaptability essential for 5G network design. Furthermore, a DL module in the SDN controller facilitates the accurate forecasting of network capacity. As SDN delineates command and data planes, targeted frequency allocation techniques may be implemented to control information traffic, which CNN-based BE forecasts will inform.

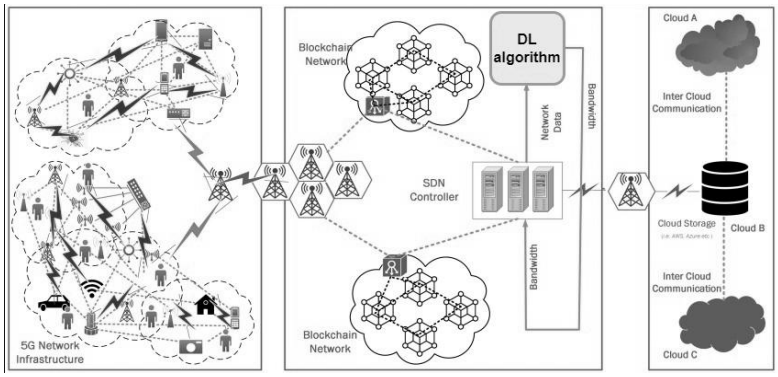


Fig. 1: Architecture of the Proposed BC-SDN-5G-MaNet Framework

Furthermore, "BC-SDN-5G-MaNet" utilizes the general-purpose Ethereum BC—while being theoretically neutral about the particular BC shown in Fig. 1—to enhance safety to achieve data consistency, decentralized governance, and accountability. This information is kept in shared cloud computing (CC) resources across many Virtual Machines (VM) of a public CC service. BC ensures safety and secrecy among information blocks across the 5G network. The 5G system is the foundational networking framework of "BC-SDN-5G-MaNet," providing various services within the proposed structure, including cost-effectiveness, diminished network outages, low delays, and enhanced portability. The primary beneficiaries of this architecture's execution are massive wireless network providers and, more broadly, network managers, particularly in intelligent environments like intelligent towns and apartments, where apps and services demand stringent criteria for minimal errors, outstanding efficiency, and privacy.

DL-BE Module

A DL-BE module has been integrated into the SDN controller to evaluate network resources and assist the management in making educated decisions to fulfill BE standards. As seen in Fig. 2, preprocessing and feature extraction have been done before partitioning the database into learning and testing datasets. This approach renders the information machine-accessible and enhances the reliability of predictions. Initially, due to the database including just four DL model characteristics, supplementary features have been generated from the current ones to assist CNN in achieving the BE objective. Furthermore, the research mitigates the association problem among the dependent variables by augmenting the number of attributes. The efficacy of network BE has been assessed using the rigorous 5-fold cross-validation method, allocating 75% of the data for learning and the rest, or 25%, for testing.

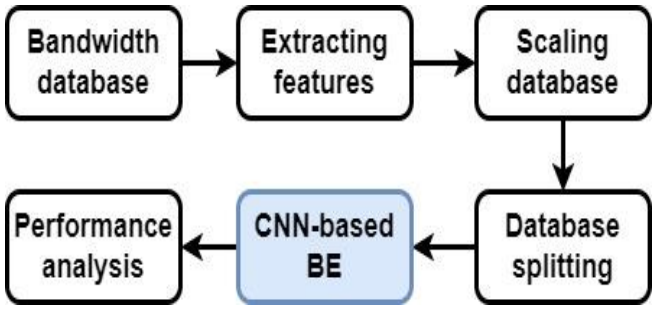
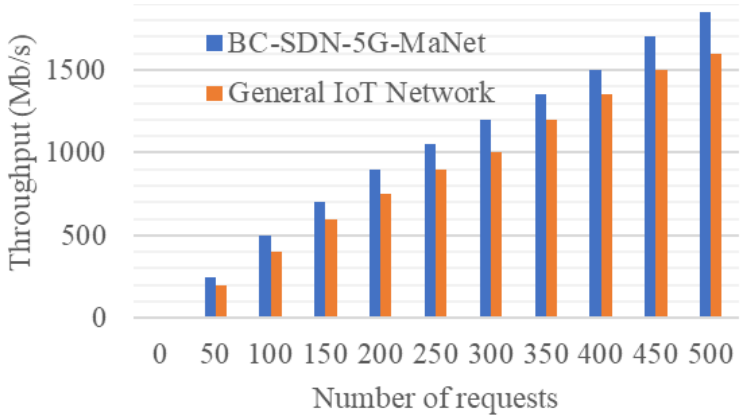


Fig. 2: DL-BE Module

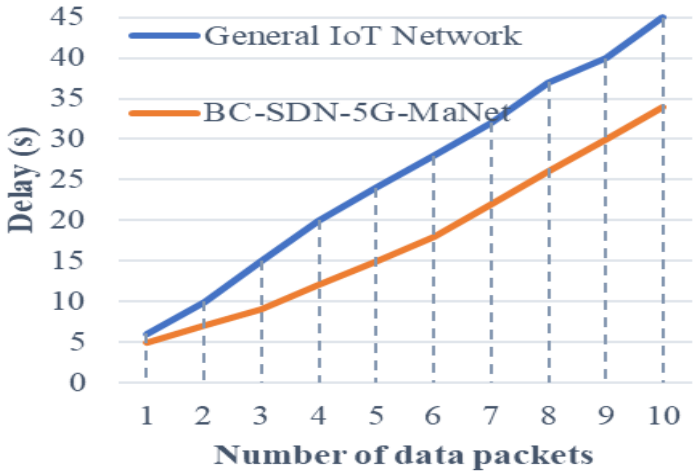
Employing BE related to the BC-SDN model captures and resolves issues dealing with security and reliability of communication in massive 5 G IoT networks. Such tasks are framed as predicting problems in which BE is performed in real time. CNN models have proven remarkable in capturing and retrieving features associated with patterns and complex temporal changes of system-monitored activities. When integrated within a BC-SDN framework, the CNN supports the dynamic resource allocation required at runtime and fortifies the data's integrity, trust, and scalability through disintegrated control. With this, system performance is markedly improved by lessening latency and boosting QoS without compromising other functions. Therefore, employing such an approach guarantees system efficiency concerning the overwhelming number of IoT devices integrated into 5G networks.

Simulation Results

The simulation results indicate that the amalgamation of SDN with BC enables "BC-SDN-5G-MaNet" to surpass all evaluated benchmarks and effectively respond to incidents impacting network efficiency, including errors and hostile attacks. Fig. 3 (a) "Throughput (Mb/s) analysis" shows the comparison of metrics between BC-SDN-5G-MaNet and a General IoT Network concerning the volume of requests made. If the number of calls goes from 0 to 500, the rate goes up for both platforms. In every way, BC-SDN-5G-MaNet works better than the General IoT Network. The result shows that BC-SDN-5G-MaNet is better at handling a lot of calls. For example, BC-SDN-5G-MaNet can handle 1850 Mb/s of requests, while the General IoT Network can only handle 1600 Mb/s. BC-SDN-5G: MaNet delivers data faster than the General IoT Network and can house more devices. This makes it a better option for significant IoT uses in 5G systems.



(a) Throughput (Mb/s) Analysis



(b) Delay (s) Analysis

Fig. 3: Performance Analysis of Proposed BC-SDN-5G-MaNet

The "Delay (s) study" depicted in Fig. 3(b) demonstrates how the delay for the General IoT Network, as well as the BC-SDN-5G-MaNet system, develops from one to ten packet count. For all packet counts, the BC-SDN-5G-MaNet's delay time is shown to be shorter than that of the General IoT Network. For 10 packets, the General IoT Network has a 45-second delay time; for instance, the BC-SDN-5G-MaNet has a 34-second delay time. The data processing capabilities of a typical IoT network are less than those of BC-SDN-5G-MaNet. In 5G-enabled IoT environments—which must move instantly—it is also far faster, more versatile, and more scalable.

Conclusion

The BC-SDN Framework for dependable and safe 5G Mass IoT Networks (5G-MaNet) is presented in this research paper. It incorporates bandwidth estimation (DL-BE) Deep Learning. Software-defined networking (SDN) divides the network into data and control planes, therefore regulating it. Blockchain (BC) technologies guard private data and provide additional design security. Consequently, the "BC-SDN-5G-MaNet" architecture can guard private data and offer safe data transfer inside and outside the infrastructure of the 5G network. The SDN controller includes a module for estimating (DL-BE), which helps the controller determine how the system operates and assist in the best management decisions to attain the bandwidth estimation (BE) targets. BC-SDN-5G-MaNet delivers data faster and can manage more devices than the General IoT Network. This makes it a better option for significant IoT uses in 5G systems.

References

Rahman, A., Khan, M. S. I., Montieri, A., Islam, M. J., Karim, M. R., Hasan, M., ... & Pescapè, A. (2024). BlockSD-5GNet: Enhancing security of 5G network through blockchain-SDN with ML-based bandwidth prediction. *Transactions on Emerging Telecommunications Technologies, 35(4),* e4965.

Hakiri, A., & Dezfouli, B. (2021, April). Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks. *In Proceedings of the 2021 ACM international workshop on software defined networks & network function virtualization security (pp. 11-18).*

Turner, S. W., Karakus, M., Guler, E., & Uludag, S. (2023). A promising integration of sdn and blockchain for iot networks: A survey. *IEEE Access, 11*, 29800-29822.

Rahman, A., Islam, M. J., Montieri, A., Nasir, M. K., Reza, M. M., Band, S. S., ... & Mosavi, A. (2021). Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot. *IEEE Access, 9*, 28361-28376.

Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., & Biswas, U. (2023, January). Blockchain enabled sdn framework for security management in 5g applications. *In Proceedings of the 24th International Conference on Distributed Computing and Networking (pp. 414-419).*

Choudhary, S., & Dorle, S. (2022). A quality of service-aware high-security architecture design for software-defined network powered vehicular ad-hoc network s using machine learning-based blockchain routing. *Concurrency and Computation: Practice and Experience, 34(17),* e6993.

Al Ghamdi, M. A. (2022). An optimized and secure energy-efficient blockchain-based framework in IoT. *IEEE Access, 10,* 133682-133697.

Gao, J., Agyekum, K. O. B. O., Sifah, E. B., Acheampong, K. N., Xia, Q., Du, X., ... & Xia, H. (2019). A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. *IEEE Internet of Things Journal, 7(5),* 4278-4291.