Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 4-B, pp. 1451–1460
DOI : 10.47974/JDMSC-2290

Blockchain and SDN-driven security and scalability for IoT based smart city network

Nawfal Radhi Jebur
Department of Advanced Information System
College of Information Technology Management
Tehran South Branch
Islamic Azad University
Tehran
Iran

Abstract

As IoT-based smart city networks expand rapidly, they face critical challenges regarding security, scalability, and network management. A Blockchain-enabled Software-Defined Networking (SDN) framework integrating a queueing model for increased security and scalability is presented in this study to address these concerns. Decentralized, tamper-resistant data management is provided by blockchain, while dynamic network traffic management is provided by SDN. SDN emulation is provided by Mininet-WiFi, blockchain security is provided by Ethereum, and optimized routing is delivered by OpenFlow. As a result of simulations, data delivery rates were improved, delays were reduced, and cyber threats, specifically DDoS attacks, were made more resilient. IoT infrastructure for smart cities can be made more secure and scalable through the integration of Blockchain and SDN.

Subject Classification: *35R02, 68M10.*

Keywords: *IoT, Smart city, Blockchain, Software-defined networking (SDN), Queueing model, Security, Scalability.*

1. Introduction

Smart cities are being developed as a result of urbanization and technological advancements, where IoT technology plays a key role in enhancing urban quality of life. Connected devices, sensors, and systems enable smart city networks to optimize infrastructure, improve public services, and promote sustainability [1]. Security, scalability, and efficient network management are among many challenges associated with this interconnected environment. Using SDN technology in conjunction with blockchain technology could be a promising solution to these problems. A blockchain system manages

E-mail: **nawfalask@gmail.com**

secure data in a decentralized, tamper-proof manner, while a software-defined network provides scalability and dynamic network management by decoupling the control plane from the data plane [2]. By combining Blockchain and SDN, IoT networks in smart cities can become more secure, more scalable, and more resilient. The IoT devices, however, accumulate information fragmentarily due to a lack of systematic and scientific procedures for arranging the data collections. SDN, which decorates the large amounts of scattered data, is used to configure and manage IoT applications. A dynamic change to the operational procedures can be performed by changing them programmatically without affecting the main physical architecture. SDN can detect vulnerabilities easily and take some preliminary steps to prevent any attacks based on the detected anomalies. In addition to these benefits, SDNs can be controlled by a large number of centralized controllers [3]. It is possible to enhance security and privacy by integrating Blockchain technology. A Smart Contract (SC) validates and checks transactions [4]. A block containing the indexed data is created for the public ledger after a block containing validated data transactions has been created and stored in storage. Intruders cannot alter the ledger because it is immutable. Blockchain technology prevents trespassers from attacking, and the SC handles transactions programmatically after establishing rules and regulations.

IoT-based smart cities can be enhanced with blockchain technology, which was originally designed to underpin cryptocurrencies like Bitcoin. Despite the complexity of IoT, its decentralized nature, immutability, and strong cryptographic security features make it a useful tool for securing data and transactions. A distributed network of nodes distributes data and processing across the network, which is more secure than traditional centralized systems with single points of failure. With a distributed ledger approach, all transactions across the network are visible and verifiable, ensuring data integrity and transparency [5]. In addition, blockchains use cryptographic techniques to prevent unauthorized access to data and unauthorized modifications [6], which substantially reduces the risk of data breaches. A smart city network's data generated by IoT devices can be managed securely and efficiently with blockchain, which combines decentralization and transparency. Smart city networks based on IoT are more scalable and efficient with SDN. As a result of the centralized control plane, we are able to allocate resources efficiently and optimize traffic in order to reduce network congestion and improve performance [7], [8]. Through the use of this centralized view, intelligent routing and load balancing can be implemented to ensure that network resources are used to their maximum potential and that data is transmitted efficiently [5], [16]. Easily scalable and resilient networks can be configured with programmatically configurable devices, which can dynamically adapt to changing traffic patterns [9]. The ability to adapt dynamically is essential in smart city environments where traffic can fluctuate dramatically as the day progresses and as events occur. A smart city infrastructure that uses SDN efficiently can respond and perform more reliably to these variations. In order to secure and scale IoT-based smart city networks, blockchain and SDN technologies must be integrated synergistically. SDN's programmable infrastructure makes it easy to manage networks efficiently [10], while blockchain's immutability and cryptographic strength enhance security. As a result, smart cities can benefit from a combined approach that overcomes the limitations of individual technologies while offering a holistic approach to scalability and security. Smart cities require a system that is both scalable and secure, which is why these two technologies work together to create a secure and highly scalable system.

2. Related Work

As described in [11], uses NFV to enable a block chain-based and SDN-based distributed architecture for smart cities. In addition, the authors present a method for identifying group leaders that is energy-optimized. SDN controllers also manage and monitor IoT components. A block chain-based approach is used in this study to detect and counter cyber-attacks against the Internet of Things (IoT) infrastructure [12]. According to the test results, the proposed architecture offers superior performance in terms of throughput, time, fuel usage, and communication overhead compared to the existing system. The distribution-based routing technique, in which packets are routed according to the network topology, is renowned for its inefficiency. They are advantageous because they have low overhead, and they have a low chances of routing failures as well. IoT-enabled wireless sensor networks can be routed smartly using Deep Reinforcement Learning (DRL), which can reduce delay while extending network lifetime simultaneously [13] [14]. It extends the lifetime of the sensor network considerably by dividing it into uneven clusters based on the amount of data transmitted by each sensor. According to the results of the experiments, the proposed strategy resulted in improved network throughput, energy efficiency, communication delay, and only a small number of nodes that were dead.

The authors of [15] proposes a SDN-based implementation of load balancing that considers both response time and server resource utilization. Among the components of SBLB are an application module, a software-defined-networking (SDN) controller, and server farms communicating through SDN-capable switches and routers. In addition to active load balancing, observing, and categorizing services, the program itself has other sub-modules. Controllers process all incoming communications automatically, as well as overseeing the pool of hosts. Using a multilayer SDN architecture [16] data monitoring & load balancing can be sped up in a local region and across networks. Using this architecture, multiple load balancing mechanisms can be implemented to prevent the controller from becoming a bottleneck within the system. In experiments, their technique reduced average turnover and waiting time, enhancing processing performance.

Enhanced transportation, healthcare, energy management, and public safety are some of the benefits of integrating the Internet of Things (IoT) within smart city infrastructures. Although IoT-based smart cities offer the benefits of scalability, security, and efficiency, they come with critical challenges.

Increasingly, researchers are exploring the synergies between Blockchain technology and Software-Defined Networking (SDN) in order to address these challenges. The resources, computing power, and security measures available to smart city IoT devices make them vulnerable to cyber threats, such as data breaches, unauthorized access, and DDoS attacks [17]. Smart cities may not be able to protect against emerging threats effectively with traditional centralized security solutions. Blockchain can be integrated with SDN to make smart city networks more secure and scalable. The Blockchain can secure the SDN control plane by validating network configurations and policies, whereas SDN enhances the performance of Blockchain by optimizing routing and reducing latency [18]. Using SDN-driven dynamic routing and Blockchain-based access control mechanisms, [11] discusses new frameworks for improving security and scalability in smart city simulations.

3. Proposed Methodology

Connecting IoT devices requires configuring an SDN controller. IoT devices are assigned IP addresses and public keys by SDN controllers. Using an SDN controller, you can monitor and control the energy status of your devices. SDN domains contain residual energy from IoT devices and sources of energy. All IoT devices can calculate their neighbours' remaining energy during packet transfer. Whenever an IoT device sends energy to a controller or other device, packets are sent in accordance with that energy. During the Internet of Things, devices send packets to their controllers based on the amount of energy they send. Those nodes trespassing the threshold or acting maliciously will have their energy resources blocked by their controllers. Further, their IDs are registered on the public blockchain, which makes it impossible for them to register anywhere else. Through their public keys, public blockchain nodes are authenticated in another SDN domain so that they can be authenticated in other SDN domains. It is possible for nodes to migrate from one SDN domain to another if their energy is below a certain level. By migrating to a new domain and receiving their private keys, nodes below the threshold can maintain their lifetimes in SDN. It is possible for the SDN controller to switch between clusters as long as the public keys of the IoT devices are stored within the block. The addition of IoT devices to SDN controllers provides a range of services in addition to improving network efficiency. The proposed architecture enables communication between two SDN domains and IoT devices. Blockchain technology is used in this controller to facilitate peer-to-peer communication over a secure network. IP addresses, private keys, and energy consumption uniquely identify each IoT device in our architecture. A blocklist (block list) is used by SDN controllers to keep track of devices and transactions. In equation 1, transmission energy is calculated based on distance and environmental characteristics. There are nearby reserves $b = 2$.

$$T = B \times d^{b} \; if \; d \leq dt \tag{1}$$

Calculation of long distances is based on equation (2) (b = 4).

$$T = B \times E \times d^{b} \; if \; d > dt \tag{2}$$

Equation (3) explains how Internet of Things devices consume energy. Received energy is represented by R in this case.

$$R = E \times B \tag{3}$$

It is possible to calculate the current energy of each Internet of Things device using Equation 4 (A).

$$A = T \times R \tag{4}$$

Equation (C) can be used to calculate each node's remaining energy.

$$C = E_i - A \tag{5}$$

3.1. *Queueing Model*

In this section, throughput, delay, energy, and energy consumption of the proposed model are also analyzed using queueing theory. In model controllers, queueing models are used, while IoT devices use queueing systems to capture cluster costs.

The $M/H/2/1$ theory of line up was used to analyze model parameters for IoT devices because their battery life is limited [19]. Our assumption is that, in a network of interconnected devices, each device's average packet arrival rate and its λ_i arrival rate are independent of one another.

There must be incorrect or malicious packets sent to SDN controllers to indicate that this has occurred.

According to $\lambda_i \times \rho$ and $\lambda_i \times (1 - \rho)$, i^{th} devices receive packets at the rate YI and distribute them accordingly. According to current probabilities, μ_1 has probability P and μ_2 has probability $(1 - \rho)$

As of now, μ_1 has probability ρ, while μ_2 has probability $(1 - \rho)$. The state of an IoT device is represented by, among the stages of service, s represents how many packages there are, and x represents the number of packages. Matrix-Geometric Technique can be used to determine the stationary distribution of IoT devices [20]. The following equations can be used to calculate the stationary probability vector: $Q(i)$.

$$Q(i) = (Q(i)_0, Q(i)_1, Q(i)_2, \dots . Q(i)_m, \dots \dots .) \tag{7}$$

$$\rho = \frac{\lambda}{\mu} < 1 \tag{8}$$

$$Q_0 = 1 - \rho \tag{9}$$

$$Q_m = (1 - \rho)\rho^m \tag{10}$$

In a queuing system, the mean packet count is calculated as follows:

$$N_i = \sum_{k=1}^{\infty} K\pi_k^i \tag{11}$$

$$N_i = \sum_{k=1}^{\infty}(1 - \rho)\rho^k \tag{12}$$

$$N_i = (1 - \rho)\sum_{k=1}^{\infty} k\rho^k = (1 - \rho)\rho\sum_{k=1}^{\infty} k\rho^{k-1} \tag{13}$$

The possibility of writing exists kp^{k-1} as $k\rho^{k-1} = d\rho k/dp$,

$$N_i = (1 - \rho)\rho\sum_{k=1}^{\infty}\frac{d}{dp}p^k = \frac{(1-\rho)\rho d}{dp}\left(\sum_{k=1}^{\infty} p^k\right) \tag{14}$$

Once,

$$\sum_{k=1}^{\infty} p^k = \sum_{k=1}^{\infty} p^k - 1 = \frac{1}{1-\rho} - 1 = \frac{\rho}{1-\rho}.$$

Achieving success

$$N_i = \frac{(1-\rho)\rho d}{dp}\left(\frac{\rho}{1-\rho}\right) \quad (15)$$

$$N_i = \left(\frac{\rho}{1-\rho}\right) \quad (16)$$

Therefore, we have $\rho < 1$ and $\rho = \frac{\lambda}{\mu}$.

$$N_i = \frac{\lambda}{\mu-\lambda} \quad (17)$$

According to the IoT devices, packet processing time is approximately as follows:

$$Ws_i = \frac{1}{\lambda} N_i = \frac{1}{\mu-\lambda} \quad (18)$$

$$Ws = \sum_{i=1}^{n} \frac{\lambda_i}{\sum_{I=1}^{n} \lambda_i} W_{si} \quad (19)$$

3.2. *SDN-BLOCKCHAIN*

A blockchain gateway on an SDN controller must deliver transactions and blocks in sync with the current state of the blockchain. Blockchain SDNs are susceptible to MAC attacks performed by attackers that prevent some nodes from sending or receiving data. Blockchain systems that consist of few nodes would be especially vulnerable to this kind of attack. Implementing appropriate security systems is necessary to protect consensus blockchains from MAC attacks. Our SDN-Blockchain approach, which is based on a list-based traffic fusion approach, assists and reduces dangerous traffic. The immutability and decentralized nature of blockchain ensures data integrity, confidentiality, and scalability. Security for IoT communications requires encryption and decryption mechanisms. Blockchain-based cryptographic algorithms use public-key cryptography (eliptic curve cryptography or RSA) when transmitting data from IoT devices. Blocks of data are then stored in the blockchain, ensuring tamper-resistant records. Decryption can only be performed by authorized parties holding the correct private key, ensuring secure access management. SHA-256, which prevents unauthorized modifications, adds further protection to data stored in blockchains. As a result of integrating Software-Defined Networking (SDN), the system is capable of managing network policies dynamically, optimizing resource allocation, and reducing security threats, such as Distributed Denial of Service (DDoS) attacks. Blockchain and SDN bridge the gap between scalability and security in a smart city by enabling secure, real-time communications between IoT devices, ensuring resilience and adaptability.

4. Result and Discussion

Smart City Networks based on IoT can be made safer and more scalable by integrating Blockchain-enabled SDN-Driven Security with queueing models. SDN emulation is provided by Mininet-WiFi, security is provided by Ethereum

Blockchain, and routing is enabled by OpenFlow rules. A comparison between the proposed model and Blockchain Fundamentals (BCF) is shown in Figure 1. Optimized models consistently perform better than BCF, reducing packet losses and delivering higher data rates. As the network scales, this efficiency is assured by the secure SDN selection algorithm and integration of Blockchain technology.

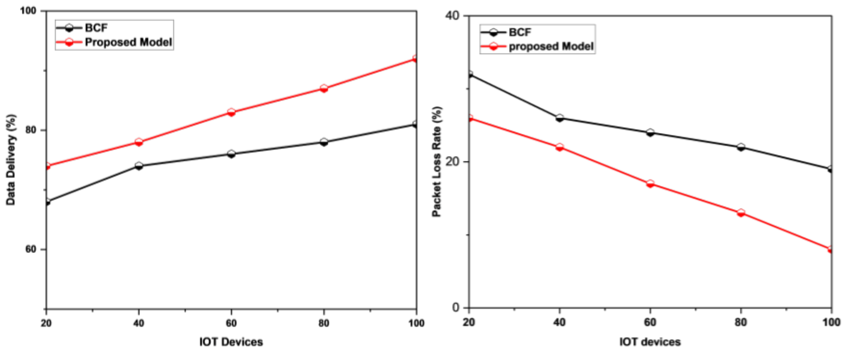

Figure 1
Data delivery (%) and packet loss (%) versus IOT devices.

The figure 2a illustrates the effect of network transactions on file sizes and response times (ms). Transaction volumes increase linearly with response time, while IoT device loads increase linearly with transaction volumes. SDN controllers process requests efficiently, compared to Blockchain transactions, confirming the scalability of our architecture. As shown in figure 2b, the core model performs better than the proposed model when it comes to file operations. However, the proposed model consistently outperforms the core model when it comes to handling larger file sizes and reducing response time.

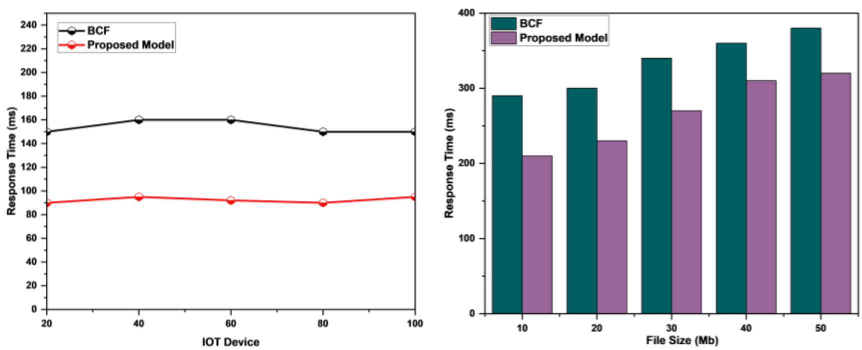

Figure 2
Response time (ms) versus IOT devices and file size (Mb).

A comparison of the proposed architecture with the baseline BCF architecture is shown in Figure 3a. There are fewer IoT devices in both models at first, so the delay values are similar. The proposed model, however, consistently outperforms BCF as node counts grow, showing that it is efficient at reducing end-to-end delays as node counts increase. A CPU analysis of Figure 3b shows CPU usage during DDoS attacks while multiple background services are running. In response to increasing file size (MB), CPU usage spikes initially but quickly stabilizes, indicating that the proposed model is resilient and has a strong resistance to such attacks.

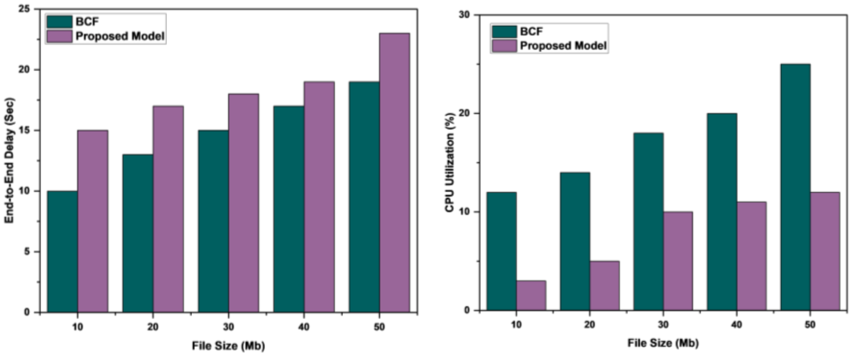

Figure 3
End-to End delay (sec) and CPU utilization (%) versus and file size (Mb).

5. Conclusion

SDN-based IoT-based smart city networks can be enhanced with blockchain-integrated SDN architectures to enhance security and scalability. A proposed model combines SDN's programmable network control with Blockchain's decentralized security to effectively mitigate cyber threats, optimize data transmission, and reduce congestion on networks. DDoS attacks are significantly reduced, data delivery is improved, and response time is faster. Resources are allocated more efficiently and the network is more efficient when a queueing model is incorporated. As a result, this approach shows promise in terms of managing IoT devices in smart cities in a secure and scalable manner. We will focus our future efforts on optimizing Blockchain consensus mechanisms to make them more energy efficient and perform better.

References

[1] P. Rani, U. C. Garjola, H. Abbas, and D. Koundal, “Federated learning-based misbehaviour detection for the 5G-enabled Internet of Vehicles,” *IEEE Transactions on Consumer Electronics,* vol. 69, no. 2, pp. 238–246 (2023).

[2] A. Singh, H. Babbar, D. Gupta, F. Al-Turjman, and H. M. Aljahdali, "Blockchain-based lightweight authentication protocol for next-generation trustworthy Internet of Vehicles communication," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 36–45 (2024).

[3] A. Rahman, S. S. Band, G. Muhammad, and K. Hasan, "DistB-Condo: Distributed blockchain-based IoT-SDN model for smart condominium," *IEEE Access,* vol. 8, pp. 209594–209609 (2020), doi: 10.1109/ACCESS.2020.3039113.

[4] P. Rani, U. C. Garjola, and H. Abbas, "A predictive IoT and cloud framework for smart healthcare monitoring using integrated deep learning model," *NJF Intelligent Engineering Journal,* vol. 1, no. 1, pp. 53–65 (2024).

[5] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digital Communications and Networks*, vol. 9, no. 2, pp. 411–421 (Apr. 2023), doi: 10.1016/j.dcan.2022.11.003.

[6] C. M. S. Ferreira, C. T. B. Garrocho, R. A. R. Oliveira, J. S. Silva, and C. F. M. D. C. Cavalcanti, "IoT registration and authentication in smart city applications with blockchain," *Sensors,* vol. 21, no. 4, p. 1323 (Feb. 2021), doi: 10.3390/s21041323.

[7] A. Rahman, M. J. Islam, G. Muhammad, and K. Hasan, "SmartBlock-SDN: An optimized blockchain-SDN framework for resource management in IoT," *IEEE Access,* vol. 9, pp. 28361–28376 (2021), doi: 10.1109/ACCESS.2021.3058244.

[8] H. Babbar, S. Rani, D. Gupta, H. M. Aljahdali, A. Singh, and F. Al-Turjman, "Load balancing algorithm on the immense scale of Internet of Things in SDN for smart cities," *Sustainability,* vol. 13, no. 17, p. 9587 (Aug. 2021), doi: 10.3390/su13179587.

[9] V. R. Tadinada, "Software defined networking: Redefining the future of Internet in IoT and cloud era," in Proc. 2014 Int. Conf. Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, pp. 296–301 (Aug. 2014). doi: 10.1109/FiCloud.2014.53.

[10] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access,* vol. 6, pp. 115–124 (2018), doi: 10.1109/ACCESS.2017.2757955.

[11] M. J. Islam, A. Rahman, S. S. Band, G. Muhammad, and K. Hasan, "Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3850–3864 (2021).

[12] B. Bhola, M. R. Islam, S. Roy, and T. Ahmad, "Quality-enabled decentralized dynamic IoT platform with scalable resources integration," *IET Communications,* vol. 16, no. 7, pp. 765–776 (2022).

[13] B. Sangamithra, B. E. Manjunath Swamy, and M. Sunil Kumar, "WITHDRAWN: A comparative study on a privacy protection in personalized web search," Materials Today: Proceedings, p. S221478532038754X (Jan. 2021), doi: 10.1016/j.matpr.2020.11.148.

[14] N. Kumar, P. Rani, V. Kumar, P. K. Verma, and D. Koundal, "Teeech: Three-tier extended energy efficient clustering hierarchy protocol for heterogeneous wireless sensor network," *Expert Systems with Applications,* vol. 216, p. 119448 (2023).

[15] S. Kumar, K. Cengiz, S. Vimal, and A. Suresh, "Energy efficient resource migration based load balance mechanism for high traffic applications IoT," *Wireless Personal Communications*, vol. 127, no. 1, pp. 385–403 (Nov. 2022), doi: 10.1007/s11277-021-08269-7.

[16] Z. Eghbali and M. Z. Lighvan, "A hierarchical approach for accelerating IoT data management process based on SDN principles," *Journal of Network and Computer Applications*, vol. 181, p. 103027 (May 2021), doi: 10.1016/j.jnca.2021.103027.

[17] S. Chaudjary, R. Kakkar, R. Gupta, S. Tanwar, S. Agrawal, and R. Sharma, "Blockchain and federated learning-based security solutions for telesurgery system: A comprehensive review," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 30, no. 7, pp. 2446–2488 (Nov. 2022), doi: 10.55730/1300-0632.3950.

[18] T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," *Electronics*, vol. 9, no. 11, p. 1864 (2020).

[19] U. N. Bhat, An Introduction to Queueing Theory: Modeling and Analysis in Applications, Boston, MA, USA: Birkhäuser Boston (2008), doi: 10.1007/978-0-8176-4725-4.

[20] R. Bhatia and J. Holbrook, "Riemannian geometry and matrix geometric means," *Linear Algebra and its Applications,* vol. 413, no. 2–3, pp. 594–618 (2006).

Received February, 2025