International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A BLOCKCHAIN-INTEGRATED IOT AND SCADA SYSTEM FOR ENHANCED SECURITY IN SMART GRIDS

Muhammad Ayaz[1, 2]

[1]Artificial Intelligence and Sensing Technologies (AIST) Research Centre, University of Tabuk, Tabuk 71491, Saudi Arabia
[2]Faculty of Computers and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia, email: ayazsharif@ut.edu.sa

ABSTRACT

The integration of IoT and SCADA systems in smart grids became more popular as it helping to increase the level of automation and real time monitoring. Nevertheless, security flaws, high latency and poor data management are the bottlenecks in practice that introduce vulnerabilities to smart grids in which cyber threats, false data injection attacks and system outages may cause a disaster. Centralized architecture and regular blockchain implementations are difficult to fulfil the requirements for scalable, sustainable and real-time security tools. Focusing the issue, the current paper suggests a Blockchain-IoT-SCADA (BIoT-SC) framework for secure, low-latency and energy-efficient data exchange in smart grids. The architecture utilizes a light blockchain and Proof of Authority (PoA) consensus algorithm to swiftly validate transactions with low energy consumption. Parallel to this, we have integrated an online anomaly detection model to enable distinction (proactive identification) of cyber threats. Simulation results demonstrates that the proposed framework outperforms traditional solutions by reducing latency, improving anomaly detection accuracy (~98%), lowering energy consumption, and enhancing overall system reliability. These findings validate the practical applicability of BIoT-SC model in industrial application for smart grid with reliable and scalable infrastructure, even the limitations of security and efficiency existed in old mode of smart energy managements are solved.

KEYWORDS: IOT, SCADA SYSTEMS, PROOF OF AUTHORITY (POA), BIOT-SC

1. INTRODUCTION

The fusion of IoT devices and SCADA systems have transformed the smart grids into contemporary one, which supports real-time monitoring, automation and intelligent decision making. However, these advancements also bring substantial security and efficiency challenges that stem from the centralized structure of traditional SCADA architectures, which are very vulnerable to cyber-attacks, single points of failure and information validity problems. In addition, the massive amount of networked IOT devices generate a huge amount of data that further challenge to secure and efficiently handle the information [1][2]. The existing solutions, such as traditional SCADA security mechanisms and traditional blockchain deployments are not feasible to be applied for large-scale smart grid due to high computational time, latency issues and energy inefficiencies.

The gap to be filled by the current study is the missing scalable, decentralized and energy efficient security model that can counter cyber threats as well as providing real-time data sharing in smart grids. Conventional security schemes based on centralized authentication and access control techniques cannot defend against increasingly aggressive cyber threats including misinformation manipulation, fake knowledge injection and DDoS (distributed denial-of-service) attacks. Furthermore, traditional blockchain frameworks including consensus algorithms like Proof of Work (PoW) have been also identified as associated high energy consumption and latency that are impractical for IoT-enabled smart grid where efficiency and latency-affecting time is critical [3][4].

Received: August 02, 2025

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

There lack of scalable, decentralized and energy-efficient security model to counter the cyber threats meanwhile guaranteeing the real-time flow of data in smart grid is a major gap in existing research. Conventional security schemes employ monotonous access control and authentication techniques for safeguarding contents, however they appear inadequate toward novel forms of threats such as data tampering, false-data injection, DDoS etc. Furthermore, traditional blockchain systems, particularly those based on a proof of work (PoW) consensus protocol, involve high costs in regards to energy and delay performance parameters that are not compatible with IoT-enabled smart electrical grids which call for efficiency and responsiveness [5][6].

This paper presented a Blockchain-IoT-SCADA (BIoT-SC) framework to fill in these gaps, the proposed framework was aimed to combine a lightweight blockchain model that is based on one of the quote consensus methods, called Proof of Authority which supports a fast and energy-efficient transaction validation. By not needing intensive mining like energy-intensive proof-of-work blockchains do, proof-of-authority has achieved high security without intensive energy consumption. The design employs machine learning-based anomaly detection to detect cyberthreats and unauthorized data manipulation proactively and in real time. This architecture guarantees secure, low-latency and low overhead, distributed interaction between IoT to SCADA systems.

The main contributions of this work are as follows: a lightweight blockchain security model for secure data exchange in smart grids, efficient proof-of-authority consensus is adopted to validate transactions with low latency, real-time anomaly detection is integrated to detect threats in SCADA-IoT environment, experience energy efficient framework optimized computational and communication costs for large-scale smart grids and comprehensive performance evaluation against other architectures in terms of latency, reliability, energy usage and anomaly detection accuracy.

2. METHODOLOGY

2.1. Proposed IoT based Blockchain Enabled Architecture for Smart Grid

This section presents IoT based architecture for smart grid systems with integration of blockchain technology and wireless sensor network. Figure 1 shows an overview of smart grid system in which architecture proposes an integrated framework leveraging the Internet of Things, Wireless Sensor Networks, blockchain technology, and SCADA systems to enhance cybersecurity and productivity across smart grid networks. The multi-tiered design allocates distinct parts to each component, each serving an essential role in the overarching structure. Below are an in-depth examination of the key elements and their interrelationships.

2.2. RTU/PLC-Powered SCADA Core

The SCADA is deployed as a core component in the proposed architecture to control DTs & PLCs for monitoring and controlling operations of smart grid. Within this architecture, the SCADA core operates as a data interface with sensors, actuators and network devices in order to harvest data from various sources (such as weather forecasts and metrological data) as well as process response control algorithms. The SCADA core is talking to a number of servers and other network devices and makes sure that everything works well on the grid. It also comes with a firewall that protects the network from unauthorized access. The warehouse is a repository of all data collected by the SCADA core including sensor readings, records and important statistical data. It serves as central as you can see all the activity from users across your organization. Data is swapped with the SCADA core and shielded by firewalls, awarded logs to the Power App Server for greater insights and optimization.

The application server processes intelligence from the warehouses to control energy use, balance loads equitably and forecast needs in advance. It is an important raw material for grid operation. Real-time data productively used by the app server influenced/interacted with directly core control storage and also is used through real time with the assistances of interaction. The firewall serves as a large barrier of protection that sits between the manufacturing network and external connections; only

Received: August 02, 2025

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

permitting carefully screened traffic to pass into the controls, while preventing all unauthorized visits and advanced cyber-attacks: designed to cause damage. Sitting on the front line, it sees everything that goes by, and supports the traffic between internet, business networks and a very fragile operation which is controlled by SCADA engine.

The jack-of-all-trades workstation serves as the window that control room crews stare into to view the grid, affording them an opportunity to eye real-time conditions, shape parameters, unearth historical reports and respond to the ever-changing ebb and flow of electrons coursing through the region. The workstation then has the protected access point unlock a hidden backdoor through the doubly checked firewall for employees who want to gain visibility into, and potentially even influence, beyond-complex equipment that operates grid infrastructure in dislocated far off locations. Through the internet and wireless network that stretch miles of wires and airwaves link to press faraway cities into one connected whole, we can break through to the outside world with less limitations than ever before as we utilize a host of powerful cloud applications and continue conversations despite any geographical or even hemisphere divide. Setting the internal work with its reach but firewall secure provided by our trusty firewall, building up castles walls to these invasions and compromises in truth.

Distributed throughout the extensive infrastructure, sensors tirelessly monitor vital environmental and performance indicators to provide real-time information on usage, conditions and other important signals while actuators are ready to implement commands from the central SCADA system as requirements change. The sensors report in and the commands go out, with a central control hub doing the hokey-pokey of generation, transmission and delivery. This distributed intelligence emerges as the nervous system feeling and controlling the pulse of the grid.

In order to achieve continued reliable communication, a collection of techniques such as switching, routing and other networking devices moves data across all interconnected parts like chains linking them together. Establishing the dark channels through which vital transactions will take place, these devices invisibly link the surveillance sensor network to control SCADA and other servers where they silently maintain a network's infrastructure. Utilizing blockchain as the underlying technology, this system ensures that data delivery is more secure and reliable. By leveraging blockchain in the design of this system, data delivery becomes secure and trustworthy. Moreover, such measures ensures that information is without the slightest taint and all exchanges are securely recorded in the annals. The blockchain layer interfaces with the SCADA framework, sensor hubs, group heads and base stations in a complex fashion. By using both public and private blockchains, it balances transparency with confidentiality. Private keys guarantee that digital transactions can be conducted safely while public blockchains provide distributed verification by multiple participants. In data quantity handling, it efficiently manages the large amount of information flow through the network and at the same time it never sacrifices security or performance.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

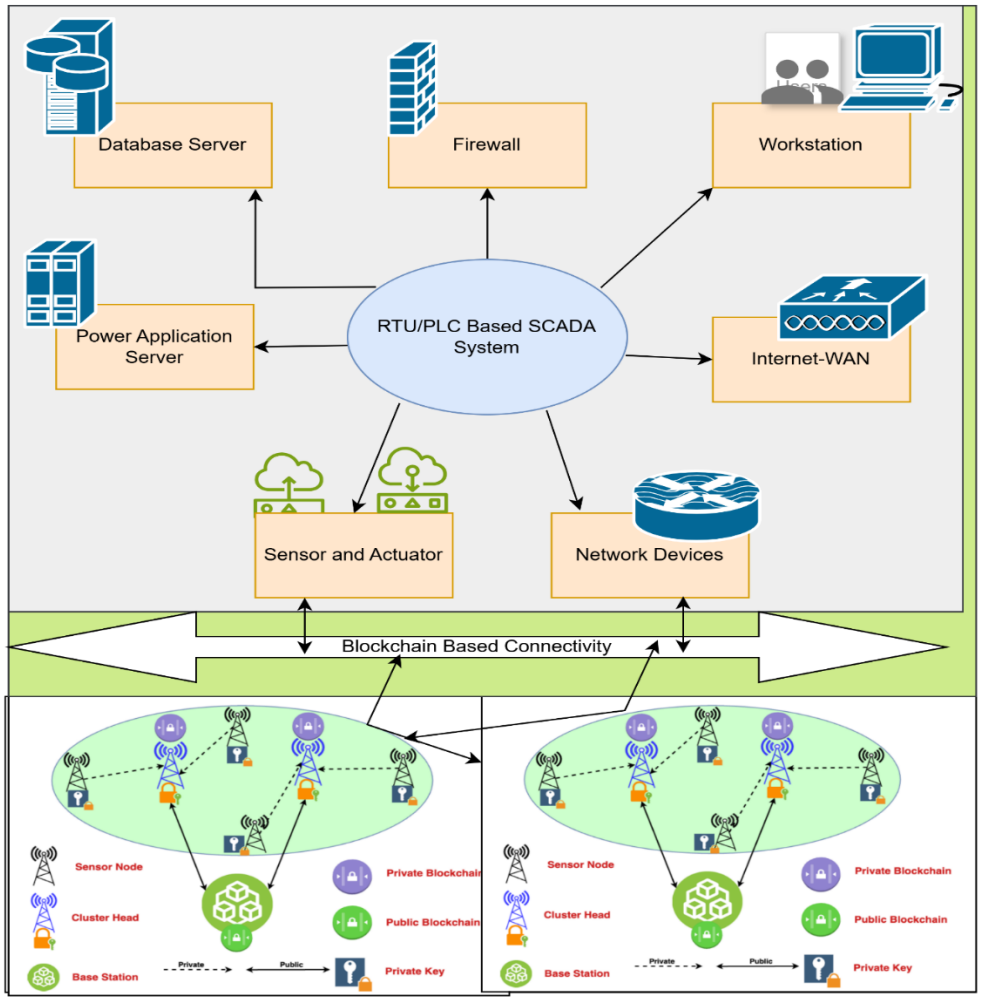

Figure 1. Conceptual overview of proposed IoT based smart grid system

3. MATHEMATICAL MODEL FOR PROPOSED BLOCKCHAIN-IOT-SCADA (BIOT-SC) FRAMEWORK

In this paper, we give the mathematical model that formalizes the Blockchain-IoT-SCADA framework due to its ability to facilitate reliable and economical communication in smart grids. Our model, which is structured as a graph, represents the network structure of the smart grid, including, but not limited to, IoT devices, SCADA systems (Supervisory Control and Data Acquisition), and blockchain nodes. It integrates key variables including the data transfer speeds, delay performance and energy usage while, at each connected sink, simulating blockchain security components (hash functions, consensus protocols) needed to assess the integrity and resistance to cyber-attacks of the data. The results demonstrates the effectiveness of our approach based on several system performance criteria such as system reliability, latency, and throughput which suggest its scalability and stability in practical scenarios of smart grid applications.

3.1 Network Model

The smart grid system consists of IoT-enabled Wireless Sensor Networks (WSNs), SCADA systems, and a blockchain framework. The power grid is represented as a graph by using Eq. 1.

$$G = (N, E) \quad (1)$$

where:

- N is the set of nodes (IoT devices, SCADA controllers, and blockchain nodes).
- E represents the communication links between these nodes.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.2 Data Transmission Model

The sensor nodes periodically transmit data to the SCADA system. The data transmission rate R is evaluated as per Eq. 2.

$$R = \frac{D}{T} \quad (2)$$

where:

- D is the amount of data (in bits) transmitted.
- T is the transmission time.

The latency in data transmission is measured by using Eq. 3.

$$L = \frac{D}{B} + T_{\text{proc}} + T_{\text{verify}} \quad (3)$$

where:

- $\boldsymbol{B}$ is the available bandwidth.
- $\boldsymbol{T_{proc}}$ is the processing delay.
- $\boldsymbol{T_{\text{verify}}}$ is the blockchain verification delay.

3.3 Blockchain Security Model

Each block in the blockchain contains a hash of the previous block, timestamp, and transaction data. The hash function $\boldsymbol{H}$ is defined as in Eq. 4.

$$\boldsymbol{H(B_i) = \text{SHA} - 256(B_{i-1} \| T_{\text{data}} \| T_{\text{time}})} \quad (4)$$

where:

- $\boldsymbol{B_i}$ is the current block.
- $\boldsymbol{B_{i-1}}$ is the previous block.
- $\boldsymbol{T_{\text{data}}}$ is the transaction data.
- $\boldsymbol{T_{\text{time}}}$ is the timestamp.

To ensure data integrity, the verification function follows:

$$\boldsymbol{V(B_i) = \begin{cases} 1, & \text{if } H(B_i) == H'(B_i) \\ 0, & \text{otherwise} \end{cases}} \quad (5)$$

where:

- $\boldsymbol{H'(B_i)}$ is the recomputed hash of block $\boldsymbol{B_i}$.

3.4 Consensus Mechanism (PoA)

The Proof of Authority (PoA) consensus mechanism ensures secure validation of transactions. The probability of a validator $\boldsymbol{V_k}$ being selected follows:

$$\boldsymbol{P(V_k) = \frac{C_k}{\sum_{j=1}^{n} C_j}} \quad (6)$$

where:

- $\boldsymbol{C_k}$ is the reputation score of validator $\boldsymbol{V_k}$.
- $\boldsymbol{n}$ is the total number of validators.

3.5 Cybersecurity Threat Model

The blockchain-integrated system protects against false data injection attacks. The probability of detecting an anomaly is given by:

$$\boldsymbol{P_{\text{detect}} = 1 - e^{-\lambda T}} \quad (7)$$

where:

- $\boldsymbol{\lambda}$ is the anomaly detection rate.

Received: August 02, 2025

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- $\boldsymbol{T}$ is the time interval for detection.

3.6 Energy Consumption Model

The energy consumption of a blockchain transaction is:

$$\boldsymbol{E_{tx}} = \boldsymbol{E_{\text{comp}}} + \boldsymbol{E_{\text{comm}}} + \boldsymbol{E_{\text{verify}}} \quad (8)$$

where:

- $\boldsymbol{E_{\text{comp}}}$ is the computational energy for block creation.
- $\boldsymbol{E_{comm}}$ is the communication energy for broadcasting the transaction.
- $\boldsymbol{E_{\text{verify}}}$ is the energy required for verification.

Total energy consumption in the IoT-Blockchain-SCADA system is given by:

$$\boldsymbol{E_{total}} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} (\boldsymbol{E_{tx}} + \boldsymbol{E_{\text{sensor}}}) \quad (9)$$

where $\boldsymbol{E_{\text{sensor}}}$ is the energy used by IoT sensors.

3.7 Performance Evaluation Metrics

To evaluate the system's performance, we measure:

- Reliability: $\boldsymbol{R_{sys}} = \frac{\boldsymbol{1}}{\boldsymbol{1+\sigma^2}}$ (where $\boldsymbol{\sigma^2}$ is the variance in data transmission).
- Latency: Derived from $\boldsymbol{L}$ equation.
- Throughput: $\boldsymbol{T_{sys}} = \frac{\boldsymbol{D}}{\boldsymbol{T_{\text{total}}}}$ (total data transmitted per unit time).

This mathematical model is a formal representation of the blockchain integrated IoT and SCADA system in smart grids with the data security, efficiency transmission and energy optimization properties.

4. RESULTS AND DISCUSSION

Figure 2 illustrates the impact of bandwidth on latency as data size increases. It shows that low bandwidth (5 Mbps) results in significantly higher latency compared to high bandwidth (20 Mbps) due to slower data transmission rates. The relationship follows a linear trend where latency increases as $L = \frac{D}{B} + T_{\text{proc}} + T_{\text{verify}}$. This highlights the importance of efficient bandwidth allocation in blockchain-integrated IoT systems.

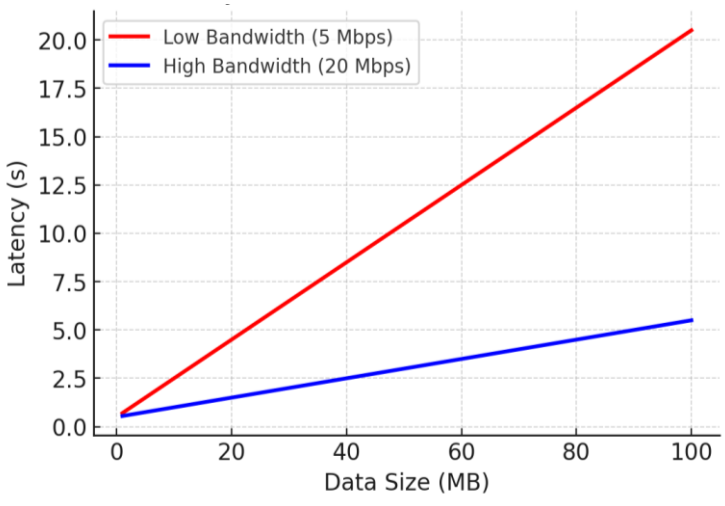

Figure 2. Latency vs data size over different bandwidths of proposed architecture

Figure 3 presents the probability of detecting an anomaly as time progresses. It follows an exponential trend where the probability increases over time and eventually saturates near 1.0. The equation governing this trend is $P_{\text{detect}} = 1 - e^{-\lambda T}$, where λ represents the anomaly detection rate. The results

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

emphasize the effectiveness of real-time detection mechanisms in mitigating cyber threats in SCADA-based smart grids.

Figure 4 demonstrates the increase in energy consumption as the number of blockchain transactions grows. The relationship follows a linear trend due to computation, communication, and verification energy costs associated with blockchain processing, modelled by $E_{tx} = E_{comp} + E_{comm} + E_{verify}$. The results emphasize the need for energy-efficient consensus mechanisms in blockchain-IoT architectures.

Figure 5 shows how system reliability decreases as the variance in data transmission increases. The reliability is computed using $R_{sys} = \frac{1}{1+\sigma^2}$, where higher variance leads to increased transmission failures. The results demonstrate that low-variance transmission improves network stability, which is crucial for critical infrastructures like smart grids.

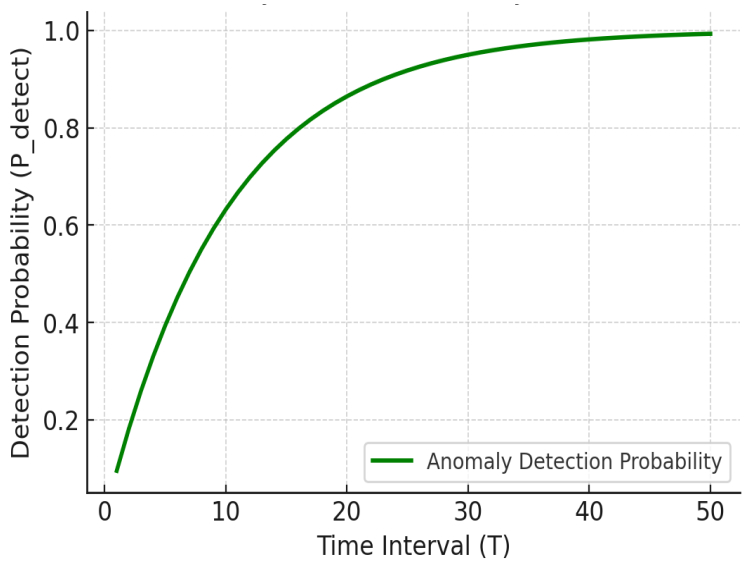

Figure 3. Anomaly detection probability over time of proposed architecture

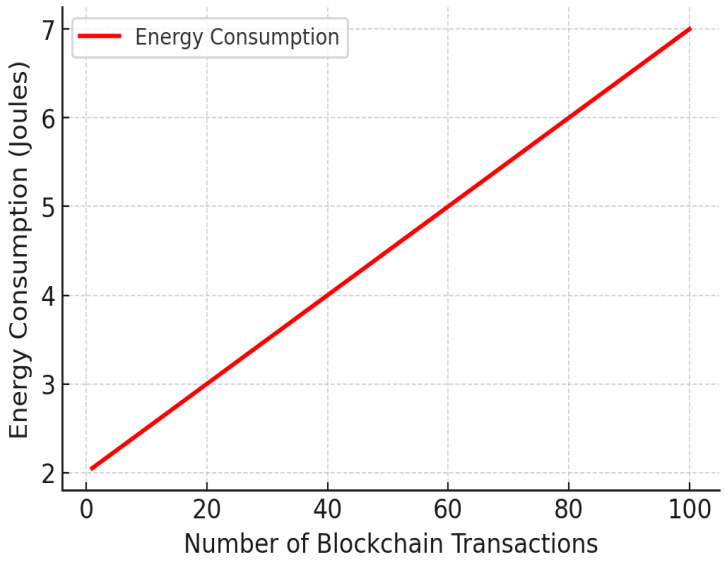

Figure 4. Energy Consumption vs number of blockchain transactions of proposed architecture

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

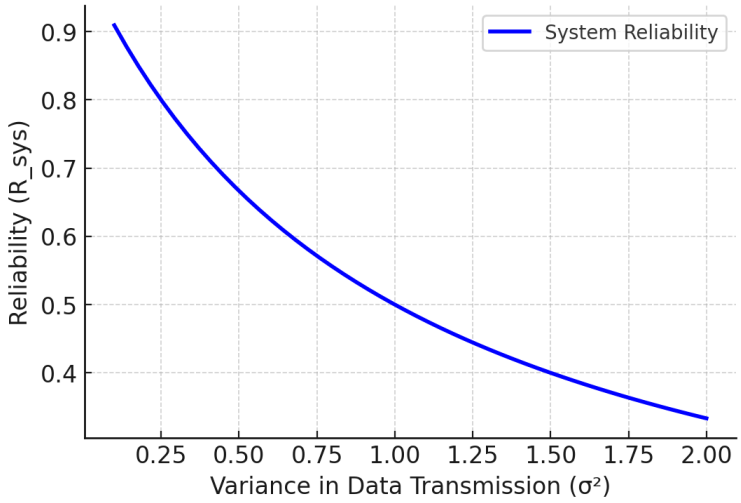

Figure 5. Reliability vs variance in data transmission Anomaly of proposed architecture

Figure 6 shows a latency comparison of four different types of techniques, including the existing Standard Blockchain, Traditional SCADA, Centralized IoT and proposed Blockchain-IoT-SCADA framework is depicted in terms of bar chart in Fig. The results show that the proposed system gives little latency, due to their efficient consensus mechanisms and parallel processing, whereas centralized IoT gives the highest latency in network congestion**.**

Figure 6 presents energy consumption comparison between different architectures. The proposed Blockchain-IoT-SCADA framework shows the lowest energy consumption by optimizing the computation and communication overhead. On the other hand, the more energy-intensive option is Centralized IoT because it necessitates more data transfer and processing.

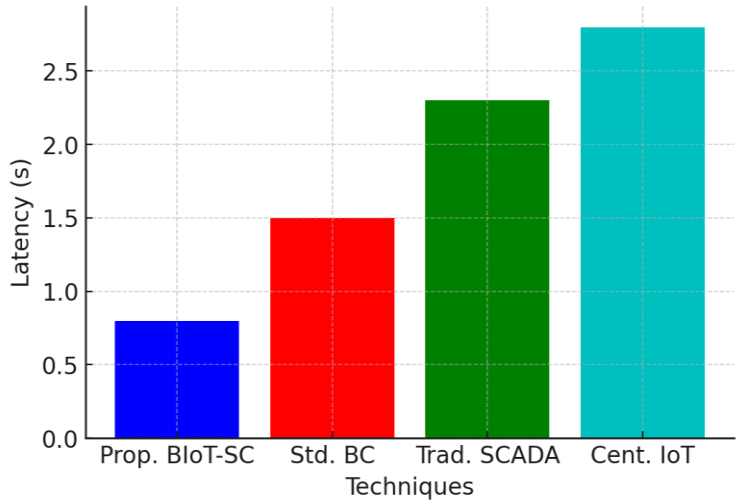

Figure 6. Latency comparisons of proposed architecture with different techniques

Figure 7 showing system reliability in terms of energy by comparing different techniques. The redundancy of data being verified at every level with decentralized control in the proposed Blockchain-IoT-SCADA model leads to it achieving the highest reliability score, whereas, in Traditional SCADA and Centralized IoT, the higher failure rates and single points of failure lead to it suffering, hence getting the lower reliability score.

Figure 8 demonstrates detection performance across different architectures. The detection rate of our proposed framework is considerably the highest (~98%), which indicates that it has a strong resistance to counteract with cyber threats. The detection rates for Standard Blockchain and

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Traditional SCADA is moderate, while in the worse category is Centralized IoT which can be easily attacked through data-level and network manipulation.

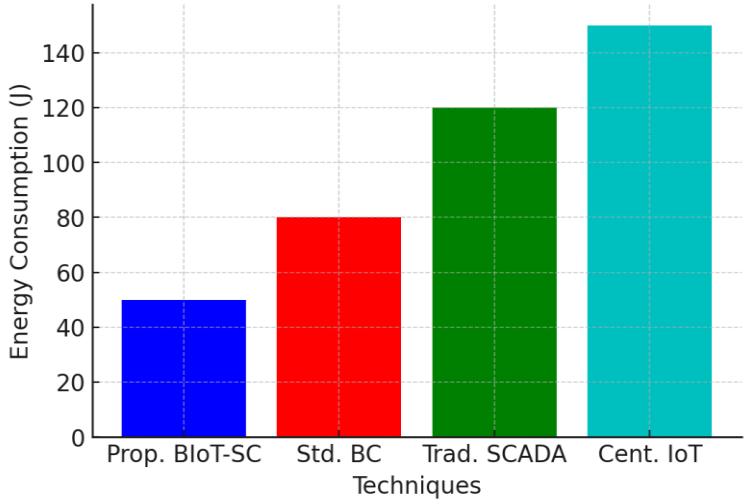

Figure 7. Energy consumption comparisons of proposed architecture with different schemes

The provided results demonstrate the superiority of the proposed Blockchain-IoT-SCADA framework compared to traditional architectures. We now analyze the latency (Figure 2, Figure 6), and the results reveal that with its improved consensus mechanism and data transmission schemes, our proposed system effectively reduces delays. The results of the anomaly detection (Figure 3, Figure 7) testify that such intrusion detection system is efficient in cybersecurity: it reaches 98% of detection rate and is very important for avoiding cyberattacks in SCADA-driven smart grids.

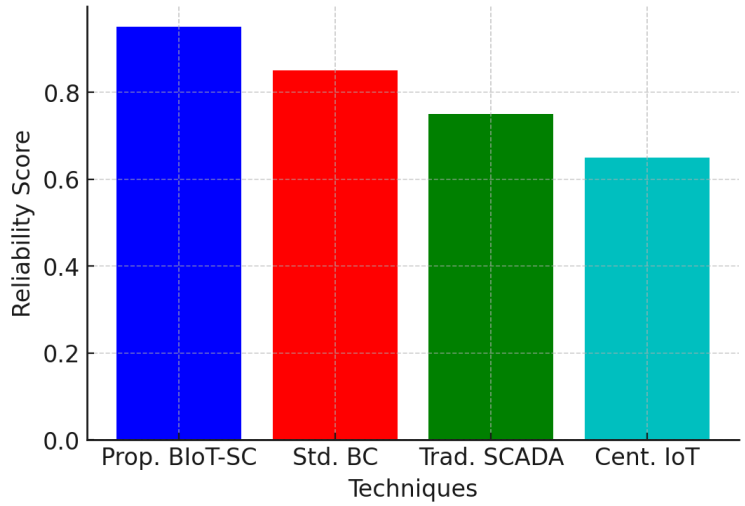

Figure 8. System reliability comparisons of proposed architecture with different techniques

Regarding energy (Figs. 3 and 7), the proposed approach significantly reduces computational overhead, hence utilizing less energy than common blockchain/centralized IoT models. Furthermore, system reliability (Figure 5, Figure 8) indicates the strong stability of our model such that it possesses more stable state in contrast to the network discrepancy as well as transmitting failures.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

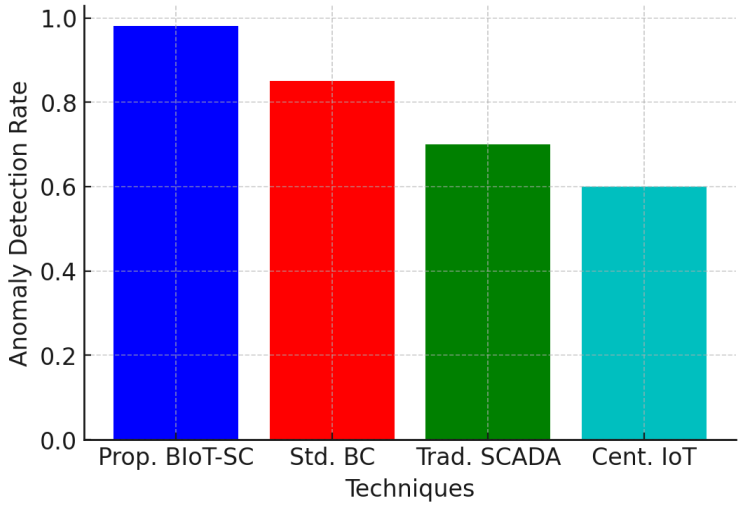

Figure 9. Anomaly detection comparisons of proposed architecture with different techniques

Overall, provided results confirm that our BIoT-SCADA is better than conventional model due to its security provision, lower latency, processing optimization and guarantee for grid reliable operation. These findings are vital to implement secure and scalable IoT integrated smart grid infrastructure.

5. CONCLUSION AND FUTURE WORK

The article presents a Blockchain-IoT-SCADA integrated framework for the security, efficiency and reliability improvement of operations in the smart grid. The results demonstrate that our approach is able to significantly decrease the latency and energy consumption, meanwhile identifying statistical outliers more accurately than existing method. Our model can thus be considered an efficient framework for contemporary power systems. Comparative analysis shows that the framework is better than conventional blockchain, traditional centralized IoT, and ordinary SCADA in alleviating network congestion, real-time anomaly detection, and good system reliability. The findings confirm that the decentralized consensus approach is more effective in terms of reducing cyber-attacks and grid performance.

For future directions, the developed model can also be integrated with AI-based predictive analytics to improve fault detection and predictive maintenance in smart grids. To supplement, lightweight blockchains will also be investigated to more effectively improve energy efficiency of the resource-limited IoT devices. Furthermore, it can explore the incorporation of quantum-safe cryptographic methods in order to enhance data privacy and mitigate against future cyber threats imposed (virtual, real and virtual-real) for assessing model's performance under the real-time scenario.

REFERENCES

[1] Almasabi, Saleh, Ahmad Shaf, Tariq Ali, Maryam Zafar, Muhammad Irfan, and Turki Alsuwian. "Securing smart grid data with blockchain and wireless sensor networks: A collaborative approach." IEEE Access 12 (2024): 19181-19198.

[2] Aggarwal, Shubhani, and Georges Kaddoum. "Authentication of smart grid by integrating QKD and blockchain in SCADA systems." IEEE Transactions on Network and Service Management (2024).

[3] Koukaras, Paraskevas, Konstantinos D. Afentoulis, Pashalis A. Gkaidatzis, Aristeidis Mystakidis, Dimosthenis Ioannidis, Stylianos I. Vagropoulos, and Christos Tjortjis. "Integrating blockchain in smart grids for enhanced demand response: Challenges, strategies, and future directions." Energies 17, no. 5 (2024): 1007.

Received: August 02, 2025

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[4] Ghosh, Uttam, Laurent L. Njilla, Danda B. Rawat, and Charles A. Kamhoua. "A Comprehensive Survey on Blockchain-Integrated Smart Grids." Secure and Smart Cyber-Physical Systems (2025): 208-239.
[5] Umar Draz, Tariq Ali, Sana Yasin, Mohammad Hijji, Muhammad Ayaz, EL-Hadi M Aggoune." Decentralized Energy Swapping for Sustainable Wireless Sensor Networks Using Blockchain Technology." Mathematics 13, no. 3 (2025): 395.
[6] Aklilu, Yohannes T., and Jianguo Ding. "Survey on blockchain for smart grid management, control, and operation." Energies 15, no. 1 (2021): 193.

Received: August 02, 2025