Journal of Advances and Scholarly Research In Allied Education
Vol.22, Issue No. 5 October-2025, ISSN 2230-7540

Design and Performance Evaluation of a Secure and Energy-Efficient Cloud-Based Architecture for Wireless Sensor Networks

Rashmi Singh Baghel[1]*, Dr. Kishan Kumar[2]

1 Research Scholar, Shri Krishna University, Chhatarpur, M.P., India

baghelrashmi805@gmail.com

2 Professor, Shri Krishna University, Chhatarpur, M.P., India

Abstract: The current IoT and its uses rely heavily on Wireless Sensor Networks (WSNs) and knowledge on how to get data from them in real time. Many fields can greatly benefit from WSNs, including healthcare, smart cities, environmental monitoring, industrial automation, and many more. Energy, security, scalability, and data management are only a few of the major limiting variables that affect WSNs, which are extensively used structures. Unfortunately, WSNs have a lot of problems when it comes to data management, security, scalability, and energy storage. There are potential ways to keep their efficiency and energy consumption low, and WSNs and cloud computing integrations can assist with this. In this article, we will go over the latest advancements in Wireless Sensor Networks (WSNs) and how they are being used to WSNs in cloud environments and frameworks. The goal is to increase and sustain efficiency while minimizing costs associated with communication, energy, and security. We will go over the latest innovations in Wireless Sensor Networks (WSNs), including WSNs in clouds and frameworks, as well as WSNs themselves, in order to keep efficiency high, reduce energy and communication costs, and increase security. To alleviate storage and processing constraints, the components of the WSN are required to pay for cloud tools that each component can use. Consequently, the proposed adapters are more difficult and expensive to implement on the Adapter. Traditional WSN methods are evaluated and contrasted with metrics such energy consumption, end-to-end latency, throughput, packet delivery ratio, detection accuracy, and network longevity. Energy efficiency, dependability, security, and scalability are all well exhibited in the results. In addition to being suitable for next-generation IoT and data-intensive applications, the suggested architecture can handle the demands of massive cloud-based WSN installations.

Keywords: Wireless Sensor Networks, Cloud Computing, Energy Efficiency, Trust-Based Security, Hybrid MAC Protocol, Internet of Things (IoT)

1. INTRODUCTION

The backbone of contemporary information systems, Wireless Sensor Networks (WSNs), have grown in popularity over the past few decades. They've made it possible for data to be continuously captured, processed, and communicated in a distributed system. A WSN is made up of a large number of tiny wireless sensor nodes that work together to monitor and report on environmental conditions including motion, humidity, pressure, and temperature in real time (Rani, S., 2024). Countless fields have made good use of them, including healthcare, smart

agriculture, industrial automation, environmental monitoring, military surveillance, smart cities, and more. Weak resources (such as energy, processing, and storage capacity) are the primary cause of WSNs' many shortcomings and difficulties, notwithstanding the benefits already mentioned (Sharma, S. K., 2021). Performance, reliability, and scalability are three areas where concentration WSNs are likely to fall short. More effort should be devoted to improving the performance of WSNs as they will be the foundation of the Internet of Things' future development (Nayak, B., 2022).

1.1 Wireless Sensor Networks: Challenges and Limitations

It is possible to substantially enhance the efficiency and overall performance of WSNs, despite the fact that they offer flexible and inexpensive solutions to meet sensing demands. The finite energy supply is an important factor. It is not possible to change, repair, or replace the batteries that power sensor nodes once they have been installed (Qaisar, M. U. F., 2025). Network lifespan is shortened due to rapid energy depletion caused by retransmissions, idle listening, and flawed communication protocols. On top of that, conventional routing protocols like MAC aren't flexible enough to handle unexpected changes (Rani, S., 2024). This causes energy consumption to be unequal between nodes, which in turn increases delay and packet loss. Low processing capability of the nodes compounds the security issue that WSNs already have as a result of their open communication. Sybil assaults, node impersonation, and packet dropping are all ways that data loss and interruption to networks can occur. In addition, the issue gets progressively worse when the number of nodes is increased (Ahmed, A. T. A., 2025). Data volume, congestion, and processing bottlenecks all take a turn for the worst when network performance suffers. Because conventional WSN architectures aren't adequate to the task of supporting secure, large-scale applications, these issues highlight the need for better and novel architectural models (Beri, R., 2025).

1.2 Role of Cloud Computing in Enhancing WSN Architecture

One possible solution to the limitations of conventional Wireless Sensor Networks (WSNs) is to combine cloud computing with WSNs. In WSNs, data is collected and sent to cloud servers by means of power-constrained sensor nodes. This integration allows sensor nodes with limited resources to outsource data gathering, analysis, and security job management to servers in the cloud (Younus Mohammed, M., 2025). By implementing this approach, the energy consumption at the node level will be significantly reduced, leading to improved efficiency in managing sensor data on a broad scale. By utilizing cloud service providers, sensor data

streams may be processed and tracked in real-time, resulting in intelligent services for consumers. By utilizing cloud servers, the limitations of storage and processing are effectively removed (Saranya S., 2024). In general, the system's scalability, dependability, and fault tolerance are greatly enhanced by combining dispersed administration with cloud services. When compared to alternative sensor node designs, cloud-based ones have the opportunity to incorporate more sophisticated security measures like attack detection and trust management. Secure, efficient, and scalable systems can be more easily created when WSNs and cloud computing work together (Mishra, R., 2025). An energy-efficient communication protocol and a trust-based security mechanism are both incorporated into this WSN design.

2. LITERATURE REVIEWS

Ali, S. A., (2024) Hybrid architecture systems have been extensively covered in the literature for their ability to optimize energy consumption and enhance security since the inception of merging cloud and mobile cloud computing with Wireless Sensor Networks (WSNs). One study proposed building an energy-efficient and safe system out of WSNs and mobile cloud computing to address both the need for low-power, battery-operated sensor nodes and concerns about data privacy and security in the cloud. In order to reduce energy usage without sacrificing data secrecy, this author proposed a method that uses authentication, encryption, and duty-cycling. In addition, the author proved that asynchronous scheduling and privacy-preserving data aggregation may reduce operating energy consumption while enhancing cost efficiency when the number of sensors was increased.

Kori, G. S., (2025) Several research efforts have focused on improving cloud-assisted WSN performance measures including throughput, successful packet delivery, latency, and energy consumption via the development of routing algorithms. The Secured Energy Efficient Framework (SEEF) was developed in one of these studies. It combines many components, including a cloud-based routing strategy, a cluster-based topology, a multi-layered MAC scheme, and a trust Sybil attack detector. The optimized routing method enhanced intra-cluster and inter-cluster communication, while heuristic MAC scheduling enhanced slot allocations and decreased collision rates. The findings of the simulation demonstrated that the end-to-end latency and throughput were enhanced, and they also demonstrated that important communication metrics may be optimized using a cloud-based architecture. In particular for large-scale, resource-constrained settings, this research highlights how cloud computing enables WSNs to execute efficient and dynamic routing.

Uchoba, K., (2024) the standpoint of cloud services, current research show that trust is an essential part of WSN architecture as it reduces the attack surface's flexibility. Concerns about data security arise, for example, when nodes are connected to the cloud; furthermore, nodes are vulnerable to assaults because to their modifiability. For example, the suggested architecture was able to obtain a high assault detection rate while using appropriate memory consumption, thanks to the device's energy consumption and fuzzy logic algorithms. When compared to the other algorithms discussed above, the fuzzy logic algorithm uses the most memory. Notably, as compared to the aforementioned algorithms and energy consumption algorithms, the suggested framework obtained superior memory consumption. It is possible to declare that substantial gains on connection and throughput compared to current solutions were achieved by using up to 500 nodes in the simulations.

Kolhar, A., (2025) The increasing number of cloud-based WSNs and IoT devices has sparked a lot of interest in studying how to best combine cyber-attack detection systems with intelligent algorithms. In order to identify various dynamically behaving attacker entities in the IoT-WSN environment, one research built several optimal neural network models. Finding assaulting nodes that exhibit certain alterations within/with Sybil, sinkhole, and selective forwarding assaults is challenging for conventional intrusion detection algorithms, according to the study. The system achieved accurate attack type classification by integrating threat intelligence with classifiers PSO-NN, EO-NN, and SCO-LSTM.

Chander, B., (2024) energy optimization for WSN is crucial because it sets the stage for the cloud-assisted architectural research. The authors of the energy-aware WSNs review talk about how the incredible variety of sensor networks, as well as the design of sensor nodes, operating systems, protocols for networks, and duty cycling, affect the network lifespan. Sleep scheduling, clustering, and topology management are just a few of the methods covered by the writers, who cover a wide spectrum of ways to WSN power saving, beginning with hardware and progressing through networking. Although WSNs and Cloud Platforms are connected, the authors' study highlights the need of optimizing the energy consumption of WSN nodes. This is because cloud support relocates data processing, but it does not remove the energy limits of the nodes themselves. The author tackles the main issues with sensor energy and resource management in the design, which is why this study is used as a basis for cloud-based WSN designs.

3. METHODOLOGY

3.1 Architectural Framework for Cloud-Based WSNs

Nodes for sensors, gateways, and cloud computing make up the suggested architectural framework's integrated architecture. Nodes that act as sensors collect and transmit raw data, whereas nodes that act as gateways compile and transmit aggregated data to the cloud. In addition to managing network operations, the cloud offers vast storage capacity and conducts sophisticated data analytics. This job delegation lessens the processing burden on sensor nodes, which in turn saves energy consumption and increases the nodes' lifespan in the network. Because of the architecture's modular design, components related to routing, security, and communication may be updated separately. The architecture ensures data agility and dependability across diverse data densities and network node counts by making use of cloud computing.

3.2 Design of Energy-Efficient MAC Protocol

An energy-efficient hybrid media access control (MAC) protocol is very helpful for controlling scheduling and channel access among the sensor nodes. Idle listening, packet collisions, and excessive retransmission are some of the issues that lead to substantial energy loss in wireless sensor networks. Preventing or reducing the severity of these issues is a primary goal of the procedure. A scheduling technique that relies on heuristics adjusts the nodes' active and sleep states to optimize the network and traffic. This type of adaptive scheduling improves packet delivery ratio, slows down the whole process, and increases throughput. On top of that, the designed MAC enables perfect control streams and data delivery synchronization, which means the procedure may be executed without an abnormally lengthy delay. Improving the network's performance and improving several elements of the network, including energy consumption, are the MAC's responsibilities.

3.3 Trust-Based Security Mechanism for Sybil Attack Detection

A trust-based security mechanism has been included into the system's design to address the weaknesses associated with trust-based security, specifically the Sybil attacks. The system was safeguarded from these vulnerabilities by doing this. Various behavioral metrics are used to assess each sensor node in the system. In order to gather information, several measures are used. Measures that come within this area include inconsistencies in packet forwarding, patterns of signal strength, residual energy, communication dependability, and Sybil detection.

Trust levels might change over time according to the actions of every single node in the network. Something like this might happen very simply. As a result, nodes that act in an unconventional or disobedient manner are penalized with lower scores and, in the long run, kicked out of the network. The application of bottom-up trust methods helps to reduce energy consumption and maintain a dependable and secure data transmission channel, eliminate compute cycle loss, and defend the network integrity. All of these objectives may be met concurrently through the development of bottom-up trust mechanisms.

3.4 Energy-Efficient Routing Protocol Integration

In order to ensure the reliable and eco-friendly transfer of data from sensor nodes to the cloud, a new routing protocol has been devised that is more energy-efficient. Residual energy, connection quality, and hop count are all factors that are considered while routing is being calculated. Doing so ensures that the network as a whole makes fair use of energy. This eliminates the potential for network fragmentation and the problem of nodes dying out too soon. A combination of the Media Access Control (MAC) and security layers, as well as the routing protocol, allows for efficient and secure communication. By prioritizing the most dependable and energy-efficient paths, the routing protocol helps to prolong the network's lifespan in situations when the network conditions are continually changing. Note that this is true regardless of the throughput or latency of the route.

3.5 Simulation Setup and Performance Evaluation

The cloud-based simulation environment and network simulation tools such as NS2 or NS3 will be used for the first evaluation of the proposed framework. We will examine several network situations in the simulations, including different node density, traffic loads, and attack intensities. Some of the performance parameters that will be examined in the assessment are energy consumption, end-to-end latency, throughput, packet delivery ratio, detection accuracy, and overall network lifespan. Improvements from conventional methods will be measured using performance measures. Results will be comprehensive in their assessment of the suggested architecture's efficacy in terms of data-handling capacity, efficiency, scalability, and security. For WSN applications hosted in the cloud, the suggested architecture will be tested.

4. RESULTS

4.1 Energy Consumption Analysis

Since sensor nodes rely on batteries for power and are often placed in locations where exchanging batteries isn't feasible, limiting energy usage is a major concern for Wireless Sensor Networks. If energy is handled well, the network's longevity, stability, and data dependability can only improve. Conversely, when energy is efficiently controlled. This section will mainly focus on the proposed hybrid protocols for media access control (MAC) and energy-aware routing. The routing methods and energy consumption will be examined in relation to the various node densities in order to achieve this. This research aims to show that balanced and planned routing algorithms outperform conventional WSN protocols in terms of efficiency and energy usage.

Table 4.1: Average Energy Consumption per Node (Joules)

Number of Nodes	Conventional Protocol	Proposed Architecture
50	1.92	1.35
100	2.48	1.72
150	3.15	2.01
200	3.89	2.37

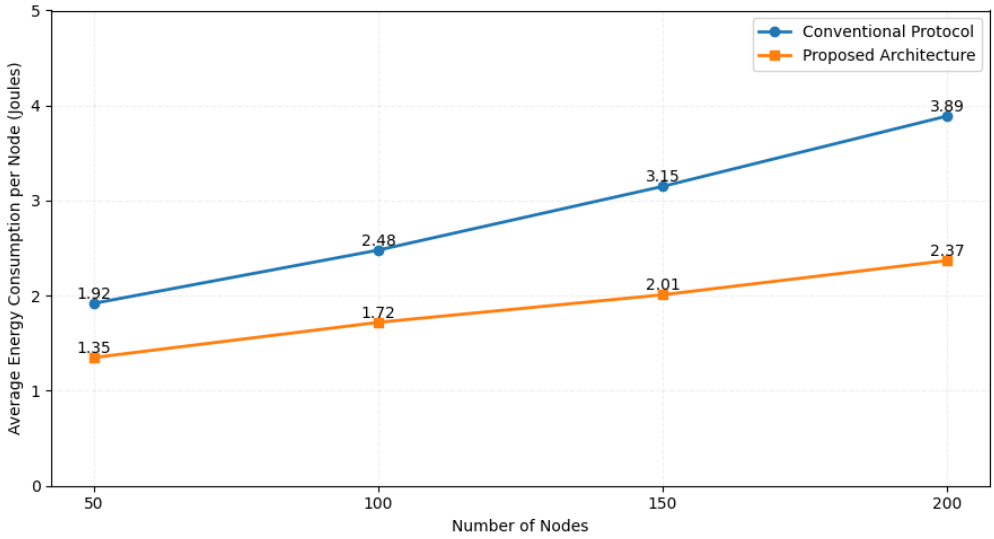

Figure 4.1: Energy Consumption per Node: Conventional vs Proposed Architecture

Energy usage rises with node density for both methods as seen in Table 4.1, which is a result of the increased communication overhead. However, compared to the standard technique, the suggested design significantly reduces energy use. Reasons for this include adaptive MAC scheduling, which cuts down on collisions and idle listening, and routing decisions based on remaining energy. In sum, the findings demonstrate that the integrated design efficiently reduces energy consumption at the node level, allowing the network to remain operational for longer.

4.2 End-to-End Delay and Throughput Performance

Not only are latency and throughput two of the most essential measures for measuring performance in wireless sensor networks (WSNs), but they are also two of the most critical metrics. The importance of a quick and precise data transfer cannot be overstated, particularly for those systems that rely on it. When there is a reduction in the amount of delay, the reaction time is decreased, and when there is an increase in the throughput, the network is able to use its resources that are available to it in a more efficient manner. In this sub-section, we analyze how the proposed architecture functions as the volume of traffic rises. We take into account the significance of effective channel access, minimum retransmission, and cloud-based data consolidation in our investigation.

Table 4.2: Delay and Throughput Comparison

Traffic Load (kbps)	Avg. Delay (ms) – Conventional	Avg. Delay (ms) – Proposed	Throughput (kbps) – Proposed
50	210	145	46
100	340	215	92
150	495	290	138
200	680	375	182

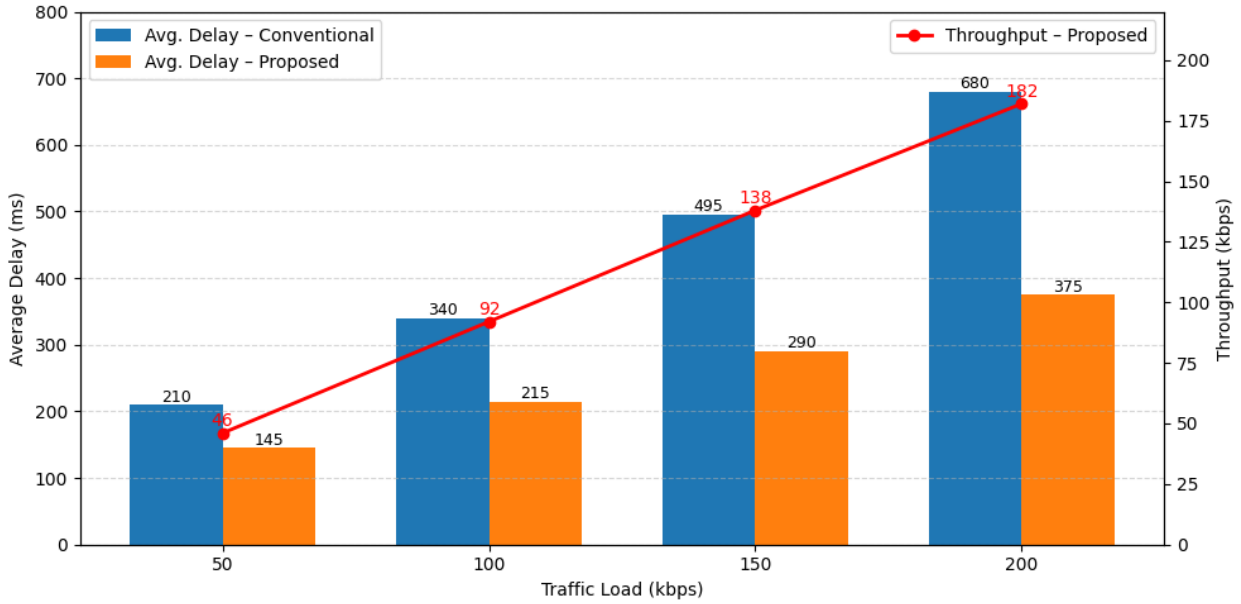

Figure 4.2: Delay and Throughput Comparison

As seen in Table 4.2, the average end-to-end delay rises due to congestion and queuing as the traffic load increases. However, when contrasted with the traditional approaches, the suggested design guarantees a significantly reduced latency. An further indicator of efficient channel usage is the fact that throughput grows in direct proportion to traffic load. With the use of cloud-based aggregation and the hybrid MAC protocol, congestion at the gateways is reduced, allowing for faster and more reliable data transfer by minimizing collisions.

4.3 Packet Delivery Ratio and Network Reliability

A statistic that is used to represent the frequency with which successful packet transfers take place is referred to as the Packet Delivery Ratio, or PDR for short. One of the metrics that is used to express this frequency is in this case. For systems that demand a high level of data dependability, the existence of PDR is absolutely important. This is especially true in networks that are crammed to the gills with information. In order to demonstrate the dependability of the system, this section will measure the PDR for the proposed design as the number of sensor nodes rises. This will be taken into consideration. In order to go to the following stage, this will be completed first.

Table 4.3: Packet Delivery Ratio (%)

Number of Nodes	Conventional Protocol	Proposed Architecture
50	91.4	97.8
100	88.6	96.2
150	84.9	94.5
200	80.7	92.1

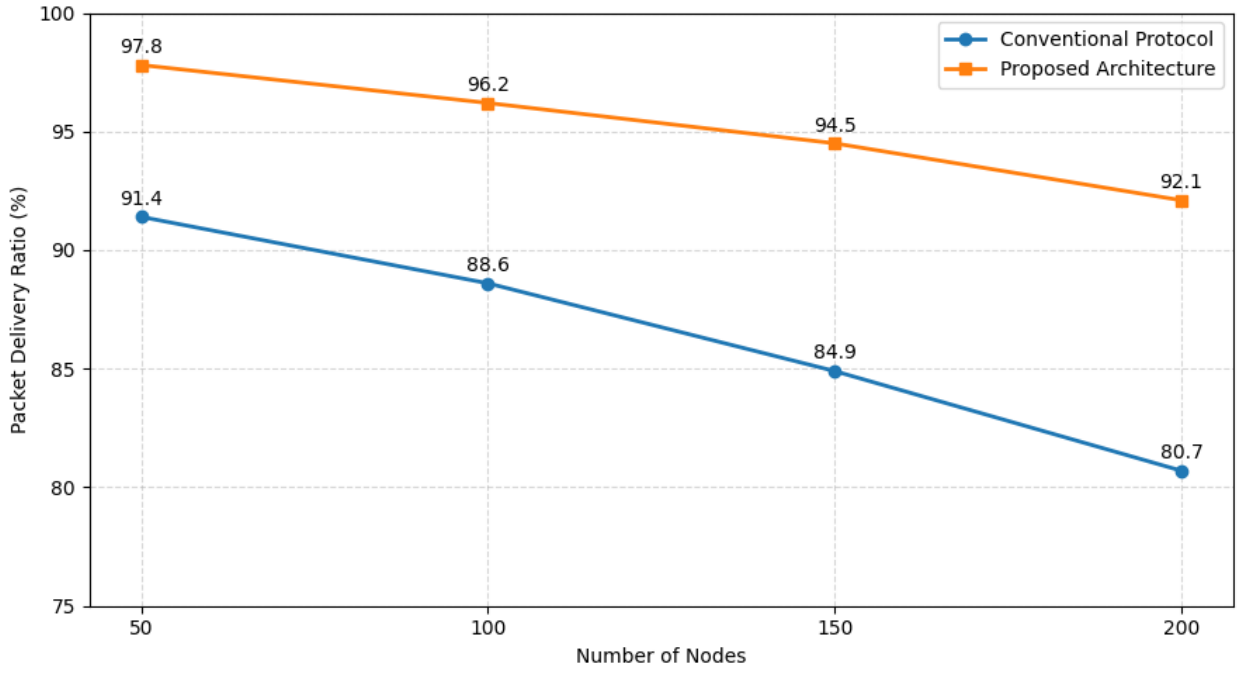

Figure 4.3: Packet Delivery Ratio (PDR) vs Number of Nodes

Table 4.3 shows that PDR drops with increasing numbers of nodes, which is because more nodes means more potential accidents and more obstacles along the pathways. Still, the new system outperforms the previous protocol in terms of PDR. The new system is more energy efficient, has better node isolation capabilities, and has coordinated MAC scheduling, which are the main reasons for this. The results show that the new system outperforms the previous one in terms of durability and dependability, even when subjected to high density situations.

4.4 Sybil Attack Detection Accuracy

In wireless sensor networks (WSN), which are susceptible to being manipulated by malicious nodes, it is feasible for rogue nodes to exert an effect on the activities that take place throughout

the network. The techniques for data aggregation and routing can be altered by these nodes, which have the ability to do so. By executing this action, the conditions that are favorable to the occurrence of Sybil attacks and other security vulnerabilities are generated. These settings are conducive conditions. For the purpose of bringing about certain conditions, this activity is carried out. Therefore, the trust-based security mechanism that has been supplied has to be fine-tuned, and the detection accuracy and false positive rates need to be explored while taking into consideration the varied levels of severity that the assaults have. That each and every one of these precautions is taken into consideration is essential.

Table 4.4: Sybil Attack Detection Accuracy (%)

Malicious Nodes (%)	Detection Accuracy	False Positive Rate
5	96.4	2.1
10	95.1	2.6
15	93.7	3.2
20	92.3	3.9

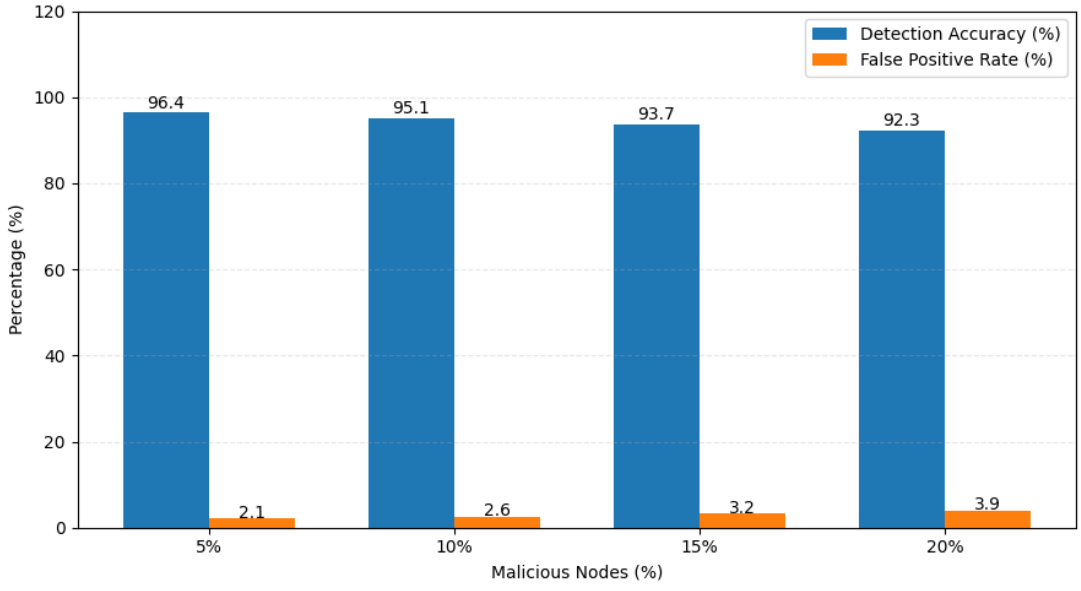

Figure 4.4: Sybil Attack Detection Accuracy vs False Positive Rate

Table 4.4 demonstrates that even when the number of rogue nodes increases, the detection accuracy remains high. The false positive rate is still within acceptable bounds, despite a little increase. The Sybil nodes may be accurately identified and separated with the use of the trust-based system, which continuously evaluates the nodes' behavior using various metrics over time. The suggested security architecture is proving to be both flexible and resilient in the face of the hostile network environment, according to the positive network nodes.

4.5 Network Lifetime and Scalability Assessment

When it comes to determining whether or not wireless sensor network deployments are practical, the importance of both the lifespan and scalability of networks cannot be overstated. This is especially true when large-scale and long-term applications are taken into consideration. The purpose of this section is to evaluate the effectiveness of the proposed design in extending the operational lifespan of networks by testing various node densities and keeping track of the amount of time until the first node dies (FND) and the amount of time until half of the nodes die (HND). This is done in order to determine whether or not the proposed design is effective in extending the lifespan of networks.

Table 4.5: Network Lifetime Comparison (Rounds)

Number of Nodes	FND – Conventional	FND – Proposed	HND – Proposed
50	820	1210	1840
100	690	1085	1675
150	540	945	1490
200	410	820	1325

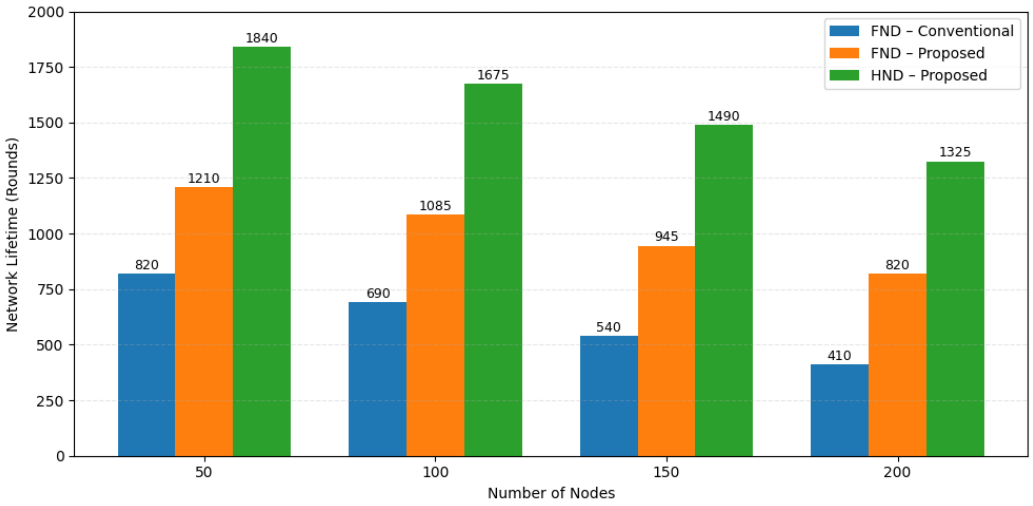

Figure 4.5: Network Lifetime Comparison

Table 4.5 displays the proposed design, which, when compared to the conventional protocol, increases the network lifespan. Problems with nodes failing, energy usage that is out of whack, reduced communication overhead, and processing delays. The system's scalability is demonstrated by its consistent performance even as the number of nodes increases. Applications in Wireless Sensor Networks, both short- and long-term, at enormous scales, justify the design.

5. CONCLUSION

In order to address the issues of basic WSNs' communication, scalability, and security in an energy-efficient manner, a creative architecture combined cloud computing with WSNs. The WSN cloud architecture is built by integrating a hybrid MAC (Media Access Control) protocol with an energy-aware routing algorithm, a trust-based security method for detecting Sybil attacks, and a MAC protocol that is both efficient and hybrid. Multiple forms of attacks, traffic volumes, and network density were tested in a synthetic environment. The suggested WSN cloud architecture outperforms conventional WSN protocols in several respects, including end-to-end latency, packet delivery and throughput, network longevity (owing to reduced energy consumption in a crowded network), and detection accuracy. When integrated with cloud WSN architecture, distributed computing enhances the framework's scalability and dependability. Built for efficient data storage, aggregation, and computation, it reduces strain on node resources, processes more sensor data, and makes use of higher-order analytics with centralized data and network management. By providing less, the trust-based system secures

the system through isolative, efficient detection of rogue nodes, addressing security and redundant computation.

References

1. Rani, S., & Taneja, A. (Eds.). (2024). *WSN and IoT: An Integrated Approach for Smart Applications*. CRC Press.

2. Sharma, S. K., Bhushan, B., Kumar, R., Khamparia, A., & Debnath, N. C. (Eds.). (2021). *Integration of WSNs into Internet of Things: A Security Perspective*. CRC Press.

3. Nayak, B., Pani, S. K., Choudhury, T., Satpathy, S., & Mohanty, S. N. (Eds.). (2022). *Wireless Sensor Networks and the Internet of Things: Future Directions and Applications*. Apple Academic Press.

4. Qaisar, M. U. F., Yuan, W., Bellavista, P., & Tabassum, H. (2025). *Empowering IoT: Reliability, Network Management, Sensing, and Probabilistic Charging in Wireless Sensor Networks*. Springer Nature Singapore.

5. Rani, S., Taneja, A., Kulkarni, S. H., Gawande, N., & Chatpalliwar, A. S. (2024). *WSN and IoT: An Integrated Approach for Smart Applications* (Chapter authors). CRC Press.

6. Ahmed, A. T. A., Sid Ahmed, N. M. O., Filali, A., & Alhomed, L. S. (2025). *Wireless Sensor Networks, IoT, and Cloud Computing* (Special Authors). MDPI Books.

7. Beri, R., & Sachdeva, P. (2025). *Smart Trends in Computing and Communications* (includes WSN cloud integration topic). Springer.

8. Younus Mohammed, M. (2025). *Enhancing Energy Efficiency in IoT Wireless Sensor Networks: AI-Driven Clustering and Routing Protocols*. Journal of Al-Qadisiyah for Computer Science and Mathematics.

9. Saranya S., Aravind, V., Marimuthu, N., & Mohanraj, D. (2024). *Energy-Efficient Routing in Wireless Sensor Networks Using Blockchain-Driven Deep Learning Architectures*. International Journal of Scientific Research in Science and Technology.

10. Mishra, R., Jha, S. K., Kshetri, N., Bhusal, B., Rahman, M. M., Rana, M. M., … Pokharel, B. P. (2025). *nodeWSNsec: A Hybrid Metaheuristic Approach for Reliable Security and Node Deployment in WSNs*. arXiv.

11. Ali, S. A., & Din, S. (2024). *Enhancing Wireless Sensor Network Security Through Integration With the ServiceNow Cloud Platform*. arXiv.

12. Kori, G. S. (2025). *Wireless Sensor Networks and Machine Learning Centric Architectures*. (*Textbook on WSN resource management and edge/cloud integration*).

13. Uchoba, K. (2024). *Integrating IoT and WSN: Enhancing Quality of Service Through Cloud and Network Architecture*. Springer (Article authorship book context).

14. Kolhar, A. (2025). *Energy-Efficiency Strategies for Wireless Sensor Networks in IoT*. IGI Global (book chapter author).

15. Chander, B., Nirmala, A. B., & Guravaiah, K. (Eds.). (2024). *Intelligent Wireless Sensor Networks and the Internet of Things: Algorithms, Methodologies, and Applications*. CRC Press.