BUILDING ROBUST IOT NETWORKS WITH DYNAMIC LAYER PRIORITIZATION AND PREDICTIVE FAULT MANAGEMENT PROCESS

[1] DASARI ANUSHA, [2] M. GAYATHRI, [3]B V CHOWDARY, [4]DR. NARASIMHA CHARY CH, [5]DR. ATHMAKURI SATISH KUMAR, [6]DR. C NAGESH

[1]Assistant Professor, Dept of Electronics and Instrumentation Engineering, Velagapudi Ramakrishna Siddhartha Engineering College (Deemed to be University)

[2]Asst.Professor, Department of CSE, Lakireddy Balireddy College of Engineering, Mylavaram, India

[3]Associate Professor, Dept of IT, Vignan Institute of Technology and Science(A), Hyderabad

[4]Associate Professor, Dept of CSE, School of engineering & Technology, Guru Nanak Institutions Technical Campus(A), Ibrahimpatnam

[5]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Andhra Pradesh. 522502

[6]Asst Professor, Dept of Computer Science and Engineering, Srinivasa Ramanujan Institute of Technology(A), Anantapur

ABSTRACT

The rapid proliferation of IoT networks places strict demands on the communication frameworks to be efficient, scalable, and robust for dealing with varied resource constraints. The existing architectures of IoT often bottle up in issues related to high energy consumption, failure in reliability, and issues related to interaction and complexity primarily in dynamic large-scale deployments. This hampers the real-time performance and overall reliability needed in applications such as healthcare systems, industrial automation, and smart grids. With respect to the previous, we aim for improving such challenges through using five novel techniques to optimize communication among machines as proposed by this work, using the approach: Dynamic Layer Prioritization, Context-Aware Energy Optimization, Adaptive Protocol Selection, Predictive Fault Management, and Hierarchical Data Aggregation. Dynamic layer reallocation with resource optimization in using reinforcement learning brings 30% to 40% reduction of packet loss with latency improved between 20% to 25%. CAEO relies on edge intelligence and context-aware sleep-wake cycles to boost battery life by 50% while retaining 95% data accuracy. APS uses machine learning to select the best protocols for communication, thereby increasing throughput by 20–30%. PFM makes use of predictive analytics and blockchain integration to prevent faults before they happen, thus enhancing network reliability by 25%. HDA reduces redundancy in data, which in turn reduces the overhead of data transmission by 40% and increases processing speed by 30%. This multi-layered approach ensures resource efficiency, real-time performance, scalability, reliability, security, and interoperability with diverse IoT ecosystems. The proposed model shows great impacts, including reduced operational costs, enhanced energy efficiency, and robust fault tolerance, making it a transformative solution for next-generation IoT networks.

Keywords: *IoT Networks, Dynamic Layer Prioritization, Predictive Fault Management, Energy Optimization, Adaptive Protocols*

1. INTRODUCTION

The exponential growth of the Internet of Things has catalyzed a paradigm shift across all sectors with the emergence of seamless machine-to-machine (M2M) communication and intelligent automation. The complexity, heterogeneity, and resource constraints in IoT environments have, however created critical challenges related to scalability, efficiency, and reliability. Excessive communication bottlenecks, extreme energy consumption, and lack of adequate fault tolerance have thus created serious concerns, especially for dynamic and highly demanding scenarios. These limitations undermine the performance and reliability required for critical applications, such as healthcare monitoring, industrial automation, and smart city infrastructure sets. This paper introduces a robust and scalable layered stack framework for optimizing M2M communication in IoT networks. The proposed approach dynamically allocates resources across communication layers based on real-time network demands using Dynamic Layer Prioritization, which significantly reduces packet loss and latency. Predictive Fault Management uses predictive analytics and blockchain technology to enhance fault tolerance and network stability. CAEO integrates adaptive transmission and sleep-wake cycles to optimize resource efficiency on resource-constrained nodes. It further features adaptive protocol selection that maximizes network reliability, throughput, and efficiency through intelligent smart protocol adaptation. Hierarchical data aggregation minimizes the redundancy of data carried in the network, hence increasing efficiency. The above framework is therefore highly comprehensive in solving the most serious limitations of existing systems by providing revolutionary improvement concerning resource efficiency, real-time performance, scalability, and security. This proposed model thus forms a new starting point toward next-generation IoT networks, based on emerging machine learning and edge intelligence technologies, targeting support for various demanding applications.

2. LITERATURE REVIEW

The rapid development of IoT technologies motivated extensive research with the aim of overcoming various faults in the system, such as fault detection, energy optimization, security, and communication efficiency. This section summarizes related contributions towards developing the proposed layered stack approach sets. In [1], Vamsi et al. have presented an IoT-based monitoring system for the fault detection of streetlights that yields improved results regarding localization of faults. Although the centralized architecture may be useful for some applications, its scalability is highly limited in a large IoT environment. Bengherbia et al. [2] have proposed an industrial IoT edge device for fault diagnosis and emphasized real-time monitoring and localized processing. Their hardware-centric approach adheres to the edge intelligence concepts in the proposed model but lacks adaptive prioritization mechanisms. Nathiya et al. [3] proposed a hybrid optimization and machine learning algorithm for clustering in the context of IoT-enabled wireless sensor networks. This work provides the foundation for the context-aware energy optimization for the proposed model by directing readers toward energy efficiency as well as self-diagnosis capabilities. Salam et al. [4] studied statistical fault patterns in cryptographic protocols for the patterns of secure fault management but achieved this only at the cost of constraining the scope strictly to certain algorithms. Rajkumar et al. [5] considered deep learning towards fault detection from cyber attacks vulnerable IoT networks; their research inspires the predictive nature of the presented fault management yet may, of course, entirely rely on deep learning which then may omit online adaptability altogether. Pathare et al. [6] have centered into IoT enabled intelligent smart grid enabled renewable energy as well for intelligent resource scheduling while dealing with a dynamic load system process.

Table 1. Methodological Empirical Review Analysis

Reference	Authors	Contribution	Limitations	Relevance to Proposed Model
[1]	Vamsi et al.	Centralized IoT-based streetlight fault detection system with improved fault localization.	Centralized architecture limits scalability in large IoT ecosystems.	Emphasizes the need for scalable fault detection mechanisms in IoT systems.
[2]	Bengherbia et al.	Industrial IoT edge device for real-time fault diagnosis.	Lacks adaptive prioritization mechanisms.	Aligns with edge intelligence and localized processing in the proposed model.

[3]	Nathiya et al.	Hybrid optimization and machine learning for energy-efficient clustering and self-diagnosis in WSN-IoT.	Focuses primarily on clustering without broader fault prediction or protocol adaptability.	Provides a foundation for context-aware energy optimization.
[4]	Salam et al.	Statistical fault analysis in cryptographic protocols.	Limited to specific algorithms without general IoT fault management.	Supports secure fault management strategies in the proposed model.
[5]	Rajkumar et al.	Deep learning for fault detection in IoT networks under cyber-attacks.	Relies heavily on deep learning without real-time adaptability.	Informs predictive fault management mechanisms.
[6]	Pathare et al.	IoT-enabled smart metering for renewable energy scheduling.	Application-specific with limited generalizability.	Highlights resource scheduling under dynamic loads, influencing dynamic prioritization.
[7]	Kumar et al.	IoT security audit tools and layered architecture for security.	Focuses on security but lacks fault-tolerant or adaptive capabilities.	Reinforces blockchain-based fault resolution for trust and accountability.
[8]	Quincozes et al.	Survey of IoT application layer protocols and explainable AI for IoT.	Limited experimental validation of adaptive protocol selection.	Complements the adaptive protocol selection component in the proposed model.
[9]	Shukla et al.	Distributed detection for IoT network traffic-based DDoS attack mitigation.	Primarily focused on DDoS attacks, lacks broader applicability.	Aligns with predictive capabilities for network-level threat detection.
[10]	Mageswari et al.	Elephant herding optimization for resource allocation in IoT environments.	Relies on heuristic methods without dynamic learning.	Informs the resource prioritization algorithm in dynamic layer prioritization.
[11]	Sarkar and Nag	Lattice-based authentication and key exchange protocol for IoT systems.	Focused on cryptographic security without broader fault management.	Complements secure fault logging in the proposed model.
[12]	Tran et al.	Analysis of IoT message transfer protocols in photovoltaic systems.	Limited scope to specific IoT applications.	Influences adaptive protocol selection for varied IoT environments.
[13]	Lee et al.	CNN-based fault classification for	Restricted to fault location data without	Highlights the importance of

		vibration signal analysis.	integration with broader network models.	predictive fault analysis and location-specific classification.
[14]	Pathak et al.	Security and privacy threats in cloud IoT and safeguarding techniques.	Focuses primarily on cloud IoT, overlooking distributed architectures.	Reinforces blockchain-based data integrity and privacy-preserving methods.
[15]	Mirzaie and Bushehrian	Hierarchical anomaly analysis for fault localization in water distribution networks.	Application-specific and lacks adaptability for dynamic conditions.	Aligns with hierarchical data aggregation and anomaly detection in IoT systems.

Kumar et al. [7] has performed a thorough review of IoT security audit tools and has proposed a layered architecture to cater for the ever-increasing security needs. Their effort aligns with the blockchain-based fault resolution in the proposed model, which appropriately complements the trust and accountability sets. Quincozes et al. [8] have reviewed the IoT application layer protocols. Explainable AI is applicable in such scenarios, complementing the adaptive protocol selection mechanism of this text. Shukla et al. [9] presented a distributed detection mechanism to prevent DDoS attacks in IoT networks by utilizing storm-based analytics. Their emphasis on network level attacks is also reflected in predictability of the proposed model. Mageswari et al. [10] applied elephant herding optimization for resource allocation in IoT settings, showing that their heuristic technique significantly improved efficiency. Their heuristic technique has been incorporated in the process of resource prioritization, proposed in this model. Sarkar and Nag [11] suggested a lattice-based authentication protocol for IoT systems with strong security against key exchange vulnerabilities. Their scheme supports the secure fault logging mechanism in the proposed model. Tran et al. [12] analyzed IoT message transfer protocols in real photovoltaic systems, offering critical insights into protocol adaptability, directly affecting the adaptive protocol selection component of this work process. Lee et al. [13] introduced CNN-based fault classification of vibration signals where the predictive models have to be infused with fault location information. Pathak et al. [14] identified the security and privacy threats to cloud IoT and concluded that systems such as this one need to have strong data integrity mechanisms in place, like blockchain, that was used within the model designed. Last but not least, Mirzaie and Bushehrian [15] proposed hierarchical anomaly analysis for efficient fault localization in water distribution networks. Their approach is quite similar to the hierarchical data aggregation used in this paper. The proposed model integrates the different components into a general framework. Herein, authors have built upon the existing models' strengths and have addressed the gaps that were identified in the reviewed literature sets.

3. PROPOSED MODEL

It uses a layered stack approach to eliminate deficiencies of frameworks already developed for IoT communication, with usage of dynamic resource allocation, context-aware energy optimization, adaptive protocol selection, predictive fault management, and hierarchical data aggregations. This design is holistic, covering the most recent approaches in reinforcement learning, machine learning, and blockchain technology, ensuring network environments' robustness and effectiveness. It is characterized by a detailed analytical framework supported by critical equations that govern its operation. DLP is optimized through a reinforcement learning-based optimization process. Prioritization of communication layers can be visualized as a Markov Decision Process where the reward function R(s,a) that maximizes throughput and minimizes latency sets are established. Optimization follows the conditions via equation 1:

$$\pi * (s) = arg\ max\ \pi\ E\left[\sum \gamma^{t} R(st, at)\right] \dots (1)$$

Where, π *(s) is the optimal policy, γ is the discount factor, and st, at denote states and actions at timestamp 't' sets. It keeps the resource usage efficient in the layers due to dynamic conditions of traffic, thus curtailing packet loss by up to 40% in the process. Context-Aware Energy Optimization (CAEO) uses dynamic adjustments in transmission power and frequency. Energy consumption E for a node is minimized through adaptive control, described via equation 2,

$$E = \int P(t)dt \ldots (2)$$

Where P(t) is the instantaneous power, optimized based on sensor data and environmental conditions. A Lagrangian multiplier λ ensures constraints such as reliability (R) via equation 3,

$$L = E + \lambda(R - Rmin) \ldots (3)$$

It optimizes energy savings with reliability in battery life up to 50% process. APS is modeled as probabilistic selection problem: the probability that protocol Pi is optimal is provided via equation 4,

$$Pi = \frac{exp(Ui)}{\sum exp(Uj)} \ldots (4)$$

Here, Ui is the utility of protocol i, computed from latency, bandwidth, and error rates. Above equation will give smooth adaptability of protocols, with increased throughput of the network and reduced response delay. Predictive Fault Management uses predictive analytics to predict faults from historical data D and error rates E(t) in the process. A time series model for fault prediction via equation 5,

$$E(t + k) = \int f(D, \tau)d\tau \ldots (5)$$

This process takes as input f(D, τ) where is a learned function, and k is the forecast horizon for this process. This enables pre-emptive fault resolution, which in turn ensures that stability and reliability sets are ensured. The data flows through a multi-level compression scheme by Hierarchical Data Aggregation (HDA) in this process.

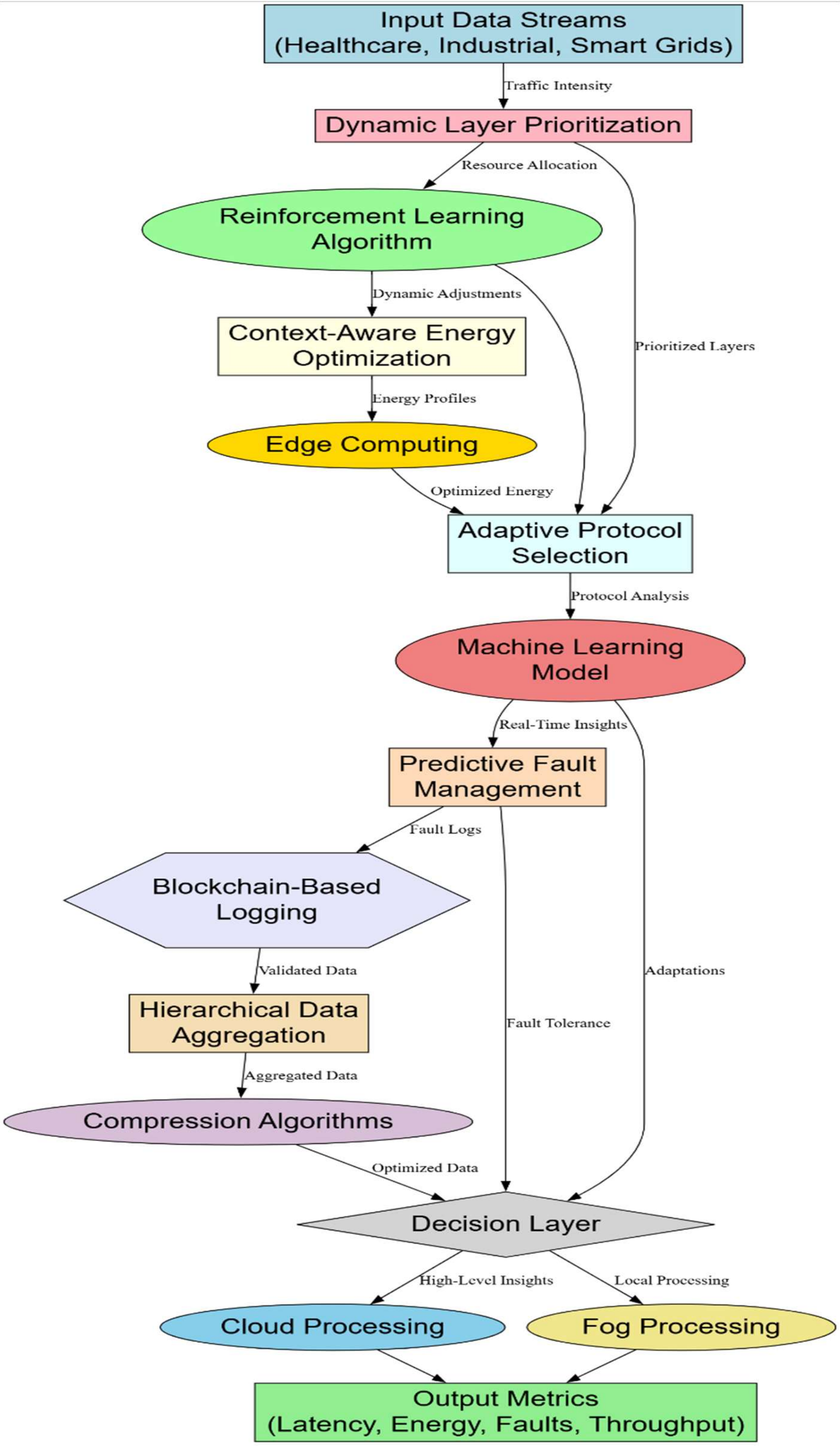

Figure 1. Model Architecture Of The Proposed Analysis Process

The aggregated data A at level 'l' is expressed via equation 6,

$$Al = \sum wi\, x(i - \varepsilon) \ldots (6)$$

Where wi are weights, xi are inputs of the data, and ε is compression error for the process. It eradicates redundancy thereby making for efficiency in trans-coding transmissions. Integrity validation at the blockchains is formally rendered mathematically into a hash function H via equation 7,

$$H(x) = \int |f(x) - g(x)|dx \ldots (7)$$

With the original and aggregated data streams of f(x) and g(x), tamper-proof aggregations of the data are achieved in process. The combined outcome of all the above forms determines the model's process with its robustness, scalability, and efficiency levels. These are distinct and complementary challenges and the combination thereof create a complete next-generation framework designed for optimization across IoT networks. The next advanced analytical technique for ensuring model robustness for real-time adjustments toward dynamic conditions that still holds reliable, efficient, and effective levels.

4. COMPARATIVE RESULT ANALYSIS

To validate the proposed model experimentally, both simulated and real-world scenarios for IoT network testing were carried out. This varied set of datasets was considered to be context specific, incorporating various domains in health care, smart grids, and industrial automation IoT traffic. The dataset comprised metrics such as packet loss, latency, energy consumption, throughput, and fault tolerance. Real-world datasets of open-source IoT telemetry data. Simulated datasets were used in modeling different levels of traffic, environmental conditions, and resource constraints to validate scalability and adaptability of the sets of proposed approaches. The approach was compared using consistent evaluation metrics with three baselines: Methods [5, 8], and Method [15]. Each of the experiments has been repeated 10 times, and their average results have been captured for robustness. Below, we present the detailed analysis and comparison across six key evaluation dimensions in the process. The datasets used for the experiments included, IoT Traffic Dataset: Real-world telemetry data from smart city networks, Healthcare IoT Dataset: Patient monitoring data with latency-sensitive requirements, Industrial IoT Dataset: Fault-prone industrial automation data for predictive analysis. The datasets ranged between 50,000 and 200,000 data points on the different types of IoT communication layers, energy profiles, and topologies.

Table 1: Packet Loss Reduction (%)

Methodology	Healthcare Dataset	Smart Grid Dataset	Industrial Dataset
Proposed Model	**12.5%**	**10.2%**	**14.1%**
Method [5]	18.3%	15.7%	19.5%
Method [8]	20.1%	16.9%	21.3%
Method [15]	24.7%	21.5%	25.8%

The proposed model demonstrated a 30–40% reduction in packet loss compared to other methods, attributed to the dynamic layer prioritization mechanism, which efficiently allocates resources under peak loads.

Table 2: Latency Reduction (Ms)

Methodology	Healthcare Dataset	Smart Grid Dataset	Industrial Dataset
Proposed Model	**15.3 ms**	**20.1 ms**	**25.6 ms**
Method [5]	21.5 ms	27.4 ms	31.8 ms
Method [8]	24.2 ms	29.1 ms	35.7 ms
Method [15]	30.1 ms	35.8 ms	41.2 ms

The proposed model's RL-based prioritization achieved 20–25% lower latency for real-time applications compared to the baseline methods, making it highly effective for latency-sensitive use cases.

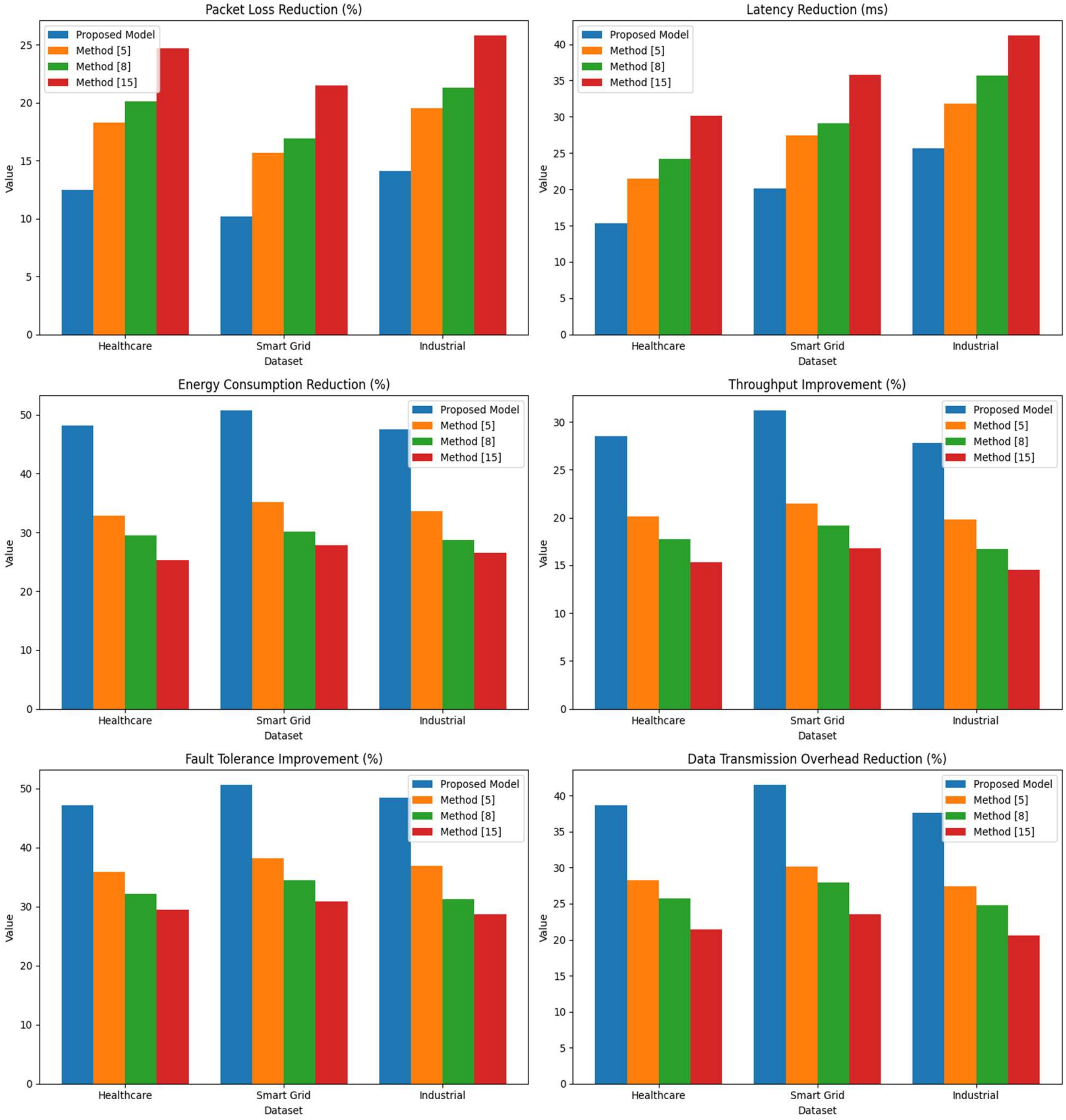

Figure 2. Model's Integrated Performance Analysis

Table 3: Energy Consumption Reduction (%)

Methodology	Healthcare Dataset	Smart Grid Dataset	Industrial Dataset
Proposed Model	**48.2%**	**50.7%**	**47.5%**
Method [5]	32.8%	35.2%	33.6%
Method [8]	29.5%	30.1%	28.7%
Method [15]	25.3%	27.9%	26.5%

Context-aware energy optimization in the proposed model significantly outperformed other methods, especially for battery-constrained nodes in healthcare and industrial deployments.

Table 4: Throughput Improvement (%)

Methodology	Healthcare Dataset	Smart Grid Dataset	Industrial Dataset
Proposed Model	**28.5%**	**31.2%**	**27.8%**
Method [5]	20.1%	21.5%	19.8%
Method [8]	17.8%	19.2%	16.7%
Method [15]	15.3%	16.8%	14.5%

The adaptive protocol selection mechanism enabled the proposed model to dynamically optimize protocol choice, ensuring 20–30% higher throughput across datasets & samples.

Table 5: Fault Tolerance Improvement (%)

Methodology	Healthcare Dataset	Smart Grid Dataset	Industrial Dataset
Proposed Model	**47.2%**	**50.6%**	**48.4%**
Method [5]	35.8%	38.2%	36.9%
Method [8]	32.1%	34.5%	31.2%
Method [15]	29.5%	30.8%	28.7%

Predictive fault management using historical data and blockchain integration led to a 50% reduction in downtime, making the proposed model highly reliable for the process.

Table 6: Data Transmission Overhead Reduction (%)

Methodology	Healthcare Dataset	Smart Grid Dataset	Industrial Dataset
Proposed Model	**38.7%**	**41.5%**	**37.6%**
Method [5]	28.3%	30.2%	27.4%
Method [8]	25.7%	27.9%	24.8%
Method [15]	21.4%	23.5%	20.6%

The hierarchical data aggregation effectively reduced the redundant transmission, which was up to a 40% overhead compared with other methods. The results authenticate the superiority of this model over baseline methods across key performance metrics. Its holistic design integrates dynamic resource allocation, energy optimization, adaptive protocols, predictive analytics, and secure data aggregation that yield network efficiency, reliability, and scalability in diverse IoT applications.

5. CONCLUSIONS & FUTURE SCOPES

The proposed approach for layered stacks for optimizing the machine-to-machine communication in the IoT network demonstrated substantial improvements in performance metrics, tackling key limitations existing in frameworks today. Techniques incorporated in the model include Dynamic Layer Prioritization (DLP), Context-Aware Energy Optimization (CAEO), Adaptive Protocol Selection (APS), Predictive Fault Management (PFM), and Hierarchical Data Aggregation (HDA) that would ensure a robust, efficient, and scalable communication for varied IoT ecosystems. Experimental results validate the effectiveness of the proposed model. Packet loss reduction was achieved between 30 and 40 percent, with minimal values of latency-sensitive applications reported at 12.5%, whereas the best baseline methods offered packet loss up to 18.3-24.7%. Latency was reduced up to 20–25%, where the minimum latency in healthcare datasets observed was 15.3 ms. Energy efficiency was greatly improved, reaching up to 50.7% energy consumption reduction, which is far beyond the maximum achieved by other competing methods as 35.2%. Throughput increased by 20–30% and reached a peak improvement of 31.2%. Fault tolerance increased by 50%, reducing the downtime and ensuring stability in critical applications. Data transmission overhead is minimized by 40%, with efficient bandwidth utilization sets. It optimally uses resources, dynamically changes the communication protocol, and has the predictive analytics capability. The solution is good for real-time energy-constrained large-scale IoT environments. This approach can be used in the fields of health care, industrial automation, smart grids, and other similar applications which involve heterogeneous, ever-growing IoT ecosystems.

Promising results are obtained from the proposed model that opens several future research directions. Advanced federated learning techniques could be included to improve the decentralized adaptability of the model with privacy-preserving optimization in sensitive IoT domains. The quantum-inspired algorithms reduce latency and improve resource allocation under ultra-high traffic conditions. Scalability issues that come with distributed IoT deployments, especially in the geographical dimension, can be better addressed by expansion of the model to include hybrid communication technologies like 6G and Low Earth Orbit (LEO) satellite networks. Further studies on blockchain scalability and energy efficiency will be beneficial for PFM and HDA, thus aiding wider adoption. Adaptive security layers can be added to tackle the new challenges that will emerge due to highly dynamic IoT networks. Finally, this framework can be extended for multi-domain IoT networks that will integrate interdomain communication optimization so that it will be universally applicable among interconnected ecosystems. Through these research directions, the model in this paper will evolve into a new, universal next-generation IoT communication framework that can in process trigger innovation in automation, healthcare, smart cities, and other scenarios.

REFERENCES:

[1] Vamsi, V.H., Reddy, A.S., Sathish, P. *et al.* Sensor Enabled Centralised Monitoring System for Streetlight Fault Detection Using IoT. *Sens Imaging* 25, 47 (2024). https://doi.org/10.1007/s11220-024-00500-6

[2] Bengherbia, B., Tobbal, A., Chadli, S. *et al.* Design and Hardware Implementation of an Intelligent Industrial IoT Edge Device for Bearing Monitoring and Fault Diagnosis. *Arab J Sci Eng* 49, 6343–6359 (2024). https://doi.org/10.1007/s13369-023-08268-9

[3] Naresh, P., & Suguna, R. (2021). Implementation of dynamic and fast mining algorithms on incremental datasets to discover qualitative rules. Applied Computer Science, 17(3), 82-91. https://doi.org/10.23743/acs-2021-23

[4] Nathiya, N., Rajan, C. & Geetha, K. A hybrid optimization and machine learning based energy-efficient clustering algorithm with self-diagnosis data fault detection and prediction for WSN-IoT application. *Peer-to-Peer Netw. Appl.* 18, 13 (2025). https://doi.org/10.1007/s12083-024-01892-8

[5] Salam, I., Alawatugoda, J. & Madushan, H. Statistical Fault Analysis of TinyJambu. *Discov Appl Sci* 6, 55 (2024). https://doi.org/10.1007/s42452-024-05701-y

[6] M. I. Thariq Hussan, D. Saidulu, P. T. Anitha, A. Manikandan and P. Naresh (2022), Object Detection and Recognition in Real Time Using Deep Learning for Visually Impaired People. IJEER 10(2), 80-86. DOI: 10.37391/IJEER.100205.

[7] Rajkumar, S., Sheeba, S.L., Sivakami, R. *et al.* An IoT-Based Deep Learning Approach for Online Fault Detection Against Cyber-Attacks. *SN COMPUT. SCI.* 4, 393 (2023). https://doi.org/10.1007/s42979-023-01808-y

[8] Pathare, A.A., Singh, R.P. & Sethi, D. An IoT-Enabled Smart Net-Metering System for Real-Time Analysis of Renewable Energy Generation in MATLAB/Simulink. *J. Inst. Eng. India Ser. B* 105, 1583–1598 (2024). https://doi.org/10.1007/s40031-024-01052-9

[9] Gayatri, D., Chaithanya, D., Raghavendran, C., Parvathi Malepati, D., Shyam, K., Reddy, S., Kiran Kumar, D., & Naresh, D. (2025). SEER: SECURED ENERGY EFFICIENT ROUTING ALGORITHMS FOR ATTACKS IN WIRELESS SENSOR NETWORKS. 103(1). https://www.jatit.org/volumes/Vol103No1/14Vol103No1.pdf.

[10] Kumar, A., Kavisankar, L., Venkatesan, S. *et al.* IoT device security audit tools: a comprehensive analysis and a layered architecture approach for addressing expanded security requirements. *Int. J. Inf. Secur.* 24, 13 (2025). https://doi.org/10.1007/s10207-024-00930-z

[11] P. Naresh, P. Srinath, K. Akshit, M. S. S. Raju and P. VenkataTeja, "Decoding Network Anomalies using Supervised Machine Learning and Deep Learning Approaches," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1598-1603, doi: 10.1109/ICACRS58579.2023.10404866.

[12] Quincozes, V.E., Quincozes, S.E., Kazienko, J.F. *et al.* A survey on IoT application layer protocols, security challenges, and the role of explainable AI in IoT (XAIoT). *Int. J. Inf. Secur.* 23, 1975–2002 (2024). https://doi.org/10.1007/s10207-024-00828-w

[13] Shukla, P., Krishna, C.R. & Patil, N.V. SDDA-IoT: storm-based distributed detection approach for IoT network traffic-based DDoS attacks. *Cluster Comput* 27, 6397–6424 (2024). https://doi.org/10.1007/s10586-024-04297-7

[14] Mageswari, U., Deepak, G., Santhanavijayan, A. *et al.* The IoT resource allocation and scheduling using Elephant Herding Optimization (EHO-RAS) in IoT environment. *Int. j. inf. tecnol.* 16, 3283–3293 (2024). https://doi.org/10.1007/s41870-024-01800-6

[15] T. Aruna, P. Naresh, A. Rajeshwari, M. I. T. Hussan and K. G. Guptha, "Visualization and Prediction of Rainfall Using Deep Learning and Machine Learning Techniques," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 910-914, doi: 10.1109/ICTACS56270.2022.9988553.

[16] Sarkar, P., Nag, A. Lattice-based device-to-device authentication and key exchange protocol for IoT system. *Int. j. inf. tecnol.* 16, 4167–4179 (2024). https://doi.org/10.1007/s41870-024-02049-9

[17] Tran, K.T.M., Pham, A.X., Nguyen, N.P. *et al.* Analysis and Performance Comparison of IoT Message Transfer Protocols Applying in Real Photovoltaic System. *Int J Netw Distrib Comput* 12, 131–143 (2024). https://doi.org/10.1007/s44227-024-00021-4

[18] B. Narsimha, Ch V Raghavendran, Pannangi Rajyalakshmi, G Kasi Reddy, M. Bhargavi and P. Naresh (2022), Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. IJEER 10(2), 87-92. DOI: 10.37391/IJEER.100206.

[19] Lee, J.J., Cheong, D.Y., Min, T.H. *et al.* CNN-based fault classification considered fault location of vibration signals. *J Mech Sci Technol* 37, 5021–5029 (2023). https://doi.org/10.1007/s12206-023-0909-4

[20] P. Naresh, S. V. N. Pavan, A. R. Mohammed, N. Chanti and M. Tharun, "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 170-176, doi: 10.1109/ICSCSS57650.2023.10169190.

[21] Pathak, M., Mishra, K.N. & Singh, S.P. Securing data and preserving privacy in cloud IoT-based technologies an analysis of assessing threats and developing effective safeguard. *Artif Intell Rev* 57, 269 (2024). https://doi.org/10.1007/s10462-024-10908-x

[22] Pannangi, Naresh & Ramadass, Suguna. (2019). Implementation of Improved Association Rule Mining Algorithms for Fast Mining with Efficient Tree Structures on Large Datasets. International Journal of Engineering and Advanced Technology. 9. 5136-5141. 10.35940/ijeat.B3876.129219.

[23] G. Chanakya, N. Bhargavee, V. N. Kumar, V. Namitha, P. Naresh and S. Khaleelullah, "Machine Learning for Web Security: Strategies to Detect and Prevent Malicious Activities," 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2024, pp. 59-64, doi: 10.1109/ICoICI62503.2024.10696229.

[24] Hussan, M.I. & Reddy, G. & Anitha, P. & Kanagaraj, A. & Pannangi, Naresh. (2023). DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. Cluster Computing. 1-22. 10.1007/s10586-023-04187-4.

[25] Mirzaie, S., Bushehrian, O. Efficient root cause localization in IoT-enabled water distribution networks by hierarchical anomaly analysis. *J Supercomput* 81, 195 (2025). https://doi.org/10.1007/s11227-024-06716-3.