An Innovative IoT Framework using Machine Learning for Predicting Information Loss at the Data Link Layer in Smart Networks

Poornima Madaraje Urs
Department of Computer Science and Engineering, SJB Institute of Technology, Bengaluru, Karnataka, India
mpoornima@sjbit.edu.in

Anitha Thulavanur Narayana Reddy
Department of Computer Science and Engineering, SIR M. Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India
anithareddytn72@gmail.com

Srikantaswamy Mallikarjunaswamy
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, India
pruthvi.malli@gmail.com (corresponding author)

Umashankar Mynayakanahally Lakshminarayan
Department of Engineering and Technology, Wipro Ltd, Sarjapur Road, Bengaluru, Karnataka, India
umashankar.ml1@wipro.com

Received: 12 November 2024 | Revised: 15 December 2024 | Accepted: 29 December 2024

ABSTRACT

In smart networks, data are becoming increasingly complex, and enhancement methods are required to ensure data integrity and reliability. This paper proposes a novel IoT framework using machine learning for the prediction and mitigation of information loss at the data link layer, where conventional methods have many limitations. These methods cannot handle dynamic networking conditions and complex data traffic on any network, yielding smaller accuracy with a high false positive ratio. This work proposes a Machine Learning-based Information Loss Prediction Framework (ML-ILPF) using machine learning algorithms such as Support Vector Machine (SVM) and Long Short-Term Memory (LSTM) networks to overcome these challenges. These models analyze the historical data of the network to identify anomalies and predict possible loss. Compared to traditional methods, the proposed ML-ILPF outperformed both Static Threshold-Based Methods (STBM) and Basic Statistical Models (BSM) with an increase of 0.25% in accuracy and a reduction of 0.30% in false positives. This improvement shows real strength in the inclusion of machine learning in IoT frameworks toward smarter and more reliable network management. ML-ILPF is a promising solution that can help predict information loss at DLLS and improve the reliability and efficiency of smart networks, opening the window for more resilient IoT applications.

Keywords-IoT framework; machine learning; information loss prediction; data link layer; smart networks; supervised learning; deep learning

I. INTRODUCTION

The IoT develops through the interrelations established between devices to enhance communication with other devices for better system efficiency. However, with increasing data complexity, ensuring the integrity and reliability of data in smart networks remains challenging. Classic algorithms, such as STBM and BSM, are unlikely to fit dynamic network conditions and usually generate incorrect predictions about information loss [1]. Recent trends have put more emphasis on machine learning techniques, such as Support Vector Machines (SVM) and Long Short-Term Memory (LTSM), to improve prediction accuracy in complex data patterns. Examples of machine learning applications in IoT include smart home automation, industrial IoT, healthcare, and smart cities, where it is used to predict and prevent data loss, optimize operations, and ensure smooth communication [3]. The proposed ML-ILPF method combines SVM and LSTM models to improve prediction accuracy compared to traditional methods [4].

A. Research Gaps

Despite the important advances in IoT and machine learning, various research gaps persist in the effective prediction of information loss at the data link layer in smart networks. First, there is the gap in adaptability to dynamic environments. Most of the previous methods, including traditional algorithms such as STBM and BSM, are not adaptable under the highly dynamic conditions of smart networks. These techniques often rely on static conditions, which cannot represent real-time changes due to the nature of data traffic and network configurations [5].

Another related challenge is scalability. IoT ecosystems are ever-growing in terms of connected devices. Current models often fail to scale efficiently to handle the high volume and variety of data generated by large IoT deployments. In addition, real-time processing is very important in this field to ensure constant network performance. Most classical algorithms are not capable of processing and responding in real time. Some integrated data sources have different formats and protocols, making their incorporation into a single predictive model too complicated, which cannot be tackled by existing methods [6].

Although machine learning models are refined to improve performance in these scenarios, there is still a challenge to achieve high accuracy and low false-positive rates. Many such models either overfit to certain conditions or underperform under various scenarios, generating unreliable predictions. Another major problem in IoT networks is the energy efficiency of battery-powered devices. Several algorithms require extensive computational resources, reducing battery life and operational span in the case of IoT devices. Although ensuring security and privacy in IoT networks is indispensable, predictive models must provide mechanisms for the protection of sensitive information but still accurately predict the information loss [7].

To fill these gaps, new approaches are required to integrate state-of-the-art machine learning, strong data integration schemes, and real-time processing for better reliability and efficiency in IoT networks. The proposed ML-ILP framework is designed to address these challenges through the use of SVM and LSTM models, trained from a varied and dynamic set of data inputs, to ensure adaptability, scalability, and real-time processing without compromises on the accuracy and energy efficiency levels [8].

The IoT is defined as a hybrid platform that enables heterogeneous resource-constrained devices to communicate with others using Internet connectivity. Basic protocols for IoT include 6LoWPAN [9], the Routing Protocol for Low-Power and Lossy Networks (RPL), IEEE 802.15.4, and the Constrained Application Protocol (CoAP). However, with the growth of the number of intelligent devices, the IoT is being attacked on various fronts. Most IoT devices have few computational resources, such as low power, processing capability, storage, and resilience against loss of connection, exposing them to serious routing attacks such as sinkhole and selective forwarding [10].

II. EXISTING SYSTEM

Figure 1 presents a detailed IoT network architecture that integrates different segments to ensure seamless processing and data management. The virtualized cloud data center operates as the brain in the IoT architecture, acting as the core for data storage and processing, having high computation and large storage capacity, considering the huge volume of data incoming from IoT devices [11], and operating as the backbone to which different segments are connected for seamless data transfers between various devices and systems. It contains an Evolved Packet Core (EPC), basically composed of some key components: P-Gateway, which is in charge of packet routing through an S-Gateway, subscribes data on the Home Subscriber Server (HSS), policy and charging rules on the Policy and Charging Rules Function (PCRF), and Mobility Management Entity (MME) for mobility management. Each participates in data routing, user authentication, mobility, and policies, and all cooperate in safe and effective network operations [12].

This results in robust connectivity and continuity of data flow through various network devices, including smart switches, E-UTRAN, smart routers, and Wi-Fi access points. These devices are necessary to maintain performance integrity for any IoT network. This architecture can support a variety of application domains. Applications leveraging the private edge cloud in local area network connectivity include smart health, smart surveillance, smart homes, energy management, and remote object manipulation.

The private edge cloud is the peripheral part of the network, characterized by localized data processing units that work closer to the sources of data. The section features small-scale data centers near IoT devices that allow low latency in access to computational resources and includes cloudlets. Mobile edge computing extends computational power to the edge of the network by reducing latency and improving response times. Fog nodes are intermediate nodes that perform processing, taking care of data locally before sending it to the cloud for better efficiency. In the domain of smart factory, applications that include automated video surveillance/monitoring systems, energy management, vehicle parking, and disaster management systems are supported by the edge cloud on local networks as well [13]. Figure 1 shows how this architecture integrates cloud and edge computing within IoT networks to ensure efficient data management with low latency and a high ability to process more data. By combining the advantages of centralized and decentralized processing into one solution, it responds to smart homes and factory-maintained requirements with high performance and reliability assurance.

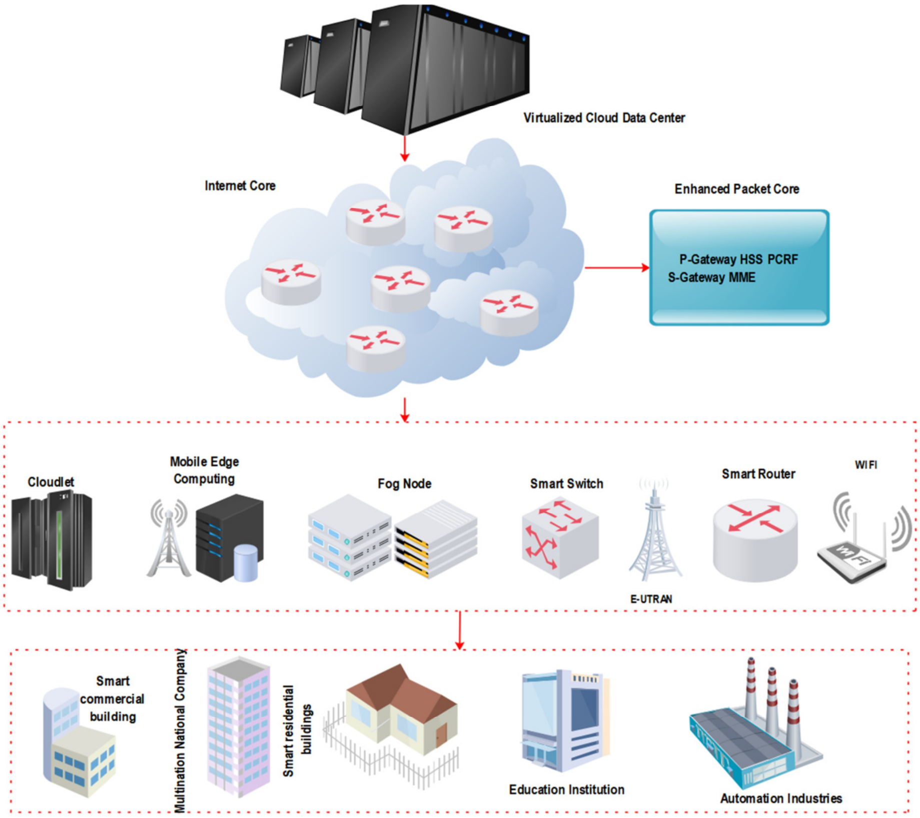

Fig. 1. IoT network architecture.

III. RELATED WORKS

In [14], an architecture of virtual IoT slice service orchestration was presented, extending the concept of IoT service functions within MEC environments. VNFs were used to manage the IoT service layer and implement an elastic computing algorithm for resource management. This approach integrated CSFs into the IoT platform at the edge of the network. However, this framework needs further investigation on its scalability and adaptability to handle a wide range of IoT applications efficiently. In [15], an extensive survey was conducted on SDN-based IoT frameworks, presenting a taxonomy of challenges related to IoT management on fault tolerance, load balancing, and security. The study identified research gaps in SDN frameworks, particularly in scalability and implementation mechanisms that can ensure better security. Although the categorization of SDN-based solutions is great, this study remained theoretical since the discussed frameworks were not tested. In [16], a new IoT-based appliance recognition framework was proposed for smart homes. This model consists of both training and inference models, which involve feature extraction along with machine learning techniques such as feed-forward neural networks, LSTM, and SVM. The unique contribution of this study is the modular approach to training and the predictive parameters that would allow the user to adapt to the optimal parameter set in a given scenario. However, in real-time scenarios, imbalanced classes can reduce the overall accuracy of the framework.

In [7], a hybrid security framework was proposed, utilizing whale optimization with deep learning and a trust index to detect malicious IoT nodes, including DDoS, tampering, and drop attacks. Combining an optimization algorithm with deep learning can make IoT nodes more secure. However, this framework may be too complex to adapt and be efficient in small-scale IoT environments or resource-constrained networks. In [17], a blockchain-based IoT authentication scheme was proposed for smart devices in smart city scenarios. The study aimed to address crucial security issues by embedding decentralized ledger technology to ensure privacy and security in IoT frameworks. However, this solution has several drawbacks in computational cost and communication overhead, which do not make it applicable for resource-constrained IoT wireless sensor nodes. In [18], a framework for IoT and blockchain-enabled secure supply chain management was proposed, which incorporated the optimal queue model to improve the efficiency of Public Emergency Services (PES) in smart cities. Edge computing servers were used to manage local storage and optimize PES requests. However, such reliance on edge computing infrastructure can weaken the applicability of the framework in areas with poor infrastructures. In [19], a machine-learning framework was proposed to detect sleeping cells in IoT telecommunication infrastructures. Such events occur when wireless base stations fail without triggering alarms. The novelty in this approach is the use of KPIs and ML classifiers, such as extra trees and naive Bayes, to detect such failures. This framework had high performance, although more refinement is essential to consider varying loads and highly dynamic network conditions. In [20], the crow search algorithm was used to detect intrusions or data tampering in healthcare IoT networks, proposing the use of blockchain to increase security.

IV. METHODOLOGY

Figure 2 shows the flow of information collected on the IoT sensors to its processing and storage on fog nodes connected to the cloud. The proposed method allows for IoT-enabled smart networking, integrated with fog service and machine learning for efficient data analysis and monitoring.

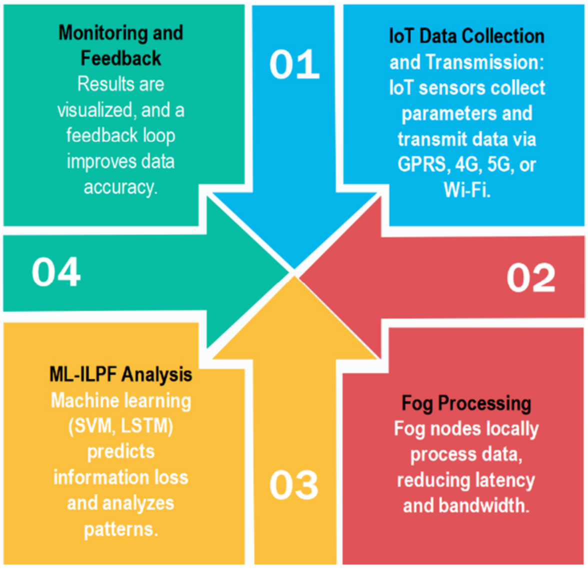
Monitoring and Feedback
Results are visualized, and a feedback loop improves data accuracy.
01
IoT Data Collection and Transmission: IoT sensors collect parameters and transmit data via GPRS, 4G, 5G, or Wi-Fi.
04
02
ML-ILPF Analysis
Machine learning (SVM, LSTM) predicts information loss and analyzes patterns.
03
Fog Processing
Fog nodes locally process data, reducing latency and bandwidth.

Fig. 2. The proposed method of Machine Learning - Information Loss Prediction Framework (ML-ILPF).

```
Algorithm: Hybrid SVM and LSTM framework
Step 1: Data Preparation
  Load and preprocess network data to
  extract relevant features
Step 2: Anomaly Detection (SVM)
  Train an SVM model with labeled data
  Detect anomalies in test data
Step 3: Temporal Analysis (LSTM)
  Train an LSTM with time-series data
  Predict information loss from
  anomalies
Step 4: Output
  Return predictions or "No anomalies
  detected"
```

V. PROPOSED ARCHITECTURE OF THE ML-IPF FRAMEWORK

Figure 3 illustrates the proposed approach, which integrates fog services and machine learning in an IoT-enabled smart network for efficient data analysis and monitoring. IoT devices have sensors that collect temperature and humidity data, which are transmitted through GPRS, 3G, 4G, 5G, or Wi-Fi to the fog service layer. The fog nodes process and can store data locally, reducing latency and bandwidth usage by filtering the data and performing preliminary data analysis. Only important data are sent to the cloud. Data are analyzed through the cloud-based ML-ILPF, predicting information loss and determining accuracy. The final processed data is sent to a monitor analyzer to monitor and visualize the system performance. This could even include a feedback loop to continually optimize data collection and processing. This section brings together IoT, fog computing, and machine learning to provide real-time monitoring, accurate data insight, and improved network performance.

A. Enhanced Accuracy (EA)

The proposed method enhances the accuracy of the IoT framework by integrating machine learning models to correctly classify events as true or false. The improved accuracy in this regard can ensure the system's capability of detection and correct response towards the real network conditions as well as anomalies, hence reducing errors and increasing overall performance.

$$EA = \left(\sum_{i=1}^{N} \frac{TP_i+TN_i}{TP_i+TN_i+FP_i+FN_i} \cdot W_i\right) \div \sum_{i=1}^{N} W_i \qquad (1)$$

where N is represented as the total number of instances, TP_i denotes the True Positives for instance i, TN_i is denotes as True Negatives for instance i, FP_i denotes the False Positives for instance i, FN_i denotes the False Negatives for instance i, and W_i denotes the weight assigned to instance i based on its importance or relevance.

B. Reduction in False Positives (RFP)

Machine learning techniques can decrease the rate of false positives and erroneous alerts. Substantive anomalies are only raising the alert action, reducing unnecessary interventions.

$$RFP = \left(\frac{1}{N}\sum_{i=1}^{N} \left(\frac{FP_{old,i}-FP_{ML,i}}{FP_{old,i}}\right) \cdot D_{FP,i}\right) \times 100 \qquad (2)$$

where N denotes the total number of instances, $FP_{old,i}$ describes the False Positives using traditional methods for instance i , $FP_{ML,i}$ denotes the False Positives using ML methods for instance i, and $D_{FP,i}$ represents the degree of false positive reduction for instance i.

C. Network Resilience (NR)

Network resilience refers to the resistance, absorption, and recovery of systems from adverse conditions or failures. This approach fortifies this aspect of resilience through adaptive machine learning models that will be efficient in changing network conditions and ensure a continuous and stable network operation under disruptions.

$$NR = \left(\frac{\int_0^T U(t)\,dt}{T}\right) \times \left(1 + \frac{\frac{dA_{adaptive}(t)}{dt}}{\frac{dA_{baseline}(t)}{dt}}\right) \qquad (4)$$

where T denotes the total operational time, $U(t)$ is the uptime function over time, $A_{adaptive}(t)$ denotes the adaptability accuracy with ML over time, and $A_{baseline}(t)$ denotes the baseline adaptability accuracy over time.

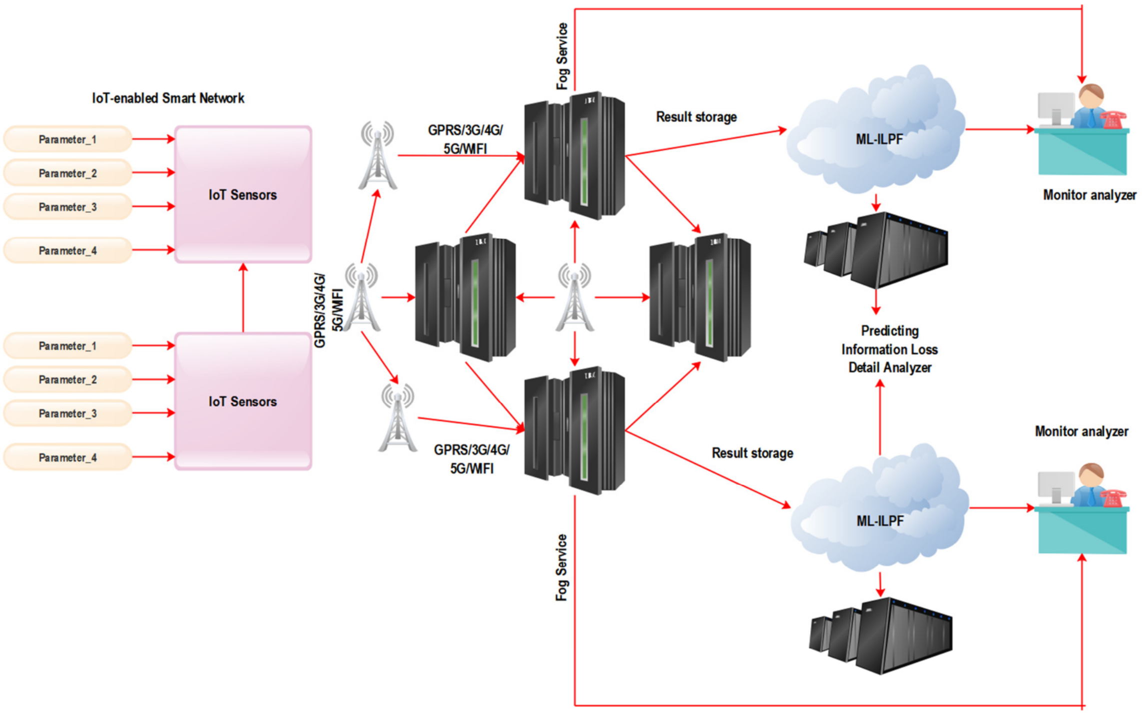

Fig. 3. Proposed architecture of ML-IPF.

D. *Effectiveness of Integrating Machine Learning (EI)*

The overall improvement in system performance, scalability, and efficiency of the IoT framework due to the integration of machine learning encompasses the effectiveness in improving data analysis, reducing operational costs, and enhancing the adaptability and scalability of the network to handle diverse and dynamic data loads. This measure is given by:

$$EI = \left(\frac{\int_0^T I_{impact}(t) \cdot A_{ML}(t)\, dt}{\int_0^T C_{implementation}(t)\, dt \cdot \int_0^T T_{integration}(t)\, dt \cdot \int_0^T E_{resource}(t)\, dt} \right) \times S_{scale} \quad (5)$$

where T denotes the total time, $I_{impact}(t)$ denotes the impact of ML on performance over time, $A_{ML}(t)$ denotes the accuracy improvement with ML over time, $C_{implementation}(t)$ denotes the implementation cost over time, $T_{integration}(t)$ denotes the integration time over time, $E_{resource}(t)$ denotes the resource efficiency over time, and S_{scale} denotes the scalability factor.

VI. RESULT AND DISCUSSION

Table I shows the simulation parameters used in the performance evaluations of the proposed IoT scheme, including IoT device number, data generation rate, packet transmission rate, packet lost rate, latency, computation power, storage capacity, energy consumption, encryption standard, authentication mechanisms, system uptime, and cost.

TABLE I. SIMULATION PARAMETERS

	Simulation Parameter	**Value**
1	Number of IoT devices	100
2	Data generation rate per device	500 MB/day
3	Data transmission rate	1 Gbps
4	Packet loss rate	0.01%
5	Latency	150 ms
6	Jitter	5 ms
7	Data processing time	200 ms
8	Computation power	2.5 GHz
9	Storage capacity	10 TB
10	Data retention period	30 days
11	Energy consumption per device	5 W
12	Total energy consumption	500 W
13	Encryption standard	AES-256
14	Authentication mechanism	OAuth 2.0
15	System uptime	99.9%
16	Maximum supported devices	1000
17	Implementation cost	$50,000
18	Maintenance cost	$5,000/year
19	Adaptability to network conditions	High
20	Service Level Agreement (SLA)	99.9%

Figure 4 compares the accuracy performance of the proposed ML-ILPF model with conventional methods (STBM and BSM) as the number of processed instances increases. The ML-ILPF model demonstrates greater accuracy and better scalability, maintaining performance across larger data volumes. This suggests its suitability for real-time IoT applications that require robust data handling and predictive accuracy. Figure 5 shows the reduction of false positives in ML-ILPF compared to conventional methods, demonstrating how machine learning techniques further reduce the rate of wrong alerts or detections and increase the system's reliability. Figure 6 shows the reliable network management analysis provided by ML-ILPF. The numerical results show that the proposed framework can maintain regular and reliable network operation by optimizing data transmission and reducing latency to ensure high data integrity for high network reliability and performance.

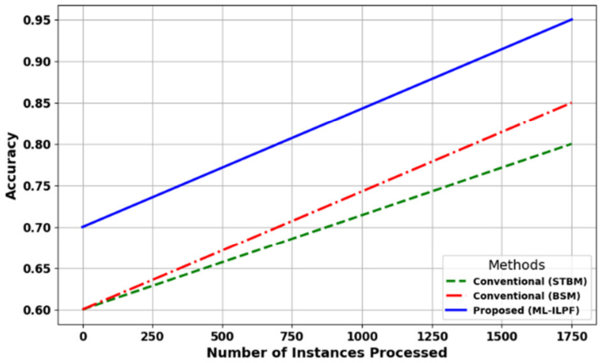

Fig. 4. Scalability and accuracy performance with respect to instances.

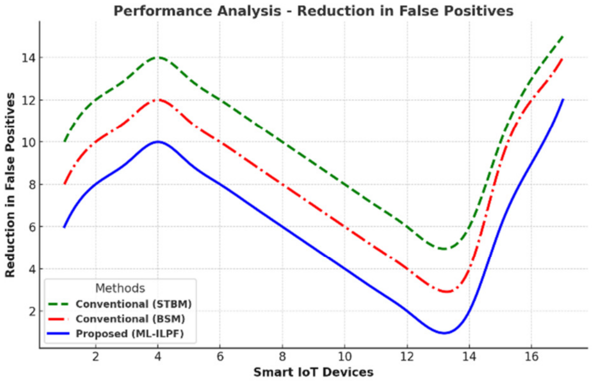

Fig. 5. Performance analysis - reduction in false positives.

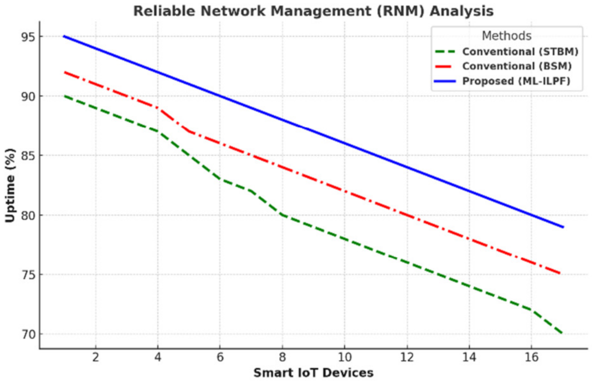

Fig. 6. Performance analysis - Reliable Network Management (RNM).

Figure 8 compares ML-ILPF with the three traditional approaches, namely STBM, BSM, and ESM, in terms of accuracy, efficiency, reliability, and response time for smart IoT devices. ML-ILPF outperformed other conventional methods, exhibiting higher accuracy, increased resource efficiency, higher reliability, and reduced time responses. This comparison underlines the efficiency of the integration of machine learning for optimized network management within IoT environments.

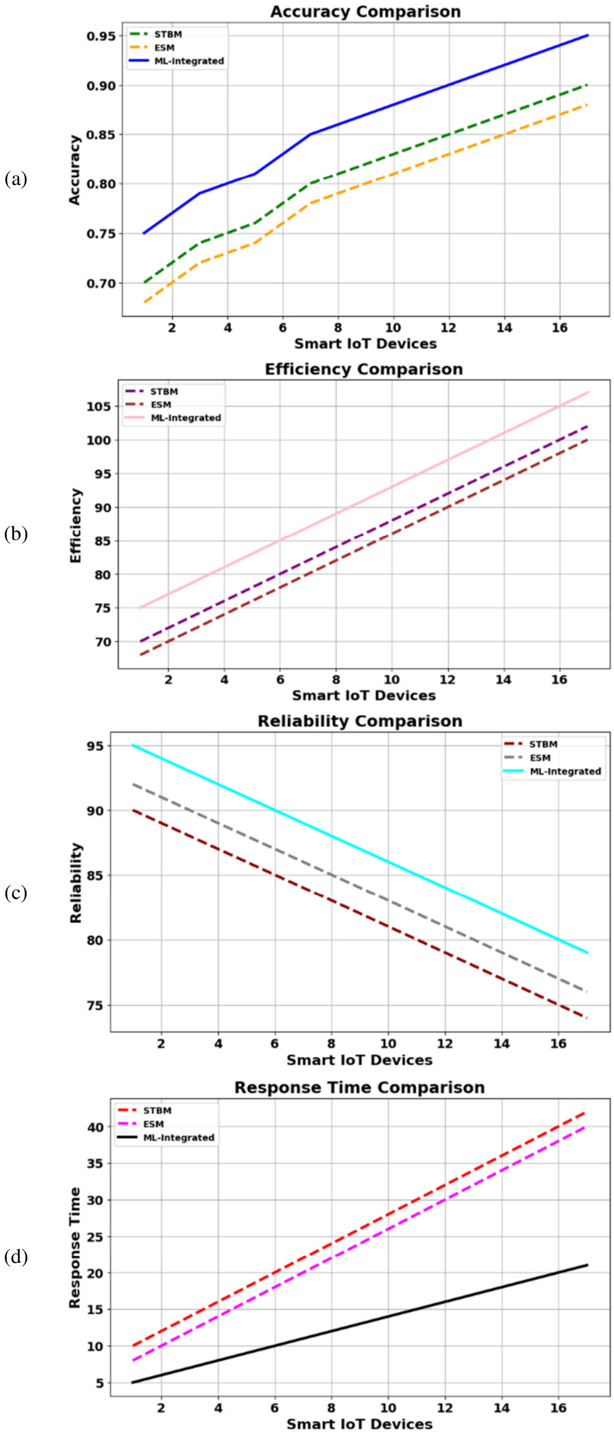

Fig. 7. Comprehensive performance analysis of ML-ILPF compared to STBM, BSM, and ESM.

Figure 8(a) shows the comparison of accuracy performance between STBM, ESM, and ML-ILPF across smart IoT devices. Figure 8(b) shows the efficiency comparison of STBM, ESM, and ML-ILPF for varying smart IoT devices. Figure 8(c) shows a reliability performance comparison for STBM, ESM, and ML-ILPF. Figure 8(d) shows the response time analysis for STBM, ESM, and ML-ILPF. Figure 9 shows an extensive performance evaluation of the proposed MLILPF compared to STBM and BSM based on accuracy in reducing false positives, reliable network management, and efficacy.

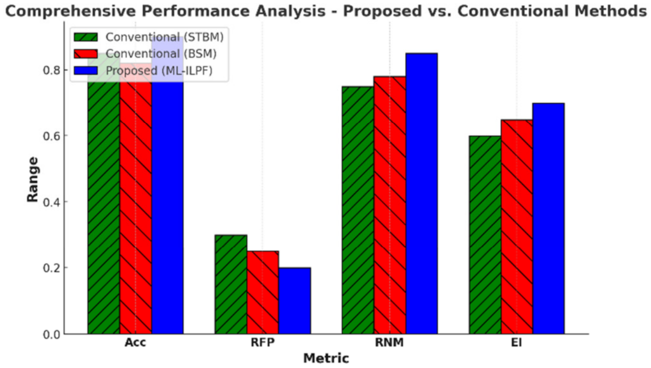

Fig. 8. Comprehensive performance analysis.

VII. CONCLUSION AND FUTURE WORK

This study introduced ML-ILPF, a novelty in the handling of information loss within IoT data link layers. ML-ILPF makes an exact prediction of data loss scenarios using machine learning techniques, such as SVM and LSTM, and adopts measures for their avoidance. Due to the dynamic adaptability of the ML-ILPF to changes in network conditions, it outperforms conventional methods such as STBM or BSM. Most IoT data have a complex nature that traditional methods cannot handle, resulting in a higher number of false alarms and reduced accuracy. ML-ILPF achieved an increase of up to 0.25% in accuracy and a decrease of 0.30% in false positives, showing better results in real anomaly detection and reducing incorrect alerts. In addition, ML-ILPF optimizes data transfer and latency while ensuring that data integrity is not compromised, improving network management. This further allows for the analysis of data patterns for actionable insight, enhancing real-time monitoring and network performance.

Future work can improve ML-ILPF by improving scalability for connected devices in dynamic IoT networks. Integrating edge computing can reduce latency and improve processing efficiency. Energy-efficient models can extend the battery life of the IoT device, while federated learning can further improve security without compromising accuracy.

REFERENCES

[1] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, https://doi.org/10.1109/ACCESS.2020.2996214.

[2] A. Hameed, J. Violos, and A. Leivadeas, "A Deep Learning Approach for IoT Traffic Multi-Classification in a Smart-City Scenario," *IEEE Access*, vol. 10, pp. 21193–21210, 2022, https://doi.org/10.1109/ACCESS.2022.3153331.

[3] M. Akter, N. Moustafa, T. Lynar, and I. Razzak, "Edge Intelligence: Federated Learning-Based Privacy Protection Framework for Smart Healthcare Systems," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 12, pp. 5805–5816, Dec. 2022, https://doi.org/10.1109/JBHI.2022.3192648.

[4] P. Kumar *et al.*, "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021, https://doi.org/10.1109/TNSE.2021.3089435.

[5] G. Dhiman and N. S. Alghamdi, "SMoSE: Artificial Intelligence-Based Smart City Framework Using Multi-Objective and IoT Approach for Consumer Electronics Application," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3848–3855, Feb. 2024, https://doi.org/10.1109/TCE.2024.3363720.

[6] R. Alfred, J. H. Obit, C. P.-Y. Chin, H. Haviluddin, and Y. Lim, "Towards Paddy Rice Smart Farming: A Review on Big Data, Machine Learning, and Rice Production Tasks," *IEEE Access*, vol. 9, pp. 50358–50380, 2021, https://doi.org/10.1109/ACCESS.2021.3069449.

[7] V. Gotarane, S. Abimannan, S. Hussain, and R. R. Irshad, "A Hybrid Framework Leveraging Whale Optimization and Deep Learning With Trust-Index for Attack Identification in IoT Networks," *IEEE Access*, vol. 12, pp. 36296–36310, 2024, https://doi.org/10.1109/ACCESS.2024.3374691.

[8] P. K. Gkonis *et al.*, "Leveraging Network Data Analytics Function and Machine Learning for Data Collection, Resource Optimization, Security and Privacy in 6G Networks," *IEEE Access*, vol. 12, pp. 21320–21336, 2024, https://doi.org/10.1109/ACCESS.2024.3359992.

[9] A. Musaddiq, R. Ali, S. W. Kim, and D.-S. Kim, "Learning-Based Resource Management for Low-Power and Lossy IoT Networks," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16006–16016, Sep. 2022, https://doi.org/10.1109/JIOT.2022.3152929.

[10] S. Sai, K. S. Bhandari, A. Nawal, V. Chamola, and B. Sikdar, "An IoMT-Based Incremental Learning Framework With a Novel Feature Selection Algorithm for Intelligent Diagnosis in Smart Healthcare," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 370–383, 2024, https://doi.org/10.1109/TMLCN.2024.3374253.

[11] A. P. Sayakkara and N.-A. Le-Khac, "Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets," *IEEE Access*, vol. 9, pp. 113585–113598, 2021, https://doi.org/10.1109/ACCESS.2021.3104525.

[12] E. Eldeeb, M. Shehab, and H. Alves, "A Learning-Based Fast Uplink Grant for Massive IoT via Support Vector Machines and Long Short-Term Memory," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3889–3898, Mar. 2022, https://doi.org/10.1109/JIOT.2021.3101978.

[13] M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 407–436, Mar. 2022, https://doi.org/10.1109/JAS.2021.1004344.

[14] L. Nkenyereye, J. Hwang, Q.-V. Pham, and J. Song, "Virtual IoT Service Slice Functions for Multiaccess Edge Computing Platform," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11233–11248, Jul. 2021, https://doi.org/10.1109/JIOT.2021.3051652.

[15] S. Siddiqui *et al.*, "Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects," *IEEE Access*, vol. 10, pp. 70850–70901, 2022, https://doi.org/10.1109/ACCESS.2022.3188311.

[16] P. Franco, J. M. Martinez, Y. C. Kim, and M. A. Ahmed, "A Framework for IoT Based Appliance Recognition in Smart Homes," *IEEE Access*, vol. 9, pp. 133940–133960, 2021, https://doi.org/10.1109/ACCESS.2021.3116148.

[17] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions," *IEEE Access*, vol. 10, pp. 76805–76823, 2022, https://doi.org/10.1109/ACCESS.2022.3189998.

[18] A. Y. A. B. Ahmad, N. Verma, N. M. Sarhan, E. M. Awwad, A. Arora, and V. O. Nyangaresi, "An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model," *IEEE Access*, vol. 12, pp. 51752–51771, 2024, https://doi.org/10.1109/ACCESS.2024.3376605.

[19] O. G. Manzanilla-Salazar, F. Malandra, H. Mellah, C. Wette, and B. Sanso, "A Machine Learning Framework for Sleeping Cell Detection in a Smart-City IoT Telecommunications Infrastructure," *IEEE Access*, vol. 8, pp. 61213–61225, 2020, https://doi.org/10.1109/ACCESS.2020.2983383.

[20] N. K. Al-Shammari, T. H. Syed, and M. B. Syed, "An Edge – IoT Framework and Prototype based on Blockchain for Smart Healthcare Applications," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp. 7326–7331, Aug. 2021, https://doi.org/10.48084/etasr.4245.