STM JOURNALS

International Journal of
Satellite Remote Sensing

Volume 2, Issue 2, 2024
July–December
DOI (Journal): 10.37591/IJSRS

https://journals.stmjournals.com/ijsrs

Research IJSRS

Deep Learning Enhanced Compressive Sensing for Wireless IoT Data Optimization and Weather Monitoring

Hemant Rajoriya[1,*], Balajee Sharma[2]

Abstract

This research explores the application of deep learning and compressive sensing in order to optimize data traffic in non-orthogonal multiple access (NOMA)-based wireless internet of things (IoT) networks and weather monitoring. Such a framework would be very effective and overcome pilot attacks and reconstruction losses for secure data transmission. In this regard, a strong communication model has been adopted based on power-domain NOMA for simultaneous wireless transmission by multiple IoT devices. The system utilizes spreading codes based on advanced transformations to prevent collisions in signals. It uses a novel deep compressive sensing algorithm, which employs a combination of greedy reconstruction techniques, like CoSAMP, with deep learning to improve the accuracy with which signals are reconstructed. It ensures resilience against noise and pilot contamination attacks while it maintains very low latency and high accuracy in methodology. Simulations run on MATLAB confirm the model with substantial enhancements regarding mean square error (MSE) and root mean square error (RMSE) performances from various signal-to-noise ratios (SNRs) as well as compression ratios. This study introduces an improved compressive sensing framework for weather data acquisition, utilizing deep learning-driven reconstruction algorithms. The proposed method enhances the sampling process, minimizes the data needed for precise reconstruction, and boosts the efficiency of weather monitoring systems. Through comprehensive simulations and analysis of real-world data, the performance of the suggested approach is assessed, showing notable advancements in reconstruction precision and computational efficiency over traditional methods. These results suggest promising prospects for the development of scalable, real-time, and cost-effective weather monitoring solutions. Extensive scalability, robustness, and high potential to meet the stringent demands of next-generation IoT networks come out clearly in the results. Future research directions would span the model over multi-hop IoT environments, and blockchain-based security mechanisms would be integrated.

Keywords: Wireless internet of things (IoT), deep learning, compressive sensing, non-orthogonal multiple access (NOMA), pilot attack, signal reconstruction

*Author for Correspondence
Hemant Rajoriya
E-mail: hemantrajoriya25@gmail.com

[1,2]Assistant Professor, Department of Electronics and Telecommunication Engineering, Ram Krishna Dharmarth Foundation (RKDF) University, Bhopal, Madhya Pradesh, India

Received Date: November 23, 2024
Accepted Date: November 25, 2024
Published Date: December 05, 2024

Citation: Hemant Rajoriya, Balajee Sharma. Deep Learning Enhanced Compressive Sensing for Wireless IoT Data Optimization and Weather Monitoring. International Journal of Satellite Remote Sensing. 2024; 2(2): 20–36p.

INTRODUCTION

For the past decade, people in the world have dramatically increased their reliance on the internet in daily operations and corporate undertakings. This rise is attributed to the internet technology revolution (fiber and 5G connections), easy access through various devices, relatively competitive offered prices, and other services by the internet [1]. The International Telecommunication Union said in 2019 that there were 4.1 billion internet users worldwide, up more than 53% from 2005 and 5.3% from 2018. This has brought a heavy burden over internet service providers (ISPs) to find a solution for network traffic classification and identification of the causal application, protocol, or service to fulfill quality of service (QoS), content filtering, lawful interception, and malicious behavior identification objectives. Low latency is necessary for real-time applications like video conferencing and voice over internet protocol (VoIP) to distribute network traffic; other applications, including web browsing, are not. This is achieved by implementing QoS, where the flow of real-time applications' traffic is given higher priority for processing by the network nodes. Many regulations restrict the use of certain applications within a country's boundary and block the content accordingly. For instance, China banned the use of Skype back in 2013, citing its protocol did not comply with Chinese national regulations. In many countries, lawful interception is a requirement of the law where ISPs are, by the security authorities' mandate, required to provide the capability of lawful interception when needed by the local law enforcement agencies [2, 3].

Essentially, internet of things (IoT) is an extension of the concept where everyday things are powered with computing and Internet connectivity and can sense, compute, communicate, and control the surrounding environment. Such capabilities have been in demand because of potential impacts in various applications, ranging from streamlining and securing everyday life to making improvements and simplifications in current approaches. In fact, IoT creates a new perspective about what kind of data should be collected and how often, as well as from which location, so that information unavailable before could be achieved [4]. The proliferation of communication systems and networks, in the number of users, as well as the amount of generated traffic, presents network traffic monitoring and analysis (NTMA) with different daily challenges, such as: (1) traffic data storage and analysis; (2) use of traffic data for business objectives through insight, (3) traffic data integration, (4) validation of traffic data, (5) security traffic data, and (6) acquiring traffic data. The unprecedented increase in the number of connected nodes and the volume of data amplify the network complexity, calling for continuing studies to analyze and monitor the networking performance. In addition, the availability of such a massive and heterogeneous amount of traffic data calls for new approaches for monitoring and analyzing network management data. Due to these challenges, most of the works would focus on one aspect of NTMA, for instance, anomaly detection, traffic classification, or QoS [5].

A significant amount of geographically scattered and heterogeneous data is available in real time due to the variety of devices that continuously transmit data. In this context, therefore, there is a need for study and the design of database management techniques that take all such specificities of applications based on IoT into consideration. Data management has traditionally been a very wide concept that relates architectures, practices, and procedures for managing the requirements of the data lifecycle of systems. Data management in the context of the IoT should be a layer that sits between the devices and objects, where applications use the data for services and analysis. Using a typical database system would not be a better option because of the vast volume of data and its unique features. In fact, a number of concepts serve as the foundation for the design of IoT data management systems [6]. A number of data management strategies have been put forth based on these various tenets, such as IoT data schema support solutions, data storage and indexing solutions, and middleware-based IoT-oriented on data and sources. A middleware is provided between objects and data storage places via middleware-based IoT techniques. As a result, the middleware makes data stream routing easier. IoT data can be produced at a very fast rate, the quantity of the data can become incredibly big and diversified with many types of data. To mitigate these possible issues, data storage solutions put forward the idea for data storage environments that not only can efficiently store large amounts of IoT data but also integrate both structured and unstructured data, allowing the possibility of access through NoSQL queries. However, data indexing systems enable effective data discovery and search. While some of these systems use distributed indexing in dynamic IoT networks, others use hash tables with centralized indexing. Data volumes are diverse and schema definition support that allows for flexible schema will definitely ensure interoperability [7, 8].

LITERATURE REVIEW

Ji [9] studied that deep learning technologies have experienced tremendous growth due to their nonlinearity in recent years. Numerous advances in computer vision, natural language processing, and speech recognition were made possible by deep learning, which encouraged researchers in other domains to investigate the potential for implementing deep learning methods. In the fields of bioinformatics, medicine, material science, civil engineering, etc., a lot of work has been done and significant advancements have been seen. This is also seen in the computer network and communications field. Significant advancements have been made in the upper layers, such as the deployment of communication networks, as well as in the lower layers, such as coding and modulation methods. But because it is still in its infancy, there are still a lot of problems to be resolved and a lot of untapped potential. It specifically addresses the viability of applying deep learning techniques to increase the efficiency of next-generation communication and expand the range of radio frequency (RF) sensing.

The latest research on the deep learning-assisted non-orthogonal multiple access (NOMA) system was given by Andiappan and Ponnusamy [10]. We also demonstrate how deep learning is being used in various wireless technologies. NOMA has garnered significant interest in wireless communication as a crucial strategy for next-generation communication systems. Unlike orthogonal multiple access (OMA) approaches, NOMA allows users to send information at the same time and frequency, improving spectral efficiency. The fundamental components of a NOMA-assisted communication system are power allocation, channel estimation, and successive interference cancellation (SIC). In addition to making the system computationally simpler than the traditional method, deep learning has garnered attention recently as a solution to wireless communication issues. Their deep learning applications demonstrated further wireless technology.

Nelavallai et al. [11] addressed the key challenge of prolonging network lifespan without compromising performance by inventing the new paradigm of a deep reinforcement learning−enhanced particle swarm optimization (DRL-EPSO) model for the optimization of energy consumption within wireless sensor networks (WSNs). The work combined the global search ability of PSO with the adaptive learning capability of DRL to allow real-time dynamic optimization of operational parameters and energy consumption strategies in WSNs. The DRL-EPSO model resulted in a realistic increase in energy efficiency via simulations on a 500-node network, achieving 25% energy savings against standard PSO procedures and 40% energy savings compared to conventional DRL methods. The network's operating lifetime was increased by an average of 30% with a 15% improvement in latency and a proportionate increase in data transmission reliability under various climatic conditions. The application of DRL and PSO together for energy management in WSNs has been demonstrated in this work, offering a scalable and adaptable method that can significantly increase networks' sustainability and efficiency.

Srividhya et al. [12] proposed a novel method of applying deep learning to enhance the performance of radio communication channels. Our proposal is called the "Proposed Method" and uses complex neural network structures to model and improve features from the channel. They tested the performance of the proposed method relative to six well-known ones, namely, orthogonal matching pursuit, maximum likelihood estimation, least squares, compressive sensing, singular value decomposition and beamforming, to establish how well it may perform in practical application. This includes mean absolute error (MAE), signal-to-noise ratio (SNR), bit error rate (BER), computational complexity, and root mean squared error (RMSE) for rating how good something works. From the results, it was found that the Proposed Method is better as it models and estimates channels more correctly and has lower RMSE, MAE, BER, and MSE. The Proposed Method also has a higher SNR, which means the quality of the data is better. Plus, since it is simple to compute, it is a good answer for real-world problems.

Kumaram et al. [13] demonstrated a new approach that integrates DL for signal processing in wireless body area networks (WBANs) to better extraction and processing of signals. For better precision and reliability, DL models are used for extracting features and for classification of physiological signals. The proposed system allowed real-time processing and immediate medical response through smooth integration into existing WBAN frameworks. The comparative analysis shows improved performance metrics: 93% F1-score, 94% recall, 92% precision, and 95% accuracy obtain higher values compared to the 87%, 85%, 88%, and 86% values of the system in existence. In addition, the proposed system optimizes resource usage by increasing memory and central processing unit (CPU) utilization and reducing graphics processing unit (GPU) usage. All these results highlight potential used in transforming remote patient monitoring with increased diagnostic accuracy and resource economy.

Ma et al. [14] proposed two new views of applying deep learning to the R17 Type-II codebook for improvement, where the dominant angular-delay-domain port selection is effectively executed with deep learning, considering the low signal-to-noise ratio uplink channels and incorporating the focal loss to solve the class imbalance problem. In this work, they suggested using the sparse knowledge of the structures in the R17 Type-II codebook's feedback to leverage deep learning to rebuild the downlink channel state information (CSI) at the base station. A weighted shortcut module is created for that reason in order to support proper reconstruction. According to simulation results, the suggested approaches may outperform the deep learning benchmarks and the conventional R17 Type-II codebook in terms of sum rate performance.

Ballard et al. [15] talked about computational sensing with an emphasis on designing intelligent sensor systems. Acquisition gear was radically altered to 'lock-in' to the best sensing data in relation to a user-specified cost function or design constraint using inverse design and machine learning approaches. In order to create low-cost and compact sensor implementations that are developed through iterative analysis of data-driven sensing outcomes, they would conceptualize and design a new generation of computational sensing systems that both improve sensing capabilities and lessen the load of data. According to them, the methods discussed here will take center stage in the design of sensing hardware, radically changing and rightfully challenging conventional, intuition-guided sensor and readout designs in favor of implementations that are application-specific and possibly very counterintuitive. Therefore, machine learning-based computational sensors have the potential to create new, widely dispersed applications that will leverage "big data" analytics and the internet of things to build robust sensing networks. These applications will impact a variety of fields, including environmental sensing, global health, and biomedical diagnostics.

Kokila and Reddy [16] proposed a concept called BlockDLO, which is essentially IoT security based on blockchain technology integrated with deep learning. The five-phase edge computing blockchain architecture was proposed. In the first phase, chaotic map-based identification and authentication resolved network localization. In the second phase, page rank-based clustering was proposed for edge computing. Then, BlockDLO combined the shared-chain technique with a deep distributed file system to address concerns over block creation and ledger distribution, and an ethereum smart contract to address concerns relating to data security issues. The phase of optimization on the communication route was done by way of page rank centrality search optimization. Lastly, the integration of the deep learning model to detect malicious data on the IoT network was achieved via the use of the authenticated received data. BlockDLO is efficient due to intrusion detection by making a deep convolution neural network and blockchain combine. The proposed system was trained using public data sources and tested using an in-house network testbed. Utilizing energy, packet loss rate, end-to-end delay, routing overhead, network lifetime, accuracy, and security strength, the results showed that the suggested system performed better than existing work. A comparative analysis of recent research in deep learning applications for wireless communication and IoT is shown in Table 1.

OBJECTIVES

- To analyze the existing compressed sensing and reconstruction methodologies for wireless IoT network.
- To design a framework to improve the data transmission accuracy and reconstruction accuracy and to solve this optimization problem of reconstruction model that exploit some data structures such as sparsity in some transformation domains, low rank, etc.
- To support multi-data transmission simultaneously and reduce the losses during reconstruction of data.
- To mitigate the pilot attack and minimize the reconstruction error

Table 1. Comparative analysis of recent research in deep learning applications for wireless communication and internet of things (IoT).

Reference	Focus Area	Proposed Methodology	Key Metrics/Results	Advantages
[9]	Deep Learning (DL) in Communication	Exploration of DL for enhancing next-generation communication efficiency and radio frequency (RF) sensing.	Highlighted the potential of DL across physical and upper layers of communication systems.	Established the foundation for using DL in diverse communication layers.
[10]	DL in NOMA Systems	Applications of DL for Non-Orthogonal Multiple Access (NOMA) including SIC, channel estimation, and power allocation.	Improved spectral efficiency and computational simplicity compared to OMA.	Enhanced system design efficiency and spectral utilization.
[11]	Energy Optimization in Wireless Sensor Networks (WSNs)	Deep reinforcement learning (DRL)-enhanced particle swarm optimization (PSO) model for dynamic energy optimization.	25% reduction in energy consumption (vs. PSO), 40% (vs. DRL), 15% latency improvement, 30% increase in network life.	Efficient energy management and extended network lifespan.
[12]	Channel Performance Enhancement	Deep learning models for radio channel modeling and enhancement, compared with six baseline methods.	Achieved lower RMSE, MAE, BER, and MSE, with improved SNR and computational simplicity.	High-quality channel modeling with practical computational requirements.
[13]	DL in Wireless Body Area Networks (WBANs)	DL models for real-time processing and classification of physiological signals.	F1-score: 93%, Recall: 94%, Precision: 92%, Accuracy: 95%.	Improved diagnostic accuracy and resource optimization in WBANs.
[14]	DL for Codebook Design	DL methods for R17 Type-II codebook improvement, including focal loss and weighted shortcut modules.	Enhanced sum rate performance compared to traditional and DL benchmarks.	Superior performance in uplink and downlink CSI reconstruction.
[15]	Computational Sensing Design	Integration of machinle learning (ML) techniques in sensor hardware design for targeted data acquisition.	Reduced data burden and improved sensing capabilities.	Low-cost, compact sensors with broad applications in biomedical and environmental sensing.
[16]	IoT Security with Blockchain and DL	BlockDLO framework integrating blockchain with DL for IoT security using edge computing.	Superior energy usage, packet loss rate, end-to-end delay, network lifetime, and security metrics.	Robust and scalable intrusion detection with efficient communication route optimization.

THE TRANSFORMATIVE ROLE OF IOT IN WEATHER AND ENVIRONMENTAL MONITORING

The IoT has revolutionized the field of weather and environmental monitoring, enabling real-time data collection and analysis that enhances our understanding of climatic patterns and ecological changes. By interconnecting a wide array of smart sensors and devices, IoT allows for the continuous measurement of various atmospheric parameters such as temperature, humidity, air pressure, and wind speed. This granular data helps meteorologists and environmental scientists to achieve more accurate weather forecasts and to track environmental variables that could signify climate change or natural disasters.

Moreover, IoT-based solutions facilitate the deployment of networks of remote sensors in diverse locations, including urban areas, forests, and oceans. These networks can monitor pollution levels, assess water quality, and track wildlife movements, providing invaluable insights into the health of ecosystems. For instance, smart sensors can detect spikes in air pollutants, alerting authorities to take action and protect public health. In agriculture, IoT-enabled weather stations can inform farmers about local weather conditions, allowing them to optimize irrigation and crop management practices based on precise weather forecasts.

In addition to improving data collection, IoT technologies also enable predictive modeling and analytics. With vast amounts of real-time data at their disposal, researchers and decision-makers can employ advanced algorithms and machine learning techniques to identify trends and make informed predictions about environmental shifts. This proactive approach not only enhances preparedness for disasters such as hurricanes and floods but also aids in the design of more sustainable urban and agricultural systems. Ultimately, the integration of IoT in weather and environmental monitoring represents a significant advance in our capability to understand and respond to the complex challenges posed by our ever-changing environment.

In an era characterized by rapid technological advancement, the IoT stands as a pivotal innovation, reshaping various sectors, including weather and environmental monitoring. By seamlessly connecting a vast array of devices and sensors to the Internet, IoT has ushered in a new age of data collection, analysis, and communication, enabling more accurate and timely insights into weather phenomena and environmental changes.

The IoT refers to the network of interconnected devices that communicate and exchange data with one another, often autonomously. Sensors, actuators, and smart devices form the backbone of IoT, allowing for real-time data capture and analysis. In weather and environmental monitoring, IoT devices enable stakeholders—from scientists to policymakers—to gather critical information about atmospheric conditions, environmental health, and climate patterns over large geographical areas [17–40].

How Internet of Things Enhances Weather Monitoring

Data Collection and Accessibility

- Traditional weather monitoring often relied on fixed meteorological stations, which, while effective, could be sparse and limited in geographic coverage. IoT dramatically expands data collection capabilities through the deployment of low-cost, portable sensors that can be installed in diverse locations. These sensors gather metrics such as temperature, humidity, wind speed, and atmospheric pressure, transmitting data in real-time to cloud-based platforms for analysis. This proliferation of data not only enhances accuracy but also allows for better predictive modeling.

Real-time Monitoring and Alerts

- One of the most significant advantages of IoT in weather monitoring is the capacity for real-time data analysis. IoT-enabled systems can detect severe weather patterns such as storms, hurricanes, or floods, and send instant alerts to local communities and emergency services. By facilitating timely action, these systems potentially save lives and minimize property damage.

Improved Predictive Modeling

- IoT devices continuously gather and transmit environmental data, which can be analyzed using advanced algorithms and machine learning techniques. This ongoing input allows meteorologists to refine their predictive models, leading to more accurate weather forecasts. A more reliable forecast aids various sectors, including agriculture, aviation, and disaster management, allowing for informed decision-making.

Internet of Things in Environmental Monitoring

Pollution Tracking

- Environmental monitoring has become increasingly crucial as pollution levels rise in urban environments. IoT sensors can measure air quality by detecting pollutants such as particulate matter, nitrogen dioxide, and ozone. This data is invaluable for public health officials and urban planners, enabling them to take corrective measures and create policies that promote cleaner air and healthier communities.

Biodiversity and Ecosystem Monitoring

- IoT technologies can also play a critical role in preserving biodiversity. By deploying sensors in forests, wetlands, and oceans, researchers can monitor species populations, habitat conditions, and environmental changes over time. This information is vital for conservation efforts, allowing for targeted interventions and management strategies to protect endangered species and fragile ecosystems.

Water Quality and Resource Management

- Water scarcity is an ever-growing concern, and IoT helps tackle this challenge through real-time monitoring of water bodies. Sensors can measure parameters such as pH, temperature, turbidity, and contaminants in lakes, rivers, and reservoirs. This data enables timely responses to pollution events and helps manage freshwater resources more effectively.

Challenges and Considerations

- While the potential of IoT in weather and environmental monitoring is tremendous, challenges remain. Data security and privacy are paramount, as the vast amount of collected data can be susceptible to cyber threats. Moreover, there are concerns about the accuracy and reliability of inexpensive sensors, and the integration of disparate data sources can pose technical hurdles.
- Additionally, the digital divide remains a significant issue, particularly in developing countries where access to such technology can be limited. Ensuring equitable access to IoT resources and capabilities is crucial for maximizing the benefits of these innovations for all communities.

The integration of IoT technologies into weather and environmental monitoring marks a significant advancement in our ability to understand and respond to the complexities of our planet's systems. By leveraging real-time data and advanced analytical capabilities, IoT not only enhances predictive accuracy but also empowers decision-makers to take proactive measures in tackling environmental challenges. As we continue to innovate and overcome existing challenges, IoT promises to play a vital role in shaping a sustainable future, one sensor at a time.

THE ROLE OF DATA OPTIMIZATION IN IOT APPLICATIONS FOR WEATHER AND ENVIRONMENTAL MONITORING

In an era driven by rapid technological advancements, the IoT has emerged as a transformative force across various sectors, including environmental sciences and meteorology. As climate concerns and environmental changes escalate, the need for accurate and timely data monitoring has never been more critical. IoT applications play a pivotal role in weather and environmental monitoring, where data optimization becomes essential for enhancing performance and decision-making.

IoT refers to a network of interconnected devices that communicate and share data collected from their surroundings. In weather and environmental monitoring, IoT allows for the deployment of various sensors, such as temperature gauges, humidity sensors, air quality monitors, and precipitation meters, across diverse geographic locations. These sensors collect real-time data, which is then transmitted to centralized systems for analysis.

The continuous flow of data from numerous sources increases the volume and variety of information, which, if not managed properly, can lead to overwhelming inefficiencies. This is where data optimization comes into play, ensuring that the vast quantities of data generated are processed, analyzed, and utilized in the most effective manner possible.

THE IMPORTANCE OF DATA OPTIMIZATION

Enhanced Data Quality

Data optimization ensures that the quality of the data collected is high, which is crucial for making reliable forecasts and decisions. Techniques such as data cleansing remove inaccuracies and redundancies, allowing only the most relevant and accurate information to inform weather predictions and environmental assessments. High-quality data leads to better models and more precise predictions, thus enhancing operational efficiency.

Real-Time Insights and Faster Decision-Making

IoT applications discharge an enormous volume of data every second. To make swift and impactful decisions—be it for disaster management, agricultural planning, or climate research—data optimization techniques such as edge computing can be employed. By processing data closer to where it is generated, the latency is minimized, and insights can be drawn in real time. This prompt analysis is crucial for effectively responding to natural disasters, monitoring climate patterns, and optimizing resource management.

Efficient Resource Utilization

Optimizing data can lead to significant savings in bandwidth, storage, and processing capabilities. By employing techniques like data compression and prioritization, non-essential information can be filtered out, ensuring that only critical data is transmitted and stored. This not only reduces costs but also minimizes the environmental impact associated with data storage and transmission.

Scalability and Flexibility

As environmental monitoring demands grow, IoT systems must scale effectively. Data optimization frameworks facilitate the integration of new sensors and data sources, thus ensuring that the system can adapt to increased data influx without compromising performance. Predictive analytics, powered by machine learning, can also be utilized to forecast future data requirements, allowing for proactive scaling.

Despite its numerous benefits, achieving effective data optimization in IoT applications comes with its challenges:

- *Data security and privacy*: The more data is collected and transmitted, the higher the risk of breaches. Ensuring data security while optimizing data flow is an ongoing concern that must be addressed.
- *Interoperability*: With a diverse array of devices and protocols, ensuring that different IoT systems work effectively together poses a significant hurdle.
- *Cost of implementation:* The upfront investment in advanced systems for data processing, storage, and analytics can be substantial, particularly for smaller entities.

As climate change issues become more pressing, the demand for robust IoT solutions in weather and environmental monitoring will only escalate. Future innovations in data optimization, such as artificial intelligence (AI)-driven anomaly detection, predictive maintenance for IoT devices, and advanced data analytics algorithms, will bolster the capabilities of IoT applications in these fields.

Moreover, with the integration of edge intelligence and the development of federated learning models, data can be analyzed while still preserving user privacy and enhancing security—addressing two of the most significant challenges currently faced.

In conclusion, data optimization plays a crucial role in enhancing the efficiency and efficacy of IoT applications for weather and environmental monitoring. By improving data quality, enabling real-time insights, optimizing resource utilization, and ensuring scalability, data optimization not only enhances predictive accuracy but also supports better decision-making in addressing environmental challenges. As technology continues to evolve, the role of data optimization in IoT applications will remain integral to fostering sustainable practices and resiliency against the impacts of climate change [41–60].

METHODOLOGY

A thorough framework in the section is defined to mitigate the reconstruction losses and pilots' attacks in NOMA-IoT networks. In a multi-antenna network, having adequate computational resources, the proposed system model uses power-domain NOMA techniques to ensure effective communication among the IoT devices and the base station (BS). In channel estimation, superimposed pilot signals carrying unique information from IoT users are transmitted to the BS. The BS then processes these signals to estimate individual user channels and facilitate communication. However, the system is vulnerable to pilot contamination attacks where malicious entities manipulate the pilot sequences to disrupt the channel estimation process. These attackers impersonate other users by changing or mimicking pilot signals and hence subvert the integrity of compressive sensing systems to compromise secure communication.

To counter these issues, the communication model uses a spreading code matrix obtained from the strong process of generation, such as a generation of Gaussian random vector, circulant shifting, and Bernoulli transformation to produce different spreading codes for legitimate IoT users, resulting in low collision probability chances. A greedy approach-based DeepCS algorithm is introduced for signal reconstruction and attack detection. It combines the CoSAMP algorithm for iterative reconstruction of signals with a deep learning network to improve performance. CoSAMP iteratively selects the largest projections and refines the signal estimate based on least squares, then produces a sparse signal that becomes the target for training the network. The compressed measurements are mapped to the reconstructed signal by a separately trained deep network that guarantees efficient and secure communication under the NOMA-IoT framework. NOMA-IoT System Data Secure Communication and Reconstruction Process: The process starts by initializing the channel parameters and the sensing matrix, followed by the data communication process via the channel. Subsequently, compression of data and data collection occur, along with addressing potential attacks in the system. Using that model, deep learning is used on data reconstruction; the process is completed by ensuring a reconstruction error assessment for performance analysis as shown in Figure 1.

RESULTS AND DISCUSSION

This section describes the system setup and tools used for performance evaluation of the proposed methodology. The system is set up with a system configuration of 16 GB RAM, 1 TB HDD, and a Windows 64-bit operating system, with MATLAB being used as the primary software tool. MATLAB is versatile. Known for its versatility, MATLAB provides a robust platform for technical simulations and mathematical computations. Its wide range of features with object-oriented programming, debugging tools, and predefined functions coupled with a vast array of specialized toolboxes make it ideal for conducting this research. The various apps integrated into MATLAB, those focused on control systems, neural networks, signal processing, and optimization among others, enhance its usability with efficient implementation and analysis of the NOMA-IoT framework. The result analysis is obtained by running a simulation on the MATLAB platform. Two result analysis is carried out, that is, on the basis of a lossy environment and on the basis of a variable compression ratio.

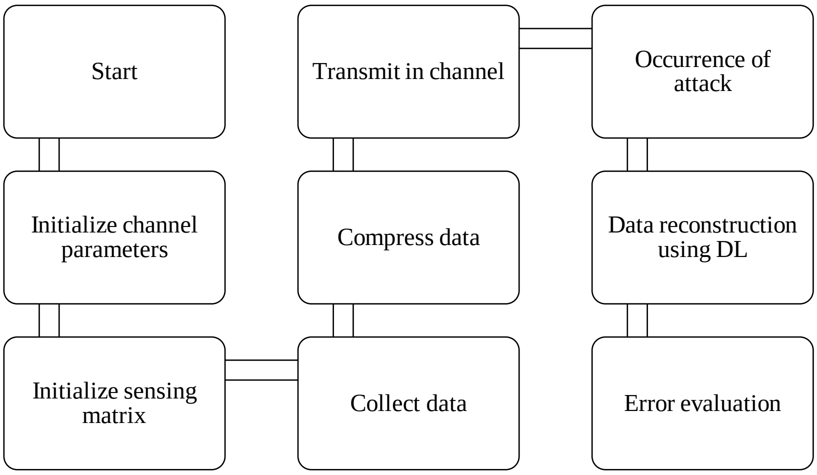

Figure 1. Flowchart of working.

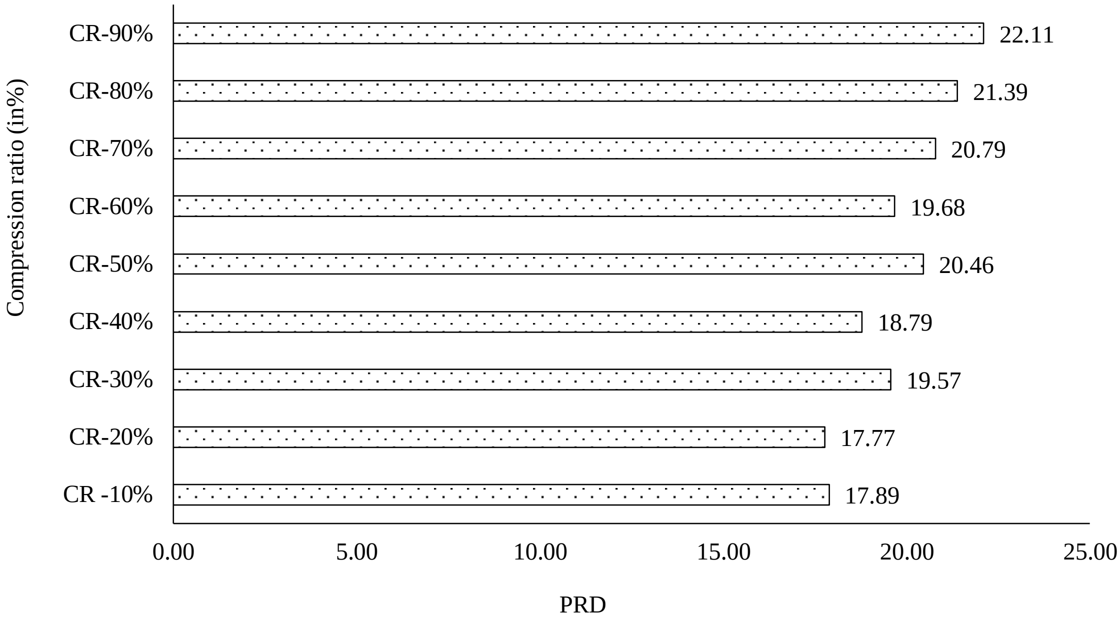

Figure 2. Percentage root mean square difference (PRD) analysis with respect to compression ratio.

Figure 2 shows the percentage root mean square difference (PRD) analysis with respect to compression ratio where PRD values are 17.89, 17.77, 19.57, 18.79, 20.46, 19.68, 20.79, 21.39, and 22.11 with compression ratio 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, respectively. Figure 3 shows the MSE analysis with respect to compression ratio where MSE values are -38.09, -34.59, -33.97, -35.16, -33.57, -33.81, -34.88, -34.40, and -34.31 with compression ratio 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, respectively.

Figure 4 shows the performance comparison of various algorithms (Deep Code Search (DeepCS), Open Multi-Processing (OMP), Back Propagation (BP), Compressive Sampling Matching Pursuit (CoSAMP), Iteratively Reweighted Least Squares (IRLS), Least Mean Squares (LMS), and Normalized Least-Mean-Square (NLMS)) in terms of the metric for different SNRs (SNR: 10 dB, 20 dB, and 30 dB). The y-axis indicates the respective values of metrics, with better performance typically at higher values. DeepCS always performs far better, and the variations are much smaller at each SNR level compared to the traditional methods LMS and NLMS, which have large spikes. This pattern indicates how robust DeepCS is compared to its counterparts LMS and NLMS at higher SNRs, where the performance of LMS and NLMS degrade.

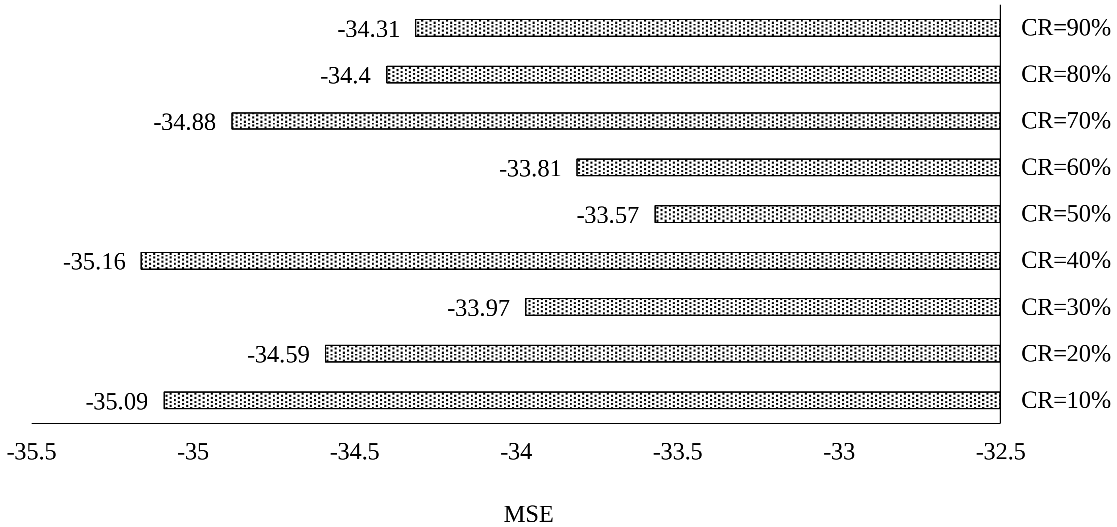

Figure 3. MSE analysis with respect to compression ratio.

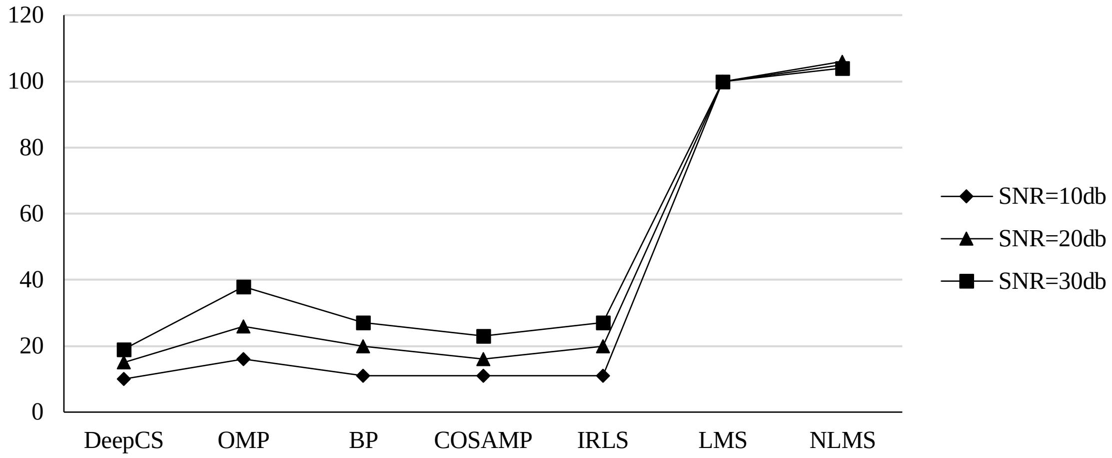

Figure 4. Comparison of percentage root mean square difference (PRD) with state-of-art models.

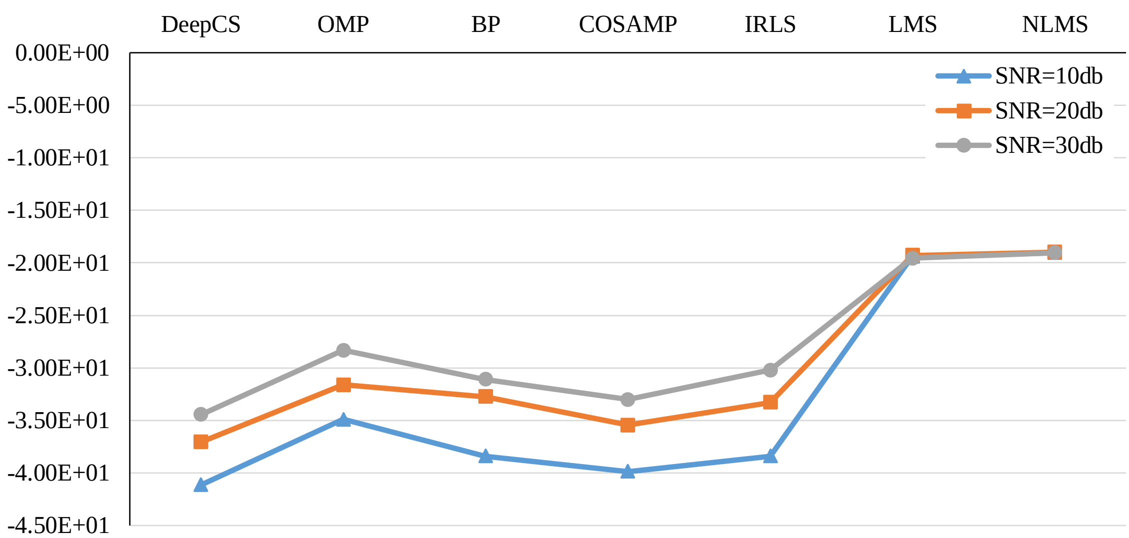

Figure 5. Comparison of meas square error (MSE) with state-of art models.

Figure 5 compares the performance of different algorithms like DeepCS, OMP, BP, CoSAMP, IRLS, LMS, and NLMS at three different SNR conditions: 10 dB, 20 dB, and 30 dB. In the plot, y-axis represents one form of the performance metric in which lower values represent poor performance. DeepCS always demonstrates superior performance with less error levels compared to others at every stage of SNR conditions. Traditional algorithms, such as LMS and NLMS, make more significant errors and under low SNR, which proves noisy. The pattern is indicative of DeepCS's performance, which does not yield to noise and is worthy of reconstruction for the signal.

Figure 6 plots the reconstruction MSE under two different scenarios: with attack and without attack, for compression ratios ranging from 10% to 90% across different bars as blue and red, respectively. It shows that MSE is always higher in the presence of attacks, with a difference mostly notable at higher compression ratios, such as CR = 90%, where MSE with attack reaches 6.072 compared to 4.855 MSE without attack. As the CR drops, the difference in MSE in both scenarios decreases, showing that lower compression ratios are less sensitive to attacks. This means that strong defense mechanisms must be in place to counter this attack, especially since reconstruction errors are largest at higher compression levels.

Figure 7 shows the RMSE for data reconstruction under two conditions: with attack in blue bars, and without attack in red bars, at compression ratios (CRs) ranging from 10% to 90%. The differences between these two cases clearly show that higher values of RMSE occur when there are attacks, meaning their reconstruction accuracy degraded. For CR = 90%, the difference is the most extreme, with RMSE values of 2.464 and 2.203 for the two scenarios, respectively. When the CR takes on smaller values, the RMSE difference between the two scenarios diminishes, and the performance of the two scenarios approaches equality at low CR levels; for example, at CR = 10%. These results highlight the effects of attacks on reconstruction accuracy, especially when the compression level increases, and point to the particular need for secure reconstruction mechanisms to ensure reconstruction accuracy.

Table 2 shows the MSE result for two different image compression algorithms: DeepCS and L&S, at varying SNR levels. In general, it suggests that lower MSE means better image quality after compression. So, from this table, we can find that L&S makes better performance than the DeepCS algorithm on low SNR values: 10 dB and 20 dB. Meanwhile, the DeepCS outperforms L&S at high SNR value: 30dB. However, it is worth noting that the power of these algorithms may depend on so many parameters; and other performance measures aside from MSE are also to be taken into consideration.

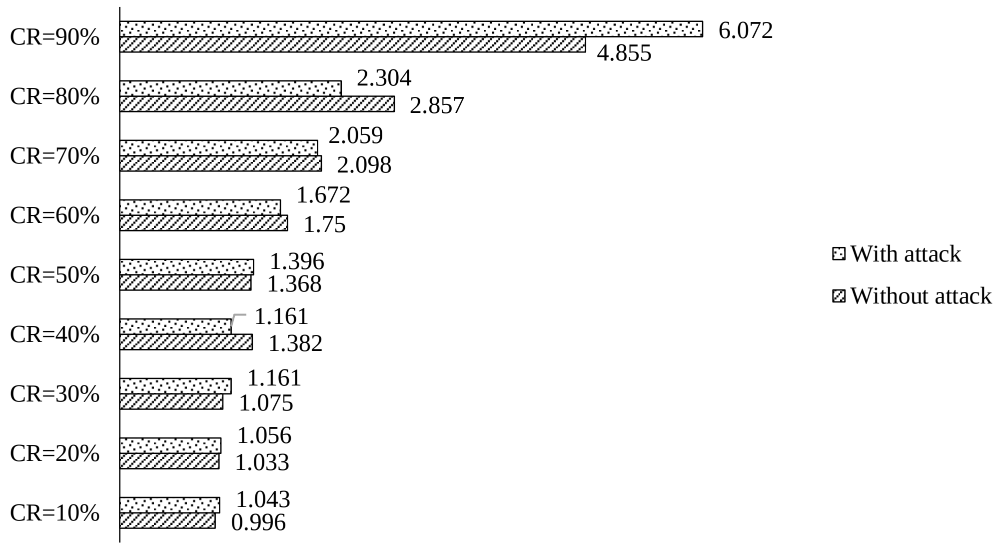

Figure 6. Reconstruction mean square error (MSE) comparison with and without attack.

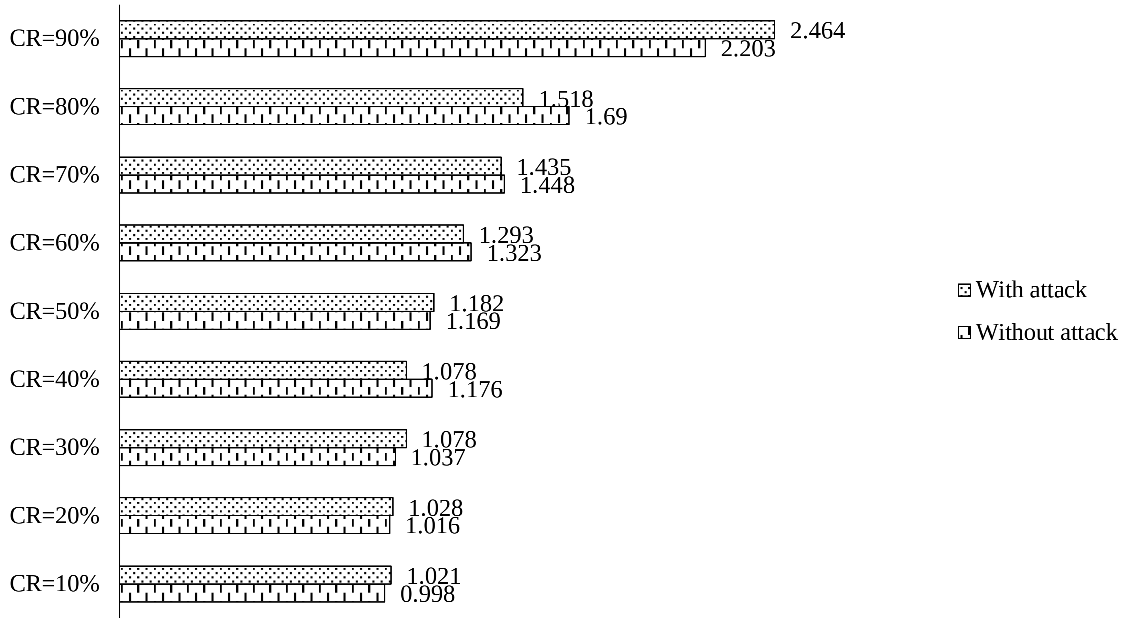

Figure 7. Reconstruction root mean square error (RMSE) comparison with and without attack.

Table 2. Comparative state-of-art.

Mean squared error (MSE)	Deep Code Search (DeepCS)	L&S [105]
SNR = 10 dB	-41	-7
SNR = 20 dB	-37	-14
SNR = 30 dB	-34	-18

The MATLAB results of compressive sensing analysis and reconstruction algorithms across various scenarios in a lossy IoT scenario evince quite a number of trends. From the results obtained, for the varying SNR, it is clear that an increase in SNR is indicated by the high values of PRD but lower MSE values across the scenarios. For various compression ratios, both PRD and MSE typically rise with the increase of the compression ratio, thus showing that the quality of the data decreases as compressions become higher. The results are consistent in many applications like massive IoT with multi-data transmission as well as under pilot attack with different strengths. With cases having different numbers of IoT devices, larger number of devices leads to higher MSE and also larger RMSE.

CONCLUSION

This paper presents a novel framework that unifies deep learning with compressive sensing to address key challenges in Wireless IoT, specifically focusing on NOMA systems. The main contributions have been to ameliorate the pilot attack issue, reduce reconstruction losses, and increase data transmission efficiency along with security. The proposed framework utilizes power domain NOMA for co-channel data transmission and generates unique spreading codes based on advanced mathematical transformations to avoid overlapping signals. A novel DeepCS algorithm has been introduced, which combines the strengths of both CoSAMP greedy approaches and deep learning models to achieve efficient signal reconstruction. To validate the proposed framework, simulations are performed with MATLAB under various scenarios such as varying SNR and compression ratio. The MSE values and the results of RMSE have greatly improved over traditional algorithms like LMS and NLMS. The system also shows robustness against noise and pilot attacks, which justifies its use for safe communication of IoT networks. Higher compression ratios and complex attack scenarios further justify the importance of the proposed framework in terms of data integrity and reconstruction errors. The framework's scalability and viability for IoT applications are demonstrated in this paper. Future work will be on extending the model to multi-hop communication scenarios, carrying out dynamic attack simulations, and further integrating blockchain technologies for enhanced security. All these advancements further solidify the framework as a scalable and robust solution in optimizing data traffic in diverse and evolving IoT ecosystems. In conclusion, data optimization plays a crucial role in enhancing the efficiency and efficacy of IoT applications for weather and environmental monitoring. By improving data quality, enabling real-time insights, optimizing resource utilization, and ensuring scalability, data optimization not only enhances predictive accuracy but also supports better decision-making in addressing environmental challenges. As technology continues to evolve, the role of data optimization in IoT applications will remain integral to fostering sustainable practices and resiliency against the impacts of climate change.

REFERENCES

1. Al Neyadi E, Al Shehhi S, Al Shehhi A, Al Hashimi N, Mohammad QH, Alrabaee S. Discovering public Wi-Fi vulnerabilities using Raspberry Pi and Kali Linux. In: 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC), Dubai, UAE, April 15–16, 2020. pp. 1–4.
2. AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo KKR. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers Security. 2022; 119: 102754.
3. Azab A, Khasawneh M, Alrabaee S, Choo KKR, Sarsour M. Network traffic classification: techniques, datasets, and challenges. Digital Commun Netw. 2024; 10 (3): 676–692.
4. Pekar A, Mocnej J, Seah WK, Zolotova I. Application domain-based overview of IoT network traffic characteristics. ACM Comput Surv.. 2020; 53 (4): 1–33.
5. Abbasi M, Shahraki A, Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): a survey. Computer Commun. 2021; 170: 19–41.
6. Kuthadi VM, Selvaraj R, Baskar S, Shakeel PM, Ranjan A. Optimized energy management model on data distributing framework of wireless sensor network in IoT system. Wireless Pers Commun. 2022; 127 (2): 1377–1403.
7. Azad P, Navimipour NJ, Rahmani AM, Sharifi A. The role of structured and unstructured data managing mechanisms in the internet of things. Cluster Comput. 2020; 23: 1185–1198.
8. Diène B, Rodrigues JJ, Diallo O, Ndoye EHM, Korotaev VV. Data management techniques for internet of things. Mech Syst Signal Process. 2020; 138: 106564.
9. Ji S. Empowering Wireless Communications and Sensing with Deep Learning Technology. Doctoral Thesis. Singapore: Nanyang Technological University; 2023.
10. Andiappan V, Ponnusamy V. Deep learning enhanced NOMA system: a survey on future scope and challenges. Wireless Pers Commun. 2022; 123 (1): 839–877.
11. Nelavalli S, Rammohan Reddy D, Neelima G, Rao SS. Balancing energy efficiency with robust security in wireless sensor networks using deep reinforcement learning-enhanced particle swarm optimization. Telecommun Radio Eng. 2025; 84 (1): 9–26.
12. Srividhya C, Sapthami I, Nagpal A, Pachauri P, Chandrashekar R, Jabbar AsAAZ. Deep learning techniques for enhancing near-field spatially varying channels in wireless communications. In: 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, May 9–11, 2024. pp. 1190–1195.
13. Kumaran S, Samyuktha PM, Bhavyashree MR. Deep learning enhanced signal processing techniques for WBAN-enabled telemedicine applications. In: 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, July 10–12, 2024. 1010–1015.
14. Ma K, Sang Y, Ming Y, Lian J, Tian C, Wang Z. Improving the performance of R17 Type-II codebook with deep learning. In GLOBECOM 2023 – 2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, December 4–8, 2023. pp. 4823–4828.

15. Ballard Z, Brown C, Madni AM, Ozcan A. Machine learning and computation-enabled intelligent sensor design. Nat Mach Intell. 2021; 3 (7): 556–565.
16. Kokila M, Reddy KS. BlockDLO: blockchain computing with deep learning orchestration for secure data communication in IoT environment. IEEE Access. 2024; 12: 134521–134540.
17. Liyakat KKS. Machine learning approach using artificial neural networks to detect malicious nodes in IoT networks. In: Udgata SK, Sethi S, Gao XZ, editors. Intelligent Systems. ICMIB 2023. Lecture Notes in Networks and Systems, Volume 728. Singapore: Springer; 2024. pp. 123–134. doi: 10.1007/978-981-99-3932-9_12.
18. Respati MA, Lee BM. A survey on machine learning enhanced integrated sensing and communication systems: architectures, algorithms, and applications. IEEE Access. 2024; 12: 170946–170964.
19. Srividhya C, Sapthami I, Nagpal A, Pachauri P, Chandrashekar R. Deep learning techniques for enhancing near-field spatially varying channels in wireless communications. In: 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, May 9–11, 2024. pp. 1190–1195.
20. Kasat K, Shaikh N, Rayabharapu VK, Nayak M. Implementation and recognition of waste management system with mobility solution in smart cities using internet of things. In: 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), August 23–25, Trichy, India, 2023. pp. 1661–1665. doi: 10.1109/ICAISS58487.2023.10250690.
21. Gong L, Chen Y. Machine learning-enhanced loT and wireless sensor networks for predictive analysis and maintenance in wind turbine systems. Int J Intell Netw. 2024; 5: 133–144.
22. Nelavalli S, Rammohan Reddy D, Neelima G, Rao SS. Balancing energy efficiency with robust security in wireless sensor networks using deep reinforcement learning-enhanced particle swarm optimization. Telecommun Radio Eng. 2025; 84 (1): 9–26.
23. Sui R, Baggard J. Wireless sensor network for monitoring soil moisture and weather conditions. Appl Eng Agric. 2015; 31 (2): 193–200.
24. Ma RH, Wang YH, Lee CY. Wireless remote weather monitoring system based on MEMS technologies. Sensors. 2011; 11 (3): 2715–2727.
25. Liyakat KKS, Magadum PK. Machine learning for predicting wind turbine output power in wind energy conversion systems. Grenze Int J Eng Technol. 2024; January: 2074–2080. 15th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2024, 2024.
26. Mabrouki J, Azrour M, Dhiba D, Farhaoui Y, El Hajjaji S. IoT-based data logger for weather monitoring using Arduino-based wireless sensor networks with remote graphical application and alerts. Big Data Mining Analytics. 2021; 4 (1): 25–32.
27. Sose DV, Sayyad AD. Weather monitoring station: a review. Int J Eng Res Appl. 2016; 6 (6): 55–60.
28. Subashini MJ, Sudarmani R, Gobika S, Varshini R. Development of smart flood monitoring and early warning system using weather forecasting data and wireless sensor networks – a review. In: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, February 4–6, 2021. pp. 132–135.
29. Veena C, Sridevi M, Liyakat KKS, Saha B, Reddy SR, Shirisha N. HEECCNB: an efficient IoT-cloud architecture for secure patient data transmission and accurate disease prediction in healthcare systems. In: 2023 Seventh International Conference on Image Information Processing (ICIIP), Solan, India, November 22–24, 2023. pp. 407–410, doi: 10.1109/ICIIP61524.2023.10537627.
30. Chandana LS, Sekhar AR. Weather monitoring using wireless sensor networks based on IOT. Int J Sci Res Sci Technol. 2018; 4: 525–531.
31. Devaraju JT, Suhas KR, Mohana HK, Patil VA. Wireless portable microcontroller based weather monitoring station. Measurement. 2015; 76: 189–200.
32. Kazi K. Machine learning (ML)-based Braille lippi characters and numbers detection and announcement system for blind children in learning. In Sart G, editor. Social Reflections of Human-Computer Interaction in Education, Management, and Economics. Hershey, PA, USA: IGI Global; 2024. pp. 16–39. doi: 10.4018/979-8-3693-3033-3.ch002.

33. Kazi KS. Artificial intelligence (AI)-driven IoT (AIIoT)-based agriculture automation. In: Satapathy S, Muduli K, editors. Advanced Computational Methods for Agri-Business Sustainability. Hershey, PA, USA: IGI Global. pp. 72–94. doi: 10.4018/979-8-3693-3583-3.ch005.
34. Konnur RG. Vehicle health monitoring system (VHMS) by employing IoT and sensors. Grenze Int J Eng Technol. 2024; June: 5367–5374. 15th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2024.
35. Wang L, Chen Z, Zou H, Huang D, Pan Y, Cheang CF, Li J. A deep learning-based high-temperature overtime working alert system for smart cities with multi-sensor data. Nondestruct Testing Eval. 2024; 39 (1): 164–184.
36. Renugadevi K, Jayasankar T, Selvi JA. Cloud-based digital twinning for structural health monitoring using deep learning. In Tyagi AK, editor. Artificial Intelligence-Enabled Blockchain Technology and Digital Twin for Smart Hospitals. New York, NY, USA: Wiley; 2024. pp. 309–325.
37. Liyakat KKS. Explainable AI in healthcare. In: Kamaraj AA, editor. Explainable Artificial Intelligence in Healthcare Systems. Hauppauge, NY, USA: Nova Science; 2024. pp. 271–284.
38. Revathi S, Ansari A, Susmi SJ, Madhavi M, Gunavathie MA, Sudhakar M. Integrating machine learning-IoT technologies integration for building sustainable digital ecosystems. In: Kajla T, Kansra P, Singh N, editors. Multidisciplinary Applications of Extended Reality for Human Experience. Hershey, PA, USA: IGI Global; 2024. pp. 259–291.
39. Rahman MH, Sejan MA, Aziz MA, You YH, Song HK. HyDNN: a hybrid deep learning framework based multiuser uplink channel estimation and signal detection for NOMA-OFDM system. IEEE Access. 2023; 11: 66742–66755.
40. Abdel-Basset M, Hawash H, Chang V, Chakrabortty RK, Ryan M. Deep learning for heterogeneous human activity recognition in complex IoT applications. IEEE Internet of Things J. 2020; 9 (8): 5653–5665.
41. Cohen SN, Leeds MP. The moonlighting dilemma: balancing education, service, and quality care while limiting risk exposure. JAMA. 1989 Jul 28;262(4):529–31.
42. Liyakat KK. Heart health monitoring using IoT and machine learning methods. In: Shaik A, editor. AI-Powered Advances in Pharmacology. Hershey, PA, USA: IGI Global; 2025. pp. 257–282. doi: org/10.4018/979-8-3693-3212-2.ch010.
43. Hussain M, O'Nils M, Lundgren J, Mousavirad SJ. A comprehensive review on deep learning-based data fusion. IEEE Access. 2024; 12: 180093–180124.
44. Kazi KS. AI-driven-IoT (AIIoT)-based decision making in drones for climate change: KSK approach. Aouadni S, Aouadni I, editors. Recent Theories and Applications for Multi-Criteria Decision-Making. Hershey, PA: IGI Global; 2025. pp. 311–340. doi: 10.4018/979-8-3693-6502-1.ch011.
45. Bourechak A, Zedadra O, Kouahla MN, Guerrieri A, Seridi H, Fortino G. At the confluence of artificial intelligence and edge computing in IoT-based applications: a review and new perspectives. Sensors. 2023; 23 (3): 1639.
46. Gao X, Xing F, Hang X, Guo F, Wen J, Sun W, Song H, Wang ZL, Chen B. Scalable-produced micro-elastic triboelectric sensing ground for all-weather large-scale applications. Chem Eng J. 2024; 493: 152645.
47. Salau BA, Rawal A, Rawat DB. Recent advances in artificial intelligence for wireless internet of things and cyber–physical systems: a comprehensive survey. IEEE Internet of Things J. 2022; 9 (15): 12916–12930.
48. Abdel-Basset M, Chang V, Hawash H, Chakrabortty RK, Ryan M. Deep learning approaches for human-centered IoT applications in smart indoor environments: a contemporary survey. Ann Oper Res. 2021; 339: 3–51.
49. Shwetabh K, Pathrotkar N. Solar energy forecast for integration of grid and balancing power using profound learning. E3S Web Conferences. 2024; 540: 10025.

50. Yu J, Chen J, Wan H, Zhou Z, Cao Y, Huang Z, Li Y, Wu B, Yao B. SARGap: a full-link general decoupling automatic pruning algorithm for deep learning-based SAR target detectors. IEEE Trans Geosci Remote Sensing. 2024; 62: Article 5202718.
51. Liyakat KKS. Malicious node detection in IoT networks using artificial neural networks. In: Singh VK, Sagar AK, Nand P, Astya R, Kaiwartya O, editors. Intelligent Networks: Techniques and Applications. Boca Raton, FL, USA: CRC Press; 2024. pp. 182–197.
52. Gopalakrishnan K, Adhikari A, Pallipamu N, Singh M, Nusrat T, Gaddam S, Samaddar P, Rajagopal A, Cherukuri AS, Yadav A, Manga SS. Applications of microwaves in medicine leveraging artificial intelligence: future perspectives. Electronics. 2023; 12 (5): 1101.
53. Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Poor HV. Federated learning for internet of things: a comprehensive survey. IEEE Commun Surv Tutorials. 2021; 23 (3): 1622–1658.
54. Liu R, Shi J, Chen X, Lu C. Network anomaly detection and security defense technology based on machine learning: A review. Computers and Electrical Engineering. 2024 Oct 1;119:109581.
55. Miao Y, Bai X, Cao Y, Liu Y, Dai F, Wang F, Qi L, Dou W. A novel short-term traffic prediction model based on SVD and ARIMA with blockchain in industrial internet of things. IEEE Internet Things J. 2023; 10 (24): 21217–21226.
56. Boddu RSK, Chandan RR, Thamizharasi M, Shaikh R, Goyal AA, Gupta PP, Gupta SK. Using deep learning to address the security issue in intelligent transportation systems. J Auton Intell. 2024; 7 (4): 1–13.
57. Lopukhova E, Abdulnagimov A, Voronkov G, Grakhova E. Machine learning-driven calibration of traffic models based on a real-time video analysis. Appl Sci. 2024; 14 (11): 4864.
58. Liyakat KKS. AI-powered-IoT (AIIoT) based decision making system for BP-patient healthcare monitoring: bp-patient health monitoring using KSK approach. In: Lytras M, Alajlan S, editors. Transforming Pharmaceutical Research with Artificial Intelligence. Hershey, PA, USA: IGI Global; 2025: 205–238.
59. Darwish H, Darwish W, Darwish H, AlHmoud IW, Alshraideh O. Artificial intelligence, machine learning, and deep learning applications in the engineering fields – a comprehensive review. Sigma J Eng Nat Sci. 2024; 42(6): 00126.
60. Liyakat KKS. KK approach to increase resilience in internet of things: a T-cell security concept. Darwish D, Charan K, editors. Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions. Hershey, PA, USA: IGI Global; 2025: 87–120.

