IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 November 2023, accepted 7 January 2024, date of publication 17 January 2024, date of current version 26 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3355312

TOPICAL REVIEW

Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review

YAZEED YASIN GHADI[1], **TEHSEEN MAZHAR**[2], **TAMARA AL SHLOUL**[3], **TARIQ SHAHZAD**[4], **UMAIR AHMAD SALARIA**[5,6], **ARFAN AHMED**[7], **AND HABIB HAMAM**[8,9,10,11], **(Senior Member, IEEE)**

[1]Department of Computer Science and Software Engineering, Al Ain University, Abu Dhabi, United Arab Emirates
[2]Department of Computer Science, School Education Department, Government of Punjab, Layyah 31200, Pakistan
[3]Department of General Education, Liwa College of Technology, Abu Dhabi 15222, United Arab Emirates
[4]Department of Computer Sciences, COMSATS University Islamabad, Sahiwal Campus, Sahiwal 57000, Pakistan
[5]Department of Electrical Engineering, Mirpur University of Science and Technology, Mirpur, Azad Kashmir 10250, Pakistan
[6]Department of Electrical Engineering, The University of Azad Jammu and Kashmir, Muzaffarabad, Azad Kashmir 13100, Pakistan
[7]AI Centre for Precision Health, Weill Cornell Medicine—Qatar, Doha, Qatar
[8]Faculty of Engineering, University of Moncton, Moncton, NB E1A 3E9, Canada
[9]International Institute of Technology and Management, Commune d'Akanda, Libreville 1989, Gabon
[10]Bridges for Academic Excellence, Centre Ville, Tunis, Tunisia
[11]School of Electrical Engineering, Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa

Corresponding authors: Arfan Ahmed (ara4013@qatar-med.cornell.edu) and Tehseen Mazhar (tehseenmazhar719@gmail.com)

This research work is supported by the Qatar National Library.

ABSTRACT Energy efficiency and safety are two essential factors that play a significant role in operating a wireless sensor network. However, it is claimed that these two factors are naturally conflicting. The level of electrical consumption required by a security system is directly proportional to its degree of complexity. Wireless sensor networks require additional security measures above the capabilities of conventional network security protocols, such as encryption and key management. The potential application of machine learning techniques to address network security concerns is frequently discussed. These devices will have complete artificial intelligence capabilities, enabling them to understand their environment and respond. During the training phase, machine-learning systems may face challenges due to the large amount of data required and the complex nature of the training procedure. The main objective of the article is to know about different machine learning algorithms that are used to solve the security issues of wireless sensor networks. This study also focuses on the use of wireless sensor networks in different fields. Furthermore, this study also focuses on different Machine learning algorithms that are used to secure wireless sensor networks. Moreover, this study also addresses issues of adapting machine learning algorithms to accommodate the sensors' functionalities in the network configuration. Furthermore, this article also focuses on open issues in this field that must be solved.

INDEX TERMS Wireless sensor networks, machine learning, WSNs security, LoWPAN, IoT.

I. INTRODUCTION

As new standards are developed or executed to enhance the adaptability of WSNs in various operational contexts, the administration of WSNs may become more accessible. WSNs must cope with two significant challenges, security and energy consumption, continuously enhancing each other. As the level of security of WNS increases or decreases, the system's energy requirements also increase accordingly. Recent studies in this domain aim to enhance the security and energy efficiency of WSNs, as there is a possible requirement for their operation in challenging environments. Due to the extensive use of WSNs enabling sensitive data, such as environmental information, surveillance data, and health indicators, it is essential to prioritize implementing robust security measures. To safeguard sensitive

The associate editor coordinating the review of this manuscript and approving it for publication was Zhangbing Zhou.

data and infrastructure, it is necessary to uphold the three fundamental security pillars of the CIA [1]. In light of the rapid progress of technology and the development of novel threats, there is a growing need to reconsider and employ these notions in novel ways. Nevertheless, developing elaborate safety protocols demands significant personnel and ongoing assessment. To ensure the confidentiality of their connection, two interconnected devices, referred to as nodes, commonly employ measures to safeguard data and exchange cryptographic keys before transmission [2].These devices exhibit significant energy consumption when they are utilized. This argument holds particular significance in WSN nodes that show mobility within dynamic network designs. Furthermore, the dynamic nature of nodes in a WSN increases this issue. The dynamic nature of a WSN necessitates the continuous adaptation of its structure due to the mobility of nodes. Therefore, necessary to explore alternative methodologies that offer rapid solutions but with potential challenges. One approach to tackling this problem is utilizing applications with

AI functionalities. Executing these programs provides nodes with the necessary information and capabilities to establish communication with adjacent nodes, remove software defects, analyze incoming and outgoing data packets, verify the authenticity of other nodes, and uphold stable online connections [3]. Rapid technological progress in domains within artificial intelligence AI. Computers can acquire knowledge and enhance their performance through machine learning, with minimal to acquire knowledge and enhance their performance through machine learning, with minimal human intervention. The automated, efficient, and precise processing of a substantial volume of data constructs the model of a substantial volume.ML has the potential to use data obtained from a comprehensive framework and includes comments from the community to enhance the overall performance of the system [4].

In addition, we analyze various challenges that may develop while applying ML techniques to WSNs and propose corresponding solutions. To enhance the security of WSNs, it is essential to adopt a comprehensive and multi-faceted strategy that leverages advanced ML methodologies [5]. Nevertheless, the integration of ML into WSNs, as depicted in Figure 1, presents several unsolved issues. In addition, an in-depth evaluation of the statistical analysis of each WSN security architecture is performed.ML quickly gained prominence as AI grew in popularity in the 1950s and established itself as a crucial element in the field. Classification, sorting, regression, and optimization are computer-executable algorithms commonly used to solve various engineering, computing, and healthcare challenges. Technological improvements and the passage of time have made these processes easier to carry out, and time has passed. This phenomenon became more frequent as the algorithms reached their convergence [6]. ML is a tool of great importance and interest in modern society. Certain WSNs can perform security-related functions without the need for ML algorithms. Self-government, alternatively known as autonomous administration, is a term used to describe the ability of a group or entity to govern itself independently, without external interference or control. Conventional network security methods, however, are insufficient in effectively protecting WSNs due to limited resources and processing capabilities [7], [8]. The efficacy of employing ML techniques to enhance the security of WSNs has been well-established. The notion of "user authorization" is deemed inappropriate within the present context.

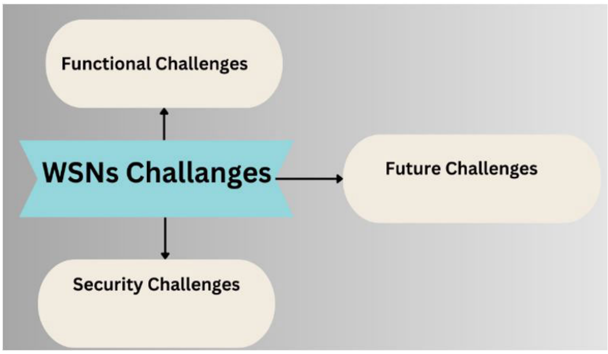


FIGURE 1. Classification of WSNs challenges [7].

The author of [9] employed ML classification methods such as RF, KNN, and NB to examine the operational mechanisms of IoT malware networks. The researchers found that the KKNN technique yielded the most reliable results. The authors of [10] demonstrates the potential resolution of privacy concerns to facilitate SVM training on IoT data. Both transactions have the potential to be executed inside a single cycle without the assistance of a dependable third party. Applying the usual SVM method implies greater complexity than utilizing this alternative approach. As a result, the efficient utilization of ML technology could decrease security expenses. Anomaly detection [11] can prevent various adverse effects, such as DoS attacks and monitoring of packet analysis. ML also assists in identifying physical layer approaches by enabling network access, reducing traffic congestion, and detecting faults [12]. The application of ML techniques to WSNs has the potential to enhance their accuracy and mitigate their vulnerability to failure. A substantial expansion has been observed in these two domains in recent years [13].

A. CONTRIBUTION OF THE STUDY

The major contributions and objectives of the study are:

- This study explores the potential application of machine learning approaches in minimizing security concerns inside WSNs.
- In addition, we analyze the challenges that need to be addressed to achieve the complete implementation of ML techniques for enhancing the efficiency and security of WSNs.

- The first focus of this study refers to a variety of previous research efforts concerning WSNs, focusing on identifying ML methodologies that show the possibility of enhancing the security of WSNs. Next, we analyze many challenges associated with the security of WSNs and how ML could potentially support addressing these concerns. The concluding part of our discussion focuses on some unresolved issues that, if addressed, might improve the efficacy and safety of WSNs and open the complete capabilities of ML.

B. MOTIVATION OF THE STUDY

Due to its adaptability, it finds application across various scientific disciplines. Significant improvements have been made in various domains, including medicine, agriculture, the physical sciences, and computer technology. Recent studies have shown that ML can effectively address various challenges encountered in WSNs. The process of updating the network, accessing large volumes of data directly, and extracting valuable insights from the data can be facilitated by applying ML techniques in WSNs [14]. ML algorithms can extract valuable information from vast amounts of data. Numerous rationales exist for utilizing multi-hop networks in WSNs. The complex nature of WSN environments presents a significant challenge in conducting analytical studies [15]. Moreover, specific software applications necessitate data inputs from multiple groups to ensure optimal functionality. Moreover, ML methods do not necessitate human intervention, matching the decentralized characteristics of WSNs [15] and their tendency to display unexpected patterns and behaviors. The limited availability of resources within WSNs, the constrained processing capabilities of individual nodes, and the requirement for substantial amounts of data for effective learning pose significant challenges in utilizing ML in this context [16]. Table1 provides a comprehensive overview of the criteria for employing ML techniques in WSNs.

Using ML techniques to safeguard WSN networks poses significant challenges due to various factors, such as the need to train ML algorithms to comply with privacy regulations. The conventional approaches for safeguarding WSNs exhibit some drawbacks. However, the utilization of ML techniques has the potential to address these limitations by assisting in mitigating concerns such as congestion, physical layer authentication, and gap detection [17]. Furthermore, ML algorithms exhibit higher accuracy than traditional techniques when evaluating the transit of packets in WSNs and identifying problematic nodes [18]. Several papers have discussed the practical applications of ML techniques in WSNs [19]. Additionally, the role of ML in enhancing security measures, specifically in addressing congestion and intrusion issues in the context of the IoT and WSNs, has been explored [20]. Furthermore, the need to implement safety measures in WSNs has also been emphasized [21]. This led us to conduct a comprehensive investigation into the role of ML algorithms in WSN security, adhering to various standards. While encryption is commonly employed to enhance the security of WSNs, it may not always be the most optimal choice. Conversely, ML-based technologies present a more suitable alternative.

TABLE 1. Requirements of ML techniques in WSN.

Requirements of ML techniques in WSN	Description
Energy Harvesting	This study estimates the power consumption required to maintain a sensor network operating in a low-power environment.
Target Area coverage problem	ML made another attempt to fix this issue in WSN. Using machine learning techniques can make identifying the required number of sensor nodes easier to achieve coverage of a given region. This factor fundamentally influences the issue of adequate target coverage.
Localization Problem	WSNs also work under challenging conditions, such as, e.g., deep water. The movement of nodes from their current position can be due to a combination of internal and external forces. ML makes it easier to get fixed localizations in a more accessible way.
False node detection	The general view is that most sensor nodes will likely exhibit some form of inaccuracy. ML enables faulty sensors to be precisely identified, thereby improving the overall efficiency of an ML system.
Routing	Routing is a crucial technique to ensure the optimal operation of a network, as it enables the proper transmission of data packets along the right path. Various ML methods are used to overcome the challenge of predicting route plans.
Different Levels of data abstractions	Routing is a crucial technique to ensure the optimal operation of a network, as it enables the proper transmission of data packets along the right path. Various ML methods are used to overcome the challenge of predicting route plans.

C. ORGANIZATION OF STUDY

The rest of the paper is organized as follows. Section II describes a literature review in which some past studies about WSNs, ML, and their application architecture are discussed. Section III describes the methodology for defining the research question and inclusion-exclusion criteria. Section IV explains the research question's result and provides a detailed discussion. In the end, section IV describes the conclusion and future work.

II. LITERATURE REVIEW

WSNs play an essential role in the IoT as they collect, transmit, and analyze data from multiple sources. IoT offers numerous advantages in addressing global challenges, its potential to complicate daily tasks, and facilitate secure data exchange. IoT is enabled by various technologies, including embedded systems, control automation systems, and WSNs that enable multiple data communication modes [22]. This indicates that data can be passed between networks quickly and without human intervention. Currently, most

TABLE 2. List of abbreviations.

Abbreviations	Description	Abbreviations	Description
ML	Machine Learning	CNN	Conventional Neural Network
DoS	Denial of services attacks	DDoS	Distributed Denial of Services
IoT	Internet of Thing	MES	Mathematical Encryption Standard
SVM	Support Vector Machine	IPS	Internet Protocol Security
KNN	K-Nearest Neighbor	TLS	Transport Layer Security
CIA	Confidentiality, integration and authentication	DT	Decision Tree
LMS	Least Mean Square	ANN	Artificial Neural Network
MLP	Multi-Layer Perceptron	LR	Logistic Regression
WSN	Wireless Sensor Networks	VCBV	Proportional Integral Derivative
AI	Artificial Intelligence	PSO	Particle Swarm Optimization
BNN	Backpropagation Neural Network	LSTM	Long-Short-Term Memory

IoT functions can be found in smart homes and cities. These systems generally include three essential components: namely, the users' perception of them, their functional effectiveness, and the results they ultimately achieve [23]. In the context of network architecture, it can be observed that high-performance devices are responsible for managing the network and application layers. Conversely, low-power wireless sensors are mainly tasked with managing the detection layer. Sensor nodes within WSNs use radio waves to communicate, facilitating the transmission of information while performing various activities, including sensing, measuring, tracking, and monitoring (as shown in Figure 2). The wireless nodes represent a technological component limited by capacity, operating performance, battery life, and storage capacity [24].

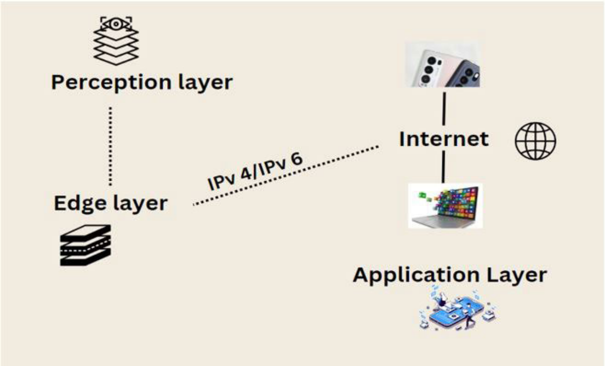


FIGURE 2. The communication among the WSN layers [25].

WSNs use perception layer protocols to describe the network's structure effectively and ensure their designs remain current [26]. One way the nodes exhibit this property is that they function autonomously without a central control Centre. This represents the first differentiation that sets them apart. In addition, the nodes within the WSN can either move freely in the network or remain in a fixed position. Third, it is essential to understand the precise limitations of data transmission. By considering these attributes, one can gain further insight into the capabilities and behaviour of WSNs [27].

The author [28] presents a novel DHCO method designed to extend the life of wireless sensor networks (WSNs) by effectively distributing the energy consumption rate among sensor nodes. The DHCO algorithm, compared to other popular WSN routing algorithms like LEACH, HEED, GASONeC, and DCFR, builds a hierarchical network structure based on node distance attributes. It also produces an achievable routing set, which is the basis for solving a combinatorial optimization problem. Using the maximal minimum criteria, the DHCO technique finds the best path for every sensor node inside its respective solution spaces. The energy properties of the nodes are used to achieve this. Extensive experimental results have demonstrated the feasibility of the DHCO algorithm and illustrate its superior performance compared to other WSN routing algorithms. This is particularly true when taking into account the improvement in total WSN endurance and the balancing of energy usage among sensor nodes.

The author [29] focused a great deal of interest on wireless sensor networks, or WSNs, particularly in the area of monitoring and surveillance operations. However, a major challenge that needs to be addressed is how to effectively balance off conflicting optimization objectives, such as energy dissipation, packet loss rate, coverage, and lifetime. The goal of this work is to present an overview and tutorial on current research and development efforts that have been directed toward solving this problem by utilizing multi-objective optimization (MOO) techniques. The main optimization objectives are used in wireless sensor networks (WSNs). After that, explore some well-known approaches that have been developed for MOO. These include heuristic and metaheuristic optimization algorithms, mathematical programming-based scalarization techniques, and a range of advanced optimization methodological techniques. Furthermore, it provides an overview of the results from current research on MOO in relation to WSNs

Energy efficiency is a critical network function and one of the primary performance criteria in ultra-dense wireless sensor networks. The author [30]presents an unsupervised learning technique for topology control. This strategy aims to extend the lifetime of ultra-dense wireless sensor networks by efficiently controlling the energy consumption of the

TABLE 3. Different aspects of WSN.

Ref.	Focus	Details	Advantages	Disadvantages
[13]	Role of WSNs in IoT	Collect, transmit, and analyze data from multiple sources	Essential for data aggregation and communication in IoT	Can complicate daily tasks due to the complexity and vastness of IoT networks
[22]	Technologies Enabling IoT	Embedded systems, control automation systems, WSNs with multiple data communication modes	Facilitate secure, versatile data exchange	Dependency on technology; potential for quick obsolescence
[23]	Components of IoT Systems in WSN	Users' perception, functional effectiveness, results achieved.	Enhances user interaction and effectiveness of IoT applications	Requires balancing between user expectations and actual system performance.
[24]	Network Architecture of WNS	High-performance devices for network and application layers; low-power sensors for the detection layer	Efficient management of network and application layers	Low-power sensors might have limited capabilities
[25]	Communication in WSNs	Use of radio waves for information transmission; various activities like sensing, measuring, tracking, monitoring	Enables wireless, flexible communication and data collection	Limited by sensor capacity, battery life, and storage
[26]	WSN Network Architecture and Capacity	Continuously changing architecture; issues with insufficient capacity	Adaptable to emerging technologies and needs	Struggles with insufficient capacity, particularly in dense networks.
[27]	Node Functionality of WSN	Autonomy of nodes, mobility, data transmission limitations	Nodes can function independently, enhancing network resilience	Limitations in data transmission and power may restrict node performance.
[31]–[34]	Protocols in WSN	ZigBee and 6LoWPAN for sensor layer; modifications for Bluetooth, WLAN, sub-1 GHz RF.	ZigBee mitigates channel failures and enhances security. 6LoWPAN ideal for low-power devices	Performance limitations in certain protocols
[35]	Power Consumption in WSN	6LoWPAN ideal for low-power IP devices; performance and power limitations of WSN nodes	Energy-efficient, suitable for battery-powered devices	Charging infrastructure can be challenging; power limitations affect performance
[37]	Security and Privacy in WSN	Threats to privacy and security; potential security breaches	Advanced security measures in newer technologies	High risk of privacy breaches and unauthorized access.
[38]–[41]	Applications of WSNs	Military, health surveillance, industrial automation, intelligent living environments	Diverse applications in critical sectors	Complex setups required; security concerns in sensitive applications
[40], [41]	Network Function and Security in WSN	Connectivity issues (losses, collisions); layers assigned different responsibilities for data security	Physical layer improves performance; transport layer manages external network data transfer	Vulnerability to various network attacks and security threats
[42], [43]	Security Protocols of WSN	Techniques like encryption and decryption; non-repudiation concept in network security	Ensures secure communication and data protection	Inherent limitations of WSNs necessitate ongoing research for better security solutions
[44]–[47]	Threats to WSN Layers	Various types of attacks on different layers (Physical, Data Link, Network, Transport, Application).	Security protocols in place to address different layer-specific attacks	Each layer susceptible to specific attacks, indicating a continuous need for comprehensive security strategies.

networks. Based on network clusters, the genetically based method that has been shown encodes sensors as genes. It creates an ideal chromosome through the use of unsupervised learning in order to approximate the optimal network architecture.

Furthermore, the approach incorporates spatially adaptive reliability to schedule individual cluster members for rest, with the aim of preserving node energy. The simulation's outcomes show that the recommended approach performs better in terms of increasing energy efficiency. These results show advances with respect to state-of-the-art techniques maintaining a reasonable level of computational complexity.

- WSN network architecture is continually changing.
- Too many leaps between insufficient capacity.

WSN nodes can work effectively even when deployed in experimental environments. The present situation poses a threat to both privacy and security. Unauthorized persons can easily and quickly access private information. ZigBee and 6LoWPAN have widely recognized protocols commonly used to operate the sensor layer in WSNs [31]. The above protocols can be modified for use over various network media, such as Bluetooth [32], low-power WLAN [33], and sub-1 gigahertz radio frequencies. In addition, the network in your home can be monitored intelligently and remotely. In addition, it offers a large number of cost-effective and energy-efficient nodes. The accessible data transmission over long distances made this possible. Compared to alternative systems, ZigBee can mitigate channel failures. It uses the latest security technology to protect the data, uses the latest security technology, and implements additional security measures [34]. In contrast, 6LoWPAN, due to its lower power requirements, represents an ideal choice for low-power consumption (IP) devices such as controllers and sensors. WSN nodes have comparable functionality to existing protocols but have operational performance and power headroom limitations [35]. The charging infrastructure in certain areas can pose difficulties due to the different nature of the WSNs, which are designed to operate under many conditions [36]. A possible solution to this problem is reducing the safety requirements while increasing the battery's capacity. Figure 3 comprehensively shows the essential components that form the basis for many technologies.

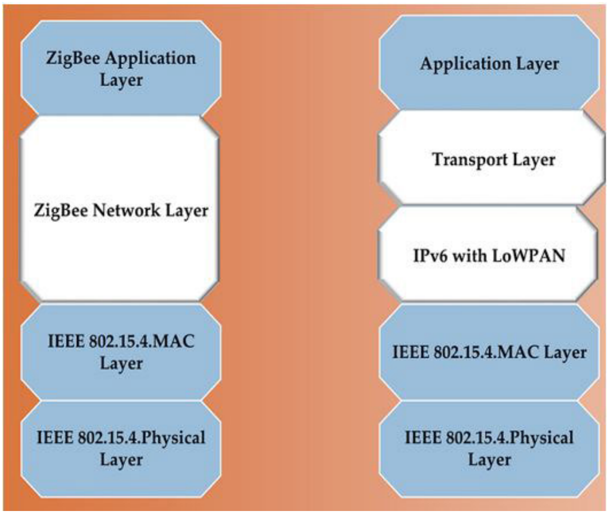


FIGURE 3. WSN management protocols [25].

The individual elements of a WSN can be powered by sustainable and renewable sources such as wind, thermal, and solar energy. Given the complexity and advanced nature of WSN technology, several of the proposed solutions appear impractical. Nevertheless, it is more likely that data could be compromised if security measures are insufficient [37].WSNs have demonstrated their use in different scenarios, as shown in Figure 4. The applications mentioned above include military operations [38], health surveillance [39], industrial process automation [40], and intelligent living environments [41]. Various companies have made more than fifty efforts to improve the goal of Layer 6LoWPAN-based thread technology. Thread's primary purpose is to facilitate user connectivity and management of smart home devices [42].

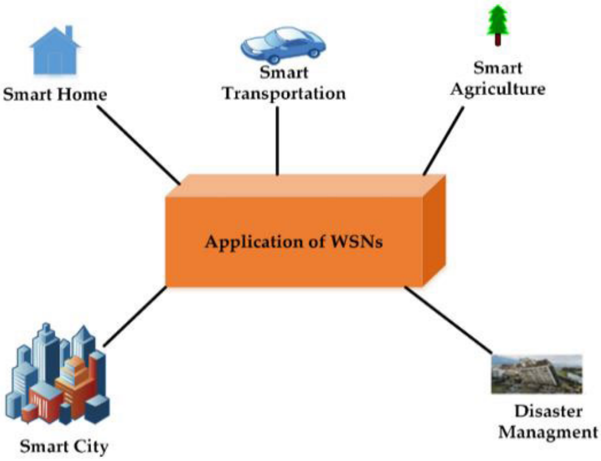


FIGURE 4. WSN management protocols [43].

Disturbances, losses, and collisions can affect the connectivity and function of a network. Nonetheless, it is crucial to acknowledge the existence of significant privacy and security issues [40]. Impeding access and communication is commonly referred to as an active attack. Conversely, depending on contextual factors, certain acts of aggression can be classified as passive or active. However, these layers are assigned different responsibilities to ensure the data's security throughout storage and transmission between network points. The physical layer improves network performance by mitigating the effects of shadows and route loss. Error detection and correction techniques are used to establish a connection between the data link layer in WSNs [41].

The network layer determines how to transmit data to the top-level router. In a WSN, each node acts as a router, facilitating data routing. The security protocols implemented at this level are intended to prevent unauthorized persons from accessing the communication channel. The transport layer is responsible for managing data transfer to external networks. In contrast, the application layer takes responsibility for data collection, management, and arrangement [42]. Solving identification remains a significant concern that requires attention to ensure the security of WSNs. This unique identification technique makes exploiting the network impossible for malicious WSN nodes. In addition to these areas, the security sector uses encryption and decryption methods to protect WSNs and their users. Due to the inherent limitations of WSNs, scientists are actively investigating alternative security solutions, as indicated by reference [43]. The concept of non-repudiation is essential in the field of network security. Therefore, any WSN device must be able to document its activities in the event of a security breach. (Table 3 lists several hazards associated with WSN layers). Additionally, the ease with which unauthorized persons could gain direct access to the network is facilitated by the

TABLE 4. Types of attacks on layers.

Reference	Layer	Threat
[44]	Physical	DOS, Jamming, Node Capture
[45]	Data Link	Wormhole, Sinkhole, Sybil, Resource exhaustion
[26]	Network	DOS, Misdirection, Selective forwarding, Eavesdropping
[46]	Transport	Flooding, Session hacking, Resource exhaustion, DOS
[47]	Application	DOS, Data corruption, Malicious node

sterile environment of a WSN. The installation of a cable connection would significantly increase the level of access difficulty for unauthorized persons. Using this particular user authentication approach can result in potential network latency and the potential compromise of sensitive data [44].

This study [129] into a new way to control the topology in very dense wireless sensor networks by mixing unsupervised learning and genetic algorithms. The goal is to make these networks use less energy. The method combines an unsupervised learning framework with a genetic algorithm to handle network topology well and make the network last longer. The results show that this method greatly improves how much energy the sensor network uses. The results show that the network works better and uses less energy, but the initial summary doesn't give any exact accuracy metrics or quantitative results. The success of this method points the way to further study that will help improve wireless sensor networks, especially in situations where a lot of sensors need to be placed close together. With an emphasis on multi-objective optimization in wireless sensor networks (WSNs), [130] provides a comprehensive assessment, outlining important measurements, techniques, and open difficulties. The goal is to explain how WSNs' performance can be improved by multi-objective optimization, especially for monitoring and surveillance jobs. The process starts with an analysis of the current literature, whereby different optimization strategies and their effects on WSN performance are classified and compared. The results of the poll highlight the difficulty of striking a balance between different, often conflicting, goals in WSNs, such as energy efficiency, accuracy, and coverage. [130] continues by outlining many open problems and research possibilities, suggesting that while great progress has been made, many areas of multi-objective optimization in WSNs remain unexplored and offer fertile ground for future research. In [131] present a hierarchical, dynamic, and energy-efficient approach for WSNs by use of combinatorial optimization. The method is simulated to see if it improves the energy efficiency of WSNs. Although the initial summary does not disclose precise accuracy or performance indicators, the results imply considerable gains in network lifetime and energy efficiency [131]. The author [48] proposed an approach based on fuzzy inductive reasoning to choose an optimal Cluster Head (CH) from a group of CHs that may provide data to a mobile Base Station (BS). This selection is based on optimizing features including distance to clusters, BS mobility, and remaining electrical power. The majority of the time, a significant amount of energy is lost when sending the data to the BS. In another study [49], a grid-based CHs technique was employed, in which the system area was divided into M N separators of the same width. Reducing the quantity of power lost by the sensors and extending the system's lifespan are the main goals. In order for this regulated approach to work, the positions of the networking sites must be known. Each node must communicate its location to the mobile sink. The efficient use of network energy is one of the most crucial aspects to take into consideration while designing and running wireless communication networks. The author [50] developed a dense radio access network (dense-RAN) with the capability of managing radiated power at the base station (BS). Long-term network energy efficiency is to be maximized through cooperatively managing radiated power levels across different base stations (BSs) while maintaining user traffic generation limits and maximum achievable rates. The author [50] formulate the problem as a Markov decision process (MDP) and provides a novel deep reinforcement learning (DRL) framework to address the issues caused by time-varying network interference and stochastic traffic arrivals in the context of the cloud-RAN operation scheme.This enables us to handle the problems caused by time-varying network interference and stochastic traffic arrivals. To balance the differences between complexity and performance, the optimization of multi-BSs' energy efficiency is estimated using a deep Q-network (DQN) to achieve near-optimal performance. This is achieved by applying a multiplicative complexity constraint to the optimizer. Under the DQN framework, each BS strives to increase the energy efficiency of its own operations first, then collaborates with other BSs' activities to increase the multi-BSs' total energy efficiency. Table3 illustrates different aspects of WSN. High-performance standards will apply to ultra-reliable and low-latency wireless sensor networks (uRLLWSNs), which will prove to be crucial in the development of 5G networks, as opposed to traditional WSNs. The author of [51] employs a combination of genetic algorithms and machine learning techniques, resulting in the creation of the MLPGA algorithm. With this design, uRLLWSNs can effectively communicate while simultaneously achieving a number of network goals. These goals include making the network more reliable, improving its connection, and extending its lifespan. Furthermore, the method that has been shown uses the widely recognized K-means clustering algorithm from machine learning to generate a 2-tier network architecture that is visualized as a chromosome. Furthermore, it develops a clustering approach for energy conversion to prevent Cluster Heads (CHs) from overloading. To find the most suitable chromosome for the organism, the technique builds a multi-objective optimization model based on important network indicators. A genetic algorithm is used in the optimization process, and the convergence condition is defined as the minimal schema of

TABLE 5. Research questions and motivation.

Research Questions	Motivation
RQ1: What ML methods are used in WSN?	To know about the different types of supervised and unsupervised ML techniques used in WSN.
RQ2: What are WSN Security Challenges in ML?	TTo know about the different types of security issues in ML.
RQ3: What are the Challenges of Using ML Algorithms in WSN Security?	To know about the different types of challenges faced during using of different types of ML algorithms.
RQ4: What are the open issues still in this field?	To know about the open issues that need to be solved in the future.

the population. The principal component analysis algorithm is used to transform the multi-objective function of the optimization model into the fitness function. This transformation eliminates dependencies between several optimization targets and arranges them in decreasing order of relevance. The most common method for selecting Cluster Heads (CH) in Wireless Sensor Networks (WSN) is by combining the Black Hole algorithm with Hybrid Grey Wolf Optimisation based on Ant Colony Optimisation (HGWACO). The goal of this integration is to extend the network's lifespan and lower its energy consumption. One of the main objectives while creating routing protocols for wireless sensor networks (WSNs) is to minimize the energy consumption of the network nodes. The creation of a routing protocol that is both simple and power-sensitive is prioritized for this purpose. To ensure a just and equitable allocation of energy among the network nodes, this protocol must consider power usage and the distance between nodes while choosing suitable CHs. The Grey Wolf Optimization (GWO) method does global optimization, for which the Ant Colony Optimisation (ACO) technique is employed as compensation. The GWO algorithm's parameter matrices improve the efficiency of usage. The system's efficiency is greatly increased because the outcomes are at the best possible level. Metrics like the quantity of remaining energy, the amount of energy consumed, the number of alive nodes, the number of dead nodes, and the network's longevity show the superiority of the HGWACO method over alternative approaches [52].

III. METHODS AND MATERIALS

A. EXCLUSION AND INCLUSION

Using ML and WNS techniques, keywords were used to search for publications in various databases, including Scopus, Springer, IEEE, Google Scholar, Wiley, Science Direct, and ACM. They chose the keywords based on their security, WNS, and ML categorization discussions. The submitted articles were examined more closely after the first evaluation. In this section, you will find articles related to ML-based WSN strategies found through literature searches. This shed light on the development of ML and the operation of SG security. Articles written in other languages were not included in this study. We just examined a few publications to understand how ML works and what further studies are needed to advance the field.

B. RESEARCH QUESTION

The research questions are given below in Table 5

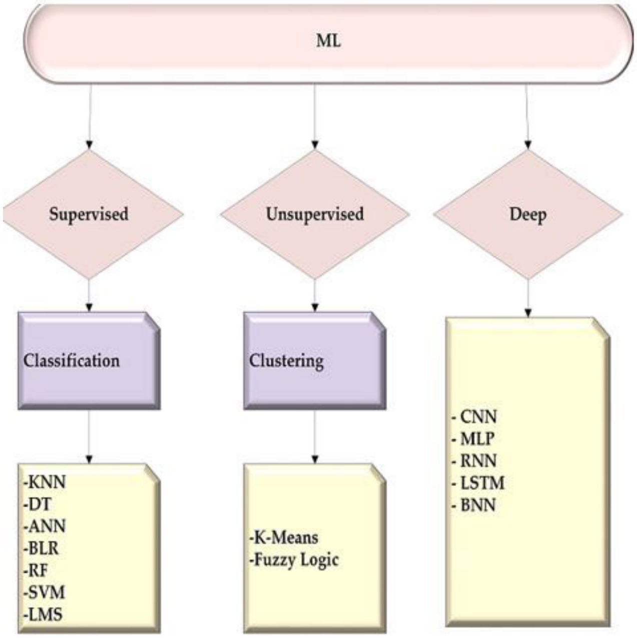


FIGURE 5. Classification of ML algorithms in the context of WSN's security [53].

IV. RESULTS

A. MACHINE LEARNING TECHNIQUES

ML algorithms play a crucial role in enhancing the security of WSNs, and they are classified based on their application and influence (Figure 6.

B. SUPERVISED LEARNING

Supervised machine learning relies on utilizing labelled training data collections, as depicted in Figure 6, to enhance the objective of improving users' expertise in their respective domains. The training set comprises the input item, typically represented as a vector, and the desired output value, which serves as a prediction indication. A machine learning model is constructed with these data instances. Supervised learning algorithms can generate a mapping function, which may be employed to predict outcomes for novel instances by utilizing the information in training [54]. If the problem has been effectively resolved, identifying the solution will be simplified, especially in concealed categorization cases, the categorization is classified. A mathematical model is constructed utilizing known qualities of sampled data to predict the characteristics of unexpected novel samples [55].

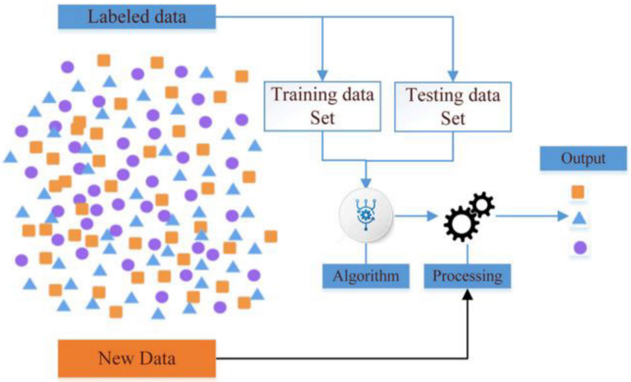


FIGURE 6. Supervising learning process [56].

However, supervised learning requires a lot of time and CPU resources during the training phase, so it is unsuitable for use in programs requiring real-time results. On the other hand, it is very effective and accurate in predicting future samples.

C. K-NEAREST NEIGHBOR

The KNN classification algorithm is considered one of the most challenging ML applications in real-world situations. This strategy assumes that a given sample belongs to the same group as the k-feature vector samples closest to it. The practical use of the K-Nearest technique can be seen by including a new element in the training data set. The data are categorized accordingly once the machine finds the k samples with the highest similarity [57].

D. DECISION TREE

The DT technique begins by gathering a list of relevant information. The meaning of each piece of information is indicated by assigning it a numerical value called a tree leaf. Predictive modelling is a technique used in various fields, such as statistics, data mining, and map learning. Trees visually represent the number of variables, with each tree representing a possible conclusion. The leaves of these trees are structurally and visually similar to those of natural tree species [58]. The term "regression trees" often means indecision trees focusing on continuous variables that show variation over time in linear regression. DTs are also part of analysis trees. However, the classification tree results are considered when making a decision [59].

E. RANDOM FOREST

RF can generate more accurate predictions for a given dataset because it integrates the results of many DTs working with different subsets of data. The RF model differs from previous iterations in that it only uses the output of a single DT. Based on the principles of this particular theory, many decision trees (DTs) are believed to yield more favorable outcomes than the DT's implementation. Accuracy and avoidance of overfitting can be improved by increasing the number of trees used in the analysis [60].

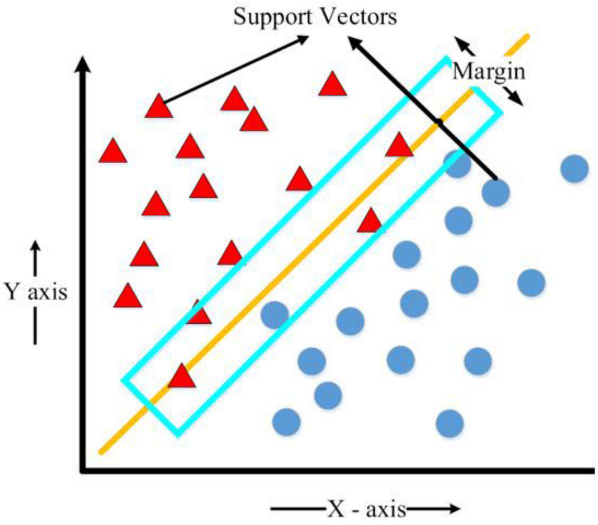


FIGURE 7. The SVM method [62].

F. SUPPORT VECTOR MACHINE

The SVM technique applies classification and regression tasks in the domain of supervised ML. The main goal of this methodology is to categorize the data by assigning a numerical value to each feature based on its position in n-dimensional space after moving each data point to that position [61]. The first step in categorizing objects is to identify the boundary between the two different groups of objects (see Figure 7)

G. NAÏVE BAYES

The Naive Bayes classification approach assumes that expertise is not required at any stage of the attribute formation process. The first step is to find the probability distribution of inputs and outputs within a given training data set using a unique theoretical framework based on feature conditions. The model uses Bayes' theorem to find the output variable y that optimizes the likelihood of future outcomes given a specific input variable x [63]. For the classifier to perform optimally, the training data used for its training process must contain the imperative. By using this methodology, the results will be maximally precise. During training, the algorithm generates classification rules to categorize the given data. Next, let's change the order of the predictions based on these criteria. Because the training process is supervised, the classifications used to train the naive Bayesian classifier are assumed to be predetermined and known [64].

H. ARTIFICIAL NEURAL NETWORK (ANN)

A model for sorting data called ANN follows the function of human neurons. An ANN uses many neurons or functional units to analyze data and provide accurate results. Layers and nodes are used in ANN to connect objects in essential ways. In an ANN network, each node has a specific task to perform [65]. The input, hidden, and output layers are the three components that make up a neural network. The amount of new data that can be contributed is limited by some other categorization algorithms but not by ANN. This is a more effective tool for organizing complex and unstructured datasets. ANN is a computational model that simulates the functionality of biological neurons in humans. ANN uses many neurons, or functional units, to process inputs and get an accurate solution. ANN uses layers and nodes to create meaningful connections between objects. Different tasks are assigned to individual nodes in ANN. The artificial neural network consists of three layers: the input, the hidden, and the output. Unlike alternative categorization techniques, ANN does not limit the amount of data that can be used as input [66]. This feature is an exceptional tool for effectively managing complex and disorganized information.

I. LEAST-MEAN-SQUARE (LMS)

The ML filter uses the LMS algorithm based on the sophisticated random gradient descent method. Filter weights often change due to descent gradients. This gives an accurate idea of the expected result. Due to the way LMS works, there is no correlation between how ML is learned in theory and how it is learned in practice [67]. These theories aim for convergence, which occurs when repeated learning leads to a single outcome rather than many outcomes.

V. UNSUPERVISED LEARNING

One of the main goals of both ANN and ML is the ability to learn autonomously. ML systems must independently recognize patterns in data to be effective. This type of statement is also known as an unlabeled statement. One of the most essential tasks that can be performed with ML is estimating the volume of data. This allows customers to quickly identify products with similar characteristics and order them according to specific standards. Knowledge-based learning aims to determine a graphical distribution according to what it already knows from more bits, in contrast to supervised learning, which aims to determine how the original data was distributed [68]. The first exemplifies this because it can monitor where critical information is being disseminated.

A. K-MEANS

The K-Means algorithm groups data points that are physically close together. The originality of a point within a set is demonstrated by the average distance between it and its other points. Most often, this can be done using the arithmetic mean of the point. So, there is no need for a learning model that uses this approach. Instead, the cluster with which the new location shares the most significant area is selected. Close a point in a group can be determined using a distance measure, for example, the distance between two points [69].

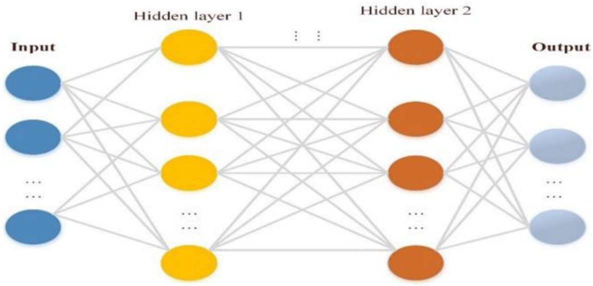


FIGURE 8. Deep learning [73].

B. FUZZY LOGIC (FL)

The main goal of FL is to provide accurate numerical values, elements, or magnitudes to facilitate the participation of all regions throughout the universe in cosmic processes. Values in the range of 0 to 1 are considered appropriate for the level of engagement. The concept that multiple entities could have different levels of truth is a core tenet of FL. The dominant convention for representing truth values is the [0, 1] scale, where 0 means complete untruth, 1 means absolute truth, and the remaining numbers represent varying degrees of partial truth, often referred to as intermediate degrees of truth [70].

C. DEEP LEARNING

The data grouping is achieved through deep learning, a particular form of ANN technology. ANNs employing deep learning involve a variety of representations between the input layer and the output layer that explains how data is collected during the learning process [71]. The composition consists of simple, non-linear elements that improve the representation and ensure the most advantageous result [72]. Deep learning offers several advantages, such as the ability to extract high-level features from data and the flexibility to work with or without labels. Figure 8 shows the architecture of deep learning.

D. CONVOLUTIONAL NEURAL NETWORKS

CNNs, which perform like multi-layer perceptrons, are an aspect of the deep learning system. Conversely, CNNs are designed differently from perceptrons and can perform different tasks with the data they collect [74]. A wide range of different uses for CNNs exist, including data analysis. The first step of the perceptron approach is to find and choose potential feature possibilities. Before the classification process begins, this must be done. It differs from the others in that it has one or more hidden layers that combine elements from the photographs or videos and addition to a fully linked layer that creates the final visual [75].The layers employed in this method include convolutional, activation functions, padding, pooling, and link layers. When new layers are added on top of existing ones, the order of the levels also changes. Straight lines are drawn in the first layer and curves in the second the first layer

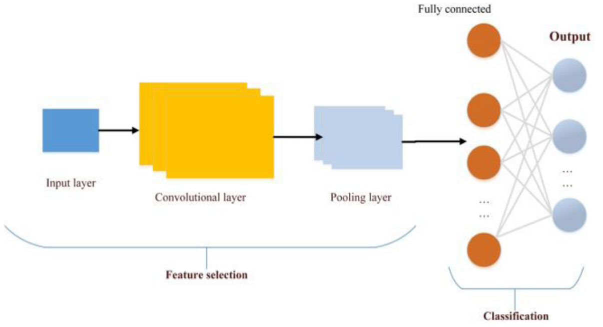


FIGURE 9. CNN [77].

[76]. Figure 9 illustrates the development and usage of the CNN algorithm.

E. RECURRENT NEURAL NETWORKS (RNN)

RNNs can identify and modify patterns in many situations, greatly benefiting them in various fields such as genetic code manipulation and machine translation. RNNs have a mechanism called ''memory'' that facilitates the generation of current and future results by leveraging input information from previous instances. RNNs exhibit different characteristics from other deep neural networks due to their frequent lack of connection between inputs and output [78]. Nevertheless, RNN considers the preservation of long-term memory to be complex. Passing knowledge from generation to generation can be challenging when the information sequence or arrangement is imprecise.

F. LONG-TERM SHORT MEMORY

RNNs with LSTM have gained attention due to their exceptional ability to store and retrieve past information. The over-reliance on quick fixes has significantly influenced the development of LSTM models. The transmission of environmental information occurs sequentially through connected cells, with each cell serving as an information channel and resembling a complex system of communication pathways. The likelihood of memory loss decreases when engaging in learning and remembering processes, as knowledge acquired in the past can be used effectively in the present. The cell's content can be modified by adding or removing information during movement [79].

G. MULTI-LAYER PERCEPTRON (MLP)

MLP is an example of a feedforward network, sometimes called ANN. A linear perceptron can allow fundamentally identical elements to be distinguished linearly due to multiple layers and non-linear activation functions. MLP includes nodes involved in the transmission and reception of data. Activation of this neuron involves stimulating network nodes that are not directly connected to the input nodes, which is achieved using a nonlinear activation function. During the training process, MLP uses the backpropagation algorithm and targeted learning techniques [80].

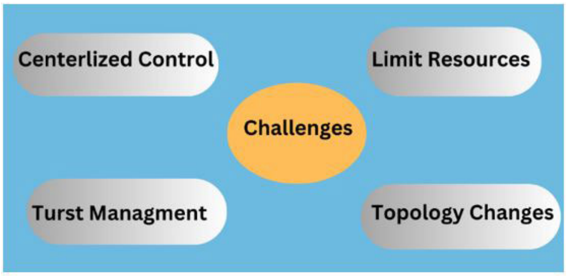


FIGURE 10. WSN security chalenges [25].

H. BACKPROPAGATION NEURAL NETWORKS (BNN)

BNN can be used to modify deep feedforward neural networks. Supervised learning methods such as stochastic gradient descent train feed-forward neural networks. During the training of NN, the use of grade drop involves the computer calculating the loss rate. The loss rate serves as a measure to quantify the extent of the deviation between the observed labels and the expected labels. Through a series of iterative training sessions, the model's loss function can be minimized by changing each weight separately [78]. In a feedforward neural network, the backpropagation algorithm calculates the changes that must be made from the output layer to the input layer. The height of a particular layer within a multi-layer system can be determined by summing the slopes of the layers below [79]. This can be achieved before the specific height of the target layer is determined.

VI. WSN SECURITY CHALLENGES

Engineers can use WSN to design and develop systems with accurate functionality and the ability to send data across the entire layer in real-time seamlessly. Including this extra layer compromises the overall design of the network as it uses unencrypted Wi-Fi channels [17]. The above aspect is the main factor in the difficulty involved. Although WSN nodes can cause several problems, most of these difficulties are related to security and can be traced back to concerns [83]. Due to the inherent challenges in realizing the network, as mentioned earlier, the confidentiality of private data on WSN is at risk (see Figure 10).

A. ABSENCE OF CENTRALIZED CONTROL

When WSN nodes are placed close to each other, they can independently perform activities like authentication without the awareness layer [84]. It is essential to use processes that allow the exchange of authentications between adjacent nodes and the grouping of WSN nodes into clusters [85].

B. WSNs TOPOLOGY CHANGES

WSN nodes may be moved to different locations while the environment in which they operate may change. In addition, there is a possibility that new nodes will be integrated into the network while current nodes may be eliminated [86]. The above aspects contribute to the continuous modifications of

WSN architecture. To accommodate the dynamic nature of topologies, it is advisable to use multi-hop communication methods, which include routing and authentication protocols. These mechanisms facilitate the delivery of messages across multiple hops, ensuring effective communication in the face of changing network topologies. A network with numerous nodes is susceptible to these changes. WSN receives the message, and all adjacent nodes encounter identical signal strength [87]. When making changes to the network hardware, all WSN nodes must be close to the transmitter.

C. TRUST MANAGEMENT

Trust management is a crucial aspect of WSNs as it allows for identifying and differentiating nodes that can be considered reliable. Trust management in sensor networks presents significant challenges due to several factors, including the limitations of limited power, the need for large nodes, and the complex process of restoring trust. The considerations included in this analysis relate to the potential occurrence of security breaches, the subsequent need to revoke trust, and the complexity of trust management [88]. The potential limitation of WSN is setting up complex key pairs or paths between nodes that may be limited by power availability and processing speed. Replication of this technique may not be possible even once successfully performed. It is recommended that a limited number of nodes within a network can exchange cryptographic keys. The attacks could be mitigated if a WSN node was subject to physical tampering. To accomplish this task, the promotion of fundamental management strategies is essential [89]. Before sending or receiving data from the nodes within the WSN, a node must establish trust with those nodes, which takes time. Before building or broadcasting a network, you must remove all potentially dangerous components. Each node must have the imperative that each node has an introductory deduction paradigm for individuals and an introductory deduction paradigm for individual and group defenses. Through targeted practice and systematic training, it is possible to achieve this paradigm shift with limited resources [90].

D. LIMITED RESOURCES

Another problem arises from the limitation that WSN nodes cannot obtain all the data that sensors can collect. This highlights the importance of reducing the cost of these devices in meeting consumer demand. The uncertainty about the security level of these technologies is due to the lack of basic security procedures [91]. Nevertheless, WSNs must have limited connections, calculations, and storage capacities to maintain security measures [92].

WSNs, typically operate in resource-constrained situations. Under these conditions, sensor nodes have to deal with constraints related to memory, processing power, and energy. It is crucial to develop algorithms with minimal computational complexity to ensure that these nodes can perform tasks without quickly running out of resources. WSNs frequently require the cooperation of multiple sensor nodes in order to gather, process, and share data. This is carried out to achieve common objectives, such as keeping an eye on the surroundings or identifying events.

Convergence issues arise when nodes find it difficult to come to an agreement because of many factors, including communication limitations, discrepancies in data veracity, or variations in processing capabilities. Efficient algorithms for wireless sensor networks (WSNs) should decrease computational complexity in order to save energy. Among the strategies that can be used to achieve this are the application of lightweight cryptographic algorithms, data aggregation optimization, and the use of effective routing protocols. WSN methods must be designed to handle issues like node failure, communication delays, and inconsistent data quality since they often necessitate a distributed architecture in which nodes collaborate to interpret information.

Convergence problems must be mitigated by incorporating adaptive approaches that consider the network's constantly changing conditions. This could include the implementation of robust consensus mechanisms, efficient and effective error handling, and dynamic parameter adjustments. Wireless sensor network (WSN) practitioners and researchers are always trying to come up with ways to overcome these obstacles. Their objective is to raise the general effectiveness, dependability, and efficiency of wireless sensor networks for a variety of uses, such as industrial automation, environmental monitoring, and healthcare.

TABLE 6. Types of attacks on layers.

Sr.	Challenges
1.	Accurate projections for the present
2.	WSN security issues still exist, and ML implementation cannot fix them.
3.	This is a broad illustration of the outcomes.

VII. CHALLENGES OF USING ML ALGORITHMS FOR WSN SECURITY

Further research and investigations are needed as advances in ML techniques have facilitated the identification of vulnerabilities and improved defences for WSN nodes against attacks. This wireless network presents problems when faced with insufficient power or computing capacity [93]. These challenges are illustrated in Table 6

ML systems face limitations in accurately predicting future outcomes because they learn from past data. These types of programs have the potential to improve their task performance by receiving additional information [81]. The existence of a more significant number of facts must be satisfied. It is necessary to estimate the additional effort the ML algorithm requires relative to the limited resources of the WSN. ML techniques should be extended to the whole system to mitigate this trade-off. Therefore, it can be argued that these strategies directly threaten WSN environments [94]. The WSN security requirements cannot be adequately met by ML alone. Applying these techniques in areas of information security, such as authentication and data integrity, can pose specific difficulties [95]. Power consumption and computational resources are significant when these services are distributed across nodes in a WSN. A possible way to illustrate this concept is to implement authentication protocols [96] between the car and the driver. However, setting up authentication between two WSN nodes poses a more significant challenge. While it is conceivable that this might be the case, empirical studies have shown that machine learning algorithms can effectively identify individuals using various physical modalities [97]. A significant portion of ML techniques have some form of bugs. To protect the information, maintaining a high level of confidentiality is essential. The study conducted by the authors, as shown in reference [75], suggests that a medical expert system can effectively use ML technology to improve case-based monitoring of private health data for risk assessment.

A. INTRUSION DETECTION

In a WSN, each node acts as a network device and server. Consequently, each node must detect intrusions autonomously [6]. The anomaly-based strategy performs better than the signature-based method in deploying new functionality to WSN nodes and effectively deploys new functionality to WSN nodes. Despite advances in the ML training process, there is still a need to resolve difficulties that need to be addressed. The main goals of improving ML services in WSNs are to reduce training time, improve learning accuracy, and optimize data usage. The authors of the [98] developed an innovative approach to improve the detection of DoS attacks while reducing the power consumption of WSNs. Researchers developed an innovative cluster architecture using the Low-Energy Adaptive Clustering Hierarchy protocol to increase message transmission efficiency through a more significant number of WSN nodes. Identifying DDoS attacks has been further enhanced by integrating a feature selection and classification mechanism. The term "feature selection" refers to the methods used to remove unnecessary attributes from a given dataset. Prioritizing essential information and discarding less critical information is a recommended approach to using this method effectively in the context of the learning process. The researchers investigated the potential impact of their proposed methodology on the energy consumption of WSNs. A 5% increase in energy consumption was observed. After examining various ML techniques, the authors concluded that DT is the most appropriate strategy to defend WSNs from DoS assaults due to its reliability and consistency. In a study conducted by researchers, the influence of several ML algorithms on the occurrence of DoS attacks in WSNs was examined [99].

Different ML methods such as statistical, logical, instance and deep learning were used for datasets of different sizes to investigate the influence of data volume on the training of ML algorithms. In addition, the researchers examined the WSN nodes that use ML to a lesser extent, as documented in reference [58]. The results suggest that it is advisable to limit the number of records in files to a range of 3, 0006,000. In addition, it is recommended to balance the proportion of entries that have experienced attacks and those that have not. Before the proposal, it was decided to ensure a fair distribution of both companies. The results also showed that the logic-based technique is the most precise. After implementing the best method for detecting DoS attacks, the power consumption of the network, the best method for detecting DoS attacks, increased by 32%. The previous example compares DL and standard ML techniques, specifically when using data packets received from WSN. The study's authors used DL techniques [97] to demonstrate the ability of simple models to detect intrusions in real scenarios. Detection efficiency was assessed using binary logistic regression in a real-time tracking tool. Data from surrounding WSN nodes were collected and classified as safe or dangerous. After [6] running LR, the researchers analyzed the behavior of the WSN nodes to assess the effectiveness of threat detection [79] This analysis was conducted after a comprehensive review of the data associated with LR. Their accuracy rate varied between 96% and 100%. The author of [101] proposed an alternative to develop multiple strategies to address these challenges. The author of [102] proposed an innovative approach to improve network stability and intrusion detection. A flexible chicken swarm optimization technique was developed to facilitate the procurement of the required energy by WSN nodes. The authors used a two-stage SVM method for intrusion detection. The researchers used SVM as a computational tool to analyze the given data set and first used it to identify the node with problems. This made it easier for them to identify potential security vulnerabilities. In contrast, researchers are currently trying to identify methods to increase the longevity of WSNs. However, it is imperative to identify the potential energy savings that can be achieved by implementing the proposed approach. The study's authors [103] used deep neural networks to develop an adaptive approach to intrusion detection. The statistics also showed that deriving accurate deductions from the diverse network traffic was becoming more accessible and manageable. The authors of [104] used particle swarm optimization and backpropagation neural networks to develop a solution for WSNs that can detect moderate levels of infiltration. Table 7 illustrates the ML methods for intrusion detection.

The authors in [108] improved intrusion detection by using a two-level classifier in conjunction with a hybrid feature selection technique. To identify the faulty WSN nodes, the traffic data was analyzed using SVM and MLP algorithms. Conversely, some authors have integrated many ML algorithms to develop a hybrid classifier. The

TABLE 7. ML-based intrusion detection.

Reference	Method	Advantages	Disadvantages
[99]	Water Cycle + DT	Detection has become significantly more precise. Reducing the WSN's energy consumption	This study examined only one form of packet flow on a WSN.
[105]	Various ML algorithms	Determine which ML techniques are most effective for detecting attempts to sneak into WSNs. Determine how much data must be collected to detect intrusions in WSN.	This study examined only one form of packet flow on a WSN.
[106]	Fuzzy logic association rules	Improved detection accuracy	The power consumption of intrusion detection was not examined in WSN.
[107]	LTSM + Gaussian Bayes	Improved the detection accuracy. The cost power for WSN intrusion detection was determined.	Not enough benchmark studies existed.
[99]	MLP + GA	Improved the detection accuracy	No analysis existed for intrusion detection power consumption in WSN

authors comprehensively describe a classifier that integrates techniques from ML and DL. The methods provided better results compared to an alternative strategy that used a combination of an MLP model and a GA to detect impacts in WSNs. LTSM and Gaussian Bayes models were combined to achieve this result [109]. In their paper, the authors explain the methodology used in training an ML model to detect the purpose of intruder detection. This approach involves a hierarchical structure consisting of a manager [110]. The model was found to have possible security vulnerabilities. The problems can be mitigated by implementing measures to restrict communication between nodes. After the initial phase, controls were established using DTs, ANN, NB, and LR techniques. The study should have included a comprehensive analysis of the specific modifications and improvements the researchers made when implementing SDN practices to align with their recommended methodology. The study by [111] used ANN, evolutionary computations, and the arithmetic optimization approach to develop a framework for AI with superior intelligence compared to human capabilities. Just as SDN has been deployed to help identify cyber activity. The change came through the implementation of a software-defined network. The optimization process integrates techniques with an innovative method called feature extraction, which collects data from website content and URLs. The entire data packets that the user sends are removed from the system. The present study used the NB technique to transform actual data into attributes. When a change is made to a flow rule within the library, the controller informs the switches. This document guides managers on the appropriate handling procedures for each package that meets the specified requirements. The identical action is repeated if there is no corresponding element in the rule action table.

VIII. ERROR DETECTION

ML approaches are considered the most essential methods for problem identification. WSNs can face challenges arising from differences in operating systems, hardware configurations, and other components. Advanced application detection techniques are required to identify security vulnerabilities in WSNs efficiently. The authors of [112] used different classification algorithms, including ANN, ELM, SVM, and Recurrent Learning Machines. However, this approach does not consider the potential occurrence of a failure in a WSN node. In the study by [113], the authors integrated the SVM regression model with conventional ML approaches. In a previous study, the authors used SVM classification techniques to detect and classify vulnerabilities in WSNs [114]. The authors of [115] used a combination of recursive principal component analysis and a multi-class support vector data description classifier to efficiently detect anomalies in data streams. To determine the problem with WSNs, a simple recursive technique for analyzing core components was used. The SVDD approach successfully distinguished between different error types. A deeper understanding of the physiological response of the body's sensory system in the event of an error could help medical diagnoses. The author of reference [116] presented a method to detect errors in the body detection network by studying the temporal and spatial interactions between sensors using a Bayesian network approach. Furthermore, a study by [117] proposed analyzing battery life and network data to detect faulty nodes within WSNs. Identifying faulty nodes becomes visible in the subsequent round of design testing. In the first phase of analysis, a naive Bayesian technique was used. Empirical evidence shows that this approach produces accurate results. Additionally, researchers designed it to effectively manage and allocate nodes within a wireless network using fuzzy parameters. The main objective of this technique was to determine the most efficient routes to the base station, thus allowing degraded WSN nodes to be reused. Improving the security and reliability of networks and services is a crucial outcome. By observing abnormal responses from the sensors, researchers developed the k-NN method to discriminate between faulty nodes and traditional WSN nodes effectively [118]. WSN component uses the error rate of nodes exhibiting abnormal behavior as a troubleshooting tool. Table8 illustrates the ML methods for error detection.

A. CONGESTION CONTROL

Integrating congestion control into the context of service quality is a concept specific individual's advocate. However, it is undoubtedly crucial to ensure the usability of the network

TABLE 8. ML-based error detection.

Reference	Method	Acuuracy	Limitations
[119]	SVM, KNN, and RNN	97%	Calculating the reliability of the decision is complex
[120]	Hidden Markov model + NNs	96%	Training speed is slow
[121]	SVM	99%	Does not consider the load management between nodes
[122]	SVM + PCA	99%	complexity is high

for all users. ML methods have greatly facilitated progress in this particular area. Congestion occurs when a node or its communication route is flooded with data that exceeds its processing capacity [69]. Congestion can be caused by various circumstances, including but not limited to high transmission rates, packet collisions, dynamic time shifts, and systems that allow data to be sent to multiple destinations simultaneously. Congestion has broader implications than simple travel time between two points. In addition, it affects energy consumption and the occurrence of packet loss. One possible approach to mitigating congestion is to use ML algorithms that use network traffic analysis to determine the most efficient route. Previous research used Random Early Detection [97] to identify congested areas and predict the likelihood of packet loss. The proposed protocol improves the data transfer efficiency at each WSN node and reduces the buffer queue size by utilizing the principles of percent integration differencing theory and FL. The approach consists of three sequential steps: first, identifying and reporting congestion; second, the change in transmission rate; and finally, once again, the identification and reporting of traffic jams. RED and fuzzy PID thresholds are first implemented to identify high-activity areas. The use of RED and Fuzzy PID thresholds will be implemented first. In the event of traffic jams, reports are automatically generated and distributed. A fuzzy controller adjusts the transmission rate to deal effectively with the overload. In addition, the authors of [98] use an active queue management method by monitoring the cumulative buffers to anticipate potential traffic volume problems. The process involves determining the number of packets lost given the line length and changing the queue size to accommodate that amount. The researchers used a novel approach to address the delays at WSN nodes. The close integration derivative controller's percentage, integral, and derivative values are adjusted via a live weight system. This system takes advantage of the inherent ability of neurons to self-learn and self-regulate. According to reference [99], PSO can be used to determine the optimal control parameters for proportional, integral, and derivative control and the most appropriate learning rates for neurons. This strategy aims to achieve the desired result efficiently and quickly. The buffer overflow problem in cluster nodes was investigated in a separate study using the fuzzy clustering method [100]. Using FL may be a more beneficial approach to congestion mitigation in specific scenarios.

IX. OPEN ISSUES

A. LOCATION OF THE ML TRAINING PROCESS

Due to the lack of a central location for ML training within this particular network architecture and the sharing of CPU and power resources of all embedded devices, this location becomes indispensable for the deployment of ML. In a significant part of the research studies on ML techniques [108], there is a need for more clarity on the specific implementation of these algorithms in WSNs. The proper educational context for training these methods remains unclear, as extensive previous research has facilitated the identification of attacks and faulty nodes [101]. The level of performance degradation that occurs when using these embedded devices for training or to identify the origin of DoS.

B. LIGHTWEIGHT ML ALGORITHMS

Furthermore, it has come to our attention that specific authors have implemented complex ML algorithms to enhance accuracy and efficiency without adequately considering the hardware requirements [123]. As previously mentioned, ML algorithms can be categorized into various groups, each accompanied by algorithms that contribute to reducing training time and improving accuracy. Therefore, there is a potential to develop a hybrid ML approach that is lightweight and well-suited for embedded devices. Additionally, it is conceivable to enhance the capabilities of WSN nodes to differentiate between types of ML algorithms and automatically select the most appropriate one based on factors such as data type, volume, and remaining power. This aspect represents an open issue that researchers should address to further advancements in the field. Moreover, none of the reviewed studies concerning ML applications supporting WSN security addressed using reinforcement learning [124] or transfer learning [125]. These technologies are increasingly becoming a focal point in the future of ML. Reinforcement learning relies on experience-based learning rather than training on data, while transfer learning is based on leveraging pre-trained models. Thus, exploring both these methods, alongside Software-Defined Networking [126], is another avenue to consider in future research endeavours. There are two main difficulties with using reinforcement learning (RL) in wireless networks: computational complexity and convergence. The huge state and action spaces in RL for wireless networks introduce computational complexity. The exponentially huge state spaces of wireless networks are the result of their dynamic environments and multiple characteristics (such as channel statuses, user demands, and network structure). The processing resources and time required to process these states and make optimal decisions provide a substantial challenge for real-time applications. The capacity of the RL algorithm to converge on a stable optimal policy is the second significant concern. It is challenging to ensure that the RL algorithm reliably converges to an optimal or near-optimal solution in the dynamic environment of wireless networks, where network conditions and parameters are constantly changing. The performance and dependability of the network's decisions can be negatively impacted by the non-stationarity of wireless networks, which can cause learning algorithms to become stuck in local optima or take too long to converge.

C. PRIVACY CONCERNS

As previously mentioned, all WSN nodes are uniform in terms of CPU, energy, and tasks, and they operate in dynamic and mobile environments [127] leading to constantly changing interrelationships between nodes during communication. Consequently, the nodes' current authentication mechanism must be revised to cope with such dynamic changes. To address this issue, the authors have proposed a novel approach by leveraging the first layer (physical layer) in the authentication process and incorporating ML algorithms to assist with authentication. This innovative solution offers advantages such as reduced synchronization and acknowledgement requirements, leading to node energy savings [128]. However, one of the unresolved concerns is the privacy condition. The privacy of sensors remains vulnerable to potential hacking by peers, whether intentionally or unintentionally. Therefore, researchers must explore and develop methods to enhance sensor privacy, safeguarding them from potential threats. This remains an open field for further investigation and improvements in WSN security [129].

D. TRUST DOMAIN

One critical aspect that can significantly enhance the security of WSNs is the establishment of trust between WSN nodes [109]. To achieve this, the adjacent of each WSN node is observed and analyzed using ML algorithms. Nodes with a positive reputation among their adjacent nodes are labelled "Reliable," establishing a sense of trust within the network [130]. This process entails an improved management system for WSNs, enabling the analysis of each node's adjacent and facilitating sharing of results with other nodes. ML algorithms play a vital role in this context, as they are responsible for the adjacent analysis of adjacent nodes, working in collaboration with the SD-Controller [131]. By fostering trust through behavioral observation and ML-based assessments, the security of WSNs can be significantly enhanced as the network becomes more adept at identifying and relying on nodes with a proven track record of reliability [132]. Figure 11 illustrates some open issues in WSN.

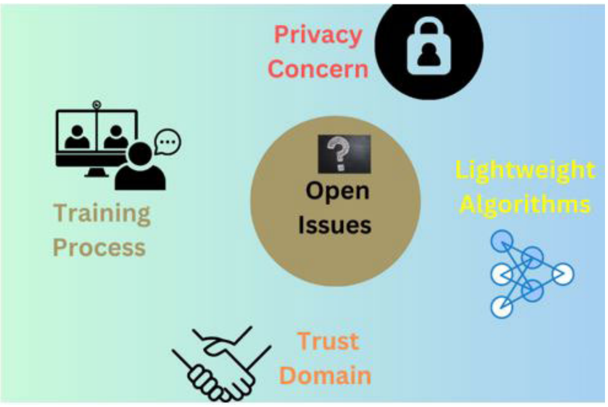


FIGURE 11. Open issues [133].

X. CONCLUSION

WSNs are crucial in performing routine tasks across various environments, such as data collection and monitoring. The rise of the IoT has further increased the reliance on WSNs due to their simplicity, specialization capabilities, and cost-effectiveness. However, this proliferation has also brought about several challenges, with security being a prominent concern. Ensuring fundamental security in WSNs is particularly challenging due to their inherent CPU and power resource limitations. Consequently, novel approaches are necessary to address these security issues effectively. ML methodologies have emerged as promising solutions to tackle these challenges. Nevertheless, adapting ML algorithms to WSNs comes with its own set of difficulties. This paper comprehensively studies the WSN infrastructure, environmental factors, applications, operational processes, and the security challenges associated with these networks. The research delves into the ML algorithms employed in addressing WSN security concerns and analyzes recent studies focused on enhancing WSN security using ML techniques. The advantages and disadvantages of each study are carefully examined. Moreover, this paper endeavors to present future solutions that can harness the potential of ML algorithms in bolstering WSN security. These algorithms show great promise for the security domain in WSNs and are considered critical enablers for further advancements in this field. Through statistical analysis, intrusion and error detection are the most common applications of ML algorithms in WSN security. By leveraging these ML-based approaches, researchers aim to fortify the security of WSNs, making them more resilient and effective in their data collection and monitoring tasks.

XI. FUTURE WORK

Integrating SDN technology with ML algorithms presents an optimistic and strategic approach to enhance security in WSNs further. SDN separates the control plane from the data plane, allowing for centralized control and programmability of the network, which can significantly improve the efficiency and flexibility of WSN nodes. By utilizing SDN, WSN nodes can offload specific tasks related to security management to a centralized controller, relieving the nodes from complex computations and memory-intensive operations. The centralized controller can implement ML-based security algorithms and decision-making processes, enabling more efficient real-time threat detection and response. Here are some new avenues and potential benefits of combining ML with SDN in WSN security:

A. ADAPTIVE SECURITY

SDN allows dynamic network reconfiguration based on real-time conditions. By integrating ML algorithms, the network can adaptively adjust security settings, detect anomalies, and respond proactively and precisely to emerging threats.

B. ENERGY EFFICIENCY

ML algorithms, combined with SDN, can optimize energy consumption by strategically managing data transmission and activating specific security mechanisms only when necessary. This leads to reduced energy usage and extended node lifespan.

C. SCALABILITY

SDN's centralized control facilitates more effortless scalability of the WSN. When ML algorithms optimize the security framework, the network can effectively handle a more significant number of nodes and data streams, accommodating future growth and expansion.

D. ANOMALY DETECTION

ML algorithms excel in identifying patterns and anomalies in data. By leveraging SDN's programmability, ML-based anomaly detection techniques can be seamlessly integrated into the network, enabling rapid identification of unusual activities and potential security breaches.

E. SECURITY ORCHESTRATION

ML-powered SDN can streamline security orchestration, automating incident response and mitigation procedures. This reduces human intervention and enhances the network's ability to react quickly to security incidents.

F. ADAPTIVE RESOURCE ALLOCATION

SDN with ML can dynamically allocate resources to nodes based on their security requirements and the overall network traffic, ensuring that critical security tasks receive priority without compromising other network functionalities.

ML techniques like federated learning or secure multi-party computation can be incorporated into SDN-enabled WSNs to maintain data privacy while benefiting from collaborative security analysis. By exploring these new avenues and leveraging the synergies between ML and SDN, researchers can significantly advance the security capabilities of WSNs, making them more resilient, efficient, and cost-effective in safeguarding critical data and operations. Collaboration among researchers, industry stakeholders, and policymakers is crucial to foster innovation and implement these advanced security measures in real-world applications

REFERENCES

[1] M. Bouaziz and A. Rachedi, "A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology," *Comput. Commun.*, vol. 74, pp. 3–15, Jan. 2016.

[2] H. A. A. Al-Kashoash, H. Kharrufa, Y. Al-Nidawi, and A. H. Kemp, "Congestion control in wireless sensor and 6LoWPAN networks: Toward the Internet of Things," *Wireless Netw.*, vol. 25, no. 8, pp. 4493–4522, Nov. 2019.

[3] M. A. Moridi, Y. Kawamura, M. Sharifzadeh, E. K. Chanda, M. Wagner, and H. Okawa, "Performance analysis of ZigBee network topologies for underground space monitoring and communication systems," *Tunnelling Underground Space Technol.*, vol. 71, pp. 201–209, Jan. 2018.

[4] M. A. Ertürk, M. A. Aydın, M. T. Büyükakkaşlar, and H. Evirgen, "A survey on LoRaWAN architecture, protocol and technologies," *Future Internet*, vol. 11, no. 10, p. 216, Oct. 2019.

[5] S. Schwendemann, Z. Amjad, and A. Sikora, "A survey of machine-learning techniques for condition monitoring and predictive maintenance of bearings in grinding machines," *Comput. Ind.*, vol. 125, Feb. 2021, Art. no. 103380.

[6] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019.

[7] P. Nayak, G. K. Swetha, S. Gupta, and K. Madhavi, "Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities," *Measurement*, vol. 178, Jun. 2021, Art. no. 108974.

[8] W. Gouda, S. Tahir, S. Alanazi, M. Almufareh, and G. Alwakid, "Unsupervised outlier detection in IoT using deep VAE," *Sensors*, vol. 22, no. 17, p. 6617, Sep. 2022.

[9] A. A. Rezaee and F. Pasandideh, "A fuzzy congestion control protocol based on active queue management in wireless sensor networks with medical applications," *Wireless Pers. Commun.*, vol. 98, no. 1, pp. 815–842, Jan. 2018.

[10] M. Masdari, "Energy efficient clustering and congestion control in WSNs with mobile sinks," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 611–642, Mar. 2020.

[11] G. Sangeetha, "A heuristic path search for congestion control in WSN," in *Industry Interactive Innovations in Science, Engineering and Technology*. Cham, Switzerland: Springer, 2018.

[12] S. Chen, H. Wen, J. Wu, J. Chen, W. Liu, L. Hu, and Y. Chen, "Physical-layer channel authentication for 5G via machine learning algorithm," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–10, Oct. 2018.

[13] R. I. Bhopal, "Evolution of fifth generation technology in wireless communication," 2023.

[14] V. Kumar and S. Tiwari, "Routing in IPv6 over low-power wireless personal area networks (6LoWPAN): A survey," *J. Comput. Netw. Commun.*, vol. 2012, pp. 1–10, Mar. 2012.

[15] K. A. Darabkh, M. Z. El-Yabroudi, and A. H. El-Mousa, "BPA-CRP: A balanced power-aware clustering and routing protocol for wireless sensor networks," *Ad Hoc Netw.*, vol. 82, pp. 155–171, Jan. 2019.

[16] K. A. Darabkh, N. J. Al-Maaitah, I. F. Jafar, and A. F. Khalifeh, "EA-CRP: A novel energy-aware clustering and routing protocol in wireless sensor networks," *Comput. Electr. Eng.*, vol. 72, pp. 702–718, Nov. 2018.

[17] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Netw.*, vol. 115, Apr. 2021, Art. no. 102448.

[18] R. Ahmad, E. A. Sundararajan, and T. Abu-Ain, "Analysis the effect of clustering and lightweight encryption approaches on WSNs lifetime," in *Proc. Int. Conf. Electr. Eng. Informat. (ICEEI)*, Oct. 2021, pp. 1–6.

[19] M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," *Comput. Commun.*, vol. 134, pp. 52–69, Jan. 2019.

[20] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Gener. Comput. Syst.*, vol. 129, pp. 77–89, Apr. 2022.

[21] H. Sharma, A. Haque, and F. Blaabjerg, "Machine learning in wireless sensor networks for smart cities: A survey," *Electronics*, vol. 10, no. 9, p. 1012, Apr. 2021.

[22] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, and M. Cao, "Deep-learning-based physical layer authentication for industrial wireless sensor networks," *Sensors*, vol. 19, no. 11, p. 2440, May 2019.

[23] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, "Physical layer authentication based on channel information and machine learning," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 364–365.

[24] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51915–51932, 2019.

[25] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," *Sensors*, vol. 22, no. 13, p. 4730, Jun. 2022.

[26] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless sensor network security: A recent review based on state-of-the-art works," *Int. J. Eng. Bus. Manage.*, vol. 15, Jan. 2023, Art. no. 184797902311572.

[27] R. A. Al-Kaabi, H. F. Fakhruldeen, and H. A.-J. Al-Asady, "An overview of the status, challenges, and trends of the advanced crypto algorithms to enhance the security of wireless networks," *AIP Conf. Proc.*, vol. 2591, no. 1, 2023, Art. no. 030039.

[28] Y. Chang, H. Tang, Y. Cheng, Q. Zhao, and B. Yuan, "Dynamic hierarchical energy-efficient method based on combinatorial optimization for wireless sensor networks," *Sensors*, vol. 17, no. 7, p. 1665, Jul. 2017.

[29] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, "A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 550–586, 1st Quart., 2017.

[30] Y. Chang, X. Yuan, B. Li, D. Niyato, and N. Al-Dhahir, "A joint unsupervised learning and genetic algorithm approach for topology control in energy-efficient ultra-dense wireless sensor networks," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2370–2373, Nov. 2018.

[31] P. William, "Analysis of data aggregation and clustering protocol in wireless sensor networks using machine learning," in *Evolutionary Computing and Mobile Sustainable Networks*. Cham, Switzerland: Springer, 2022, pp. 925–939.

[32] D. Shinkar, "Wireless voice transmission using WiFi and Bluetooth on Android platform," *Int. J.*, vol. 3, no. 2, pp. 1–6, 2018.

[33] H. Hong, Y. Kim, and R. Kim, "A low-power WLAN communication scheme for IoT WLAN devices using wake-up receivers," *Appl. Sci.*, vol. 8, no. 1, p. 72, Jan. 2018.

[34] M. Gupta and S. Singh, "A survey on the zigbee protocol, its security in Internet of Things (IoT) and comparison of zigbee with Bluetooth and Wi-Fi," in *Applications of Artificial Intelligence in Engineering*. Cham, Switzerland: Springer, 2021.

[35] I. A. Ismaili, "Comparative study of ZigBee and 6LoWPAN protocols," in *Proc. ICCWCS 3rd Int. Conf. Comput. Wireless Commun. Syst.*, Apr. 2019, p. 264.

[36] O. A. G. Osorio, B. S. R. Daza, and O. J. S. Parra, "Comparative study of performance for 804.15. 4 ZigBee and 6LoWPAN protocols," in *Proc. SOFSEM (Student Res. Forum Papers/Posters)*, vol. 1548, 2016, pp. 59–71.

[37] Salau, A.O., N. Marriwala, and M. Athaee, "Data security in wireless sensor networks: Attacks and countermeasures," in *Mobile Radio Communications and 5G Networks*. Cham, Switzerland: Springer, 2021.

[38] M. N. Ismail, M. Shukran, M. R. Mohd Isa, M. Adib, and O. Zakaria, "Establishing a soldier wireless sensor network (WSN) communication for military operation monitoring," *Int. J. Informat. Commun. Technol. (IJ-ICT)*, vol. 7, no. 2, p. 89, Aug. 2018.

[39] J. Bhola, S. Soni, and G. K. Cheema, "Recent trends for security applications in wireless sensor networksa technical review," in *Proc. 6th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2019, pp. 707–712.

[40] M. Majid, S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu, and J. C.-W. Lin, "Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, p. 2087, Mar. 2022.

[41] G. Marques, J. Saini, M. Dutta, P. K. Singh, and W.-C. Hong, "Indoor air quality monitoring systems for enhanced living environments: A review toward sustainable smart cities," *Sustainability*, vol. 12, no. 10, p. 4024, May 2020.

[42] S. Rani, *ntegration of WSN and IoT for Smart Cities*. Cham, Switzerland: Springer, 2020.

[43] Z. Zhang, A. Mehmood, L. Shu, Z. Huo, Y. Zhang, and M. Mukherjee, "A survey on fault diagnosis in wireless sensor networks," *IEEE Access*, vol. 6, pp. 11349–11364, 2018.

[44] J. Wang, S. Jiang, and A. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors*, vol. 17, no. 6, p. 1227, May 2017.

[45] M. Z. Hasan and Z. Mohd Hanapi, "Efficient and secured mechanisms for data link in IoT WSNs: A literature review," *Electronics*, vol. 12, no. 2, p. 458, Jan. 2023.

[46] B. Savoudsou, B. Yenke, T. Yelemou, M. Atemkeng, and F. Tchakount, "An enhanced dissection of attacks in wireless sensor networks," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 589–612, Aug. 2023.

[47] A. D. Nimbalkar, A. Azmat, and Y. Patil, "Security issues in wireless sensor networks," *I-Manager's J. Wireless Commun. Netw.*, vol. 11, no. 2, p. 32, 2023.

[48] K. Haseeb, K. Abu Bakar, A. H. Abdullah, and A. Ahmed, "Grid based cluster head selection mechanism for wireless sensor network," *TELKOMNIKA (Telecommun. Comput. Electron. Control)*, vol. 13, no. 1, p. 269, Mar. 2015.

[49] S. Tabibi and A. Ghaffari, "Energy-efficient routing mechanism for mobile sink in wireless sensor networks using particle swarm optimization algorithm," *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 199–216, Jan. 2019.

[50] Y. Chang, W. Chen, J. Li, J. Liu, H. Wei, Z. Wang, and N. Al-Dhahir, "Collaborative multi-BS power management for dense radio access network using deep reinforcement learning," *IEEE Trans. Green Commun. Netw.*, 2023.

[51] Y. Chang, X. Yuan, B. Li, D. Niyato, and N. Al-Dhahir, "Machine-learning-based parallel genetic algorithms for multi-objective optimization in ultra-reliable low-latency WSNs," *IEEE Access*, vol. 7, pp. 4913–4926, 2019.

[52] S. Siamala Devi, C. Kuruba, Y. Nam, and M. Abouhawwash, "Hybrid optimisation with black hole algorithm for improving network lifespan," *Intell. Autom. Soft Comput.*, vol. 35, no. 2, pp. 1873–1887, 2023.

[53] D. Praveen Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Inf. Fusion*, vol. 49, pp. 1–25, Sep. 2019.

[54] S. Modak, D. Sehgal, and J. Valadi, "Applications of artificial intelligence and machine learning in viral biology," in *Global Virology III: Virology in the 21st Century*, 2019, pp. 1–39.

[55] G. Vashisht, "ML algorithms for smart sensor networks," in *Smart Sensor Networks: Analytics, Sharing and Control*. Cham, Switzerland: Springer, 2021, pp. 73–103.

[56] M. S. I. Sagar, H. Ouassal, A. I. Omi, A. Wisniewska, H. M. Jalajamony, R. E. Fernandez, and P. K. Sekhar, "Application of machine learning in electromagnetics: Mini-review," *Electronics*, vol. 10, no. 22, p. 2752, Nov. 2021.

[57] M. Ali, L. T. Jung, A.-H. Abdel-Aty, M. Y. Abubakar, M. Elhoseny, and I. Ali, "Semantic-k-NN algorithm: An enhanced version of traditional k-NN algorithm," *Expert Syst. Appl.*, vol. 151, Aug. 2020, Art. no. 113374.

[58] I. H. Sarker, A. Colman, J. Han, A. I. Khan, Y. B. Abushark, and K. Salah, "BehavDT: A behavioral decision tree learning to build user-centric context-aware predictive model," *Mobile Netw. Appl.*, vol. 25, no. 3, pp. 1151–1161, Jun. 2020.

[59] R. F. Bikmukhamedov and A. F. Nadeev, "Lightweight machine learning classifiers of IoT traffic flows," in *Proc. Syst. Signal Synchronization, Generating Process. Telecommun. (SYNCHROINFO)*, Jul. 2019, pp. 1–5.

[60] A. Sekulić, M. Kilibarda, G. B. M. Heuvelink, M. Nikolić, and B. Bajat, "Random forest spatial interpolation," *Remote Sens.*, vol. 12, no. 10, p. 1687, May 2020.

[61] Pisner, D.A. and D.M. Schnyer, "Support vector machine," in *Machine Learning*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 101–121.

[62] R. Muzzammel and A. Raza, "A support vector machine learning-based protection technique for MT-HVDC systems," *Energies*, vol. 13, no. 24, p. 6668, Dec. 2020.

[63] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private naive Bayes learning over multiple data sources," *Inf. Sci.*, vol. 444, pp. 89–104, May 2018.

[64] C.-H. Lee, "An information-theoretic filter approach for value weighted classification learning in naive Bayes," *Data Knowl. Eng.*, vol. 113, pp. 116–128, Jan. 2018.

[65] P.-T. Ngo, N.-D. Hoang, B. Pradhan, Q. Nguyen, X. Tran, Q. Nguyen, V. Nguyen, P. Samui, and D. T. Bui, "A novel hybrid swarm optimized multilayer neural network for spatial prediction of flash floods in tropical areas using Sentinel-1 SAR imagery and geospatial data," *Sensors*, vol. 18, no. 11, p. 3704, Oct. 2018.

[66] C.-Y.-J. Peng, K. L. Lee, and G. M. Ingersoll, "An introduction to logistic regression analysis and reporting," *J. Educ. Res.*, vol. 96, no. 1, pp. 3–14, Sep. 2002.

[67] G. Wang, X. Yang, L. Wu, Z. Fu, X. Ma, Y. He, and B. Peng, "A kernel recursive minimum error entropy adaptive filter," *Signal Process.*, vol. 193, Apr. 2022, Art. no. 108410.

[68] R. M. Sonia, "A review on classification of machine learning," *Lampyrid, J. Bioluminescent Beetle Res.*, vol. 13, pp. 758–767, May 2023.

[69] K. P. Sinaga and M.-S. Yang, "Unsupervised K-means clustering algorithm," *IEEE Access*, vol. 8, pp. 80716–80727, 2020.

[70] S. Kambalimath and P. C. Deka, "A basic review of fuzzy logic applications in hydrology and water resources," *Appl. Water Sci.*, vol. 10, no. 8, pp. 1–14, Aug. 2020.

[71] P. Yadav and S. C. Sharma, "A systematic review of localization in WSN: Machine learning and optimization-based approaches," *Int. J. Commun. Syst.*, vol. 36, no. 4, Mar. 2023, Art. no. e5397.

[72] G. Lăzăroiu, M. Andronie, M. Iatagan, M. Geamănu, R. Ştefănescu, and I. Dijmărescu, "Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the Internet of manufacturing things," *ISPRS Int. J. Geo-Inf.*, vol. 11, no. 5, p. 277, Apr. 2022.

[73] J. F. Barraza, E. López Droguett, and M. R. Martins, "Towards interpretable deep learning: A feature selection framework for prognostics and health management using deep neural networks," *Sensors*, vol. 21, no. 17, p. 5888, Sep. 2021.

[74] A. Alahmadi, M. Hussain, and H. Aboalsamh, "LDA-CNN: Linear discriminant analysis convolution neural network for periocular recognition in the wild," *Mathematics*, vol. 10, no. 23, p. 4604, 2022.

[75] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a convolutional neural network," in *Proc. Int. Conf. Eng. Technol. (ICET)*, Aug. 2017, pp. 1–6.

[76] T. Kim, L. F. Vecchietti, K. Choi, S. Lee, and D. Har, "Machine learning for advanced wireless sensor networks: A review," *IEEE Sensors J.*, vol. 21, no. 11, pp. 12379–12397, Jun. 2021.

[77] S.-C. Lim, J.-H. Huh, S.-H. Hong, C.-Y. Park, and J.-C. Kim, "Solar power forecasting using CNN-LSTM hybrid model," *Energies*, vol. 15, no. 21, p. 8233, Nov. 2022.

[78] A. Sherstinsky, "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network," *Phys. D, Nonlinear Phenomena*, vol. 404, Mar. 2020, Art. no. 132306.

[79] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink, and J. Schmidhuber, "LSTM: A search space Odyssey," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2222–2232, Oct. 2017.

[80] G. V. Reddy et al., "An intrusion detection using machine learning algorithm multi-layer perceptron (MlP): A classification enhancement in wireless sensor network (WSN)," 2022.

[81] Y. Xue, Y. Tong, and F. Neri, "An ensemble of differential evolution and Adam for training feed-forward neural networks," *Inf. Sci.*, vol. 608, pp. 453–471, Aug. 2022.

[82] D. S. Manoharan and P. Sathish, "Population based meta heuristics algorithm for performance improvement of feed forward neural network," *J. Soft Comput. Paradigm*, vol. 2, no. 1, pp. 36–46, Mar. 2020.

[83] M. Elhoseny, X. Yuan, H. K. El-Minir, and A. M. Riad, "An energy efficient encryption method for secure dynamic WSN," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2024–2031, Sep. 2016.

[84] T. Mazhar, R. N. Asif, M. A. Malik, M. A. Nadeem, I. Haq, M. Iqbal, M. Kamran, and S. Ashraf, "Electric vehicle charging system in the smart grid using different machine learning methods," *Sustainability*, vol. 15, no. 3, p. 2603, Feb. 2023.

[85] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, and A. Tolba, "A greedy model with small world for improving the robustness of heterogeneous Internet of Things," *Comput. Netw.*, vol. 101, pp. 127–143, Jun. 2016.

[86] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. 6, pp. 7234–7243, 2018.

[87] R. Zakrzewski, T. Martin, and G. Oikonomou, "Topology change localisation in WSNs," in *Proc. 11th Medit. Conf. Embedded Comput. (MECO)*, Jun. 2022, pp. 1–6.

[88] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, "RobustTrust—A pro-privacy robust distributed trust management mechanism for Internet of Things," *IEEE Access*, vol. 7, pp. 62095–62106, 2019.

[89] L. Wei, J. Wu, and C. Long, "Blockchain-enabled trust management in service-oriented Internet of Things: Opportunities and challenges," in *Proc. 3rd Int. Conf. Blockchain Technol.*, 2021, pp. 90–95.

[90] E. Alemneh, S.-M. Senouci, P. Brunet, and T. Tegegne, "A two-way trust management system for fog computing," *Future Gener. Comput. Syst.*, vol. 106, pp. 206–220, May 2020.

[91] M. Pundir and J. K. Sandhu, "A systematic review of quality of service in wireless sensor networks using machine learning: Recent trend and future vision," *J. Netw. Comput. Appl.*, vol. 188, Aug. 2021, Art. no. 103084.

[92] S. C. Padwal, M. Kumar, P. Balaramudu, and C. K. Jha, "Analysis of environment changes using WSN for IoT applications," in *Proc. 2nd Int. Conf. Converg. Technol. (I2CT)*, Apr. 2017, pp. 27–32.

[93] J. Amutha, S. Sharma, and S. K. Sharma, "Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100376.

[94] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, "Safety, security and privacy in machine learning based Internet of Things," *J. Sensor Actuator Netw.*, vol. 11, no. 3, p. 38, Jul. 2022.

[95] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The rise of 'Internet of Things': Review and open research issues related to detection and prevention of IoT-based security attacks," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Aug. 2022.

[96] M. Sajjad, T. Safdar Malik, S. Khurram, A. A. Gardezi, F. Alassery, H. Hamam, O. Cheikhrouhou, and M. Shafiq, "Efficient joint key authentication model in E-healthcare," *Comput., Mater. Continua*, vol. 71, no. 2, pp. 2739–2753, 2022.

[97] T. Mazhar, H. M. Irfan, S. Khan, I. Haq, I. Ullah, M. Iqbal, and H. Hamam, "Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods," *Future Internet*, vol. 15, no. 2, p. 83, Feb. 2023.

[98] R. Ahmad, R. Wazirali, Q. Bsoul, T. Abu-Ain, and W. Abu-Ain, "Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime," *Sensors*, vol. 21, no. 14, p. 4821, Jul. 2021.

[99] R. Wazirali and R. Ahmad, "Machine learning approaches to detect DoS and their effect on WSNs lifetime," *Comput., Mater. Continua*, vol. 70, no. 3, pp. 4922–4946, 2022.

[100] C. Ioannou and V. Vassiliou, "An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression," in *Proc. 21st ACM Int. Conf. Modeling, Anal. Simulation Wireless Mobile Syst.*, Oct. 2018, pp. 259–263.

[101] Q. Tian, X. Lu, L. Duan, and D. Han, "Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network," *Int. J. Comput. Sci. Eng.*, vol. 1, no. 1, pp. 221–232, 2020.

[102] G. M. Borkar, L. H. Patil, D. Dalgade, and A. Hutke, "A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept," *Sustain. Comput., nformat. Syst.*, vol. 23, pp. 120–135, Sep. 2019.

[103] S. El Khediri, "MWLEACH: Low energy adaptive clustering hierarchy approach for WSN," *IET Wireless Sensor Syst.*, vol. 10, no. 3, pp. 126–129, 2020.

[104] M. Z. Ghawy, G. A. Amran, H. AlSalman, E. Ghaleb, J. Khan, A. A. AL-Bakhrani, A. M. Alziadi, A. Ali, and S. S. Ullah, "An effective wireless sensor network routing protocol based on particle swarm optimization algorithm," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–13, May 2022.

[105] N. Temene, C. Sergiou, C. Georgiou, and V. Vassiliou, "A survey on mobility in wireless sensor networks," *Ad Hoc Netw.*, vol. 125, Feb. 2022, Art. no. 102726.

[106] C. Fernandez-Basso, K. Gutiérrez-Batista, R. Morcillo-Jiménez, M.-A. Vila, and M. J. Martin-Bautista, "A fuzzy-based medical system for pattern mining in a distributed environment: Application to diagnostic and co-morbidity," *Appl. Soft Comput.*, vol. 122, Jun. 2022, Art. no. 108870.

[107] R. A. Ahmad, M. Azhar, and H. Sattar, "An image captioning algorithm based on the hybrid deep learning technique (CNN+GRU)," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2022, pp. 124–129.

[108] E. Mushtaq, A. Zameer, and A. Khan, "A two-stage stacked ensemble intrusion detection system using five base classifiers and MLP with optimal feature selection," *Microprocessors Microsyst.*, vol. 94, Oct. 2022, Art. no. 104660.

[109] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, "LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5244–5253, Aug. 2020.

[110] A. A. Najar and S. M. Naik, "DDoS attack detection using MLP and random forest algorithms," *Int. J. Inf. Technol.*, vol. 14, no. 5, pp. 2317–2327, Aug. 2022.

[111] K. J. Singh and T. De, "MLP-GA based algorithm to detect application layer DDoS attack," *J. Inf. Secur. Appl.*, vol. 36, pp. 145–153, Oct. 2017.

[112] M. Emperuman and S. Chandrasekaran, "Hybrid continuous density hmm-based ensemble neural networks for sensor fault detection and classification in wireless sensor network," *Sensors*, vol. 20, no. 3, p. 745, Jan. 2020.

[113] S. Zidi, T. Moulahi, and B. Alaya, "Fault detection in wireless sensor networks through SVM classifier," *IEEE Sensors J.*, vol. 18, no. 1, pp. 340–347, Jan. 2018.

[114] D. A. Tran and T. Nguyen, "Localization in wireless sensor networks based on support vector machines," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 7, pp. 981–994, Jul. 2008.

[115] Q.-Y. Sun, "Study on fault diagnosis algorithm in WSN nodes based on RPCA model and SVDD for multi-class classification," *Cluster Comput.*, vol. 22, pp. 6043–6057, May 2019.

[116] M. Masdari and S. Özdemir, "Towards coverage-aware fuzzy logic-based faulty node detection in heterogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 581–610, Mar. 2020.

[117] R. R. Swain and P. M. Khilar, "Composite fault diagnosis in wireless sensor networks using neural networks," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2507–2548, Aug. 2017.

[118] P. Chanak and I. Banerjee, "Fuzzy rule-based faulty node classification and management scheme for large scale wireless sensor networks," *Expert Syst. Appl.*, vol. 45, pp. 307–321, Mar. 2016.

[119] W. He, P.-L. Qiao, Z.-J. Zhou, G.-Y. Hu, Z.-C. Feng, and H. Wei, "A new belief-rule-based method for fault diagnosis of wireless sensor network," *IEEE Access*, vol. 6, pp. 9404–9419, 2018.

[120] A. R. A. Moundounga, H. Satori, Y. Boutazart, and E. Abderrahim, "Malicious attack detection based on continuous hidden Markov models in wireless sensor networks," *Microprocessors Microsyst.*, vol. 101, Sep. 2023, Art. no. 104888.

[121] S. R. Jondhale, V. Mohan, B. B. Sharma, J. Lloret, and S. V. Athawale, "Support vector regression for mobile target localization in indoor environments," *Sensors*, vol. 22, no. 1, p. 358, Jan. 2022.

[122] L. Chelouah, F. Semchedine, and L. Bouallouche-Medjkoune, "Localization protocols for mobile wireless sensor networks: A survey," *Comput. Electr. Eng.*, vol. 71, pp. 733–751, Oct. 2018.

[123] I. Chakraborty, M. Ali, A. Ankit, S. Jain, S. Roy, S. Sridharan, A. Agrawal, A. Raghunathan, and K. Roy, "Resistive crossbars as approximate hardware building blocks for machine learning: Opportunities and challenges," *Proc. IEEE*, vol. 108, no. 12, pp. 2276–2310, Dec. 2020.

[124] E. Puiutta and E. M. Veith, "Explainable reinforcement learning: A survey," in *Proc. Int. Cross-Domain Conf. Mach. Learn. Knowl. Extraction*. Cham, Switzerland: Springer. 2020, pp. 77–95.

[125] S. Niu, "A decade survey of transfer learning (2010–2020)," *IEEE Trans. Artif. Intell.*, vol. 1, no. 2, pp. 151–166, Oct. 2020.

[126] M. Fogli, C. Giannelli, and C. Stefanelli, "Software-defined networking in wireless ad hoc scenarios: Objectives and control architectures," *J. Netw. Comput. Appl.*, vol. 203, Jul. 2022, Art. no. 103387.

[127] A. A. Kamble and B. M. Patil, "Systematic analysis and review of path optimization techniques in WSN with mobile sink," *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100412.

[128] K. Sood, S. Yu, D. D. N. Nguyen, Y. Xiang, B. Feng, and X. Zhang, "A tutorial on next generation heterogeneous IoT networks and node authentication," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 120–126, Dec. 2021.

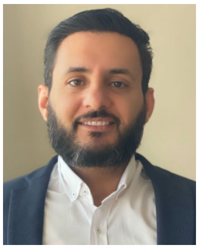
[129] B. Bhushan and G. Sahoo, "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2020, pp. 683–713.

[130] D. S. Ibrahim, A. F. Mahdi, and Q. M. Yas, "Challenges and issues for wireless sensor networks: A survey," *J. Glob. Sci. Res.*, vol. 6, no. 1, pp. 1079–1097, 2021.

[131] R. Wazirali, R. Ahmad, and A. A.-K. Abu-Ein, "Sustaining accurate detection of phishing URLs using SDN and feature selection approaches," *Comput. Netw.*, vol. 201, Dec. 2021, Art. no. 108591.

[132] T. G. Nguyen, T. V. Phan, D. T. Hoang, T. N. Nguyen, and C. So-In, "Federated deep reinforcement learning for traffic monitoring in SDN-based IoT networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 4, pp. 1048–1065, Dec. 2021.

[133] A. Djedouboum, A. A. Ari, A. Gueroui, A. Mohamadou, and Z. Aliouat, "Big data collection in large-scale wireless sensor networks," *Sensors*, vol. 18, no. 12, p. 4474, Dec. 2018.



YAZEED YASIN GHADI received the Ph.D. degree in electrical and computer engineering from The University of Queensland. Before joining Al Ain University, he was a Postdoctoral Researcher with The University of Queensland. He is currently an Assistant Professor in software engineering with Al Ain University. He has published more than 80 peer-reviewed journals and conference papers and he holds three pending patents. His current research interests include developing novel electro-acoustic-optic neural interfaces for large-scale high-resolution electrophysiology and distributed optogenetic stimulation. He was a recipient of several awards. His dissertation on developing novel hybrid plasmonic photonic on-chip biochemical sensors received the Sigma Xi Best Ph.D. Thesis Award.

TEHSEEN MAZHAR received the B.Sc. degree in computer science from Bahaudin Zakaria University, Multan, Pakistan, the M.Sc. degree in computer science from Qauid-i-Azam University, Islamabad, Pakistan, and the M.S. degree (Hons.) in computer science from the Virtual University of Pakistan, where he is currently pursuing the Ph.D. degree. He is with the School Education Department and a Lecturer with GCUF. He has more than 21 publications in well-reputed journals, such as *Electronics* (MDPI), *Health* (MDPI), *Applied Science* (MDPI), *Brain Sciences* (MDPI), *Symmetry* (MDPI), and *Future Internet* (MDPI), *Peer J*, and *Computers, Materials and Continua*. His research interests include machine learning, the Internet of Things, and networks.

TAMARA AL SHLOUL is currently an Assistant Professor in humanities with the Liwa College of Technology. She has vast experience in teaching education and humanities courses, along with experience in school supervision, thinking skills, and higher education improvement ability. Her research interests include teacher socialization and professional development.

TARIQ SHAHZAD received the B.E. and M.S. degrees from COMSATS University Islamabad, Pakistan, in 2006 and 2014, respectively, and the Ph.D. degree from the University of Johannesburg, South Africa, in 2021. He is currently an Assistant Professor with COMSATS University Islamabad. His research work has been published in top-tier IEEE conferences and well-reputed peer-reviewed journals. His research interests include the Internet of Things, machine learning, and AI in healthcare. He has served as a technical program committee member and an invited reviewer for international conferences and journals.

UMAIR AHMAD SALARIA received the B.Sc. degree in electrical engineering from The University of Azad Jammu and Kashmir, Muzaffarabad, in 2010, and the M.Sc. degree in electrical engineering from the Mirpur University of Science and Technology, Mirpur, Azad Jammu and Kashmir, in 2013, where he is currently pursuing the Ph.D. degree. Since 2014, he has been a Lecturer with the Department of Electrical Engineering, The University of Azad Jammu and Kashmir. His research interests include power system optimization, smart grids, and metaheuristic techniques.

ARFAN AHMED received the Ph.D. degree in applying software algorithms to predict chemotherapy response in breast cancer patients. He has a computer science background having spent time in industry. He was with world-class universities, including Imperial College London and the University of Birmingham, mainly on decision support systems in collaboration with the National Health Service (NHS), U.K. He worked on developing an AI-driven chatbot for anxiety and depression patients with HBKU CSE. He is currently with the AI Center for Precision Health, Weill Cornell Medicine—Qatar, working on projects utilizing AI and wearable devices for diabetes and mental health. He has many publications in collaboration with renowned scholars in the field of AI and health in high-impact journals.

HABIB HAMAM (Senior Member, IEEE) received the B.Eng. and M.Sc. degrees in information processing from the Technical University of Munich, Germany, 1988 and 1992, respectively, and the Ph.D. degree in physics and applications in telecommunications from the University of Rennes 1 conjointly with the France Telecom Graduate School, France, in 1995, and the Postdoctoral Diploma degree "Accreditation to Supervise Research in Signal Processing and Telecommunications" from the University of Rennes 1, in 2004. From 2006 to 2016, he was the Canada Research Chair of Optics in Information and Communication Technologies, the most prestigious research position in Canada which he held for a decade. The title is awarded by the Head of the Government of Canada after a selection by an international scientific jury in the related field. He is currently a Full Professor with the Department of Electrical Engineering, University of Moncton. His research interests include optical telecommunications, wireless communications, diffraction, fiber components, RFID, information processing, the IoT, data protection, COVID-19, and deep learning. He is a Senior Member of OSA and a Registered Professional Engineer in New Brunswick. He was a recipient of several pedagogical and scientific awards. He is among others the Editor-in-Chief and the Founder of *CIT-Review Journal*, an Academic Editor of *Applied Sciences*, and an Associate Editor of the *IEEE Canadian Review*. He also served as a guest editor in several journals.