Mesopotamian journal of Computer Science
Vol. 2025, **pp**. 17–63
DOI: https://doi.org/10.58496/MJCSC/2025/002 ; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Review Article

Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey

Guma Ali [1*], Wamusi Robert [1,2], Maad M. Mijwil [3], Malik Sallam[4,5], Jenan Ayad [6], Ioannis Adamopoulos [7]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda.*

[2] *Department of Computing and Technology, Faculty of Engineering Design and Technology, Uganda Christian University, Arua Campus, Arua, Uganda*

[3] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*

[4] *Department of Pathology, Microbiology and Forensic Medicine, School of Medicine, The University of Jordan, Amman 11942, Jordan*

[5] *Department of Clinical Laboratories and Forensic Medicine, Jordan University Hospital, Amman 11942, Jordan*

[6] *Electro-Mechanical Engineering Department, University of Technology, Baghdad, Iraq*

[7] *Hellenic Republic, Region of Attica, Department of Environmental Hygiene and Public Health and Sanitarian inspections, Greece*

ARTICLE INFO

Article History

Received	05	Nov	2024
Revised	02	Dec	2024
Accepted	04	Jan	2025
Published	03	Feb	2025

Keywords

Wetlands

IoWT

security threats and vulnerabilities

machine learning

deep learning

ABSTRACT

Wetlands are essential ecosystems that provide ecological, hydrological, and economic benefits. However, human activities and climate change are degrading their health and jeopardizing their long-term sustainability. To address these challenges, the Internet of Wetland Things (IoWT) has emerged as an innovative framework integrating advanced sensing, data collection, and communication technologies to monitor and manage wetland ecosystems. Despite its potential, the IoWT faces substantial security and privacy risks, compromising its effectiveness and hindering adoption. This survey explores integrating machine learning (ML) and deep learning (DL) techniques as solutions to address the security threats, vulnerabilities, and challenges inherent in IoWT ecosystems. The survey examines findings from 231 sources, encompassing peer-reviewed journal articles, conference papers, books, book chapters, and websites published between 2020 and 2025. It consolidates insights from prominent platforms such as the Springer Nature, Emerald Insight, ACM Digital Library, Frontiers, Wiley Online Library, SAGE, Taylor & Francis, IGI Global, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. Machine learning and DL methods have proven highly effective in detecting adversarial attacks, identifying anomalies, recognizing intrusions, and uncovering man-in-the-middle attacks, which are crucial in securing systems. These techniques also focus on detecting phishing, malware, and DoS/DDoS attacks and identifying insider and advanced persistent threats. They help detect botnet attacks and counteract jamming and spoofing efforts, ensuring comprehensive protection against a wide range of cyber threats. The survey examines case studies and the unique requirements and constraints of IoWT systems, such as limited energy resources, diverse sensor networks, and the need for real-time data processing. It also proposes future directions, such as developing lightweight, energy-efficient algorithms that operate effectively within the constrained environments typical of IoWT applications. Integrating ML and DL methods strengthens IoWT security while protecting and preserving wetlands through intelligent and resilient systems. These findings offer researchers and practitioners valuable insights into the current state of IoWT security, helping them drive and shape future advancements in the field.

1. INTRODUCTION

A wetland ecosystem supports a diverse array of vegetation, animals, and microorganisms that interact to create a complex and interconnected biodiversity system. This environment's species and biological populations depend on one another to sustain a stable ecological balance [1]. Wetlands can be natural or artificial, temporary or long-term, and include swamps, peatlands, and soil rich in organic matter from decaying plants. They also encompass natural or semi-natural areas that experience periodic flooding or remain covered by shallow water, supporting hydrophytic vegetation during the growing season [2-5]. Wetlands, also known as the “kidneys of the Earth” [2], are one of Earth’s three major ecosystems and encompass a diverse range of types, including mangroves, swamps, fens, deltas, bogs, tidal wetlands, peatlands, floodplains,

*Corresponding author. Email: a.guma@muni.ac.ug

lagoons, marshes, and inland valleys. Wetlands, including coastal wetlands, riverine wetlands, lakes, reservoirs, and oxbow lakes [5], differ based on region, climate, topography, and terrain. These ecosystems feature unique water depths, hydric soils, and wetland-adapted plants and animals. They are crucial in providing essential ecosystem functions and services [3-8].

Wetlands, covering about 6% of the global land surface, thrive in coastal flats, river estuaries, and permafrost regions at higher latitudes. These ecosystems support approximately 40% of the world's species and store 35% of terrestrial carbon, making them vital for biodiversity and climate regulation [10]. They help maintain ecological balance by regulating the hydrological cycle, conserving soil, and purifying water by filtering sediments and removing pollutants. Wetlands enhance water security, sequester carbon, and facilitate nutrient cycling. They also help mitigate climate change and lessen the impact of natural disasters like floods by absorbing excess water and stabilizing ecosystems. Additionally, they provide recreational opportunities, preserve cultural heritage, and serve as key sites for research and education, contributing to both environmental stability and economic development [10-19].

Human activities severely threaten wetlands despite their vital ecological functions. Urbanization, agriculture, construction, pollution, overfishing, resource overexploitation, sea reclamation, aquaculture, and dredging have caused extensive habitat loss, degradation, and fragmentation. Invasive species, climate change, industrialization, and human disturbances further accelerate biodiversity loss [1][5][8][10-13], increase flooding, alter hydrological cycles, and degrade ecosystems. These pressures significantly weaken wetlands' essential services [11][20]. Since 1970, global wetland areas have declined by approximately 35% [10][11][21][22], and between 1700 and 2020, over half of the wetlands in regions like the United States, Europe, Central Asia, India, China, Japan, and Southeast Asia have disappeared [13]. The United States, China, India, Russia, and Indonesia account for more than 40% of this global loss, intensifying ecological crises and increasing natural disasters [2][13]. This alarming decline highlights the urgent need for strong and sustained efforts to protect and restore wetlands worldwide.

The IoWT has surfaced as a revolutionary framework, integrating IoT technologies with wetland monitoring systems to enable real-time data collection, processing, and analysis. IoWT continuously tracks key environmental parameters, including water quality, biodiversity, and climate effects, using sensors, actuators, smart devices, and communication technologies. These systems measure essential indicators such as soil moisture, electrical conductivity, redox potential, salinity, pH, turbidity, temperature, and nutrient levels, providing critical insights into wetland ecosystems [23-25]. IoWT ensures seamless data transmission and enhances decision-making for effective wetland conservation and management by organizing data acquisition, communication, and computation into interconnected layers [26].

Despite its potential, the IoWT faces significant security challenges and vulnerabilities. Threats such as data breaches, unauthorized access, malware attacks, man-in-the-middle (MitM) attacks, device hijacking, botnets, and distributed denial-of-service (DDoS) attacks jeopardize the system's integrity. Other issues include weak authentication, poor encryption, outdated firmware, resource constraints, and a lack of standardization, particularly given the use of resource-limited sensors and deployment in harsh environments [27-51]. These vulnerabilities can lead to data loss, system downtime, and delayed decision-making, ultimately undermining wetland conservation efforts.

To address these challenges, secure and reliable communication is crucial for protecting sensitive ecological data. Unauthorized access, data manipulation, or tampering can severely impact IoWT's effectiveness. Machine learning and DL techniques have shown remarkable potential in mitigating these risks. Techniques such as decision trees (DT), random forests (RF), support vector machines (SVM), k-nearest neighbors (KNN), naïve Bayes (NB), logistic regression (LR), k-means clustering, principal component analysis (PCA), and gradient boosting can analyze IoWT network data to detect patterns and anomalies [52]. These methods effectively identify malware, detect intrusion attempts, analyze network traffic, and counter threats like DDoS attacks and insider breaches [22][52-60]. Deep learning models such as artificial neural network (ANN), convolutional neural network (CNN), recurrent neural network (RNN), restricted Boltzmann machine (RBM), generative adversarial network (GAN), long short-term memory (LSTM), recursive neural network (RvNN), deep neural network (DNN), deep belief network (DBN), graph neural network (GNN), feed-forward neural network (FFNN), deep reinforcement learning (DRL), dense neural networks, stacked autoencoders (SAE), and deep autoencoder analyze environmental data in the IoWT to identify and detect complex spatial and temporal patterns, effectively classify risks of breaches, identify malware, detect phishing and fraud, and analyze network traffic [44][52]. GANs generate synthetic attack data that augment real datasets, enhancing the training of resilient defense models. CNNs detect intrusions, mainly DDoS attacks, while deep autoencoders are employed to identify anomalies in sensor data from IoWT devices. Additionally, reinforcement learning (RL) is integrated into IoWT systems to develop adaptive defense mechanisms against DDoS and insider threats. ML techniques are applied in cybersecurity for anomaly detection, malware classification, threat intelligence analysis, and defense against adversarial attacks [57][58][61-65]. By leveraging their ability to detect patterns, predict anomalies, and provide adaptive responses, ML and DL methods enhance the resilience and robustness of IoWT systems [66][67]. These technologies strengthen data security and optimize resource allocation and decision-making processes, fostering the sustainable management of wetlands. This study is motivated by the increasing application of the IoWT to monitor and manage wetland ecosystems for biodiversity, water purification, and climate regulation. Despite their benefits, IoWT devices

face significant security threats, vulnerabilities, and challenges due to resource constraints, diverse architectures, and exposure to cyber threats.

This survey explores the role of ML and DL approaches in securing IoWT systems, focusing on safeguarding sensitive data and mitigating cyber threats unique to wetland IoT networks. It reviews existing methods, highlights their applications, identifies research gaps, and proposes future directions to enhance IoWT frameworks. Previous research has applied ML and DL techniques to improve the security of IoT systems in agriculture and environmental monitoring [68]. However, limited attention has been given to their specific application in securing the IoWT. This study addresses this gap by offering the first comprehensive analysis of ML and DL methods for securing IoWT systems.

The survey makes the following contributions:

- It presents the state-of-the-art advancements in IoWT, focusing on wetland ecosystems, their evolution, components, features, benefits, and applications.
- It describes the key security threats, vulnerabilities, and challenges within IoWT ecosystems.
- It explains the applications of ML and DL methods for improving IoWT security with relevant case studies and examples.
- It examines the benefits of ML and DL methods for IoWT security.
- It compares ML and DL techniques in IoWT security.
- It states the challenges in applying ML and DL methods to IoWT security.
- It identifies potential areas for future research and development.

The survey structure is as follows: Section 2 details the materials and methods used, while Section 3 reviews the state-of-the-art in IoWT. Section 4 identifies security threats, vulnerabilities, and challenges in IoWT systems, and Section 5 examines how ML and DL techniques can improve IoWT security. Section 6 highlights the challenges of applying these methods to IoWT security, and Section 7 explores future research directions. Finally, the survey concludes in Section 8.

2. MATERIALS AND METHODS

This survey on securing the IoWT using ML and DL methods takes a comprehensive approach to collecting, evaluating, analyzing, and organizing the relevant literature. The aim is to ensure thorough coverage of existing research, allowing for a structured examination of key findings, challenges, and advancements in the field. The survey assesses existing studies, identifies research gaps, and synthesizes findings related to IoWT security. It is organized around essential themes, such as the IoWT framework, associated security threats and challenges, and the application of ML and DL techniques to address these challenges. The researchers used a structured methodology to identify key research questions. They then established explicit inclusion and exclusion criteria to ensure they selected the most relevant studies for their investigation. They systematically analyzed the gathered literature, which included journal articles, conference proceedings, book chapters, and websites. Relevant keywords were used to search across various academic databases and digital libraries, such as Springer Nature, Emerald Insight, ACM Digital Library, Frontiers, Wiley Online Library, SAGE, Taylor & Francis, IGI Global, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. The researchers chose these digital libraries because they comprehensively cover peer-reviewed journal articles, conferences, books, book chapters, and websites. These sources are well-suited for capturing the latest research on various topics. The literature search specifically focused on studies published between 2020 and 2025. The primary areas of interest included wetland ecosystems, the components and features of the IoWT, and the security threats and challenges associated with IoWT. Additionally, the search explored the application of ML and DL techniques in enhancing the security of IoWT.

The literature search employed a combination of keywords, such as “Internet of Wetland Things” OR “IoWT,” “Machine Learning for IoWT security” OR “ML for IoWT security,” “Deep Learning for IoT security” OR “DL for IoWT security,” and “wetland-specific IoWT challenges” OR “IoWT security” AND “future trends” OR “research directions.” Using AND and OR Boolean operators helped refine and broaden the search results as necessary. Additionally, the researchers manually identified other relevant references from the bibliographies of selected papers.

To ensure the quality and relevance of the literature, the researchers applied specific inclusion and exclusion criteria to focus their analysis on studies related to securing IoWT using ML and DL. These criteria allowed them to filter the large volume of data and retain only the most pertinent studies for the survey. Table 1 summarizes the specific inclusion and exclusion criteria for selecting research papers.

TABLE I. SUMMARY OF THE INCLUSION AND EXCLUSION CRITERIA FOR CHOOSING RELEVANT RESEARCH PAPERS FOR THE SURVEY.

S/No	Inclusion Criteria	Exclusion Criteria
1	Research studies focused on the security of IoT systems, particularly in wetlands or similar environmental monitoring systems.	Research studies focus solely on general IoT security and do not specifically relate to wetlands or environmental applications.
2	Research papers that employ ML or DL techniques to address security threats, vulnerabilities, and challenges, such as anomaly detection or intrusion detection in IoWT networks.	Research papers that do not apply ML or DL techniques to the security domain of IoWT.
3	Researchers included peer-reviewed articles, conference papers, books, book chapters, and websites published in reputable journals and conferences.	Research studies that are not peer-reviewed or lack scientific rigor, such as blogs or non-academic sources.
4	Research studies that provide empirical results, methodologies, or frameworks relevant to IoWT security.	Studies that do not provide any practical insights, solutions, or methodologies for securing IoWT systems.
5	Research published within the past five years, i.e., 1st January 2020 to 31st January 2025, to ensure up-to-date findings.	Research papers that are not written in English unless a translated version is available for review.

Two researchers independently retrieved relevant materials from selected research databases using predefined key information, such as the title, authors, and publication year, along with objectives, research questions, study design, methods of analysis, results, and conclusions. They also extracted data related to the IoWT, including IoWT security, vulnerabilities in IoWT systems, the role of ML and DL in IoWT security, specific ML and DL methods used for IoWT security, and comparisons between ML and DL approaches. In addition, the authors reviewed the challenges and limitations associated with IoWT security.

The data extraction process followed a structured approach to ensure consistency and accuracy. Initially, over 3,210 publications were identified through academic search engines and databases. After removing duplicates and screening abstracts, the dataset was narrowed to 1,320 publications. Further eligibility assessments reduced the number to 923, and ultimately, 231 publications met the inclusion criteria for the study. These 231 publications came from various sources, including thirteen from *Springer Nature*, one from *Emerald Insight*, two from *ACM Digital Library*, five from *Frontiers*, ten from *Wiley Online Library*, one from *SAGE*, two from *Taylor & Francis*, two from *IGI Global*, twenty-one from *Springer*, thirty-one from *ScienceDirect*, fifty-one from *MDPI*, fifty-three from *IEEE Xplore Digital Library*, and thirty-nine from *Google Scholar*.

The researchers thoroughly evaluated, categorized, and assessed the relevance of these publications to the study objectives. Fig. 1 shows the distribution of selected publications across the different digital libraries.

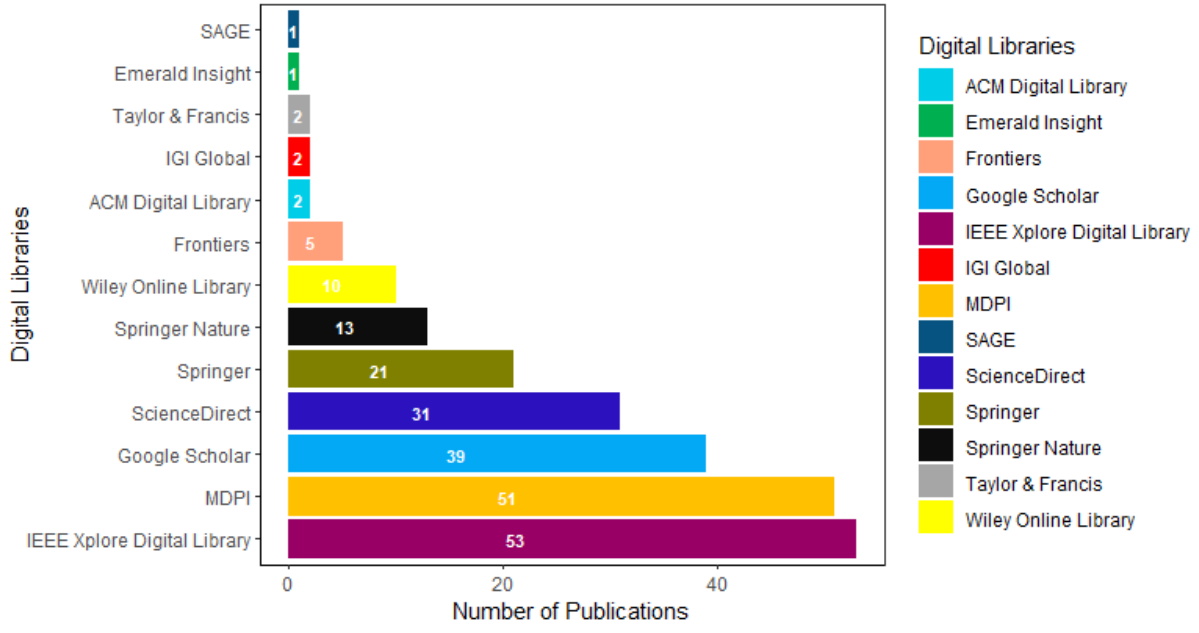

Fig. 1. Illustrates the distribution of selected research publications across digital libraries.

Fig. 2 summarizes the distribution of selected papers across digital libraries based on the paper type.

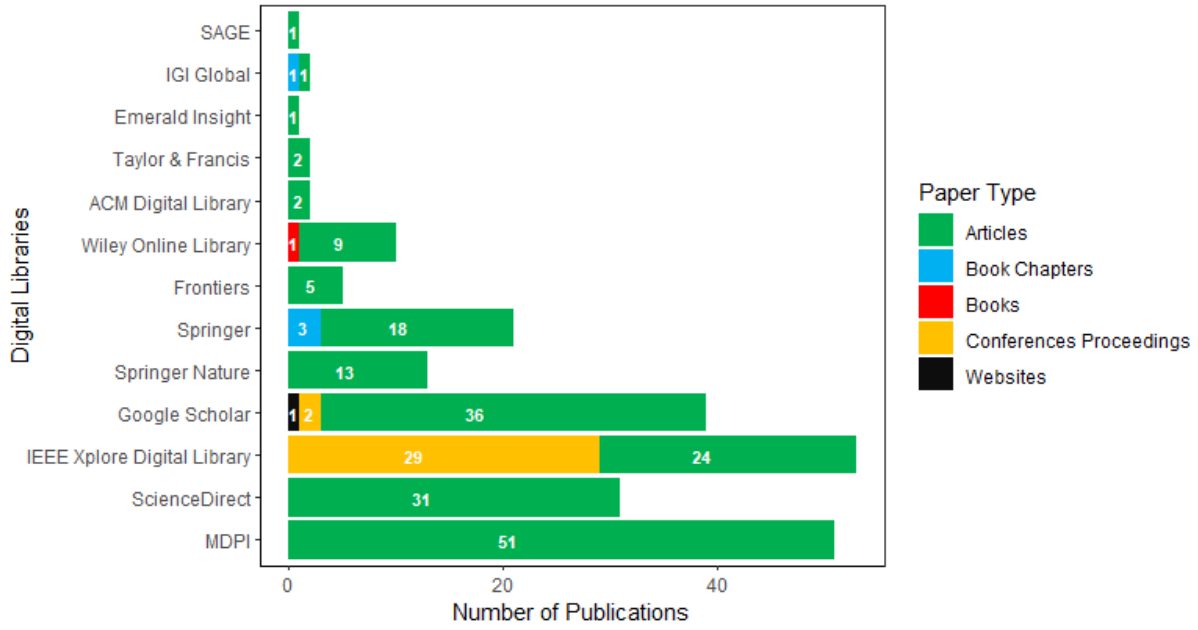

Fig. 2. Summarizes the distribution of selected papers across digital libraries based on the paper type.

Fig. 3 shows the distribution of selected papers across digital libraries, organized by publication year.

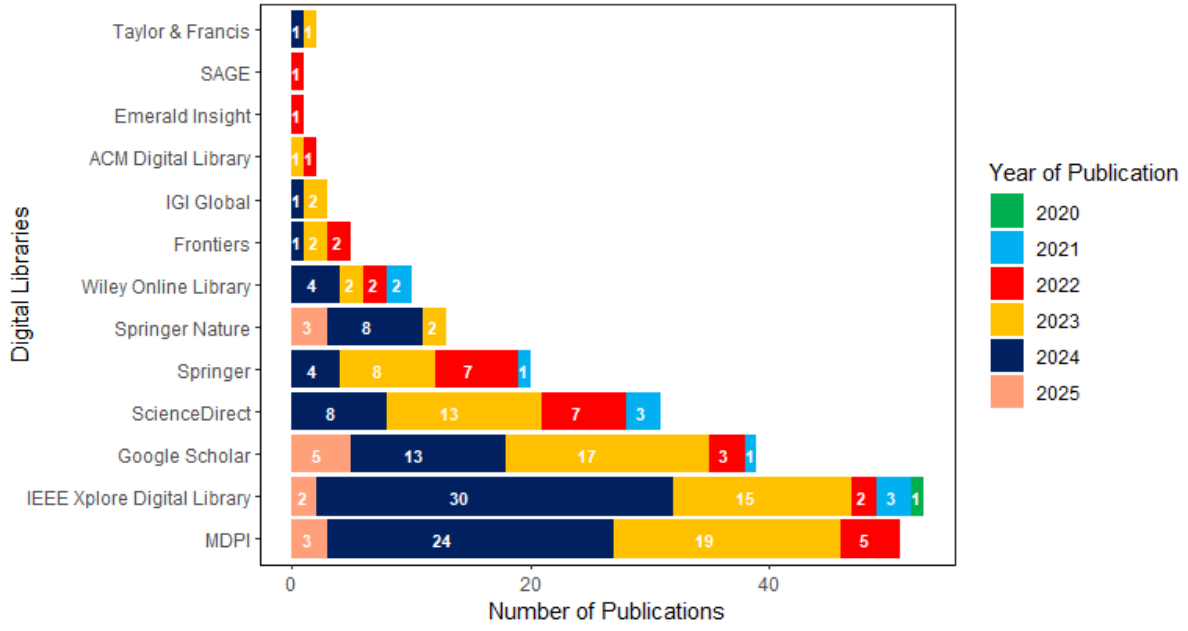

Fig. 3. Shows the distribution of selected papers by digital libraries based on the year of publications.

The research team selected studies based on several key factors, including timeliness, citations, references, relevance, methodological rigor, coherence, validity, dependability, peer-review status, and the credibility of sources. The researchers considered potential biases and confounding variables during the study to guarantee the reliability and validity of their findings. The team conducted database queries, documented all references, and created a dedicated reference database. They used a reference management tool to remove duplicates and ensure accurate citations.

The team followed a multi-step process to narrow the list of research papers, including keyword analysis, screening titles and abstracts, and performing full-text assessments. They recorded the primary reasons for rejection and eliminated studies that did not meet the eligibility criteria. The final selection of papers was organized into a database for further evaluation.

The researchers employed qualitative synthesis and thematic analysis techniques to analyze the material. They validated their findings by consulting subject-matter experts, comparing results with prior research, and carefully evaluating the conclusions' validity. Only high-quality studies were included in the final selection, assessed using a grading system that evaluated the robustness of methodology, the reliability of findings, and the contribution to the field of IoWT security using ML and DL methods. While ethical approval was unnecessary since the study relied on previously published research, the team ensured proper citation of all sources.

The paper acknowledges several potential limitations. First, it may have overlooked relevant studies excluded from the chosen databases. Second, the study recognizes the possibility of publication bias, where studies with favorable results are more likely to be published. Third, the review might not fully cover all ML and DL methodologies applied to IoWT. Fourth, the lack of quantitative analysis or empirical evidence may limit the robustness of the review, as qualitative assessments alone might not fully support the claims. Fifth, the review may prioritize theoretical applications over practical implementation issues, such as cost, scalability, and user approval. Finally, the rapid evolution of IoWT, ML, and DL techniques will likely outpace the existing literature, making it increasingly difficult to keep up with the latest advancements.

3. STATE-OF-THE-ART

The state-of-the-art covers the dynamics of wetland ecosystems, the advancement of the IoWT, and the key components and features that define it. It highlights the numerous benefits IoWT offers and explores its diverse applications across various fields.

3.1. Wetland ecosystems

Wetlands are water-saturated environments that promote the growth of diverse plants and animals, providing a range of ecological services. These dynamic ecosystems, including marshes, swamps, bogs, and fens, are defined by soil that is temporarily or permanently saturated with water, supporting the growth of hydrophytic vegetation [69]. Wetlands naturally filter water by trapping sediments, nutrients, and pollutants, improving water quality. They absorb excess rainwater and slow runoff, acting as buffers during floods while storing carbon and reducing greenhouse gas emissions to help regulate the climate. Wetlands support thriving biodiversity by providing food, breeding grounds, and shelter for many species of fish, birds, amphibians, and invertebrates. At the same time, their vegetation sustains complex food webs and adds to habitat diversity.

Agriculture, urbanization, and industrial development threaten wetlands through practices such as drainage, pollution, and land conversion for economic gain, leading to their loss and degradation. Conservation efforts work to restore these ecosystems, protect their biodiversity, and raise awareness about their ecological importance. By preserving wetlands, we enable them to continue providing essential services like purifying water, controlling floods, and regulating the climate. Wetland ecosystems support the environment and human well-being, highlighting the importance of sustainable management and proactive conservation efforts. These habitats offer water filtration, carbon sequestration, and biodiversity support, directly benefiting communities and ecosystems around the globe.

The rise of the IoWT is transforming environmental monitoring and conservation by leveraging IoT technologies for real-time data collection and analysis in wetland ecosystems. Sensors and devices track water quality, biodiversity, soil conditions, and climate patterns, providing valuable insights that drive conservation strategies and support sustainable wetland management. Advancements in wireless communication, data analytics, and cloud computing enhance the IoWT ecosystem, enabling quicker, more informed decision-making. These tools facilitate timely interventions to address climate change impacts on wetland habitats, ensuring their protection and long-term sustainability. Fig. 4 illustrates the seamless integration of nature and technology in a tranquil wetland environment.

3.2. Evolution of the IoWT

The IoWT emerged from the broader IoT movement, which gained momentum in the early 2000s. Initially, IoT focused on connecting physical devices, sensors, and actuators to the Internet to enable real-time monitoring, data collection, and automation across various industries [71][72]. IoT technology integration into resource management and environmental conservation has been fueled by the increasing need for effective and scalable solutions to monitor delicate ecosystems like wetlands. The development of IoWT has followed a series of distinct evolutionary phases.

3.2.1. Early beginnings of manual monitoring and basic sensors

Before the IoWT, wetland monitoring relied on manual methods and essential tools, including standalone sensors for measuring water levels, temperature, and soil moisture. In the 1990s, efforts to automate monitoring led to the development

of simple sensor networks that could record environmental parameters. However, these systems required significant labor, were prone to human error, and struggled to provide continuous or large-scale data. Additionally, they lacked connectivity and the ability to transmit data instantly.

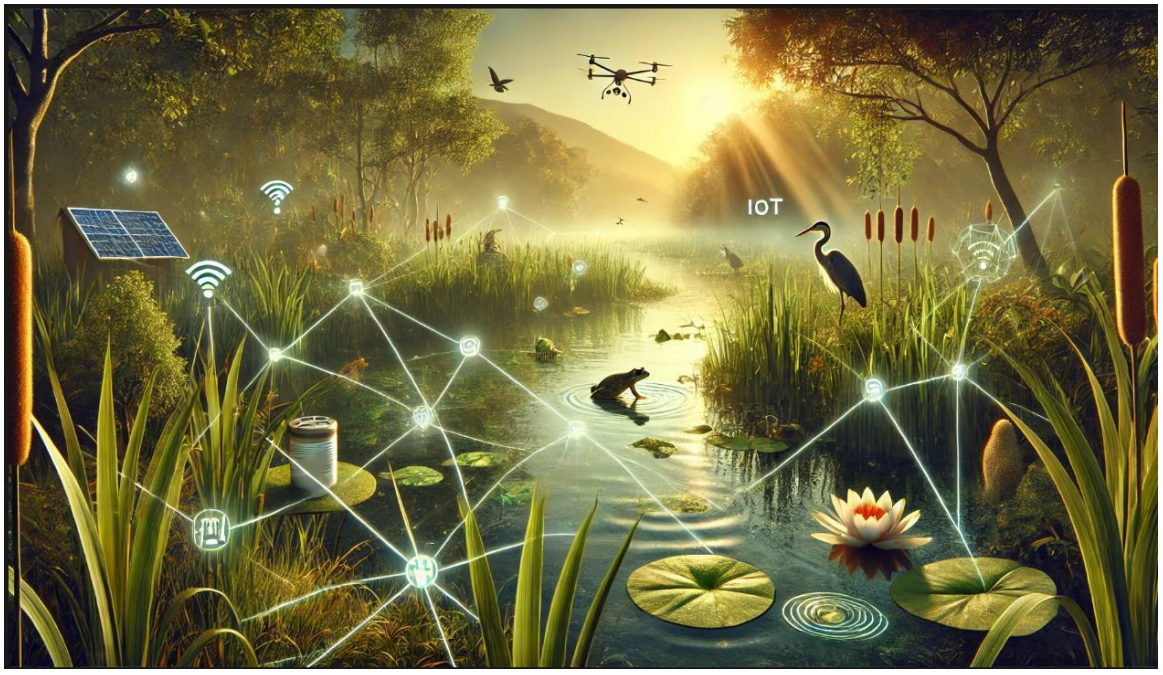

Fig. 4. Shows the conceptual illustration of the IoWT, which blends nature and technology in a serene wetland ecosystem [70].

3.2.2. The emergence of wireless sensor networks (WSNs)

Researchers and engineers revolutionized wetland monitoring in the late 1990s and early 2000s by developing wireless sensor networks (WSNs). These networks allowed multiple sensors to communicate wirelessly and transmit data across vast wetland areas. This innovation improved data coverage and minimized the need for manual intervention. However, early WSNs faced challenges such as high energy consumption, limited processing power, and vulnerability to environmental disturbances, which limited their scalability and effectiveness in dynamic ecosystems like wetlands.

3.2.3. Integration of IoT Technologies

Around 2010, the integration of WSNs with IoT technologies transformed wetland monitoring and management, giving rise to the IoWT. IoT brought advanced communication protocols, cloud computing, and real-time data analytics, which enabled seamless sensor integration into unified systems. These systems efficiently collected, analyzed, and visualized data, driving the creation of specialized applications for wetland management, such as water quality monitoring, flood prediction, and habitat assessment.

3.2.4. Evolution toward IoWT

Researchers and conservationists coined the term IoWT to address the unique challenges of wetlands, such as their remote locations, fragile ecosystems, and complex hydrological and biological processes. Unlike generic IoT systems, IoWT specifically designs solutions incorporating energy-efficient sensors, self-sustaining power sources like solar panels, and Low-Power Wide-Area Networks (LPWANs), ensuring the systems are more effective for deployment in wetland environments.

3.2.5. Advances in Edge and Fog Computing

Edge and fog computing, which emerged in the late 2010s, address latency and energy efficiency issues in IoWT systems. By processing data locally or near its source, edge computing reduces the reliance on centralized cloud platforms. This approach proves especially beneficial for wetlands in remote areas with limited Internet access, allowing real-time data processing without continuous connectivity. Fog computing built on this approach by introducing intermediate layers of processing and storage, streamlining data flow between edge devices and the cloud, and further optimizing system performance.

3.2.6. Incorporation of ML and DL

Integrating ML and DL techniques into IoWT systems marked a significant advancement, revolutionizing how these ecosystems are managed. Wetlands involve complex and non-linear interactions among their physical, chemical, and biological components, often rendering traditional data analysis methods insufficient for capturing their intricacies. ML and DL algorithms enabled IoWT systems to analyze massive data, identify insights, and generate predictive insights. For example, ML models have been used to detect pollution events, assess biodiversity, and predict water quality trends, enhancing the decision-making capabilities of wetland managers.

3.3. Components of IoWT

The IoWT consists of sensors and actuators, communication networks, data processing units, energy management systems, security mechanisms, user interfaces, decision-support systems, and applications and services as its components. Below is a brief description of these components.

3.3.1. Sensors and actuators

Sensors and actuators are crucial in the IoWT architecture because they acquire and act based on environmental data. These devices, such as water quality sensors, collect vital information like pH, turbidity, dissolved oxygen, moisture, temperature, and air quality. For instance, piezometers measure groundwater levels, while ultrasonic sensors help track water flow rates. Actuators, on the other hand, act upon environmental perceptions to regulate water inflow and outflow, helping to maintain a balanced wetland ecosystem. These devices withstand harsh conditions, including exposure to moisture, temperature fluctuations, and bio-intrusions, ensuring their durability and reliable performance even in challenging environments [73].

3.3.2. Communication networks

Communication networks facilitate the transfer of information from IoWT sensors to processing units and decision-making systems using technologies like LPWAN, ZigBee, and LoRaWAN (Long Range Wide Area Network). These technologies ensure connectivity even in hard-to-reach wetland areas. IoWT devices sometimes roam between satellite and cellular systems deployed in remote locations to extend coverage. This approach ensures that the communication infrastructure remains energy-efficient.

3.3.3. Data processing units

IoWT sensors generate large volumes of data, requiring advanced signal-processing techniques to extract valuable insights effectively. These methods enable real-time analysis of large data volumes at the source, consuming significant bandwidth and causing delays. Cloud computing supports long-term monitoring and data mining, allowing for predictive analysis of large datasets. Machine learning and DL techniques identify patterns, anomalies, and trends in the collected data, aiding effective wetland management.

3.3.4. Energy management systems

In wetland ecosystems, the lack of conventional power sources makes it challenging to access mainstream electricity, requiring standalone resources to operate IoWT devices. Solar cells, wind turbines, and microbial fuel cells are commonly used power technologies in these environments. Energy and micro power management systems maintain the continuous and reliable operation of IoWT components. They manage power distribution and energy storage systems, such as lithium-ion batteries, and store excess energy for low-power generation [74].

3.3.5. Security mechanisms

Given the crucial role of wetlands in global ecosystems, protecting IoWT systems from cyber threats is essential. To prevent unauthorized access, organizations implement security measures such as encrypting data, authenticating users, and detecting intrusions. Additionally, IoWT networks integrate Blockchain technology to ensure database credibility by facilitating secure and transparent updates [75].

3.3.6. User interfaces and decision-support systems

Interaction devices serve as interfaces that link human operators with IoWT systems, enabling them to control the systems that collect and manage wetland data. These interfaces, typically in the form of web or mobile applications, are designed to be user-friendly. Decision support systems (DSS) then utilize the processed data to provide recommendations for conserving, restoring, and maintaining wetlands [76].

3.3.7. Applications and services

IoWT systems actively monitor and manage key environmental factors such as species conservation, flood forecasting and mitigation, carbon stock estimation, and water purification. These applications contribute to advancing ecological conservation, fighting climate change, and moderating the use of natural resources. Fig. 5 shows the main components of IoWT.

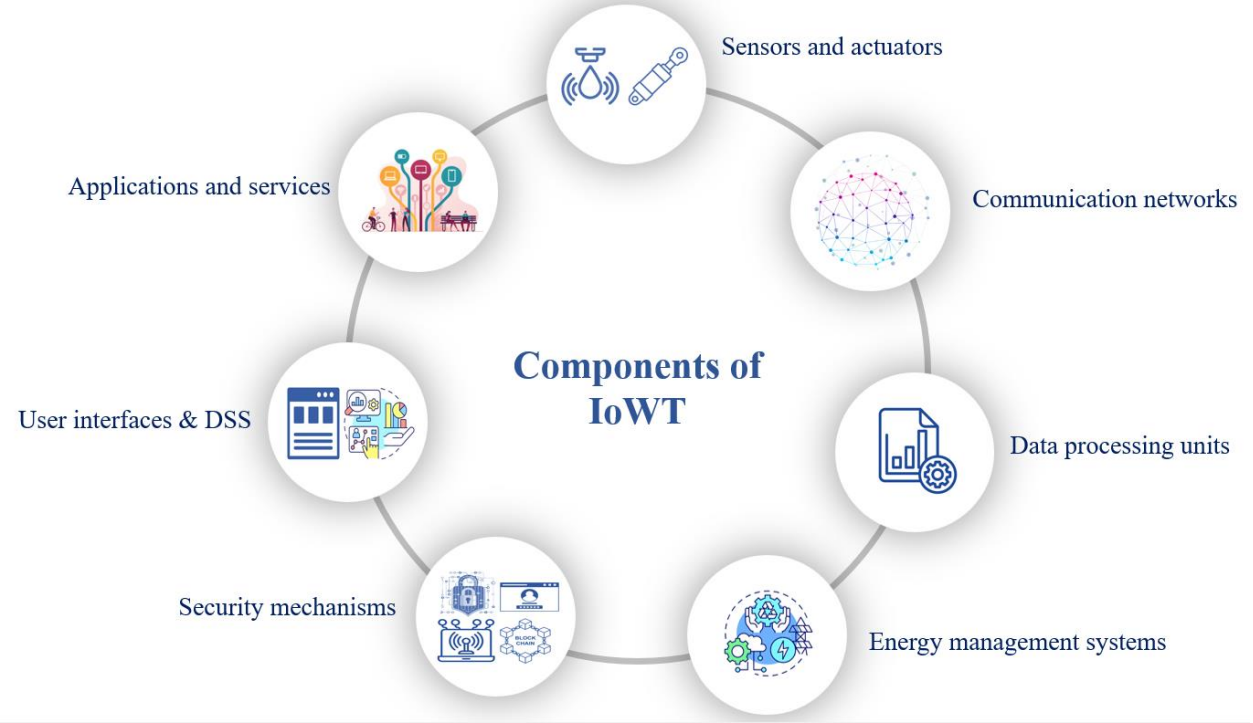

Fig. 5. Shows the main components of IoWT.

3.4. Features of IoWT

Table 2 briefly describes the key features of IoWT.

TABLE II. BRIEFLY DESCRIBE THE KEY FEATURES OF IOWT.

S/No	Key Features	Brief Description	References
1	Sensor-based monitoring and data collection	The IoWT employs wireless sensors to continuously monitor the wetland environment, collecting temperature, humidity, water quality, soil pH, and species diversity. This integrated sensor system enables precise tracking of wetland ecological changes, allowing for proactive management and protection measures. Its architecture and functionality offer valuable insights that help inform policy and management decisions regarding climate change, human activities, and wetland conservation.	[77]
2	Wireless sensing	LPWAN technology, including protocols such as LoRaWAN, allows IoWT devices to communicate efficiently over long distances while consuming minimal power. This capability is crucial for wetlands, often in areas with limited transport infrastructure. LPWAN enhances the effectiveness and sustainability of IoWT systems by guaranteeing reliable data transmission in diverse environmental conditions.	[78][79]
3	Real-time data analytics and predictive modeling	The IoWT enables real-time data processing and analysis, leveraging ML and DL algorithms to decode new data streams. This capability allows for the detection of unusual occurrences, the prediction of ecological patterns, and the anticipation of threats such as floods and degradation of flora and fauna. By providing predictive insights, IoWT enhances the ability to implement early and effective conservation interventions, ensuring wetlands' preservation and associated benefits.	[80]
4	Scalability and modularity	IoWT systems are designed for scalability and modularity, allowing them to adapt to the size and infrastructure of various wetlands. This flexibility supports adding sensors or nodes to the network, enabling easy integration of new components over time. Such an approach ensures that IoWT solutions can meet the evolving needs of wetland areas and incorporate emerging technologies as they become available.	[81][82]
5	Enhanced security and privacy mechanisms	The IoWT incorporates robust security measures to ensure data protection, recognizing the sensitivity of environmental data and the significance of wetlands for ecological balance. It employs secure communication protocols that guarantee data authenticity while protecting against interception and tampering. To strengthen security further, IoWT integrates Blockchain and quantum cryptography technologies, making it resilient to modern cyber threats.	[83]

3.5. Benefits of IoWT

The main benefits of IoWT include the following:

3.5.1. Enhanced wetland monitoring and management

The IoWT actively monitors key aspects of wetland ecosystems, such as water quality, soil moisture, acidity/alkalinity, and biodiversity, providing real-time data. Linking IoWT devices allows researchers and policymakers to track ecosystem degradation over time and take prompt action to address it. In wetland conservation projects, the IoWT systems have proven effective in detecting early signs of pollution or changes in water levels, helping to manage issues like flooding and species decline [84][85].

3.5.2. Improved data-driven decision-making

The IoWT generates large volumes of accurate streaming data from interconnected sensors, enabling data-driven decision-making. Advanced data analysis and visualization tools analyze these data, aiding in developing effective wetland management plans. For instance, the IoWT has been employed in wetland restoration and management to assess water distribution and the subsequent changes in ecosystems, particularly the effects of climate change [86].

3.5.3. Real-time anomaly detection

IoWT systems use ML and DL techniques to detect real-time environmental data anomalies, enabling the prompt identification and resolution of risks like data manipulation, access violations, or physical sensor damage. By detecting these issues early, IoWT helps mitigate critical impacts on wetland ecosystems, reducing the chance of causing irreversible environmental damage [87][88].

3.5.4. Scalable and cost-effective ecosystem monitoring

IoWT systems are highly scalable and perfect for monitoring expansive and diverse wetland ecosystems. Unlike traditional direct monitoring methods, which require substantial time, effort, and financial resources, IoWT devices facilitate efficient data collection and analysis with minimal human intervention. For instance, deploying IoWT in vast areas like the Okavango Delta has streamlined continuous monitoring, which would otherwise demand significant financial, physical, and technological effort to carry out manually [89][90].

3.5.5. Integration with advanced technologies

The IoWT can enhance modern technological innovations such as artificial intelligence (AI), Blockchain, and geographical information systems (GIS), improving the security, reliability, and accuracy of IoWT systems. For example, Blockchain ensures the integrity of IoWT data by preventing alterations. At the same time, GIS allows for real-time tracking of changes in ecosystem conditions, offering a detailed view of ecosystem health [91][92].

3.5.6. Support for conservation and policy initiatives

IoWT systems contribute significantly to wetland conservation efforts by providing accurate and valuable data that aids in policy formulation, funding allocation, and the evaluation of conservation measures. IoWT data has supported the country's international environmental commitments in Pakistani Ramsar site wetlands. This data enables policymakers to develop effective wetland policies, allocate necessary resources, and assess the success of conservation strategies [93][94].

3.5.7. Community and stakeholder engagement

IoWT fosters cooperation between the Institute, environmental agencies, researchers, and local communities by providing precise and accessible data to support wetland conservation efforts. Using this data, local populations can engage with their governments to advocate for the protection of wetlands. Additionally, the data helps communities understand how industrial or agricultural activities in other countries may impact their wetlands, allowing them to respond effectively to these changes [95][96].

3.6. Applications of IoWT

The IoWT offers several applications that enhance wildlife monitoring, conservation, disaster management, sustainable resource management, scientific research, and ecosystem management. Table 3 below summarizes the key applications of IoWT.

TABLE III. SUMMARY OF THE KEY APPLICATIONS OF IOWT.

S/No	Applications	Brief Description	References
1	Wetland monitoring and conservation	The IoWT is an innovative architecture that leverages networked sensors to collect real-time environmental data from wetlands. These devices monitor key features such as water quality, temperature, pH levels, and biodiversity, providing scientists and policymakers valuable insights into ecological dynamics, pollution sources, and conservation efforts. This comprehensive data allows for more informed decision-making and helps predict changes like eutrophication or the spread of invasive species, ultimately enhancing the protection and stability of wetland ecosystems.	[97]
2	Flood management and early warning systems	The ability of wetlands to retain excess water enhances flood control, a role further strengthened by the IoWT through hydrological sensors and predictive algorithms that monitor water levels and rain forecasts. These sensors collect data, which ML algorithms analyze to predict floods and alert residents in affected areas. This disaster risk reduction strategy minimizes property, infrastructure, and life loss while improving wetlands' flood control capacity.	[98]
3	Climate change impact assessment	Wetlands actively contribute to carbon sequestration and climate regulation by absorbing carbon compounds like methane and carbon dioxide. IoWT uses DL techniques to analyze these emissions' temporal and spatial variations, helping to understand how climate change affects wetland ecosystems and their ability to sequester carbon. This data is essential for the international community to tackle climate change and for local regions to develop targeted strategies for addressing these environmental issues.	[99]
4	Habitat and biodiversity monitoring	IoWT actively monitors animals and plants in wetland habitats using camera traps, acoustic sensors, and ML models to identify species, track their movements, and even detect population shifts. This approach helps preserve biodiversity by offering insights into the impacts of human activities and natural events on wetlands, enabling early intervention to protect endangered species and their habitats.	[100]
5	Water resource management	The IoWT monitors wetland threats by tracking water demand and supply while providing treatment solutions to ensure healthy water resource management. Supervised ML analyzes data on nitrates, phosphates, and heavy metals to detect contamination, supporting water treatment, allocation, and the protection of wetlands. This is crucial in preserving wetlands' ability to provide essential ecosystem services for the environment and people.	[101]

4. SECURITY THREATS, VULNERABILITIES, AND CHALLENGES IN IoWT SYSTEMS

The IoWT offers an innovative approach to continuously monitoring and managing wetland ecosystems by connecting sensors, devices, and networks. By gathering real-time data, IoWT can help protect wetlands and endangered species and respond more quickly to natural disasters. However, implementing IoWT in these sensitive ecosystems introduces new security threats, vulnerabilities, and challenges that can compromise the system's efficiency and reliability. Below is a brief description of the security threats, vulnerabilities, and challenges IoWT systems encounter.

4.1. Data breaches and unauthorized access

Unauthorized access and data breaches pose serious risks to the IoWT, threatening sensitive information, disrupting ecological monitoring, and jeopardizing water resource management. Hackers exploit vulnerabilities like weak authentication protocols and unpatched software to manipulate water quality data, alter real-time readings, or steal information such as water quality measurements and species diversity in wetlands. These breaches facilitate data manipulation, theft, and misuse, which can lead to inaccurate environmental decisions and unreliable wetland management, ultimately undermining conservation efforts [44][46][47][102].

4.2. Data privacy violations and misuse

Data privacy in the IoWT is crucial for safeguarding the confidentiality and security of environmental data collected through connected devices. These sensors monitor water quality, temperature, humidity, wildlife activity, and vegetation growth. Sensitive ecological and geographical information is highly susceptible to unauthorized access, which could result in privacy breaches and misuse. For example, revealing water quality data from specific wetland locations could expose them to pollution risks and make them vulnerable to exploitation for industrial or commercial use [44][46][47][103].

4.3. Malware and ransomware attacks

Malware and ransomware attacks threaten IoWT systems, jeopardizing the effectiveness of ecological monitoring and conservation efforts by potentially disrupting their operations. These devices are vulnerable to network exploits and phishing attacks, which can give attackers access to broader networks, enable DDoS attacks, or cause devices to malfunction. Malware can corrupt data, damage sensor performance, or falsify critical environmental information, undermining wetland management. For example, attackers could manipulate water quality monitoring systems, leading to inaccurate reports that hinder conservation decisions. Ransomware may lock operators out of vital systems, delaying action until a ransom is paid,

as seen in incidents like the Colonial Pipeline attack. In extreme cases, Stuxnet-like malware could target IoWT systems, disrupting water flow controls or altering sensor readings, which would endanger biodiversity and ecosystem health [44][46][47][51].

4.4. Data interception and eavesdropping

In IoWT networks used for wetland monitoring, unauthorized entities can intercept or eavesdrop on data transmitted between devices, posing a significant security threat. These networks, which rely on wireless communication to gather and share environmental data, are vulnerable if not adequately secured. Hackers can exploit insecure channels to access sensitive information, such as water quality parameters or species locations, compromising data privacy and integrity. For instance, unencrypted sensor communications measuring pH, dissolved oxygen, and turbidity may be intercepted and altered to hide pollution levels. Additionally, poachers could exploit GPS data from wildlife tracking systems to find endangered species. These breaches not only undermine conservation efforts but can also influence policy decisions, stressing the urgent need for stronger security measures [44][46][47][50][104].

4.5. Distributed denial of service attacks

DDoS attacks on the IoWT overwhelm devices and networks with excessive traffic, disrupting their ability to process legitimate requests. In IoWT systems monitoring wetland ecosystems, these attacks interfere with critical operations and hinder data collection, delaying essential actions such as flood alerts and pollution control. The limited computational power and network bandwidth of IoWT devices exacerbate the issue. For instance, a DDoS attack on a central server managing water quality sensors can block real-time data on parameters like pH, turbidity, or dissolved oxygen, delaying responses to environmental threats. In flood monitoring systems, such attacks obstruct data flow during natural disasters, delaying emergency responses and putting communities and ecosystems at risk [28][36][44][46][47][105-107].

4.6. Device hijacking and botnets

Malicious actors can hijack connected devices in the IoWT, such as environmental sensors, water quality monitors, or cameras, to perform unauthorized tasks. By taking control of these devices, attackers can manipulate or deactivate them, leading to distorted data, such as altering water level readings that misguide management decisions. Compromised devices may also become part of botnets used in cyberattacks, such as distributing spam or spreading malware. These attacks can disrupt environmental monitoring by skewing data, impairing decision-making, and causing severe issues like overwhelming servers with traffic, stealing sensitive information, or sabotaging communication, ultimately harming the protection of wetland ecosystems [29][44][47][108].

4.7. Insider threats

Insider threats in the IoWT arise when individuals within an organization—such as employees, contractors, or authorized users—intentionally or unintentionally compromise the security of connected devices and data. For instance, a wetland monitoring technician might alter environmental sensor readings to hide pollution or misreport water quality. At the same time, an employee could accidentally expose system credentials or neglect security protocols, causing a breach. Additionally, a researcher might unknowingly introduce malware via an infected USB drive, putting the entire network at risk. These threats can lead to inaccurate data, loss of trust, environmental damage, and harm to infrastructure [30][44][46][47].

4.8. Physical attacks and environmental damage

Physical attacks and environmental damage pose significant risks to the IoWT, which relies on interconnected devices in remote outdoor locations. Attackers can sabotage devices such as sensors or communication equipment, distorting environmental data. For instance, destroying a water quality sensor in a wetland can lead to inaccurate ecosystem health assessments. Floods, storms, and heat waves can damage or destroy critical hardware, disrupting data collection and communication. Floodwaters may submerge sensors, lightning damage electronics, and animals chew cables or nest in equipment. These risks undermine the reliability of IoWT data, affecting decision-making and potentially causing long-term harm to ecosystems [33][44][109][110].

4.9. Insecure communication

Insecure communication in the IoWT compromises the integrity and confidentiality of environmental data, as IoWT devices often operate in remote, vulnerable areas and rely on susceptible wireless protocols like Wi-Fi, Bluetooth, or cellular networks. These networks are prone to eavesdropping, MitM attacks, and data tampering. For example, attackers can intercept and alter unencrypted data from water quality sensors, such as pH levels or pollutant concentrations, potentially misleading decision-makers about ecosystem health and causing false alarms or unnecessary regulatory actions. Additionally, attackers may spoof devices to send fraudulent data, disrupt communication with DoS attacks, or gain unauthorized access to sensitive environmental information, leading to the exploitation of natural resources [111].

4.10. Scalability and poor key management

Scalability and poor key management present significant challenges in the IoWT as the number of devices and network complexity grows. Managing secure communication for each device through key generation, distribution, and storage as the network expands becomes increasingly challenging. Traditional key management systems fail to keep up, creating vulnerabilities. For example, improper key management allows attackers to exploit weak or reused keys or outdated encryption methods in an IoWT system monitoring a vast wetland with thousands of sensors, cameras, and drones collecting data on water quality, soil conditions, and wildlife. This can compromise multiple devices, manipulate sensor data, inject false readings, or turn off devices, disrupting ecosystem monitoring. Additionally, scalability issues arise when numerous devices need to authenticate or communicate at once, overloading the system and leading to delays, missed data, or service outages, ultimately compromising security and system reliability [37][112][113].

4.11. Resource constraints

Resource constraints, such as limited energy, bandwidth, storage, and processing power, directly impact the design of IoWT systems. For instance, battery-powered sensors in remote wetland areas face energy limitations, which demand energy-efficient designs or reliance on intermittent renewable sources like solar power. These limitations compel designers to balance security, performance, and cost, often compromising security measures. Bandwidth-intensive data transmission from drones and sensors can lead to delays or the need for data compression, reducing real-time observation quality. Edge device storage constraints require periodic offloading to central servers, balancing storage capacity with communication costs. The processing power of edge devices limits local data analysis, highlighting the need for a combination of local processing and cloud-based analytics. These challenges necessitate careful optimization to ensure the system's performance, reliability, and sustainability [35]. According to Jeon et al. [114], IoT devices with constrained resources are particularly vulnerable to cyberattacks due to low security.

4.12. Weak authentication and authorization mechanisms

Weak authentication and authorization mechanisms in the IoWT expose systems to serious security risks, including unauthorized access to sensitive data, device functionality manipulation, and critical environmental monitoring disruption. These vulnerabilities often arise from simplistic authentication methods and poor enforcement of authorization controls. For instance, wetland sensors may rely on weak default passwords or lack authentication altogether, making it easy for attackers to manipulate them. If a water quality sensor has weak authentication, attackers can impersonate it and send false data, potentially leading to harmful environmental decisions. Inadequate authorization controls allow unauthorized users to access sensitive configurations, as IoWT gateway devices often lack proper role-based access control. This enables intruders to alter settings or turn off sensors, compromising data integrity. Similarly, drones used for wetland biodiversity monitoring are vulnerable to hijacking if they depend on simple passwords and lack encrypted communication, allowing attackers to alter flight plans or steal sensitive species data [27][38][115].

4.13. Insufficient data encryption

Several IoWT systems fail to implement proper encryption, leaving data vulnerable to interception, unauthorized access, and tampering, compromising sensitive ecological information's confidentiality and integrity. Data exchanged between sensors, gateways, and drones is especially at risk of cyberattacks without encryption. For example, an attacker could intercept and alter soil moisture data from a wetland sensor, leading to inaccurate readings that impact resource management. Similarly, unencrypted images or GPS coordinates sent by a drone monitoring endangered species could be intercepted, allowing an attacker to track its movements, alter its flight path, or disrupt its mission. Additionally, unauthorized users could access and corrupt the information without encryption for stored data. This lack of end-to-end encryption significantly increases the risk of MitM attacks on data packets [31][116].

4.14. Outdated firmware and software

Outdated firmware and software in IoWT devices, including water quality sensors and wildlife tracking systems, create severe security and operational risks. These devices depend on up-to-date software to function securely and effectively, but when updates are neglected, attackers can exploit vulnerabilities, leading to data breaches or system failures. For instance, outdated sensor firmware can become susceptible to malware, allowing attackers to manipulate water quality data and undermine environmental monitoring efforts. Likewise, obsolete software in wildlife tracking devices can cause communication failures with other devices, resulting in inaccurate or lost data on animal movement patterns, jeopardizing data privacy and wetland conservation efforts [40][117].

4.15. Resource constraints

Resource constraints in the IoWT affect the performance and sustainability of devices used for wetland monitoring, especially in remote or off-grid locations. Water quality sensors and wildlife trackers often rely on batteries, which deplete quickly, causing data gaps and increasing maintenance costs. Their limited processing power restricts local data analysis,

forcing reliance on cloud systems or external infrastructure that may be unavailable in these areas. These devices' limited memory and storage capacity restricts their ability to store large sensor datasets, which undermines the effectiveness of environmental monitoring and conservation efforts. These challenges are particularly critical in large-scale IoWT deployments, where maintaining security without sacrificing performance is essential [34][49][118][119].

4.16.Lack of standardization

The lack of standardization in the IoWT creates significant challenges for interoperability, data sharing, and scaling wetland monitoring systems. Manufacturers often use proprietary protocols, data formats, and communication methods, making it challenging to integrate different systems. For instance, one monitoring system might rely on a specific water quality sensor with a unique data format, while another uses a different sensor with a distinct protocol. This inconsistency leads to data incompatibility, complicating the merging of information from various sources. The absence of standardized formats makes comparing and analyzing data from different regions or wetlands difficult, hindering large-scale environmental assessments. The lack of common technical standards also raises maintenance and scaling costs, as specialized expertise is needed for each device and protocol. Furthermore, the absence of a uniform security framework leads to inconsistent security measures across devices and networks, increasing the risk of attacks due to poorly interconnected system elements [120][121].

4.17.Limited connectivity in remote wetlands

Limited connectivity in remote wetlands, such as the Amazon rainforest or the Everglades, presents a significant challenge for the IoWT. These areas often lack reliable Internet or network infrastructure, making transmitting real-time data from sensors and devices difficult, which hampers timely monitoring and decision-making. While solutions like satellite communication or LPWAN, such as LoRaWAN, are sometimes used, they face challenges like high operational costs, limited bandwidth, and signal interference from dense vegetation or harsh weather. As a result, connectivity issues slow the scalability of wetland monitoring systems and create data gaps, hindering the ability to track environmental changes or respond swiftly to ecological threats [122][123].

4.18.Data management Complexity

Data management in the IoWT is complex due to the large volume of data collected, the variety of sensors used, and the need for efficient storage, processing, and analysis. Wetland environments require various sensors to monitor parameters such as temperature, water quality, humidity, and species movement, generating high-frequency, voluminous data that must be processed, cleaned and analyzed instantly. For instance, in the Everglades, sensors tracking water levels, soil moisture, and pollution levels produce terabytes of data that must be integrated from multiple sources. The diversity of data types—numerical, image, and video—adds further complexity, as does ensuring data accuracy and consistency, especially when sensors malfunction or connectivity issues arise. Real-time applications such as flood monitoring and wildlife tracking require rapid processing, which demands significant computational power and sophisticated algorithms. These systems are often complex to deploy in remote areas with limited resources. Data privacy and security concerns, particularly in sensitive wetland areas, complicate data management and sharing among stakeholders such as local authorities, environmental groups, and researchers [124]. Fig. 6 illustrates the security threats, vulnerabilities, and challenges in IoWT systems.

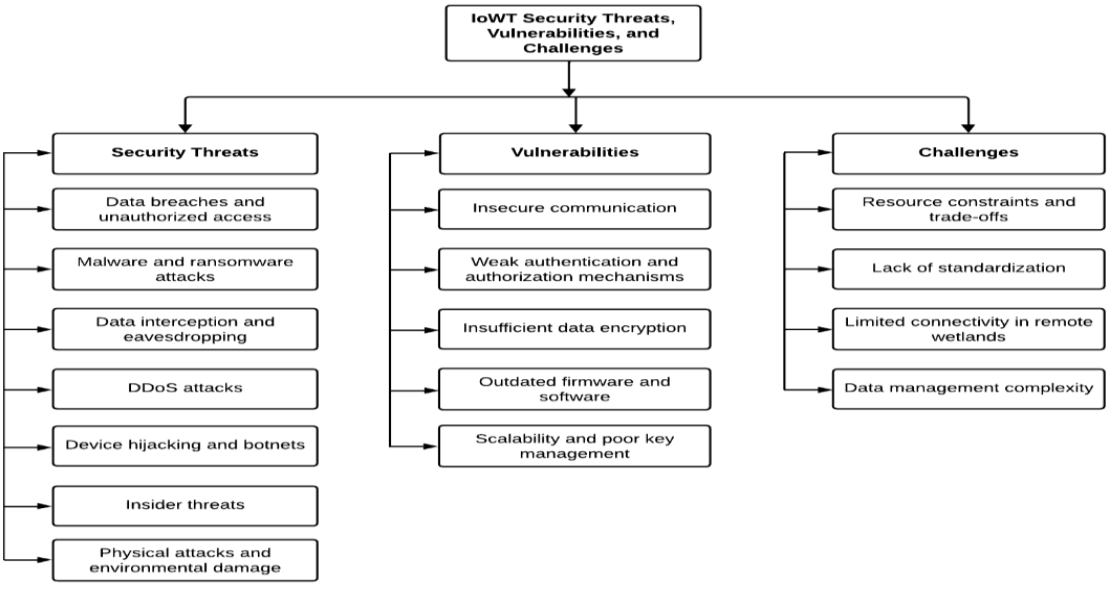

Fig. 6. Illustrates the security threats, vulnerabilities, and challenges in IoWT systems.

5. MACHINE LEARNING AND DEEP LEARNING IN IoWT SECURITY

5.1. Machine learning

Machine learning, a rapidly evolving branch of AI, integrates statistics, mathematics, and computer science concepts to develop robust algorithms and statistical models. These models analyze large datasets, extract meaningful insights, and construct mathematical representations that enable predictions or decision-making without explicit programming [44][125][126]. By recognizing patterns and relationships within data, ML algorithms perform classification, regression, clustering, and optimization tasks. Through continuous learning and adaptation, these algorithms strive to replicate human intelligence by training on vast data [126-129]. In IoWT networks, ML follows three key stages: training, testing, and validation. The process begins with collecting raw data divided into training and testing datasets. The ML algorithm learns from historical data to build a predictive model during training. In the testing phase, the trained model analyzes and classifies new data to assess its accuracy. Finally, the validation phase fine-tunes the model by incorporating additional data or refining features to enhance performance. Once trained, the IoWT system can efficiently execute specific tasks based on real-time or previously unseen data. Machine learning techniques are classified into supervised, unsupervised, semi-supervised, and reinforcement learning, while learning strategies include centralized, federated, and transfer learning [125-129].

- *Supervised learning*

Supervised learning uses labeled datasets to teach algorithms the relationship between inputs and outputs [44][52][126]. In IoWT, data is labeled before training or historical data is utilized. During training, the model compares its predictions with actual results from the dataset, learning and improving its accuracy over time. Supervised learning is divided into classification and regression algorithms: classification predicts discrete category labels, while regression predicts continuous numerical values. Popular supervised learning algorithms, such as Bayesian networks (BN), LR, DT, RF, SVM, and neural networks (NNs), are commonly used in IoWT network security [125-130]. Cybersecurity experts apply these algorithms to classify threats, detect intrusions, identify spam, and recognize malware.

- *Unsupervised learning*

Unsupervised learning algorithms analyze data without relying on predefined labels, allowing them to uncover hidden patterns or detect anomalies, such as in IoWT. Unsupervised learning algorithms are practical for identifying structures and relationships within data, making them particularly useful for tasks like clustering and anomaly detection [52][126]. These methods are employed when training data lacks annotations or classifications, with clustering being a popular approach [44]. Unsupervised learning algorithms are categorized into six types: hierarchical learning, data clustering, latent variable models, dimensionality reduction, and anomaly detection. In the IoWT, researchers often use algorithms like K-means, RBM, autoencoders, GANs, PCA, and RNNs for tasks such as exploratory data analysis, clustering, feature extraction, and dimensionality reduction [126][128][130]. These algorithms are especially beneficial for anomaly detection and network traffic analysis within the IoWT network.

- *Semi-supervised learning*

It uses labeled and unlabeled data to improve model training, which is especially useful when labeled data is limited but unlabeled data is abundant [126]. By leveraging both data types, semi-supervised learning enhances accuracy and efficiency, bridging the gap between supervised and unsupervised learning. Popular algorithms, such as generative models, graph-based models, mixture models, entropy minimization, and semi-supervised SVM, help create more accurate models while reducing the need for extensive human labeling. In the IoWT context, these algorithms are crucial in detecting threats and classifying malware in new domains [44][126][128].

- *Reinforcement learning*

Reinforcement learning involves agents actively interacting with their environment to make decisions through trial and error, guided by feedback as rewards or penalties [44][52][125][126]. This approach allows agents to learn from their actions and improve performance. Rather than relying on predefined datasets, agents gain knowledge through real-time experience, which enables them to adapt to new situations and challenges. RL techniques, such as Q-learning, State-Action-Reward-State-Action (SARSA), and Deep Q-Network (DQN), improve decision-making processes in various domains, including cybersecurity, where they help identify and address emerging threats [126][128][130]. Reinforcement learning provides a dynamic and adaptive approach to cybersecurity by enabling systems to learn from feedback and respond effectively to emerging threats. Trained RL agents can monitor network traffic, detect suspicious activity instantly, and take immediate actions such as blocking or quarantining potential attacks [126]. RL also strengthens password policies and enhances the security of IoT devices. In IoWT cybersecurity, RL algorithms optimize automated incident response and penetration testing, improving defensive strategies. While challenges remain, RL has the potential to revolutionize cybersecurity by creating agile and flexible systems that quickly identify and mitigate threats, ultimately safeguarding critical infrastructure [52].

5.1.1. Machine Learning Algorithms

Machine learning strengthens cybersecurity by leveraging algorithms to detect threats, predict attacks, and address vulnerabilities. In IoWT security, ML algorithms identify anomalies, recognize patterns, and respond to potential risks instantly.

- *Decision trees*

A DT is a supervised ML algorithm for classification and regression that recursively splits data based on feature values to form a tree-like structure. Decision trees make decisions at internal nodes using criteria like Gini impurity for classification or mean squared error for regression, with branches representing possible outcomes and leaf nodes containing predictions [131][132]. Their interpretability makes them valuable for transparent decision-making, though they risk overfitting, which can be addressed by pruning or ensemble methods like RF. DTs efficiently process numerical and categorical data with minimal pre-processing, making them ideal for applications like malware detection, intrusion detection, spam recognition, and vulnerability assessment [52]. However, imbalanced datasets can bias results, necessitating careful data handling. In the IoWT, DTs analyze real-time sensor data—such as water quality, temperature, humidity, and wildlife activity—to detect anomalies and potential threats. By identifying sudden environmental changes, DTs trigger automated responses like activating backup systems, alerting authorities, or shutting down devices, enhancing security, minimizing human error, and ensuring timely threat mitigation.

- *Random forest*

Random forest is a powerful and flexible ML algorithm that enhances classification and regression tasks by constructing multiple DTs. It improves accuracy and reduces overfitting using bootstrapping, randomly selecting data subsets and features to train diverse trees. For classification, RF predicts based on majority voting, while for regression, it averages predictions. This method effectively handles numerical and categorical data, identifies key features, and excels in noisy environments [131][133]. In cybersecurity, RF strengthens detection systems by identifying phishing websites, spam emails, and suspicious activities [134]. Within the IoWT, RF improves security by analyzing sensor data and communication patterns to detect anomalies and malicious activity. Reinforcement learning further enhances IoWT security by enabling adaptive defense strategies against threats like DDoS attacks and insider breaches. For instance, RL optimizes network routing and resource allocation in wetland flood management, ensuring uninterrupted data flow and efficient ecosystem management. It also helps control water levels and energy consumption in artificial retention systems. RF-based models, such as those developed by Attou et al. [54], detect unauthorized access in IoWT networks by analyzing long-term sensor data, water quality, and network traffic patterns. These models identify unusual activities, such as brute-force attacks or unauthorized connections, reducing false alarms and improving threat detection.

- *Support vector machines*

Support vector machines are supervised ML algorithms used for classification and regression tasks. They determine the optimal hyperplane that separates data points from different classes by maximizing the margin between the hyperplane and the nearest support vectors [131]. When data is not linearly separable, SVMs apply the kernel trick to map it into higher-dimensional spaces for better separation [135]. These algorithms efficiently manage linear and non-linear relationships, excel in high-dimensional spaces, and resist overfitting. However, they may face challenges with large datasets unless feature selection is applied. SVMs are used in intrusion detection, malware identification, fraud detection, and email security, where they classify malicious activities by distinguishing normal behavior from abnormal patterns [52] [52][133][134]. In the IoWT, SVMs enhance security by detecting anomalies, classifying device behavior, and identifying patterns that indicate unauthorized access or malfunctioning devices. Wetland monitoring systems use sensors to collect vast amounts of environmental data, which may contain legitimate patterns and security threats. By analyzing benign and malicious software behaviors, SVMs accurately label collected data, ensuring the integrity and reliability of wetland monitoring efforts while preventing compromised devices from disrupting critical operations.

- *K-Nearest Neighbors*

K-nearest neighbors is a straightforward and intuitive supervised machine learning algorithm primarily used for classification, but it can also be applied to regression. It classifies new data points by comparing them to existing points in the training set, assuming that similar objects are close together. KNN calculates distances using metrics like Euclidean distance and assigns a class based on the majority vote of the ‘k’ nearest neighbors. Regression predicts outcomes by averaging the values of the nearest points. As a non-parametric and lazy learning method, KNN does not assume any data distribution and skips a training phase, making it computationally intensive since it must calculate distances for each prediction. Selecting an appropriate ‘k’ value is crucial; a small ‘k’ increases sensitivity to noise, while a large ‘K’ can obscure essential patterns [131][133]. In the IoWT, KNN enhances security by analyzing sensor data to detect anomalies. Sensors monitor environmental factors like water quality and temperature, and KNN classifies deviations as usual or

potentially hazardous [134]. If new readings significantly differ from historical trends, the system flags them as potential threats, helping detect environmental damage or intrusions and ensuring wetland protection.

- *Naive Bayes*

Naïve Bayes is a supervised learning algorithm that leverages Bayes' theorem, assuming feature independence to reduce computational costs and simplify classification tasks. It computes the likelihood of each class based on input features and selects the class with the highest probability, making it efficient and fast with minimal data requirements. NB works well for binary and multi-class problems, even when features are irrelevant, and is widely used in text classification tasks like spam filtering. Gaussian Naïve Bayes, which assumes features follow a Gaussian distribution, provides accurate results in text categorization [52][131][132]. NB is crucial in cybersecurity, enabling quick identification of threats such as harmful emails and attacks in IoWT systems, where it classifies sensor data to detect anomalies like unauthorized access or sensor tampering [52][134]. By training on labeled data, NB predicts potential threats and enhances security by continuously monitoring and classifying incoming sensor data, enabling timely responses to mitigate risks. In projects like wetland restoration using IoWT, NB models have helped predict phishing attacks and allowed proactive measures like encryption and access control.

- *Logistic Regression*

Logistic regression is a supervised ML algorithm commonly used for binary classification tasks. It predicts outcomes by calculating probabilities using the logistic function, transforming a linear combination of input features into values between 0 and 1. LR classifies predictions into two categories by applying a threshold, typically 0.5. The model uses gradient descent to lessen the error by adjusting its parameters, ensuring the predicted probabilities align closely with the actual labels. While LR assumes a linear relationship between input features and the log odds of an outcome, limiting its effectiveness in complex scenarios, it remains a simple, interpretable, and efficient algorithm. It excels in tasks like phishing email detection and anomaly prediction in the IoWT, where it processes large datasets to detect and mitigate unauthorized access or data manipulation.

- *K-Means*

K-Means is a clustering algorithm that organizes data points into separate groups based on their characteristics. It randomly selects K initial centroids, where K is the number of desired clusters. Each data point is assigned to the nearest centroid using a metric like Euclidean distance. The centroids are then updated by calculating the mean of the points in each cluster, and this process repeats until the centroids stabilize or a set number of iterations is reached. K-Means is valuable in customer segmentation, image compression, and anomaly detection tasks. In the context of the IoWT, it aids in security by detecting unusual patterns in sensor data and supporting activities like threat detection, incident response, malware analysis, and real-time monitoring, allowing security teams to identify potential threats early and ensure the safety and sustainability of wetland ecosystems.

- *Principal Component Analysis*

Principal component analysis is a powerful dimensionality reduction technique used to simplify the analysis of large datasets by identifying and focusing on the directions of maximum variance. In the context of IoWT security, PCA helps streamline the processing of environmental data from sensors like moisture, temperature, and air quality by reducing unnecessary complexity while retaining key information, which makes it easier to detect security anomalies, such as sensor tampering or unauthorized access, by highlighting unusual patterns or outliers. In addition to anomaly detection, PCA aids in processing vast amounts of network data for IDS, accelerates malware analysis by identifying irregularities in file statistics, and enhances threat detection efficiency without sacrificing accuracy. In IoWT systems, PCA, along with clustering techniques, helps detect emerging threats in wetland ecosystems, such as pollution or sensor malfunctions, enabling early intervention and improved security [60].

- *Gradient boosting*

Gradient boosting is a robust ML algorithm that builds an ensemble of decision trees, each correcting the errors of the previous one to improve accuracy. Gradient descent iteratively minimizes a loss function by adjusting the model step by step until it meets a stopping criterion, such as a set number of trees or a small error. While excessive trees or a high learning rate can cause overfitting, techniques like shrinkage and tree depth control help prevent this. Implementations like XGBoost, LightGBM, and CatBoost enhance cybersecurity by improving threat detection in phishing, malware, and intrusions [52]. These models rapidly analyze large datasets, identify malicious activity, refine classification, detect anomalies, predict attacks, and adapt to emerging cyber threats. In IoWT systems, gradient boosting strengthens security by detecting unusual sensor data patterns, aiding in anomaly detection, intrusion prevention, and predictive maintenance. It also protects data transmission by identifying and rejecting spoofed packets, ensuring the integrity of environmental monitoring data, such as species richness and pollutant levels [59][136].

- *Federated learning*

Federated learning is a distributed ML approach that enables devices or organizations to train a shared model while keeping their data local collaboratively. Instead of transferring raw data to a central server, participants share only model updates, such as gradients or weights, which enhances security by protecting sensitive environmental data like water quality or biodiversity. FL improves real-time threat detection by allowing sensors to analyze local data for anomalies and share model updates, which helps identify threats like poaching or contamination. It also strengthens resilience against cyberattacks, such as data poisoning and DoS, by eliminating centralized data storage and enabling collaborative anomaly detection across devices in diverse ecosystems. FL supports cross-site collaboration for wetland conservation, allowing different organizations to create shared models while ensuring privacy and complying with regulations. Furthermore, integrating FL with Blockchain ensures the integrity of model updates, preventing tampering and enabling transparent auditing to reinforce trust in ecological conservation efforts.

5.2. Deep Learning

Deep learning, a subfield of ML, develops algorithms by modeling NNs inspired by the human brain. These networks use layers of interconnected nodes, or neurons, to process input data, detect intricate patterns, and generate predictions [137]. Deep learning automates feature extraction from raw data, removing the need for manual feature engineering [138]. It handles large datasets across computer vision, speech recognition, natural language processing (NLP), autonomous driving, and cybersecurity. As the networks grow more profound, they can learn more intricate features, enabling tasks such as image recognition, language translation, and speech processing. The rise of DL can be attributed to its ability to improve performance with the availability of more data and computational power. The rapid advancement of GPUs has significantly sped up the training process of large models, enhancing the effectiveness and accessibility of DL. Industries such as AI, healthcare, and autonomous vehicles have embraced DL to address complex, data-intensive challenges. As models process more data through multiple layers of computation, they refine their predictions, resulting in higher accuracy and making DL a valuable tool for real-world problem-solving.

Deep learning operates through ANNs with input, hidden, and output layers, processing data through interconnected nodes that extract hierarchical features. Techniques like CNNs, RNNs, and GANs have significantly impacted computer vision, medical diagnosis, NLP, and cybersecurity. In the IoT and IoWT, DL addresses challenges like anomaly detection and system security, improving efficiency and accuracy across applications like fault diagnosis and intrusion detection [128][139]. In cybersecurity, DL has transformed traditional security systems. While conventional IDS struggle with evolving cyber threats, DL-based IDS can analyze real-time network traffic, identify anomalies, and detect intrusions more effectively [140]. DL enhances malware and fraud detection by focusing on behavioral patterns rather than static code or predefined rules [141]. It can recognize malicious activity based on its actions and detect fraudulent transactions by identifying suspicious patterns within massive datasets. With its ability to model complex relationships, DL excels in anomaly detection, predictive maintenance, and fraud prevention, though challenges like dataset requirements and false-positive rates persist [44][52].

5.2.1. Deep Learning Algorithms

The most well-known NN and DL models include the following.

- *Artificial Neural Network*

Neural networks are pivotal in replicating human brain operations through interconnected neurons in layers. While not a DL model, the ANN is the foundation for DL models. By transmitting signals between neurons—organized in input, hidden, and output layers—ANNs aim to replicate brain-like learning processes. Neurons process inputs using weights and biases and, through techniques like backpropagation, refine the network's output. Training data subsets allow ANNs to save time and memory, which is crucial in cybersecurity applications. NNs are employed in various security contexts, such as spam detection, malware identification, phishing prevention, and identifying advanced threats like zero-day attacks and DDoS. Despite their efficiency, ANNs face hardware dependence, complex structures, and vulnerability to adversarial attacks [52]. In the IoWT context, NNs significantly enhance environmental security and monitoring. They detect anomalies in key ecological metrics, such as water quality and temperature, helping identify pollution or illegal activity [52]. Neural networks evaluate the behavior of IoT devices to identify threats such as unauthorized access or tampering. They also integrate data from sensors and drones, providing a detailed and holistic view of the ecosystem's health. They employ predictive analytics to anticipate risks such as flooding or drought and optimize IoT energy use for sustainable wetland management. NNs are vital in safeguarding wetland ecosystems and advancing conservation efforts through these capabilities.

- *Convolutional Neural Network*

Convolutional neural networks are powerful DL models used extensively in image analysis, pattern recognition, and intrusion detection tasks. Convolutional, pooling, and fully connected layers collaborate to extract and process features from structured grid data, such as images and sequences. The convolutional layers apply filters to detect patterns such as edges or textures, while pooling layers reduce the spatial dimensions, improving efficiency and preventing overfitting [132]. Fully

connected layers process the high-level features for classification or regression tasks, enabling CNNs to manage complex data effectively. This combination makes them ideal for network intrusion detection, image classification, and IoT security applications [142]. In network security, CNNs detect intrusions and analyze network traffic. They identify patterns in packet data through convolutional layers and use pooling layers to consolidate essential features, helping to differentiate between benign and malicious traffic. Fully connected layers then classify the traffic based on these features, while activation functions like ReLU introduce non-linearity to learn complex patterns better. CNNs can adapt to emerging threats by retraining with updated data, reducing false positives and negatives, and providing reliable real-time threat detection [141][143]. In IoT security, CNNs also detect visual threats, sensor anomalies, and potential risks, analyzing large datasets from IoT sensors and predicting security breaches, thereby enhancing system protection [52][135][140][144].

- *Recurrent Neural Network*

Recurrent neural networks process sequential data using loops that enable information to be carried over time. RNNs excel at tasks where data order is crucial, such as time-series forecasting, NLP, and speech recognition. They power applications like language translation, image captioning, and cybersecurity, playing a key role in detecting fraud, malware, phishing, and DDoS attacks [52]. Advanced models like LSTMs address challenges like the vanishing gradient problem, improving their ability to handle complex tasks in dynamic environments [141]. In IoWT systems, RNNs—especially LSTMs—detect anomalies and patterns in sensor time-series data, identifying sudden environmental changes that signal device malfunctions, manipulation, or cyber threats. They enhance predictive maintenance, recognize unusual traffic patterns that indicate cyberattacks, and ensure data integrity. By analyzing historical performance data, RNNs predict device failures, reducing downtime and security risks. Their ability to learn from past events helps forecast security threats, strengthening the safety and effectiveness of IoWT deployments in sensitive ecosystems.

- *Restricted Boltzmann Machine*

A Restricted Boltzmann Machine is a generative NN used for unsupervised learning, which captures the probability distribution of input data by training on samples. With their two-layer architecture of visible and hidden layers, RBMs excel in dimensionality reduction, feature learning, and classification by effectively modeling complex data distributions. These fully connected networks, which lack intra-layer connections, enable RBMs to identify intricate patterns, making them valuable for anomaly detection, malware identification, DDoS detection, and spam filtering [52]. In IoWT applications, RBMs enhance security by analyzing sensor data from wetland monitoring devices that measure temperature, humidity, and pollutants. By detecting anomalies, they can identify equipment malfunctions or illegal activities like poaching, triggering alerts for unusual environmental changes. RBMs also strengthen data encryption to protect sensitive information during transmission and optimize resource management by analyzing energy usage and balancing computational loads. Additionally, FL enables IoWT devices to share models securely, preserving data privacy while fostering a robust and secure network.

- *Generative Adversarial Network*

Generative adversarial networks consist of two NNs—the generator and the discriminator—that work in opposition. The generator creates synthetic data, such as images, designed to mimic actual data, while the discriminator's job is to distinguish between authentic and generated data. Through iterative training, the generator improves its output to make it more realistic, and the discriminator gets better at detecting fakes. This process continues until the generated data resembles the actual data [141]. GANs are widely applied in image generation, NLP, time-series synthesis, and cybersecurity, excelling in tasks like pose estimation, malware classification, intrusion detection, DDoS attack detection, spam filtering, and anomaly detection [52]. In the IoWT, GANs enhance security by generating synthetic attack data to improve anomaly detection, intrusion detection, and system testing. By simulating cyberattacks, GANs help security models become more accurate and resilient. For example, they can generate synthetic sensor data that mimic environmental conditions, aiding in identifying pollution, illegal activities, or tampered sensors [62]. GANs also help ensure data privacy and integrity by creating synthetic datasets that preserve statistical properties while protecting sensitive information. Furthermore, they help detect deepfakes, guaranteeing the authenticity of sensor readings and environmental data, which is crucial for improving the security and efficiency of IoWT systems.

- *Long Short-Term Memory*

LSTM networks excel in sequence prediction tasks by effectively capturing long-range dependencies and addressing the vanishing gradient problem that limits traditional RNNs [140]. Their architecture, which includes memory cells and gating mechanisms, allows them to store and manage information over extended periods, making them ideal for analyzing sequential data like network traffic [144]. In cybersecurity, LSTMs excel at detecting anomalies, identifying malicious activities, and recognizing temporal patterns in network behavior. They use input, forget, and output gates to manage the flow of information, allowing them to retain critical past data, integrate new information, and make precise predictions [145][146]. This functionality is widely applied in NLP, speech recognition, and anomaly detection [141]. LSTM has been utilized in various cybersecurity applications, including malware detection, intrusion detection, anomaly detection, DDoS

detection, APT detection, and spam identification [52][135]. In the context of the IoWT, LSTMs are valuable for monitoring and securing sensor networks. They detect anomalies like unusual water quality or temperature fluctuations, which could signal potential attacks or malfunctions. By training LSTM models on historical data, predictions of environmental changes like flooding or pollution spikes can be made, allowing for proactive measures. LSTMs also monitor traffic patterns and detect suspicious activity, such as denial-of-service attacks or tampering. Their ability to recognize deviations from normal behavior helps identify intrusion attempts and ensures the security of IoWT systems by distinguishing legitimate requests from potential threats.

- *Recursive Neural Network*

Recursive neural networks are ideal for addressing security challenges in the IoWT by effectively processing and analyzing hierarchical or tree-like structures in sensor data. Their ability to understand sequential and spatial patterns allows RvNNs to detect anomalies such as unauthorized access, abnormal data transmissions, and unusual environmental changes. RvNNs enhance IoWT security by leveraging hierarchical data relationships to detect threats and system malfunctions, effectively classifying behaviors as normal or suspicious. They identify attacks such as DoS, data injection, and eavesdropping while analyzing complex network interactions to strengthen security [52]. By facilitating real-time decision-making, RvNNs optimize security measures, automate responses, and alert operators to potential breaches. These networks improve threat detection, minimize false positives, and adapt to seasonal patterns and geographical variations. Continuously learning from new data, RvNNs ensure security models remain robust and responsive to emerging threats, protecting the ecosystem from cascading risks.

- *Deep Neural Network*

Deep neural networks are advanced ANN with multiple layers, including input, hidden, and output layers. Deep neural networks effectively learn complex patterns and data representations by modeling hierarchical and non-linear relationships. They achieve this through learned weights and activation functions, which enable them to process and transform data at multiple levels of abstraction. They effectively handle high-dimensional data, making them valuable for image recognition, NLP, and intrusion detection. In cybersecurity, DNNs detect cyberattacks, malware, spam, and DDoS attacks, though they struggle with novel threats that differ significantly from known patterns [52]. Their application requires extensive training data, substantial computational power, and careful hyperparameter tuning, while challenges like overfitting and lack of explainability complicate deployment in sensitive fields [143]. In the IoWT, DNNs are crucial in real-time monitoring and security by detecting anomalies in IoT sensor data, ensuring accurate water level and pollution tracking, and identifying sensor malfunctions or cyber threats. They enhance data integrity, secure transmission, and predictive maintenance while optimizing real-time threat detection and access control. By safeguarding IoWT systems against cyber threats and environmental risks, DNNs strengthen technological security and environmental protection.

- *Deep Belief Network*

Deep belief networks are multi-layered ANNs that utilize RBMs for unsupervised learning. These generative models focus on learning data distributions by extracting features and reducing dimensionality. DBNs play a crucial role in cybersecurity by detecting intrusions, identifying malware, preventing fraud, and filtering spam. However, their deployment in sensitive environments requires caution due to high computational demands, the need for large datasets, and susceptibility to advanced cyberattacks. In the IoWT, DBNs enhance security by detecting anomalies that signal sensor tampering or unauthorized access and learning standard environmental data patterns to identify threats. They improve data privacy by generating secure representations and protecting sensitive information during transmission. Additionally, DBNs strengthen malware detection and network intrusion prevention by analyzing IoT communication patterns. DBNs efficiently filter and prioritize sensor data by predicting device failures, optimizing resource allocation, ensuring reliable IoWT operations, and improving monitoring system efficiency.

- *Graph neural network*

Graph neural networks are powerful tools in ML for analyzing graph-structured data, where entities are represented as nodes and their relationships as edges. GNNs enhance tasks like node classification, link prediction, and graph classification by iteratively combining node features with those of neighboring nodes. This process creates enriched embeddings that capture local and global structural contexts [135]. In the IoWT context, GNNs improve network security by analyzing traffic patterns and identifying anomalies, such as unusual communication behaviors or compromised devices. Through message passing, GNNs detect potential threats like MitM attacks, eavesdropping, and privacy breaches while ensuring robustness against data manipulation. Additionally, GNNs address critical challenges in IoWT, including sensor spoofing and maintaining network resilience in dynamic environments. GNNs can detect immediate and long-term anomalies by modeling spatial-temporal interactions, bolstering IDS. They also support FL frameworks, enabling secure, localized data analysis while detecting collaborative threats. In harsh environments where devices frequently join or leave the network, GNNs help optimize resource allocation and predict potential communication failures, ensuring the network adapts to changes. This

decentralized approach enables IoWT devices to collectively enhance security, improving the overall resilience of the network and maintaining effective operation in remote and challenging environments.

- *Feed-forward neural network*

Feed-forward neural networks are essential tools in ML, processing information by directing data through layers in a one-way flow from the input to the output layer. In hidden layers, these networks use activation functions like ReLU, Sigmoid, or Tanh to perform complex computations. Weighted links connect neurons in a neural network, and each neuron has a bias that helps adjust the output. During training, the network adjusts these weights and biases to minimize prediction errors, improving its accuracy over time [140]. FNNs play a crucial role in IoWT networks by enhancing security and data integrity. They detect and mitigate security threats such as unauthorized access, cyber-attacks, and data tampering by analyzing network traffic and sensor behavior. FNNs also identify anomalies to ensure sensor data integrity, preventing the influence of faulty or manipulated sensors. They monitor incoming sensor data, compare it with environmental models to spot alterations, and verify data before it enters the network, ensuring that only trustworthy information impacts decision-making. Additionally, FNNs support predictive maintenance, access control, network traffic optimization, and encryption, forecasting sensor failures, optimizing traffic flow, and improving privacy through strong encryption protocols that secure sensitive data and communications.

- *Stacked Autoencoders*

A stacked autoencoder is a DL model consisting of multiple layers of autoencoders arranged hierarchically to learn complex features from input data. Each autoencoder compresses the data into a latent representation through its encoder and reconstructs it via the decoder. Each layer's output acts as the input for the next, allowing the network to identify more complex and abstract patterns progressively. This structure benefits unsupervised feature learning, dimensionality reduction, and initializing DNN. Stacked autoencoders excel at tasks like anomaly detection, data denoising, and generative modeling, as they can handle non-linear relationships, work with unlabeled data, and learn hierarchical features. They have proven effective in various cybersecurity applications, including malware detection, intrusion detection, spam filtering, DDoS mitigation, fraud detection, and phishing identification [52]. In IoWT systems, stacked autoencoders are effective for anomaly detection by identifying unusual patterns in sensor data, such as changes in water quality or unauthorized access attempts [63][64]. Researchers use them to monitor wetland systems, ensuring reliable data by detecting sensor anomalies and preventing data falsification. The models also improve classification performance by extracting relevant features. In IoWT security, stacked autoencoders enhance defense mechanisms by detecting deviations in standard sensor data, compressing data to protect against unauthorized access, and analyzing network traffic to identify potential intrusions. Their ability to detect abnormal behavior strengthens network security and ensures data integrity.

- *Deep autoencoder*

Deep autoencoders are NNs with multiple hidden layers designed to learn hierarchical representations of data. They work by compressing input data into a lower-dimensional form and then reconstructing it to match the original input, minimizing the reconstruction error. This process helps extract significant features from the data, making them effective in tasks such as dimensionality reduction, data compression, and anomaly detection. By using metrics like L2-norm or Euclidean distance, deep autoencoders optimize their performance to capture complex patterns and structures in the data, making them particularly adept at identifying anomalies by flagging deviations in reconstruction errors [140]. In IoWT environments, deep autoencoders effectively detect sensor data anomalies. They learn patterns from standard operational data and identify unusual fluctuations, such as tampered sensor readings or suspicious network traffic indicative of intrusions like spoofing or DoS attacks. Their ability to validate data integrity by reconstructing sensor inputs is invaluable for detecting inconsistencies. Blockchain technology and autoencoders work to ensure secure and immutable records of detected anomalies. These networks also enhance energy efficiency and security in resource-constrained environments by minimizing computational loads, making them ideal for edge devices. Cyber-physical systems can model and monitor physical behaviors, helping detect deviations that might indicate environmental changes or sabotage, ensuring robust security and efficient resource management.

- *Ensemble and hybrid deep learning*

Ensemble DL algorithms combine multiple models to enhance performance by leveraging their diversity. Ensemble DL methods combine the predictions of several base models, each with unique capabilities, to increase accuracy, robustness, and generalization. In IDS, ensemble DL approaches enhance threat detection by combining the intelligence of different models, making them more effective at identifying threats in complex environments like IoT networks with diverse attack patterns [140]. Hybrid DL algorithms, which integrate traditional ML methods with DL techniques, leverage the efficiency of conventional ML and the ability of DL to capture complex patterns. These hybrid models boost accuracy and robustness, particularly for analyzing network traffic anomalies, detecting suspicious behaviors in IoT and IoWT devices, and securing communications within these networks. They also support anomaly detection, fault diagnosis, and adaptive encryption, ensuring systems can respond to evolving security risks. By merging multiple methodologies, hybrid models strengthen the

overall security and reliability of IoWT systems, especially under challenging conditions such as noisy data or unreliable signals.

5.3. Application of ML and DL in IoWT Security

The use of ML and DL in cybersecurity for IoWT is a growing field that integrates cutting-edge technology to improve the security and efficiency of wetland operations. Below is a brief description of the primary areas where ML and DL are applied in cybersecurity for IoWT:

5.3.1. Adversarial attack detection

Adversarial attack detection in the IoWT focuses on identifying and mitigating security threats, targeting the interconnected devices and systems that monitor water quality, temperature, humidity, and biodiversity in wetland ecosystems. The increasing integration of IoT technology in these ecosystems introduces vulnerabilities that adversaries can exploit to manipulate system operations or distort environmental data. Adversarial attacks target the integrity, availability, and confidentiality of IoWT systems through false data injection, DoS attacks, data poisoning, eavesdropping, MitM attacks, replay attacks, and side-channel exploits. While traditional security measures rely on cryptographic techniques, ML and DL offer a more adaptive approach by analyzing historical sensor data to detect deviations from normal device behavior. These learning-based methods enhance cybersecurity by identifying unusual activities that may indicate an attack, making them valuable tools for adversarial attack detection in IoWT systems. Some notable applications of ML and DL techniques in Adversarial attack detection include. Imtiaz et al. [147] proposed the Explainable IoT (XIoT) model that revolutionizes IoT security by combining spectrogram-based CNNs and Explainable AI to detect complex cyber threats with exceptional accuracy (99.34%, 99.61%, and 99.21% on benchmark datasets). It instantly processes large-scale IoT data streams, leveraging high-speed optical networks to ensure scalability and efficiency. Chowdhury et al. [148] evaluated the effectiveness of ML models in detecting and mitigating adversarial attacks in cybersecurity. Using a diverse dataset, CNN and RF outperformed SVM and LSTM, achieving accuracy rates of 98.3% and 97.6%, respectively, with high precision, recall, and F1 scores. The findings emphasize the robustness of these models in identifying malicious activities and highlight the importance of resilient defense mechanisms in combating modern cyber threats. Deshmukh and Ravulakollu [149] proposed a DL framework optimized for detecting and classifying cyberattacks in IoT environments using an enhanced CNN variant called Intelligent Intrusion Detection Network (IIDNet). Through dimensionality reduction, hyperparameter tuning, and feature engineering, IIDNet achieves 95.47% accuracy on the UNSW-NB15 dataset while reducing training time and enhancing scalability. The Learning-Based Intelligent Intrusion Detection (LBIID) algorithm further improves detection performance by optimizing layers and architectural design. Taşcı [150] presented an optimized 1D CNN model for classifying IoT security data, leveraging convolutional, self-attention, and Gaussian Error Linear Unit (GELU) activation functions with dropout and normalization to prevent overfitting. Tested on CIC IoT 2023, CIC-MalMem-2022, and CIC-IDS2017 datasets, the model achieved exceptional results, including up to 99.99% accuracy and precision, demonstrating its effectiveness in detecting IoT-related attacks and malware. Becerra-Suarez et al. [151] evaluated DL models for classifying cybersecurity attacks in IoT networks using the CICIoT2023 dataset. It compares DNN, LSTM, and CNN architectures, with CNN outperforming the others in accuracy and efficiency, achieving 99.10% accuracy for multiclass and 99.40% for binary classification. The findings highlight the importance of data standardization and hyperparameter selection, positioning CNN as a promising model for IoT network security. El-Sofany et al. [152] proposed an ML-based security model to address the increasing security challenges in IoT environments autonomously. Using seven ML algorithms, the model achieves 99.9% accuracy, 99.8% detection rate, and a perfect AUC score, outperforming previous models in execution speed and accuracy. The study highlights the model's potential to enhance IoT security by analyzing network traffic, updating threat knowledge, and detecting new attacks, with future improvements possible through expanding the dataset. Parra-Jiménez et al. [153] proposed using CNN and RNN to enhance IoT security by detecting abnormal traffic patterns. The approach achieves 99% accuracy in binary attack classification and 96% in multiclass attack recognition, outperforming existing solutions. These results show the potential of ML for securing IoT infrastructures. Jullian et al. [146] proposed a distributed DL framework to prevent various vulnerabilities within the same protection system. It evaluates FFNN and LSTM models using the NSL-KDD and BoT-IoT datasets to identify multiple cyber-attacks. The results show that the framework effectively detects various attacks, achieving up to 99.95% accuracy.

5.3.2. Anomaly detection

Anomaly detection identifies behaviors that deviate from regular activity, which may signal an ongoing attack [154][155]. Anomaly detection in the IoWT involves monitoring, detecting, and analyzing data from interconnected wetland sensors to identify unusual patterns or events. These sensors collect temperature, humidity, soil moisture, water quality, and wildlife movement data. Detecting anomalies such as pollution, invasive species, or extreme weather is vital for mitigating environmental harm. Security anomalies in IoWT can disrupt services, including unauthorized access, data tampering, DoS attacks, malware, eavesdropping, physical attacks on devices, botnet attacks, spoofing, and insider threats [154]. Traditional anomaly detection methods heavily rely on data size, structure, and features [50]. Introducing ML methods (like supervised and unsupervised learning, RL), time-series analysis using Autoregressive Integrated Moving Average (ARIMA) and LSTM

networks, and hybrid approaches combining statistical, ML, and DL models is paramount in detecting anomalies in the IoWT ecosystems. Machine learning models, trained on historical data, identify deviations by learning "normal" behavior patterns [154]. They detect both short-term and long-term anomalies. For example, anomaly detection algorithms actively identify unusual network traffic patterns, signaling potential DDoS attacks [52]. Machine learning-driven anomaly detection algorithms like k-means, Gaussian mixture models, and Isolation Forests effectively identify outliers in network traffic, system logs, and user activity. These models continuously adapt to new system behaviors, enhancing detection accuracy. Deep learning methods, such as autoencoders and LSTM networks, reconstruct standard patterns and flag deviations in network traffic or time-series data as anomalies [155]. This process enhances system accuracy and minimizes false positives. Several researchers have recommended implementing ML and DL approaches for detecting anomalies in the IoT network, including the following. Ness et al. [156] investigated various ML models for detecting anomalies in network traffic, focusing on challenges like class imbalance and feature complexity. LightGBM and SVM achieved the highest test accuracy (0.85), while XGBoost (0.83) and RF (0.82) also performed well. Naive Bayes demonstrated substantial accuracy (0.81), while Isolation Forest struggled with generalization (0.4). The study highlights how combining these models in an ensemble can enhance detection capabilities by leveraging their strengths. Ayad et al. [157] introduced a lightweight detection model that enhances IoT security by addressing high-dimensional data. The model combines an asymmetric stacked autoencoder for dimensionality reduction with a DNN trained using a one-class approach. The proposed model outperforms state-of-the-art methods using the BoT-IoT dataset, achieving a detection rate of 96.27% in just 0.27 seconds. It also reaches 99.99% accuracy, 99.21% precision, and a 97.69% F1 score. These impressive results highlight the model's effectiveness and potential for real-world IoT security applications. Simon et al. [158] proposed SVM with an autoencoder to detect network traffic anomalies, enhancing network security and reliability. The autoencoder identifies deviations by learning standard traffic patterns, enabling rapid threat detection and reducing downtime. The approach outperforms existing techniques, offering a proactive threat identification and network protection solution. Rajendran et al. [159] investigated cybersecurity threat detection using DL and anomaly detection, focusing on CNNs and RNNs. The study demonstrates that the RNN outperforms the CNN, achieving 96% accuracy compared to 93%. The integrated framework effectively identifies and mitigates various cyber threats, offering a proactive and adaptable solution for modern cybersecurity challenges. Mohammed and Talib [160] used anomaly detection algorithms like one-class SVM (OCSVM), k-means clustering, and autoencoders to identify unknown attacks in IoT-IDS by learning normal system behavior and flagging deviations as anomalies. OCSVM identifies anomalies by learning a boundary around regular instances, k-means detects outliers by clustering data, and autoencoders flag anomalies based on high reconstruction errors. Kolhar and Aldossary [161] present a DL-based IDS to secure intelligent vertical networks in IoT applications. The system utilizes a stacking deep ensemble model to achieve 99.8% detection accuracy on the ToN-IoT dataset. It also attains 99.6% accuracy on the InSDN dataset. It combines deep learning with other security measures to address vulnerabilities, improve privacy through data anonymization, and maintain real-time performance in IoT environments.

5.3.3. Intrusion detection

Intrusion detection in the IoWT identifies and mitigates unauthorized access, cyber threats, and malicious activities to ensure data integrity, confidentiality, and system availability. Wetland ecosystems depend on interconnected sensors to monitor environmental conditions, but deploying IoT devices in remote, unprotected areas increases their vulnerability to cyberattacks. Intrusion detection systems proactively safeguard these networks by detecting threats such as unauthorized access, DoS attacks, MitM attacks, malware, ransomware, data tampering, and spoofing. Conventional IDS techniques, including signature-based, anomaly-based, behavioral-based, hybrid approaches, edge computing, and real-time monitoring, help counter these risks. However, IoWT faces challenges maintaining data integrity due to anomalies, and traditional signature-based methods struggle with emerging threats. Machine learning enhances IDS by enabling systems to learn from data and detect novel attacks. Supervised, unsupervised, and DL techniques—such as DT, SVMs, CNNs, and GANs—improve intrusion detection by identifying sophisticated threats and generating adversarial examples to test system resilience [155]. By leveraging computational intelligence, ML and DL enhance IDS efficiency, enabling accurate anomaly detection with minimal human intervention [44]. Several research studies have successfully applied ML and DL techniques to detect intrusions in IoT networks. Dash et al. [134] proposed DL techniques for IDS to combat network intrusions, but most models still face high false alarm rates. Deep learning, especially LSTM networks, has proven effective in improving intrusion detection. The Salp Swarm Algorithm (SSA)-optimized LSTM model demonstrates superior classification accuracy, reduced false alarms, and enhanced performance for real-time intrusion detection applications. Ahmed et al. [162] explored using ML and DL models, such as SVM, RF, LSTM, and ANN, to improve network intrusion detection. It demonstrates that these models can effectively classify network traffic, with RF achieving the highest accuracy at 99.5%. The research highlights the importance of tuning models and adapting to evolving threats to enhance network security in real-time applications. Jyothi et al. [163] developed an IDS for Industrial IoT networks using ML and DL techniques. They employed Singular Value Decomposition (SVD) for feature engineering and Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance. Their model, tested on the ToN_IoT dataset, achieved 99.98% accuracy, a 0.016% error rate for multiclass classification, and a 0.001% reduction in binary classification error. Du et al. [164] introduced MobileNet Convolution and Vision Transformer (MBConv-ViT). This transformer-based IoT intrusion detection model fuses local and global features

to enhance feature correlation and precisely classify attack traffic. Leveraging the high correlation in traffic flow, the model achieved superior accuracy of 97.14% on TON-IoT and 99.99% on Bot-IoT datasets, outperforming existing methods. The results highlight MBConv-ViT's effectiveness in extracting comprehensive spatial features and improving network data analysis. Maaz et al. [165] developed the CNN-GRU and CNN-LSTM hybrid DL models to detect IoT attacks like DDoS, injection, and backdoor vulnerabilities. They tested these models on the Kitsune and TON-IoT datasets, achieving 99.6% accuracy on Kitsune and 99% on TON-IoT. Their models demonstrated robust performance, scalability, and efficiency in identifying malicious activities, ensuring strong protection for IoT ecosystems. Al-Quayed et al. [166] developed a predictive framework to strengthen cybersecurity in Industry 4.0's WSNs by integrating ML and DL models using a multi-criteria approach. Their framework employs DT, MLP, and Autoencoder models for intrusion detection and classification, achieving over 99% accuracy with DT and MLP, while the Autoencoder reaches 91% for binary classification. Udurume et al. [167] compared DL and traditional ML models for network intrusion detection using the UNSW-NB15 and NSL-KDD datasets, finding that CNN and CNN-BiLSTM outperformed KNN, SVM, and RF, with accuracies of 94.97% and 96.67%, respectively. Similarly, Kumar et al. [168] assessed various ML and DL models on the UNSW-NB15 dataset for detecting network intrusions. The DT model achieved the highest accuracy at 94.91%, while RF and DNN models also performed well, highlighting the potential of ensemble and DL approaches. These models enhance IDS by providing high precision and recall rates for diverse attack types, ensuring more reliable security measures. El-Shafeiy et al. [137] proposed the deep complex gated recurrent network-based IoT (DCGR_IoT), an IDS using deep complex gated recurrent networks (CGRNs), and CNN for enhanced IoT network security. DCGR_IoT extracts spatial and temporal features to improve anomaly detection and filter unnecessary data. Evaluations on the UNSW-NB15, KDDCup99, and IoT-23 datasets show a 99.2% detection accuracy, demonstrating its effectiveness in defending against advanced cyber-attacks. Sayegh et al. [169] presented an LSTM-based IDS designed for IoT networks, utilizing SMOTE to address data imbalance. The system utilizes DL techniques and feature selection to achieve high detection accuracy, attaining 99.34% on CICIDS2017, 99.67% on NSL-KDD, and 98.31% on UNSW-NB15. These results highlight the effectiveness of the IDS in enhancing IoT network security. Cui et al. [170] proposed an intrusion detection model using temporal convolutional residual modules and an attention mechanism to focus on critical features, improving detection performance. They achieve accuracies of 99.55% on the ToN_IoT dataset and 89.23% on the UNSW-NB15 dataset. These results show 0.14% and 15.3% improvements over existing state-of-the-art models, demonstrating the model's superior performance. Ataa et al. [171] developed and compared two DL models, a hybrid CNN-LSTM and a Transformer encoder-only architecture, for IDS targeting SDN controllers using the InSDN dataset. The Transformer model achieves the highest accuracy at 99.02%, while the CNN-LSTM model performs slightly lower but excels with fewer features. Both models show high performance, with the CNN-LSTM model being more suitable for feature reduction and shorter testing times, and both models benefiting from grouping poorly represented attacks. Kantharaju et al. [172] presented the SAPGAN-based IDS (SAPGAN-IDS-IoT) for detecting security threats in IoT networks, evaluated using accuracy, F1-score, ROC, and computational time metrics. The framework achieves up to 22.65% higher F-score and 21.55% higher AUC compared to CNN-IDS-IoT, DNN-IDS-IoT, and DBN-CSSA-IDS-IoT.

5.3.4. Detection and prevention of man-in-the-middle attacks

Man-in-the-middle attacks seriously threaten the IoWT, where cybercriminals intercept and manipulate data exchanged between interconnected devices, such as sensors and control systems. Exploiting weak security measures and outdated communication protocols that often lack encryption and authentication, attackers can capture, modify, or inject malicious data without detection. This interference can distort environmental readings, disrupt automated processes, and grant unauthorized control over critical systems like irrigation or water quality monitoring. IoWT systems must monitor for threats using advanced anomaly detection and network traffic analysis techniques. By constantly analyzing data patterns, they swiftly detect and address suspicious activity, preventing potential security breaches before they occur. Machine learning and DL approaches are becoming essential tools for detecting and preventing MitM attacks, strengthening the security of IoWT networks. Machine learning algorithms enhance security in IoWT networks by analyzing large datasets to detect patterns and anomalies that indicate malicious activity. Trained on historical attack data, these models differentiate legitimate communication from potential threats and continuously monitor network traffic for real-time MitM attack detection. Machine learning and DL offer adaptive and scalable security solutions, evolving with new threats and integrating seamlessly with encryption and IDS for multi-layered defense. Kandasamy and Roseline [173] developed the AEXB model, which combines AutoEncoder for feature extraction with XGBoost for classification, achieving 97.24% accuracy on the IDSH dataset. This hybrid approach enables real-time threat detection in dynamic smart home environments while optimizing feature engineering, reducing false positives, and minimizing computational overhead.

5.3.5. Detection of phishing attack

Phishing attacks targeting the IoWT exploit vulnerabilities in connected devices and networks that monitor and manage wetland ecosystems. Cybercriminals deceive users with fake emails, messages, or interfaces that mimic trusted sources, such as environmental agencies or IoWT device manufacturers, to steal sensitive information like passwords and access credentials. Once attackers gain access, they can manipulate devices, disrupting data collection and ecosystem management and potentially harming fragile wetlands. The interconnectedness of IoWT systems amplifies the risk, as compromised

credentials can grant broad access. Traditional phishing detection methods struggle to keep pace with evolving tactics, necessitating advanced solutions like ML and DL to detect anomalies and patterns in network traffic, user behavior, and communication protocols. Machine learning and DL models, such as CNN and RNN, can effectively identify phishing attempts by analyzing content from emails, URLs, and sensor data, continuously adapting to emerging threats. These advanced systems enhance IoWT security, ensuring reliable ecosystem management and protection from cyber risks. The following are some notable research studies that employed ML and DL to detect phishing attacks in IoT. Mahmud et al. [174] introduced a hybrid DL model that combines CNNs and Bidirectional Gated Recurrent Units (Bi-GRUs) CNN-Bi-GRU to detect and classify smishing attacks accurately. Using the SMS Phishing Collection dataset and Word2Vec for text preprocessing, the model achieved a remarkable 99.82% accuracy in identifying phishing messages. Deep learning models demonstrate significant potential in strengthening SMS phishing security by accurately identifying and classifying phishing attempts. This approach offers a robust tool for combating cybercrime. Gupta et al. [175] proposed a phishing email detection framework that combines Bidirectional Encoder Representations from Transformers (BERT) for feature extraction and CNN for classification, achieving 97.5% accuracy in identifying phishing emails. By leveraging BERT's linguistic capabilities and CNN's classification precision, the model effectively addresses the complexities of phishing attacks in enterprise systems. Taha et al. [176] analyzed unique, categorized results from the ML dataset. Random forest achieved the highest accuracy (96.89%), outperforming DT (94.57%) and XGBoost. These results establish RF as the most effective model for classification tasks and the top recommendation. Sahingoz et al. [177] developed a phishing detection system using deep learning with five algorithms: ANN, CNN, RNN, bidirectional RNN, and attention networks. It classifies web pages quickly using URLs and evaluates performance with a five million labeled URLs dataset. The results show that CNN achieved the highest accuracy at 98.74%, highlighting DL's effectiveness in cybersecurity. Patil et al. [178] applied SVM and XGBoost algorithms to various phishing datasets, including the Phishing Dataset for ML and Website Phishing Datasets 1 and 2. It reports that XGBoost outperforms SVM, achieving accuracy, precision, and recall of 90%, 88%, and 87%, respectively, while demonstrating a remarkable computation time of 0.00894 seconds. In comparison, SVM achieves accuracy, precision, and recall values of 85%, 84%, and 86%.

5.3.6. Malware detection

Malware targeting the IoWT poses significant security risks by exploiting vulnerabilities in interconnected devices that monitor and manage wetland ecosystems. Cybercriminals can introduce malware to gain unauthorized access, manipulate data, or disrupt operations, undermining the accuracy of environmental data [179]. These attacks can remotely control devices, causing malfunctions or halting their function, leading to severe disruptions in ecosystem management [44]. Weak security protocols and reliance on wireless networks heighten the vulnerability of these devices, and the lack of human oversight often allows attacks to go unnoticed for extended periods. Organizations managing IoWT devices must implement robust security measures to address these threats. Traditional malware detection methods, like signature-based and anomaly-based approaches, struggle to identify new or polymorphic malware and are ill-suited for the scale and diversity of IoWT systems. Machine learning and DL technologies offer a more effective solution, quickly analyzing large datasets and detecting malicious activity [180]. These technologies adapt to new threats by learning from labeled datasets, enabling proactive identification of complex patterns and previously unknown malware, thus ensuring the safe and secure operation of IoWT devices that protect wetland ecosystems [181]. Several research studies have applied ML and DL techniques to detect malware in IoT networks. Hariri et al. [182] proposed a hybrid ransomware detection framework that combines entropy and frequency analysis with ML models, including Multi-Layer Perceptron (MLP), DT, RF, KNN, and LR. Using the CIC-AndMal2017 Android malware dataset, they incorporated data augmentation to enhance detection by generating synthetic ransomware samples. Their experiments revealed that DT and RF classifiers achieved the best performance, with DT attaining 98.89% accuracy, 98.81% F1-score, and 98.90% precision, while RF achieved 98.78% accuracy, 98.23% F1-score, and 98.99% precision. Data augmentation significantly improved detection metrics across all models. Jeebodh and Baliyan [183] introduced a DL approach to detect malware using the IoT Malware dataset, which consists of images generated from malware bytecode. By identifying visual patterns that differentiate malware from benign files, the method achieves a detection accuracy of 98.29%, with precision, F1-score, and recall values of 98.83%, 99%, and 99.17%, respectively. These results surpass previous benchmarks, showcasing the effectiveness of image-based analysis for cybersecurity applications. Almazroi and Ayub [181] proposed BEFSONet, a specialized BERT-based FFNN Framework optimized with the Spotted Hyena Optimizer (SO). Analyzing malware patterns across eight datasets, each representing a different type of malware. BEFSONet achieves exceptional metrics, including 97.99% accuracy, 97.96 Matthews Correlation Coefficient (MCC), 97 F1-Score, 98.37% Area Under the Curve-Receiver Operating Characteristic Curve (AUC-ROC), and 95.89 Cohen's Kappa, outperforming methods like CNN, BERT, and ResNet. Its adaptive architecture effectively detects and mitigates emerging IoT threats, offering a robust solution in dynamic environments. Charoenwong et al. [184] explored using ML techniques to classify malware in IoT devices, focusing on DT, K-NN, and XGBoost algorithms. Tested on a real-world IoT malware dataset, XGBoost achieved the highest accuracy of 98.44%, outperforming DT (95.27%) and KNN. XGBoost's regularization capabilities enhance precision and recall, making it highly effective for detecting and classifying malware. Alkhudaydi et al. [185] utilized ML and DL techniques to analyze the BoT-IoT dataset for effective malware detection. They evaluated ten models, including KNN, SVM, and ensemble classifiers like RF, Extra Trees, AdaBoost,

LGBM, and DL architectures such as LSTM, GRU, and RNN. XGBoost and CatBoost stood out, achieving 98.50% and 98.19% accuracy rates, respectively. Bokolo et al. [131] evaluated seven ML and DL techniques for detecting and classifying malware into nine families (i.e., RF, DT, SVM, KNN, SGD, LR, NB, and DL techniques) using extracted byte, opcode, and section codes. The DL model achieves the highest accuracy of 96%, outperforming traditional methods like SVM, LR, and K-NN. These findings emphasize the effectiveness of DL in addressing the complexity of modern malware, with significant implications for cybersecurity and forensics.

5.3.7. Detecting DoS and DDoS attacks

Denial-of-service and DDoS attacks significantly threaten the functionality and data integrity of IoWT systems, which are paramount for monitoring wetlands and responding to environmental changes. A DoS attack targets a single device or network, overwhelming it with excessive traffic or malicious requests, leading to disruptions in data transmission and potentially shutting down devices [186]. In contrast, a DDoS attack uses multiple compromised devices to flood the target, amplifying the impact and making detection and mitigation harder. These attacks exploit vulnerabilities in IoT devices, compromising real-time monitoring and hindering informed decision-making for wetland management [145][187]. Detecting and mitigating these attacks involves monitoring unusual traffic patterns, slow device responses, and traffic surges. Once identified, countermeasures such as traffic filtering, rate limiting, and network reconfiguration can isolate affected devices and restore normal operations. Machine learning and DL can effectively detect these attacks by analyzing data from IoWT devices to identify anomalies, such as unusual traffic spikes or suspicious behavior, and recognize patterns that indicate potential threats. In contrast, DL techniques, such as CNNs and RNNs, offer more sophisticated analysis of complex data, enhancing the accuracy and speed of attack detection. Integrating these technologies helps strengthen the resilience of IoWT systems, protecting valuable environmental data and ensuring the effective operation of wetland monitoring networks. Several research studies have applied ML and DL techniques to detect DoS and DDoS attacks in the IoWT. Sakr et al. [188] evaluated the performance of supervised ML algorithms in predicting DDoS attacks on Energy Hub (EH) systems through IoT devices using the CICDDOS2019 and KDD-CUP datasets. The SVM Classifier demonstrated notable accuracy on the KDD-CUP dataset, achieving 96.61% accuracy and a 44.50% F1 score with an 80% training size. The RF Classifier delivered a balanced performance, earning a 61.02% F1-score at the same training size for the CICDDOS2019 dataset. Gradient Boosting outperformed other models, showing high accuracy and F1 scores, particularly with the CICDDOS2019 dataset, while hybrid models also exhibited strong results. These findings highlight the need to select tailored ML models to strengthen the resilience of EH systems against evolving DDoS threats. Bukhowah et al. [133] presented a new method for detecting DoS attacks in Information-Centric Network (ICN)-IoT networks using ML algorithms. The study identifies SVM, RF, and KNN as the most effective ML approaches based on classification metrics like accuracy. The strategy, implemented on the Named-Data Networking (NDN) architecture and evaluated through ndnSIM simulation and synthetic datasets, aims to prevent DoS attacks and protect IoT devices. Alshdadi et al. [189] developed EffiGRU-GhostNet. This ensemble deep-learning model integrates GRU and GhostNet architectures optimized with Principal Component Analysis-Local Linear Projection (PCA-LLP) for efficient DDoS detection on large-scale data. Testing on IoT-23 and APA-DDoS datasets showed superior performance, achieving 98.99% recognition with a 0.11% false positive rate and 99.05% accuracy with a 0.01% error, outperforming several baselines. Statistical analyses confirmed that EffiGRU-GhostNet actively advances prominent data-driven cybersecurity by providing a reliable and scalable solution for dynamic DDoS detection. Almadhor et al. [190] proposed using Explainable AI (XAI) and FDNNs to detect and prevent DDoS attacks while ensuring privacy. By training the model across multiple client devices using distributed datasets and integrating XGBoost with SHapley Additive exPlanations (SHAP) for feature selection, the approach achieves high performance with 99.78% accuracy, 99.80% precision, and 99.76% F1 score. The server-side numerical findings highlight the effectiveness and strength of FDNN models in accurately identifying various DDoS attacks. The proposed solution demonstrates robustness, preserves privacy, offers high scalability, and is well-suited for detecting DDoS attacks in IoT networks. Berqia et al. [191] developed advanced detection mechanisms using ML and DL techniques to fortify IoT networks against DDoS attacks. By applying algorithms such as LR, KNN, and DNN on the CIC2023 IoT Dataset, it achieved exceptional accuracy (0.9999 precision, recall, and F1 scores) in detecting various DDoS attack patterns like TCP, SYN, and HTTP floods. Avcı and Koca [192] developed an enhanced algorithm that combines the Slime Mould Optimization Algorithm (SMOA) for feature selection with ANN and SVM to predict and mitigate DDoS attacks in Building Management Systems (BMS). Trained on the Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022, the model achieves 97.44% accuracy in predicting DDoS attack risk factors and an impressive 99.19% accuracy in detecting actual DDoS attacks. This high precision prevents system disruptions and manages cyber threats, providing a more robust defense than KNN and greatly enhancing DDoS detection and prevention in BMSs.

5.3.8. Detecting Insider Threats

Insider threats in the IoWT pose significant risks, as individuals with authorized access, such as disgruntled employees, contractors, or partners, may misuse their privileges to manipulate IoWT devices or tamper with environmental data. These insiders can bypass traditional security measures like firewalls or encryption, making detecting their actions more challenging. Their behavior often mimics normal operations, allowing harm to go unnoticed until it is too late. Organizations use advanced monitoring tools powered by ML and DL techniques to address these risks, analyze sensor data, and identify

unusual behaviors or anomalies that could signal insider threats [44]. These technologies classify regular activity patterns and flag deviations, helping prevent sabotage, data theft, or unintentional damage [46]. Deep learning further enhances security by processing complex data and adapting to evolving threats, enabling real-time monitoring and predictive analysis for swift response and minimal disruption, safeguarding both the system's integrity and the environment. Sridevi et al. [193] presented a hybrid model combining ML and DL to identify insider threats, achieving a 96.3% detection accuracy. The research highlights the advantages of traditional ML algorithms, such as SVM and RF, and DL models, like LSTMs and CNNs. Each offers distinct benefits for various applications. The model outperformed traditional methods by identifying subtle behavioral patterns in user activity and system logs.

5.3.9. Advanced persistent threat detection

Advanced persistent threats increasingly target interconnected devices in wetland ecosystems that rely on IoT technologies to monitor and manage environmental factors. These ecosystems, often remote and isolated, are vulnerable due to weak security in devices like sensors, communication networks, and actuators. Attackers exploit issues such as weak authentication, unsecured communication channels, or outdated software to gain unauthorized access and remain hidden for long periods. Once inside, cybercriminals manipulate data, disrupt systems, and cause environmental damage, leading to misinformed conservation decisions, endangered wildlife, or undetected pollution [194]. Machine learning and DL technologies enhance security in IoWT networks to counter this growing threat. ML algorithms analyze sensor data patterns to detect unusual behaviors and emerging threats, while DL processes large data volumes to identify sophisticated attack methods that may evade conventional systems. These technologies enable automated threat detection, faster responses, and continuous improvements through training on historical attack data. By strengthening the security of IoWT networks, they protect critical environmental data and help preserve wetland ecosystems. For example, Selvaraj and Singh used data flow parameters like Flow Packets, Flow Inter Arrival Time (IAT) Mean, and Fwd IAT Total to detect APT attacks. They applied optimized ML algorithms, including SVM, LR, BNN, and a Bayesian Optimized Ensemble model. Their Bayesian Optimized Ensemble model outperformed traditional methods, achieving an accuracy of 97.24%, an F1-score of 0.9845, a precision of 0.985, and a recall of 0.9845. The study highlights the enhanced performance of APT attack detection using the SCVIC-APT-2021 dataset.

5.3.10. Detecting botnet attacks

Botnet attacks target interconnected devices on the IoWT, compromising their functionality and security. Malicious actors exploit vulnerabilities in IoWT devices and their communication networks, turning compromised devices into botnets that can disrupt data collection, steal information, spread malware, or launch DDoS attacks, causing financial and reputational damage [196][197]. As more devices connect in wetland ecosystems, the attack surface expands, increasing the vulnerability of IoWT systems. Weak security measures enable attackers to take control of critical infrastructure, allowing botnet activities to damage both the system and the environment. Detecting these threats requires analyzing network traffic and system behaviors, with ML and DL techniques identifying anomalies and potential attacks [196][197]. By analyzing network traffic data, supervised learning helps differentiate between normal and malicious behaviors. In contrast, unsupervised learning detects new attack patterns without predefined labels, making it adaptable to the evolving IoWT environment. CNNs and RNNs are particularly effective in recognizing complex and emerging botnet threats, enhancing detection and mitigation efforts with proactive, autonomous defense and minimal human intervention. Several research studies have applied ML and DL techniques to detect botnet attacks. Arnold et al. [143] developed an IoT Botnet detection pipeline that uses a novel network traffic visualization and a CNN for cyberattack classification. The pipeline operates efficiently on an embedded system, achieving 100% and 99.78% detection rates on the N-BaIoT and IoT-23 datasets. It also provides 2.4 times greater throughput and reduces model size by 21.4% compared to a similar accuracy DNN. Wardana et al. [198] proposed a DNN model for detecting botnet attacks across heterogeneous IoT devices, using ensemble averaging to combine predictions from each training model. They validated the model with the N-BaIoT dataset, achieving high performance with 97.21% accuracy, 91.41% precision, 87.31% recall, and 88.48% F1-score. The ensemble averaging DNN outperformed individual models in detecting botnet attacks across diverse IoT devices, providing a comprehensive solution for IoT environments. Saied et al. [199] analyzed the performance of tree-based ML algorithms for detecting botnet attacks in IoT ecosystems using a public botnet N-BaIoT dataset. Their study compared DT algorithms and ensemble methods, showing that the RF algorithm outperformed others with an accuracy of 0.999991. The results highlighted RF's superior IoT botnet detection and computational efficiency performance.

5.3.11. Counter-jamming and spoofing attacks

Jamming attacks in the IoWT occur when attackers disrupt wireless communication channels by generating noise or signals on the same frequency, blocking legitimate transmissions between devices. Spoofing attacks deceive the system by sending falsified data, such as manipulated sensor readings, leading to unnecessarily incorrect actions like activating water pumps. IoWT systems use advanced techniques like frequency hopping spread spectrum, adaptive power control, and redundant communication channels to maintain reliable transmissions. Strong authentication, encrypted communication protocols, and anomaly detection algorithms protect against spoofing, ensuring data integrity through signal verification. Machine learning

and DL enhance defense mechanisms by analyzing large datasets to detect anomalies and identify potential threats. ML algorithms utilize pattern recognition and predictive analysis, while DL models process complex data to uncover subtle patterns that traditional methods may miss. Integrating ML and DL allows IoWT systems to adapt instantly, offering robust protection and ensuring reliable communications, ecosystem monitoring, and effective wetland management against sophisticated jamming and spoofing attacks. Rehman et al. [142] introduced a Fog-enabled FL-based IDS (FFL-IDS) leveraging CNNs to enhance privacy and ensure low-latency detection in Industrial Internet of Things (IIoT) networks. Validated on the Edge-IIoTset and CIC-IDS2017 datasets. The Edge-IIoTset dataset achieved 93.4% accuracy, 91.6% recall, 88% precision, 87% F1 score, and 87% specificity in detecting jamming and spoofing attacks. The system demonstrated greater robustness on the CIC-IDS2017 dataset, with 95.8% accuracy, 94.9% precision, 94% recall, 93% F1 score, and 93% specificity. This scalable, high-performance framework effectively secures IIoT environments while preserving data privacy.

5.3.12. Securing against cross-site scripting attacks and SQL injection attacks

In the IoWT, attackers can inject malicious scripts into web applications that interact with IoWT devices, enabling cross-site scripting (XSS) attacks. Attackers can exploit vulnerabilities in IoWT systems' web interfaces, stealing sensitive data, manipulating device functions, or launching further attacks within the network. These systems often involve remote monitoring and control, making them vulnerable to unauthorized access, environmental data manipulation, and the compromise of critical infrastructure. SQL injection (SQLi) attacks target IoWT systems that rely on databases to manage sensor and device data, allowing attackers to bypass security measures and manipulate, delete, or access sensitive information. IoWT systems must implement robust security measures like input validation, sanitization, and parameterized queries or prepared statements to block SQLi. Machine learning and deep learning techniques enhance security by instantly detecting and responding to attacks, analyzing large datasets for known attack patterns, and continuously adapting to emerging threats. This proactive approach helps prevent malicious scripts and SQL queries from exploiting vulnerabilities, ensuring the integrity and safety of the valuable environmental data managed by IoWT systems. Deep learning is particularly valuable in detecting sophisticated attack patterns that might evade traditional security measures. Neural networks learn complex features and correlations from large datasets, improving their ability to differentiate between legitimate and malicious activities. In the IoWT context, DL enhances the security of sensor networks, data transmission, and web interfaces by automatically identifying and neutralizing attacks. IoWT applications can better protect against evolving cyber threats by combining ML and DL. Tadhani et al. [200] developed a hybrid DL model combining CNNs and LSTMs to secure web applications from SQLi and XSS attacks. The model achieved exceptional accuracy with minimal false positives by training on multiple datasets, including the HTTP CSIC 2010, SQLi/XSS Payload, and our custom testbed dataset (99.77%, 99.84%, and 99.23%, respectively). This approach outperformed traditional ML methods, offering a robust solution for real-time threat detection and web application security.

While research on using ML and DL to enhance the security of the IoWT is limited, the application of these technologies in securing IoT systems can be extended directly to IoWT. By incorporating ML and DL, IoWT systems can significantly improve device-level security, ensuring excellent reliability, resilience, and trustworthiness. Table 4 summarizes the related works regarding the application of ML and DL in improving the security of IoT.

TABLE IV. SUMMARY OF THE RELATED WORKS REGARDING THE APPLICATION OF ML AND DL IN IMPROVING THE SECURITY OF IOT.

Reference	Year	Focus	AI Method	ML or DL Model	Dataset(s)	Best Performing	Metrics
[147]	2025	Detecting adversarial	DL	Spectrogram-based CNNs	Benchmark	Spectrogram-based CNNs	Accuracy (99.34%,
[148]	2024	Detecting adversarial	ML & DL	CNN, RF, SVM, and	Diverse	CNN and RF	Accuracy (98.3% &
[149]	2024	Detecting adversarial	DL	CNN	UNSW-NB15	CNN	Accuracy (95.47%)
[150]	2024	Detecting adversarial	DL	CNN, convolutional,	CIC IoT 2023, CIC-MalMem-	CNN	Accuracy (99.99%)
[151]	2024	Detecting adversarial	DL	DNN, LSTM, and CNN	CICIoT2023	CNN	Accuracy (99.10%)
[152]	2024	Detecting adversarial	ML	RF, NB, DT, Backpropagatio	BoTNet-IoT-L01, NSL-		Accuracy (99.9%)
[153]	2024	Detecting adversarial	DL	CNN and RNN	Bot-IoT	CNN and RNN	Accuracy (99%)
[146]	2023	Detecting adversarial	DL	FFNN and LSTM	NSL-KDD and BoT-IoT	FFNN	Accuracy (99.95%)
[157]	2024	Detecting Anomaly	DL	Asymmetric stacked	BoT-IoT		Accuracy (99.99%)

[159]	2024	Detecting Anomaly	DL	CNNs and RNNs		RNN	Accuracy (96%)
[161]	2023	Detecting Anomaly	DL	Stacking deep ensemble	ToN-IoT and InSDN		Accuracy (99.8% and
[162]	2025	Detecting intrusion	ML & DL	KNN, SVM, RF, DT,	UNSW-NB15	RF	Accuracy (99.5%)
[163]	2024	Detecting intrusion	ML & DL	SVD and SMOTE	ToN_IoT		Accuracy (99.98%)
[164]	2024	Detecting intrusion	DL	Convolution and Vision	TON-IoT and Bot-IoT		Accuracy (97.14% and
[165]	2024	Detecting intrusion	DL	CNN-GRU and CNN-LSTM	Kitsune and TON-IoT		Accuracy (99.6% and
[166]	2024	Detecting intrusion	ML & DL	DT, MLP, and Autoencoder	WSN-DS	DT and MLP	Accuracy (99%)
[167]	2024	Detecting intrusion	ML & DL	CNN, CNN-BiLSTM,	UNSW-NB15 and NSL-KDD	CNN and CNN-BiLSTM	Accuracy (94.97% and
[168]	2024	Detecting intrusion	ML & DL	DT, RF, and DNN	UNSW-NB15	DT	Accuracy (94.91%)
[137]	2024	Detecting intrusion	DL	CGRNs and CNN	UNSW-NB15, KDDCup99,		Accuracy (99.2%)
[169]	2024	Detecting intrusion	DL	LSTM and SMOTE	CICIDS2017, NSL-KDD, and		Accuracy (99.34%,
[170]	2024	Detecting intrusion	DL	Temporal convolutional	ToN_IoT and UNSW-NB15		Accuracy (99.55% and
[171]	2024	Detecting intrusion	DL	CNN-LSTM and a	InSDN		Accuracy (99.02%)
[173]	2025	Detecting and preventing	ML & DL	AutoEncoder and XGBoost	IDSH		Accuracy (97.24%)
[174]	2024	Detecting phishing	DL	CNNs and Bi-GRUs	SMS Phishing Collection		Accuracy (99.82%)
[175]	2024	Detecting phishing	DL	BERT and CNN	Kaggle data set		Accuracy (97.5%)
[176]	2024	Detecting phishing	ML	RF, DT, and XGBoost	ML	RF	Accuracy (96.89%)
[177]	2024	Detecting phishing	DL	ANN, CNN, RNN,	PhishTank	CNN	Accuracy (98.74%)
[178]	2024	Detecting phishing	ML	SVM and XGBoost	Phishing Dataset for ML	XGBoost	Accuracy (90%)
[182]	2025	Detecting malware	ML	MLP, DT, RF, KNN, and LR	CIC-AndMal2017	DT and RF	Accuracy (98.89%)
[183]	2024	Detecting malware	DL		Malware dataset		Accuracy (98.29%)
[181]	2024	Detecting malware	DL	BERT, FFNN, CNN, and	IOT23 datasets		Accuracy (97.99%)
[184]	2024	Detecting malware	ML	DT, KNN, and XGBoost	malware dataset	XGBoost	Accuracy (98.44%)
[185]	2023	Detecting malware	ML & DL	KNN, SVM, RF, Extra	BoT-IoT	XGBoost and CatBoost	Accuracy (98.50% &
[131]	2023	Detecting malware	ML & DL	RF, DT, SVM, KNN, SGD,	Kaggle	DL model	Accuracy (96%)
[188]	2024	Detecting DoS and DDoS	ML	SVM, RF, and Gradient	CICDDOS2019 and KDD-CUP	SVM	Accuracy (96.61%)
[133]	2024	Detecting DoS and DDoS	ML	SVM, RF, and KNN	Synthetic datasets		
[189]	2024	Detecting DoS and DDoS	ML	GRU, GhostNet,	IoT-23 and APA-DDoS	EffiGRU-GhostNet	Accuracy (99.05%)
[190]	2024	Detecting DoS and DDoS	ML & DL	XAI, FDNNs, XGBoost with	Distributed datasets		Accuracy (99.78%)
[191]	2024	Detecting DoS and DDoS	ML & DL	LR, KNN, and DNN	CIC2023 IoT	LR, KNN, and DNN	Accuracy (0.9999)

[192]	2023	Detecting DoS and DDoS	ML & DL	SMOA, ANN, KNN, and	CIC IoT Dataset 2022		Accuracy (99.19%)
[193]	2023	Detecting insider threats	ML & DL	SVM, RF, LSTMs, and	User activity records and		Accuracy (96.3%)
[194]	2024	Detecting APT	ML	SVM, LR, BNN, and a	SCVIC-APT-2021	Bayesian Optimized	Accuracy (97.24%)
[143]	2024	Detecting botnet attacks	DL	CNN and DNN	N-BaIoT and IoT-23	CNN	Accuracy (100% &
[198]	2024	Detecting botnet attacks	DL	DNN	N-BaIoT	DNN	Accuracy (97.21%)
[199]	2023	Detecting botnet attacks	ML	DT algorithms and ensemble	Public botnet N-BaIoT	RF	Accuracy (0.999991)
[142]	2024	Counter-jamming and	ML & DL	FL and CNNs	Edge-IIoTset and CIC-		Accuracy (95.8%)
[200]	2024	Securing against XSS	DL	CNNs and LSTMs	HTTP CSIC 2010,		Accuracy (99.77%,

5.4. Real-world implementations and case studies

Real-world deployments and case studies demonstrating how ML and DL can be used to secure the IoWT include the following:

5.4.1. Machine learning for intelligent wetland monitoring and security

Kumar and Yadav [201] integrated ML algorithms into IoWT systems to prevent cyberattacks on network infrastructure. By training the system with historical attack data, their models identified and blocked potential threats before they could cause any harm. Reddy and Raj [202] applied predictive analytics using ML to monitor the wetland ecosystem's health. The system could predict potential security threats like floods or illegal encroachment by analyzing environmental sensor data, allowing preemptive actions to secure the ecosystem. Mahamud and Alam [203] developed an intelligent wetland monitoring system using IoT sensors to collect environmental data, including water quality and weather information. They employed ML models to analyze this data and detect potential threats such as floods, contamination, or unauthorized access. To ensure data integrity and privacy, they implemented robust security mechanisms.

5.4.2. Deep learning for intrusion detection and cybersecurity in Wetland IoT networks

Sharma et al. [204] applied DL techniques, specifically CNN, to identify anomalies in IoWT communication networks. The DL model detected real-time suspicious activities, such as data breaches or unauthorized device access. Ansar et al. [205] proposed an innovative design of an IDS for IoT environments using DL-integrated CNN and LSTM networks. The model achieved high accuracy in classifying network traffic, demonstrating its applicability in securing IoWT systems. Patel et al. [206] used AI to analyze the vast data streams generated by IoWT systems, identifying anomalies that could indicate system breaches or environmental threats. The AI model employs a multi-layer defense system to protect against external attacks. Wu and Zhang [207] implemented a DL model to secure communication in IoWT networks. The model focused on detecting and mitigating unauthorized access by monitoring communication patterns across the network. Hamidouche et al. [208] introduced an unsupervised ensemble learning model capable of detecting new or unknown attacks in IoT networks. The model's ability to identify anomalies without labeled data makes it suitable for dynamic IoWT environments.

5.4.3. Machine learning and DL for cybersecurity in Wetland IoT devices

Ghaffari et al. [135] reviewed IoT security research, focusing on ML and DL approaches. It categorizes recent studies addressing security issues in IoT environments, providing insights applicable to IoWT systems. Khan et al. [209] developed a DL-based cybersecurity solution for IoWT devices, utilizing LSTM networks to detect and prevent attacks on devices used in wetland monitoring. This model identified irregular device behaviors and flagged potential security breaches. Rafique et al. [210] examined privacy and security concerns related to data exchange and storage in intelligent health applications. The research explores how ML methods can enhance security and demonstrates their adaptability to IoWT contexts, where they can protect sensitive environmental data. Zhang and Liu [211] used the FL model in IoWT systems, enabling devices to learn from local data without transmitting sensitive environmental information to a centralized server. This approach preserved privacy while allowing the efficient training of models for anomaly detection and threat prevention.

5.5. Benefits of ML and DL methods for IoWT security

Machine learning and DL techniques significantly enhance IoWT security by enabling intelligent, real-time threat detection and response. Below is a synopsis of how ML and DL improve IoWT security.

5.5.1. Anomaly detection and intrusion prevention

In IoWT networks, ML and DL models can identify anomalous activity like illegal access, odd data patterns, or unexpected communication flows that could indicate cyberattacks. A DNN, for example, may rapidly monitor sensor data traffic to spot anomalies like DoS or Zero-day attacks, illegal access, or questionable activity directed at IoWT gateways. The system can instantly identify a possible attack and remove the water quality sensor from the network if it sends data at an abnormally high frequency [212].

5.5.2. Real-time decision-making

Deep learning techniques immediately handle IoWT data, using models like RNNs and LSTMs to analyze sequential data. These networks' effective handling of time-series inputs, including sensor measurements, makes timely decision-making possible. Their rapid processing capability is crucial in wetland regions, where prompt reactions are necessary to address risks or minimize cyber threats [86].

5.5.3. Threat prediction and risk assessment

Proactive steps to safeguard IoWT systems are made possible by supervised and unsupervised machine learning algorithms that examine past attack data and environmental variables to forecast possible security risks. A random forest classifier, for example, can analyze previous phishing attempts against IoWT device control systems and predict the probability of such attacks happening at particular times, like following firmware changes.

5.5.4. Robustness to dynamic environments

Wetlands are dynamic habitats that frequently experience changes in temperature, moisture content, and water levels. Deep learning techniques, which are excellent at generalizing training data, successfully address this unpredictability. Even temporarily, strategies like autoencoders improve flexibility and permit trustworthy anomaly tracking. In constantly changing contexts, this flexibility guarantees that IoWT systems stay safe and reliable [213].

5.5.5. Secure authentication mechanisms

Machine learning models improve authentication methods and enable adaptive security features like behavioral analytics and biometric-based device authentication. For example, an IoWT device that controls water flow can evaluate user behavior, authenticate authorized users, and dynamically validate access credentials while blocking unwanted access.

5.5.6. Scalability for large-scale IoWT networks

IoWT systems monitor extensive wetlands using hundreds of networked sensors and communication devices. The high-dimensional data generated by these devices is handled effectively by DL models, which take advantage of their scalability to understand the relationships between different variables. Thanks to this capacity, the models can protect sizable wetland ecosystems vigorously [82].

5.5.7. Robust encryption and data integrity

Thanks to DL, advanced encryption methods that withstand brute-force attacks and guarantee the integrity of IoWT data while it is being transmitted can be developed. Systems can successfully protect communication between distant wetland sensors and central servers by using GANs to actively generate extremely secure synthetic encryption keys that are difficult for attackers to decode.

5.5.8. Ability to learn from unstructured data

Sensor measurements, multispectral images from monitoring cameras, and unstructured logs are just a few of the data forms that IoWT systems gather. DL algorithms, such as CNNs and GANs, efficiently process and analyze these many data types. By integrating multimodal data, these strategies improve the security of IoWT systems by using traffic analysis to identify suspicious behaviors and picture analysis to detect unwanted access [214].

5.5.9. Resource-efficient security solutions

IoT devices frequently have limitations regarding battery life and computational capability. Nevertheless, ML and DL algorithms can balance energy efficiency with strong defenses by optimizing resource allocation for security tasks. Lightweight ML models, deployed on edge devices, can locally process and filter sensor data to detect potential threats, minimizing the need for frequent communication with a central server and thus reducing power consumption.

5.5.10. Improved accuracy over traditional methods

Deep learning methods, especially those based on CNNs, deliver higher accuracy and precision than traditional ML algorithms in IDS. These systems can surpass 95% in detection accuracy while reducing false positives and false negatives, making them highly effective for IoWT systems. This improved accuracy is essential, as unnecessary alarm triggers can cause disruptions and waste valuable resources.

5.5.11. Adaptive and context-aware security

Machine learning models can adapt to dynamic changes in IoWT environments by learning from new data to improve their ability to recognize and mitigate security risks over time. For instance, a RL algorithm can adjust to seasonal variations in wetland sensor activity, ensuring it minimizes false positives in anomaly detection during periods of high biological activity, such as bird migration seasons.

5.5.12. Automation of security operations

Deep learning models autonomously perform various security tasks within the IoWT system without human intervention. After training, these models continuously monitor for vulnerabilities, offer countermeasure suggestions to the control center, or even activate them automatically. This autonomy reduces the workload for security teams, enabling them to focus on other essential tasks related to the IoWT [78].

5.5.13. Mitigating physical attacks

IoWT devices placed in remote and vulnerable locations risk physical tampering. Machine learning and DL methods can monitor physical security and alert administrators to threats. For instance, a DL-based image recognition system linked to surveillance cameras in a wetland can detect unauthorized human activity near IoWT sensors and immediately notify administrators.

5.5.14. Proactive threat prevention

Deep reinforcement learning techniques help IoWT systems predict and address security threats by dynamically adjusting security measures in response to environmental changes or emerging risks. For example, a DRL model can actively manage firewall rules, encrypt sensitive data, and optimize resource allocation to mitigate potential threats, thus strengthening the security of IoWT systems against evolving cyber risks [215].

5.5.15. Automated threat response

Deep learning models can automate responses to detected security threats, minimizing the time needed to mitigate risks and maintaining system operation during attacks. For instance, a DL-based decision system can identify a malware-infected IoWT sensor, immediately isolate it from the network, and deploy security patches to other vulnerable devices.

5.5.16. Privacy preservation

By keeping sensitive data local, ML techniques like FL enable IoWT security systems to learn and improve while safeguarding user and environmental privacy. For instance, wetland sensors measuring biodiversity data can collaboratively train anomaly detection models using FL without sharing raw data, thereby minimizing the risk of privacy breaches.

5.5.17. Real-time monitoring and alert systems

Machine learning and DL systems monitor in real-time, allowing for the rapid detection and mitigation of security threats. For instance, RNNs analyze time-series data from IoWT sensors to spot patterns that signal potential tampering or cyberattacks, such as sudden changes in water temperature readings.

5.6. Comparison of ML and DL Approaches in the IoWT Security

The IoWT focuses on analyzing wetland ecosystems for environmental monitoring and resource usage. These systems generate large volumes of diverse data, making them vulnerable to various cyber risks. While ML and DL share similarities, their unique features enable them to address different security threats in IoWT networks.

Machine learning algorithms like SVM, RF, and KNN play a vital role in decision-making for IoWT security due to their ease of implementation, efficiency, and explainability. These models accurately predict cyberattacks like DDoS by analyzing previous incidents, and feature selection methods help reduce computation, making them suitable for IoWT devices. However, ML systems rely heavily on feature engineering, which requires domain knowledge and can struggle to adapt to adversary actions' dynamic and complex nature in high-dimensional IoWT environments [216][217]. In wetland monitoring and management, ML techniques like RF and SVM perform well in wetland classification, particularly with smaller datasets. However, they depend on manual feature extraction, which limits their ability to capture complex patterns. CNNs and RNNs automatically learn hierarchical features from raw data, excelling in large-scale and complex wetland mapping tasks. While ML remains more practical for smaller datasets and limited computational resources, DL outperforms ML in handling large datasets and high-spatial-resolution data, enabling more accurate and automated wetland monitoring in the IoWT [20]. Traditional ML techniques, such as SVM, RF, and XGBoost, have been actively applied to classify wetland types and assess water areas. Guillou et al. [218] compared RF and CNN approaches for pre-locating wetlands, finding that RF achieved higher accuracy, though CNNs demonstrated potential with architectural improvements. Similarly, Günen [219] evaluated various ML methods, including SVM, Linear Discriminant Analysis, KNN, Canonical Correlation Forests, and AdaBoost.M1, for identifying wetland water areas using Sentinel-2 images, noting that these techniques struggled to capture the complex, fully non-linear relationships in wetland data. Verma et al. [220] developed a remotely operated wetland siphon

system that leverages ML algorithms to predict water levels and manage water flow during hurricanes, effectively mitigating flood risks.

Gemechu et al. [221] used ML algorithms with remotely sensed data to detect wetland area changes and highlighted the potential for enhanced accuracy through integration with DL methods. Deep learning models, especially CNNs and RNNs, play an increasingly vital role in intrusion and anomaly detection in the IoWT by extracting high-level features from raw, unstructured data. CNNs effectively differentiate signals from wetland instruments and detect intrusions, while RNNs capture temporal patterns in IoWT traffic. Their flexibility and modularity enable them to detect zero-day attacks and address real-time security challenges. However, their complexity, high resource demands, and black-box nature create challenges for IoWT systems with low-power devices, particularly at the network edge, where interpretability and reliability are crucial for environmental applications. Traditional ML models perform well in low-complexity scenarios and when data explainability is essential, but DL models excel at handling large, high-dimensional datasets and identifying complex attack patterns. A recent study reported that DL models achieved 96% accuracy in IoWT attack detection, surpassing the 89% accuracy of ML models [222][223].

Additionally, CNNs have consistently outperformed traditional ML methods in wetland classification tasks. Vynikal et al. [224] demonstrated the superiority of the U-Net architecture in delineating intricate wetland boundaries on historical topographic maps compared to other DL models. Günen [219] demonstrated that a 1D CNN model offers significant advantages in classifying wetland water areas, outperforming traditional ML algorithms in accuracy, recall, precision, specificity, and F-scores. In analyzing remote sensing images, he also presented a DL-based vision transformer model that performed better than CNN-based techniques, particularly when handling intricate satellite image features. Additionally, Günen investigated DL methods for identifying the ethnic backgrounds of individuals in wetland areas, demonstrating better results in feature selection and model building when contrasted with conventional ML techniques.

With varying levels of complexity and data needs, ML and DL each offer unique benefits to IoWT applications. ML performs exceptionally well in predictive modeling and classification jobs with little computing effort, efficiently handling structured data and smaller datasets. On the other hand, DL is more accurate at processing unstructured data, like photos, and identifying intricate, non-linear patterns, but it comes at a higher computational cost. The resource-intensive aspect of DL enables it to represent these intricacies more successfully than ML, which may find it challenging to capture the complex linkages found in wetland ecosystems. Researchers can provide the best solutions for wetland ecosystem monitoring and management by fusing the feature selection power of ML with the feature learning power of DL.

6. CHALLENGES IN APPLYING ML AND DL METHODS TO IoWT SECURITY

Securing the IoWT with ML and DL methods is challenging due to the unique conditions of wetland environments, the limited resources of IoWT devices, and the evolving complexity of cyber threats. These factors demand customized security approaches that account for environmental and technological constraints, ensuring adequate protection despite these challenges. Below is a brief description of these challenges:

6.1. Data privacy and security

IoWT systems gather vast amounts of environmental and user data, including sensitive details like geolocation and usage patterns, raising significant privacy and security concerns. Integrating ML and DL into these systems requires access to this data, making it challenging to prevent unauthorized access and breaches while ensuring model effectiveness. Cloud-based DL processing further increases data privacy risks [126][225]. Privacy-preserving ML techniques, such as FL and differential privacy, remain underexplored in IoWT, highlighting a critical gap in securing sensitive data processing.

6.2. Computational constraints

Wetland monitoring devices in IoWT systems often operate in environments with limited resources, where the high computational demands of ML and DL algorithms hinder real-time data processing and security responses. Studies highlight that DL techniques, including DNN, CNNs, and GANs, require substantial computational power, making them impractical for resource-constrained devices like low-power sensors and microcontrollers [43][126][225]. Although less demanding, ML models like RF still require optimization to operate effectively in IoWT systems. In ecologically sensitive wetlands, the substantial processing time and energy consumption of DL models raises environmental concerns, decreases operational efficiency, and increases system downtime [160].

6.3. Scarcity of high-quality labeled data

Machine learning and DL models need big, high-quality datasets for real-world training. However, sparse, noisy, or unlabeled data are common problems for IoWT applications, which lowers model accuracy and dependability. Because AI algorithms in IoT security depend on considerable, clean information to identify anomalies and forecast environmental changes, these difficulties make it challenging to create reliable models [126][226]. The scarcity of labeled data weakens

their capacity to develop trustworthy detection metrics. Furthermore, the absence of widely recognized, standardized databases makes comparing strategies and evaluating results challenging, which slows down research [227].

6.4. Heterogeneous and imbalanced data

IoWT systems generate vast amounts of diverse and imbalanced data from water quality sensors, biodiversity monitors, and weather stations, where routine events significantly outnumber anomalies or security threats [160]. Training ML and DL models on such datasets often results in biased predictions favoring the majority class, making detecting rare but critical threats challenging [126]. Researchers address this issue through oversampling, under-sampling, and synthetic data generation, but these techniques increase computational complexity and complicate training. Deep learning models, which rely on large, labeled datasets, struggle in sparsely populated environments like wetlands, where heterogeneous data require extensive preprocessing. The shortage of domain experts further slows progress, and limited training samples weaken model performance and reduce detection accuracy.

6.5. Lack of interpretability and explainability

Deep learning methods lack interpretability, making it challenging to explain their decision-making processes. This transparency issue weakens IoWT security, as understanding threat detection reasoning is essential for effective responses [126]. Despite this limitation, DL continues to gain traction in IoWT applications, emphasizing the need to understand its inner workings better. Environmental scientists and policymakers often view these algorithms as “black boxes,” highlighting the urgency of improving transparency [228].

6.6. Evolving cyber threats

Sophisticated cyber threats, including APTs, zero-day exploits, and malware attacks, increasingly target IoWT environments by leveraging complex and evolving attack vectors that challenge traditional ML models. While DL methods like RNNs and CNNs effectively capture temporal and spatial data features, their performance depends on continuously updated training datasets, which are difficult to maintain in IoWT contexts [126]. Adversarial attacks exploit NN weaknesses by subtly altering sensor data, deceiving DL-based IDS, and compromising network security. These vulnerabilities pose significant risks to IoWT applications, such as wetland hubs, where adversarial ML attacks can lead to misclassifications and flawed assessments, ultimately threatening environmental management efforts [229].

6.7. Scalability issues

Scaling ML models to handle vast data and numerous devices in IoWT systems remains a significant challenge, especially as networks grow. These systems deploy thousands of interconnected devices in wetland areas, making it increasingly complex to implement scalable security mechanisms. Ensuring security across multiple devices and data streams poses difficulties for ML and DL models. Research on ML-enabled IoT security highlights unresolved issues related to APT and stresses the need for scalable solutions. Centralized DL approaches often create bottlenecks, while decentralized, edge-based learning introduces challenges like communication overhead and data synchronization [102][126][230].

6.8. Ethical and legal considerations

Deploying ML and DL in the IoWT raises ethical and legal challenges, particularly in data ownership, user consent, and compliance with environmental regulations. Ensuring responsible and lawful implementation requires addressing these concerns to protect user rights, maintain transparency, and uphold regulatory standards.

6.9. Environmental factors

Wetland environments present dynamic and harsh conditions, such as extreme weather, high humidity, and fluctuating water levels, which lead to data transmission delays, signal degradation, and device failures. These challenges hinder the deployment and maintenance of ML and DL-based security systems, especially in IoWT networks. For instance, disruptions in data can undermine the real-time detection capabilities of IDS, leaving the networks more susceptible to attacks.

6.10. Lack of standardized security frameworks

The IoWT domain lacks standardized frameworks for implementing ML and DL-based security solutions, making it challenging to design interoperable and robust security systems that tackle the wide range of threats IoWT networks face. Deploying these advanced methods becomes more complex and costly, requiring customization to suit specific wetland use cases.

6.11. Overfitting and poor generalization

Deep learning models tend to overfit when working with large, tiny, or unbalanced datasets. This problem presents a difficulty in terms of IoWT security. Even while the model performs exceptionally well with training data, adjusting and functioning well in novel situations or dangers may be difficult. This lack of generalization compromises the model's

dependability in practical situations. Consequently, DL systems lose their ability to protect IoWT networks against sophisticated and constantly changing cyber threats [160].

6.12. Deployment challenges in remote areas

Deploying and running DL models in IoWT systems in places with dispersed infrastructure, including marshes with weak network access and low-powered devices, is challenging. These systems demand strong technology, sufficient bandwidth for real-time data processing, and frequent updates—all of which are challenging to achieve in such settings. Consequently, it is frequently ineffective and impractical to deploy DL-based security solutions in these areas [231].

6.13. High initial costs

Hardware, software, and human resources expenditures are among the high costs associated with DL-based security solution deployment in the IoWT. The cost of training and updating models can be prohibitive, particularly for pilot projects in wetlands, due to the requirement for GPUs, customized model creation, and AI specialists. These exorbitant expenses can impede the further use of DL solutions in these settings [126].

6.14. Continuous learning and adaptation

Because dynamic IoWT environments are constantly changing, developing ML models for them can be difficult. The primary challenge is creating models that can adjust to new data and changing circumstances without requiring whole retraining from scratch [126]. Fig. 7 highlights the challenges when applying ML and DL methods to IoWT security.

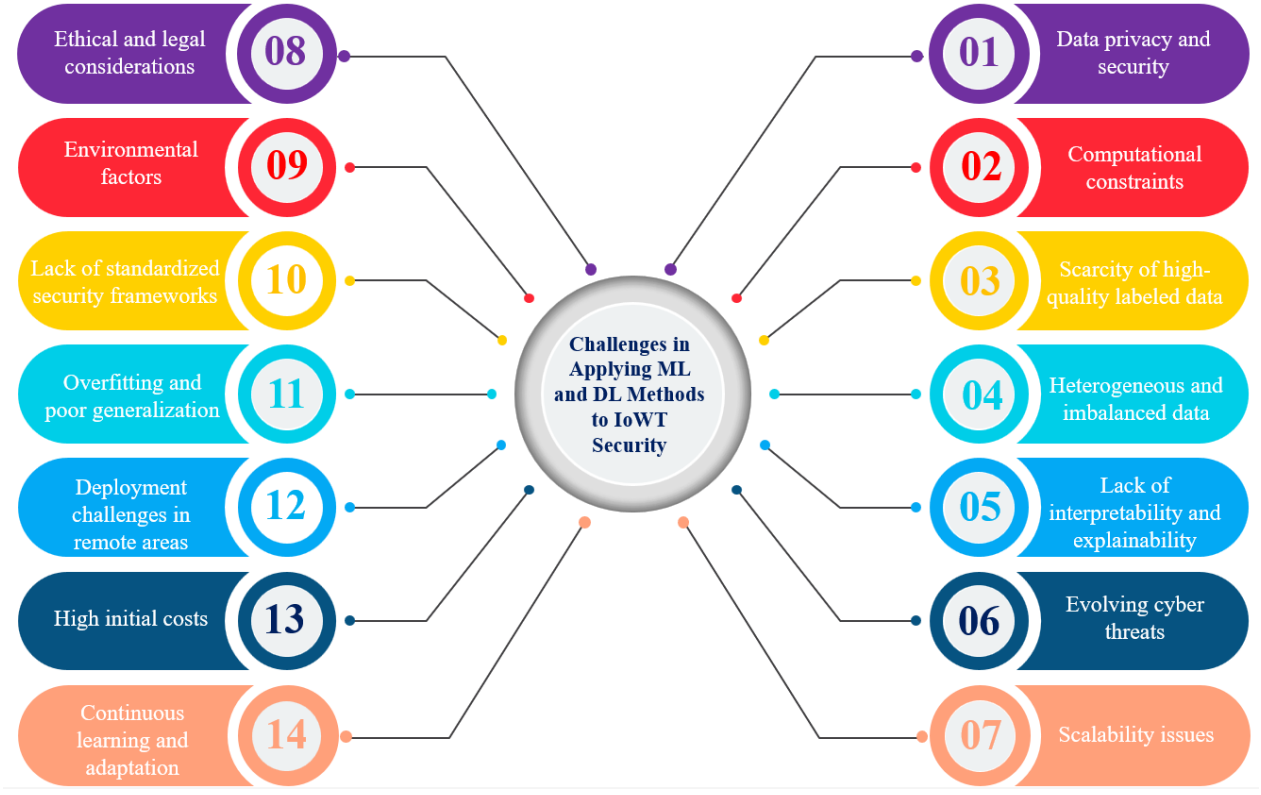

Fig. 7. Summary of the challenges in applying ML and DL methods to IoWT security.

7. FUTURE RESEARCH DIRECTIONS

By utilizing ML and DL techniques, IoWT systems can improve predictability, identify anomalies, and facilitate near-real-time decision-making. However, integrating these technologies presents challenges such as cybersecurity threats, privacy concerns, and computational limitations. Further research is needed in several key areas to address these issues and build upon recent findings.

- To protect sensitive ecological data in wetlands, ML and DL techniques like FL and homomorphic encryption can provide adaptive encryption, ensuring data privacy in decentralized networks. Additionally, integrating Blockchain

with the IoWT enhances data exchange, fostering transparency and accountability in managing ecological data while safeguarding it from unauthorized access and alteration.

- Development of lightweight ML Models: IoWT devices often operate with limited computational resources, making the implementation of complex security algorithms difficult. Future research should prioritize the development of lightweight ML and DL models optimized for resource-constrained environments. By reducing computational overhead without sacrificing detection accuracy, researchers can create efficient solutions that meet the security demands of IoWT systems.
- Enhancement of real-time threat detection: Real-time threat detection is critical for the security of IoWT applications. Researchers should enhance these capabilities by designing models capable of swiftly processing and analyzing data streams. Advanced DL architectures and edge computing technologies can minimize latency, ensuring timely threat response and improving overall system security.
- Integration of FL approaches: Data privacy remains a significant concern in IoWT systems, making FL a promising solution. Federated learning enhances privacy while maintaining robust threat detection by enabling models to train across multiple devices without centralizing sensitive data. Future studies should explore its application in IoWT security to balance data protection with effective threat management.
- Adversarial robustness of security models: Machine learning models in IoWT are susceptible to adversarial attacks, where malicious inputs aim to deceive the system. Research should concentrate on improving these models' adversarial robustness by exploring techniques such as adversarial training and implementing defensive strategies. Strengthening these models will enhance the reliability and resilience of IoWT security measures.
- Standardization of security protocols: The lack of standardized security protocols in IoWT creates challenges for interoperability and comprehensive protection. To overcome this, researchers should work on developing and promoting universal security frameworks. These standards would ensure cohesive and effective security practices across IoWT devices and networks, fostering better collaboration and protection.
- Energy-efficient security solutions: Energy efficiency is crucial for IoWT devices, especially when deployed in remote locations. Research should aim to design energy-efficient ML algorithms that offer strong security without depleting device power resources. By balancing security performance with energy consumption, researchers can create solutions that support long-term device operation.
- Explainability and transparency in AI models: Ensuring the explainability and transparency of AI models is vital for building trust and accountability in IoWT security. Future research should focus on improving the interpretability of ML and DL models, enabling stakeholders to understand better and trust the decisions these systems make.
- Scalability of security solutions: As IoWT networks grow, security solutions must scale to accommodate increasing data and devices. Researchers should investigate scalable ML approaches, including distributed learning techniques and cloud-based solutions, to maintain performance and effectiveness in expanding networks.
- Cross-layer security strategies: Cross-layer security strategies can offer comprehensive protection by addressing vulnerabilities at different levels of the IoWT architecture. Future research should explore integrating ML models across various layers, from the physical to the application layer, to provide holistic security coverage for IoWT systems.
- Ethical and legal considerations in AI-driven security: The deployment of AI-driven security solutions in IoWT raises moral and legal concerns, particularly regarding data privacy and algorithmic bias. Researchers must develop ethical frameworks and guidelines to ensure the responsible use of AI in IoWT security applications, actively addressing these issues to promote accountability and safeguard ethical standards. These efforts will promote trust, fairness, and accountability in adopting advanced security technologies.
- Future work should focus on extending edge-based DL approaches for local data processing and analysis to improve efficiency and reduce reliance on cloud servers. Advancing distributed intelligence can enable IoWT devices to identify anomalies and exchange patterns within the network collaboratively. This decentralized approach enhances scalability and fault resilience while supporting wetland monitoring systems. Prioritizing edge computing aligns with the resource constraints of IoWT devices.
- IoWT devices often face energy limitations due to their installation in hard-to-reach areas. Future studies must prioritize reducing power consumption during ML model training and usage through model quantization, pruning, and knowledge distillation. Researchers should also focus on adaptive models that adjust processing capacity based on available energy. These approaches can significantly extend the utility and lifespan of such devices.

- Developing conceptual and legal guidelines to integrate diverse IoWT devices and platforms: Future efforts can prioritize creating ML and DL models to address data format and communication protocol heterogeneities, ensuring seamless compatibility across IoWT systems. This research would also enhance the coordination of wetland protection programs globally. By addressing these challenges, researchers can drive more effective international collaboration and technological integration.
- Prioritizing human-centric frameworks for IoWT security by developing ML and DL models tailored to communities and individuals. Employing participatory design methods can ensure that security solutions are culturally appropriate, user-friendly, and practical for wetland conservation. Raising stakeholder awareness about proper IoWT usage and cybersecurity will further enhance the utility of these technologies. This approach will foster safer and more effective implementation in wetland conservation efforts.

By focusing on these future research directions, researchers can significantly enhance the security of IoWT systems, ensuring these critical networks operate safely and efficiently. This progress will empower the sustainable use of technology to protect and preserve wetlands worldwide.

8. CONCLUSIONS

This survey emphasizes the urgent need to protect the IoWT using ML and DL techniques to facilitate efficient environmental data acquisition and monitoring, ultimately supporting improved decision-making. Integrating IoWT devices poses serious security risks and problems. Cutting-edge technologies like ML and DL provide helpful answers by enhancing intrusion detection, anomaly detection, and threat prediction algorithms. These techniques improve the speed and accuracy of cyber threat identification while allowing systems to adjust to emerging attack patterns swiftly.

Nevertheless, several challenges exist in creating and applying ML/DL models for IoWT. These include the difficulty of creating models appropriate for particular wetland situations, the scarcity of resources in isolated wetland regions, and the absence of standardized reference models for IoT security. Future studies must concentrate on creating scalable, lightweight, energy-efficient security methods and algorithms so they may be used in these demanding settings. Furthermore, incorporating blockchain technology could improve data security even more.

Cooperation between cybersecurity specialists, IoT engineers, and environmental scientists is crucial to overcome these obstacles. Together, these experts provide integrated solutions that address the unique requirements of the IoWT ecosystem. Enhancements to the IoWT will ensure strong security and dependability while advancing sustainable growth and environmental conservation.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

The authors gratefully acknowledge their universities' valuable support and contributions, which were crucial to this research. They also thank the anonymous reviewers for their insightful guidance, which significantly improved the quality of the article. Additionally, the authors appreciate the resources and facilities provided by the universities, which were essential in completing this work.

References

[1] Y. Bai, and L. Wang, "Analyzing the applicability of wetland ecological modes in the Minjiang Estuary wetland," *Frontiers in Ecology and Evolution*, vol. 12, pp. 1–19, 2024. https://doi.org/10.3389/fevo.2024.1300624

[2] R. Cao, J. Wang, X. Tian, Y. Zou, M. Jiang, H. Yu, C. Zhao, and X. Zhou, "Post-Restoration Monitoring of Wetland Restored from Farmland Indicated That Its Effectiveness Barely Measured Up," *Water*, vol. 16, no. 3, pp. 1–16, 2024. https://doi.org/10.3390/w16030410

[3] C. Y. Oduro, P. A. Anokye, and M. A. Nanor, "Morphological Patterns and Drivers of Urban Growth on Africa's Wetland Landscapes: Insights from the Densu Delta Ramsar Site, Ghana," *Sustainability*, vol. 16, no. 15, pp. 1–22, 2024. https://doi.org/10.3390/su16156372

[4] C. B. Géant, J. Wellens, M. N. Gustave, and S. Schmitz, "How rural communities relate to nature in Sub-Saharan regions: Perception of ecosystem services provided by wetlands in South-Kivu," *Sustainability*, vol. 16, no. 16, pp. 1–30, 2024. https://doi.org/10.3390/su16167073

[5] S. S. Warrier, R. M. Samuel, H. Mukundan, N. B. S. Shibu, and A. R. Devidas, "Leveraging IoT and blockchain technologies for Wetland monitoring and community engagement," *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT),* Kamand, India, 24-28 June 2024, pp. 1–7. https://doi.org/10.1109/icccnt61001.2024.10724300

[6] Q. Demarquet, S. Rapinel, S. Dufour, and L. Hubert-Moy, "Long-Term Wetland monitoring using the Landsat Archive: A review," *Remote Sensing,* vol. 15, no. 3, pp. 1–26, 2023. https://doi.org/10.3390/rs15030820
[7] A. Y. A. Abdelmajeed, M. Albert-Saiz, A. Rastogi, and R. Juszczak, "Cloud-Based Remote Sensing for Wetland Monitoring—A review," *Remote Sensing,* vol. 15, no. 6, pp. 1–20, 2023. https://doi.org/10.3390/rs15061660
[8] H. Jafarzadeh, A. Verma, M. Mahdianpari, E. W. Gill, A. Bhattacharya, and S. Homayouni, "Compact-Polarimetric SAR Signature Analysis for Wetland characterization using RADARSAT Constellation Mission," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 62, pp. 1–16, 2023. https://doi.org/10.1109/tgrs.2023.3342625
[9] A. R. B. Cammerino, M. Ingaramo, and M. Monteleone, "Complementary approaches to planning a restored coastal wetland and assessing the role of agriculture and biodiversity: an applied case study in Southern Italy," *Water*, vol. 16, no. 1, pp. 1–41, 2023. https://doi.org/10.3390/w16010153
[10] W. Sun, D. Chen, Z. Li, S. Li, S. Cheng, X. Niu, Y. Cai, Z. Shi, C. Wu, G. Yang, and X. Yang, "Monitoring wetland plant diversity from space: Progress and perspective," *International Journal of Applied Earth Observation and Geoinformation,* vol. 130, pp. 1–19, 2024. https://doi.org/10.1016/j.jag.2024.103943
[11] K. J. Erratt, F. Nwaishi, T. S. Lee, A. Allison, V. A. Carney, K. Bartlett, and I. F. Creed, "Aquatic Condition Index: optimization of a rapid wetland assessment tool for evaluating urban wetland health," *Urban Ecosystems*, vol. 27, no. 6, pp. 2299–2307, 2024. https://doi.org/10.1007/s11252-024-01596-0
[12] E. A. L. Salas, S. S. Kumaran, R. Bennett, L. P. Willis, and K. Mitchell, "Machine Learning-Based Classification of Small-Sized Wetlands using Sentinel-2 images," *AIMS Geosciences*, vol. 10, no. 1, pp. 62–79, 2024. https://doi.org/10.3934/geosci.2024005
[13] L. Zeng, R. Y. M. Li, and H. Zeng, "Analyzing the Worldwide Wetland Parks Research: A Spectral-Cluster Algorithm Latent Semantic Index approach," *Buildings*, vol. 14, no. 5, pp. 1–28, 2024. https://doi.org/10.3390/buildings14051315
[14] S. Guo, Z. Feng, P. Wang, J. Chang, H. Han, H. Li, C. Chen, and W. Du, "Mapping and classification of the Liaohe Estuary Wetland based on the combination of Object-Oriented and Temporal features," *IEEE Access*, vol. 12, pp. 60496–60512, 2024. https://doi.org/10.1109/access.2024.3389935
[15] S. Helmrich, N. W. T. Quinn, M. W. Beutel, and P. A. O'Day, "Simulation of flow and salinity in a large seasonally managed wetland complex," *Hydrology*, vol. 11, no. 8, pp. 1–16, 2024. https://doi.org/10.3390/hydrology11080117
[16] Z. Xue, Y. Wang, R. Huang, and L. Yao, "Study on Wetland evolution and landscape pattern changes in the Shaanxi section of the Loess Plateau in the past 40 years," *Land*, vol. 13, no. 8, pp. 1–17, 2024. https://doi.org/10.3390/land13081268
[17] J. Zhao, Y. Wang, L. Wang, and T. He, "Analysis of Spatio-Temporal Changes and Driving Factors of Wetland Ecosystem Health based on the AHP-SOM-DPSR Model—A Case Study of Wetlands in the Qin-Mang River," *Sustainability*, vol. 16, no. 13, pp. 1–19, 2024. https://doi.org/10.3390/su16135753
[18] M. Baigaliyeva, Z. Atakhanova, and A. Kairat, "Spatiotemporal variations in urban wetlands in Kazakhstan: a case of the Taldykol Lake system in Astana City," *Sustainability*, vol. 16, no. 16, pp. 1–26, 2024. https://doi.org/10.3390/su16167077
[19] M. Gaglio, M. Lanzoni, A. N. Muresan, U. Schirpke, and G. Castaldelli, "Quantifying intangible values of wetlands as instrument for conservation in the Po delta park (Italy)," *Journal of Environmental Management,* vol. 360, pp. 1–9, 2024. https://doi.org/10.1016/j.jenvman.2024.121227
[20] H. Liu, T. Liao, Y. Wang, X. Qian, X. Liu, C. Li, S. Li, Z. Guan, L. Zhu, X. Zhou, C. Liu, T. Hu, and M. Luo, "Fine-grained wetland classification for national wetland reserves using multi-source remote sensing data and Pixel Information Expert Engine (PIE-Engine)," *GIScience & Remote Sensing,* vol. 60, no. 1, pp. 1–23, 2023. https://doi.org/10.1080/15481603.2023.2286746
[21] S. Rapinel, L. Panhelleux, G. Gayet, R. Vanacker, B. Lemercier, B. Laroche, F. Chambaud, A. Guelmami, and L. Hubert-Moy, "National wetland mapping using remote-sensing-derived environmental variables, archive field data, and artificial intelligence," *Heliyon*, vol. 9, no. 2, pp. 1–18, 2023. https://doi.org/10.1016/j.heliyon.2023.e13482
[22] S. Khan, F. Hossain, T. Pavelsky, G. M. Parkins, M. R. Lane, A. M. Gómez, S. Minocha, P. Das, S. Ghafoor, M. A. Bhuyan, M. N. Haque, P. K. Sarker, P. P. Borua, J. Cretaux, N. Picot, V. Balakrishnan, S. Ahmad, N. Thapa, R. Bhattarai, . . . A. Compin, "Understanding volume estimation uncertainty of lakes and wetlands using satellites and citizen science," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing,* vol. 16, pp. 2386–2401, 2023. https://doi.org/10.1109/jstars.2023.3250354
[23] N. Ma, A. Waegel, M. Hakkarainen, W. W. Braham, L. Glass, and D. Aviv, "Blockchain + IoT sensor network to measure, evaluate, and incentivize personal environmental accounting and efficient energy use in indoor spaces," *Applied Energy*, vol. 332, pp. 1-18, 2023. https://doi.org/10.1016/j.apenergy.2022.120443
[24] J. Hao, R. Sharma, M. B. Fleming, I. K. Kim, D. R. Mishra, S. S. Kim, L. A. Sutter, and L. Ramaswamy, "Toward Low-Cost and Sustainable IoT Systems for Soil Monitoring in Coastal Wetlands," *2023 IEEE 9th International Conference on Collaboration and Internet Computing (CIC),* Atlanta, GA, USA, 01-04 November 2023, pp. 52–61. https://doi.org/10.1109/cic58953.2023.00017
[25] V. Vandhana Devi, and C. K. Akhila, "Resilience to climate change and environmental perturbations – A road map for Chennai city, India," *Materials Today: Proceedings,* vol. 102, pp. 79-87, 2023. https://doi.org/10.1016/j.matpr.2023.03.288
[26] L. Abbad, A. Nacer, H. Abbad, M. Taieb Brahim, and N. Zioui, "A weighted Markov-clustering routing protocol for optimizing energy use in wireless sensor networks," *Egyptian Informatics Journal*, vol. *23*, no. 3, pp. 483-497, 2022. https://doi.org/10.1016/j.eij.2022.05.001
[27] A. A. Addobea, Q. Li, I. A. Obiri, and J. Hou, "Secure multi-factor access control mechanism for pairing blockchains," *Journal of Information Security and Applications*, vol. *74,* pp. 103477, 2023. https://doi.org/10.1016/j.jisa.2023.103477
[28] W. Alhalabi, A. Gaurav, V. Arya, I. F. Zamzami, and R. A. Aboalela, "Machine Learning-Based Distributed Denial of Services (DDoS) Attack Detection in Intelligent Information Systems," *International Journal on Semantic Web and Information Systems*, vol. *19*, no. 1, pp. 1-17, 2023. https://doi.org/10.4018/IJSWIS.327280

[29] R. M. Baazeem, "Cybersecurity: Botnet Threat Detection Across the Seven-Layer Iso-Osi Model Using Machine Learning Techniques," *Computing and Informatics*, *42*(5), pp. 1060–1090, 2023. https://doi.org/10.31577/cai_2023_5_1060
[30] B. Sarhan, and N. Altwaijry, "Insider Threat Detection Using Machine Learning Approach," *Applied Sciences*, vol. *13*, no. 1, pp. 1-19, 2023. https://doi.org/10.3390/app13010259
[31] M. Gazzan, and F. T. Sheldon, "An Enhanced Minimax Loss Function Technique in Generative Adversarial Network for Ransomware Behavior Prediction," *Future Internet*, vol. *15*, no. 10, pp. 1-18, 2023. https://doi.org/10.3390/fi15100318
[32] P. Li, J. Wang, L. Zhao, X. Gao, F. Song, H. Sun, and J. Ma, "Scattering and Eavesdropping in Terahertz Wireless Link by Wavy Surfaces," *IEEE Transactions on Antennas and Propagation*, vol. *71*, no. 4, pp. 3590-3597, 2023. https://doi.org/10.1109/TAP.2023.3241333
[33] M. Nelavalli, and K. Subrahmanyam, "Physical Layer Security in Interference Limited Land Mobile Satellite Communication Systems: Safeguarding Data Transmission," *International Journal of Emerging Research in Engineering, Science, and Management*, vol. *2*, no. 2, pp.23-27, 2023. https://doi.org/10.58482/ijeresm.v2i2.4
[34] L. Pei, S. Ye, L. He, G. Zhao, H. Yuan, X. Ding, S. Pei, X. Li, F. Wang, and A. L. Edward, "Wetland resources, development and protection in China and management recommendations," *Geology in China*, vol. *50*, no. 2, pp. 459-478, 2023. https://doi.org/10.12029/gc20220218001
[35] S. M. Rashed, and A. M. R. Mahjoob, "Solving Time-Cost Trade-off Problem with Resource Constraint Using Fuzzy Mathematical Model," *Journal of Engineering*, vol. *20*, no. 09, pp. 1-25, 2023. https://doi.org/10.31026/j.eng.2014.09.02
[36] D. Said, M. Elloumi, and L. Khoukhi, "Cyber-Attack on P2P Energy Transaction between Connected Electric Vehicles: A False Data Injection Detection Based Machine Learning Model," *IEEE Access*, vol. 10, pp, 63640-63647, 2022. https://doi.org/10.1109/ACCESS.2022.3182689
[37] D. Seo, K. Jung, H. Roh, S. Kim, and S. Oh, "High-Efficiency Resource Allocation Scheme Introducing the Concept of Resource Sharing Paths in Industrial IoT," *IEEE Access*, vol. *11*, pp. 63821-63833, 2023. https://doi.org/10.1109/ACCESS.2023.3284754
[38] J. Wang, W. Yi, M. Yang, J. Ma, S. Zhang, and S. Hao, "Enhance the trust between IoT devices, mobile apps, and the cloud based on blockchain," *Journal of Network and Computer Applications*, vol. 218, pp. 103718, 2023. https://doi.org/10.1016/j.jnca.2023.103718
[39] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Engineering Applications of Artificial Intelligence*, vol. 123, pp. 1-17, 2023. https://doi.org/10.1016/j.engappai.2023.106432
[40] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space Odyssey: An Experimental Software Security Analysis of Satellites," *2023 IEEE Symposium on Security and Privacy (SP),* San Francisco, CA, USA, 21-25 May 2023, pp. 1-19. https://doi.org/10.1109/SP46215.2023.10351029
[41] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," *IEEE Access*, vol. 11, pp. 145869-145896, 2023. https://doi.org/10.1109/ACCESS.2023.3346320
[42] M. A. Ferrag, O. Friha, B. Kantarci, N. Tihanyi, L. Cordeiro, M. Debbah, D. Hamouda, M. Al-Hawawreh, and K. K. R. Choo, "Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses," *IEEE Communications Surveys and Tutorials*, vol. *25*, no. 4, pp. 2654-2713, 2023. https://doi.org/10.1109/COMST.2023.3317242
[43] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT," *Information*, vol. 14, no. 2, pp, 1-26, 2023. https://doi.org/10.3390/info14020129
[44] G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, and I. Adamopoulos, "A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns," *Mesopotamian Journal of Computer Science*, vol. 2024, pp. 71–121, 2024. https://doi.org/10.58496/MJCSC/2024/007
[45] W. Robert, A. Denis, A. Thomas, A. Samuel, S. P. Kabiito, Z. Morish, and G. Ali, "A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2024, pp. 135–169, 2024. https://doi.org/10.58496/MJAIH/2024/016
[46] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 3, pp. 45–91, 2024. doi:https://doi.org/10.52866/ijcsm.2024.05.03.004
[47] G. Ali, and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 20–62, 2024. https://doi.org/10.58496/MJCS/2024/006
[48] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167-185, 2024. https://doi.org/10.1016/j.iotcps.2023.12.003
[49] A. Hamidov, U. Kasymov, N. Allahverdiyeva, and C. Schleyer, "Governance of technological innovations in water and energy use in Uzbekistan," *International Journal of Water Resources Development*, vol. *40*, no. 1, pp. 123-139, 2024. https://doi.org/10.1080/07900627.2022.2062706
[50] H. Liu, N. Lin, H. Zhang, Y. Liu, C. Bai, D. Sun, and J. Feng, "Driving Force Analysis of Natural Wetland in Northeast Plain Based on SSA-XGBoost Model," *Sensors*, vol. *23*, no. 17, pp. 1-24, 2023. https://doi.org/10.3390/s23177513
[51] Y. Xu, D. Li, Q. Li, and S. Xu, "Malware Evasion Attacks Against IoT and Other Devices: An Empirical Study," *Tsinghua Science and Technology*, vol. *29*, no. 1, pp. 127-142, 2024. https://doi.org/10.26599/TST.2023.9010005
[52] M. Özkan-Okay, E. Akin, Ö. Aslan, S. Kosunalp, T. Iliev, I. Stoyanov, and I. Beloev, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," *IEEE Access*, vol. 12, pp. 12229–12256, 2024. https://doi.org/10.1109/access.2024.3355547

[53] A. R. P. Reddy, K. Sumathi, B. Praveena, S. Chaudhary, K. Prathebha, and S. Ramesh, "Construction of Supervised Learning Model for Crop prediction based on Environmental Condition," *2023 IEEE International Conference on Integrated Circuits and Communication Systems, ICICACS 2023,* Raichur, India, 24-25 February 2023, pp. 1-7. https://doi.org/10.1109/ICICACS57338.2023.10099661
[54] H. Attou, M. Mohy-eddine, A. Guezzaz, S. Benkirane, M. Azrour, A. Alabdultif, and N. Almusallam, "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," *Applied Sciences*, vol. *13*, no. 17, pp. 1-19, 2023. https://doi.org/10.3390/app13179588
[55] H. Alamro, W. Mtouaa, S. Aljameel, A. S. Salama, M. A. Hamza, and A. Y. Othman, "Automated Android Malware Detection Using Optimal Ensemble Learning Approach for Cybersecurity," *IEEE Access*, vol. 11, pp. 72509-72517, 2023. https://doi.org/10.1109/ACCESS.2023.3294263
[56] A. El-Ghamry, T. Gaber, K. K. Mohammed, and A. E. Hassanien, "Optimized and Efficient Image-Based IoT Malware Detection Method," *Electronics*, vol. *12*, no. 3, pp. 1-21, 2023. https://doi.org/10.3390/electronics12030708
[57] M. Sewak, S. K. Sahay, and H. Rathore, "Deep Reinforcement Learning in the Advanced Cybersecurity Threat Detection and Protection," *Information Systems Frontiers*, vol. *25*, no. 2, pp. 589–611, 2023. https://doi.org/10.1007/s10796-022-10333-x
[58] Y. Shi, Y. E. Sagduyu, T. Erpek, and M. C. Gursoy, "How to Attack and Defend NextG Radio Access Network Slicing With Reinforcement Learning," *IEEE Open Journal of Vehicular Technology*, vol. *4,* pp. 1-10, 2023. https://doi.org/10.1109/OJVT.2022.3229229
[59] K. M. Kurugama, S. Kazama, Y. Hiraga, and C. Samarasuriya, "A comparative spatial analysis of flood susceptibility mapping using boosting machine learning algorithms in Rathnapura, Sri Lanka," *Journal of Flood Risk Management*, vol. *17*, no. 2, pp. 1-17, 2024. https://doi.org/10.1111/jfr3.12980
[60] L. Xi, D. Miao, M. Li, R. Wang, H. Liu, and X. Huang, "Adaptive-Correlation-Aware Unsupervised Deep Learning for Anomaly Detection in Cyber-Physical Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. *21*, no. 4, pp. pp. 2888-2899, 2024. https://doi.org/10.1109/TDSC.2023.3319701
[61] L. Dash, and A. S. Thampy, "Channel estimation using hybrid optimizer based recurrent neural network long short term memory for MIMO communications in 5G network," *SN Applied Sciences*, vol. *5*, no. 60, pp. 1-15, 2023. https://doi.org/10.1007/s42452-022-05253-z
[62] N. Aldausari, A. Sowmya, N. Marcus, and G. Mohammadi, "Video Generative Adversarial Networks: A Review," *ACM Computing Surveys*, vol. 55, no. 2, pp. 1-25, 2023. https://doi.org/10.1145/3487891
[63] B. Ghojogh, M. Crowley, F. Karray, and A. Ghodsi, "Adversarial Autoencoders," In *Elements of Dimensionality Reduction and Manifold Learning* (pp 577–596). Springer, 2023. https://doi.org/10.1007/978-3-031-10602-6_21
[64] K. Berahmand, F. Daneshfar, E. S. Salehi, Y. Li, and Y. Xu, "Autoencoders and their applications in machine learning: a survey," *Artificial Intelligence Review*, vol. *57*, no. 2, pp. 1-52, 2024. https://doi.org/10.1007/s10462-023-10662-6
[65] N. Duraimutharasan, N. Rao, N. Poongavanam, K. Kanimozhi, and S. Manikandan, "Boosting Cybersecurity Effectiveness through Machine Learning for Proactive Detection and Mitigation of New Threats," *2024 Second International Conference on Advances in Information Technology (ICAIT),* Chikkamagaluru, Karnataka, India, 24-27 July 2024, pp. 1–6. https://doi.org/10.1109/icait61638.2024.10690534
[66] C. M. Fernández, "Is AI used in conservation biology a good environmental justice strategy?," *Daimon*, vol. *90,* 2023. https://doi.org/10.6018/daimon.561551
[67] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms," *Future Internet*, vol. *15*, no. 6, pp. 1-30, 2023. https://doi.org/10.3390/fi15060210
[68] J. O. Ogala, S. Ahmad, I. Shakeel, J. Ahmad, and S. Mehfuz, "Strengthening KMS Security with Advanced Cryptography, Machine Learning, Deep Learning, and IoT Technologies," *SN Computer Science*, vol. *4*, no. 5, 2023. https://doi.org/10.1007/s42979-023-02073-9
[69] L. Yang, Z. Zhang, W. Zhang, T. Zhang, H. Meng, H. Yan, Y. Shen, Z. Li, and X. Ma, "Wetland Park Planning and Management Based on the Valuation of Ecosystem Services: A Case Study of the Tieling Lotus Lake National Wetland Park (LLNWP), China," *International Journal of Environmental Research and Public Health*, vol. *20*, no. 4, pp. 1-26, 2023. https://doi.org/10.3390/ijerph20042939
[70] OpenAI. "*ChatGPT [Large language model],"*. ChatGPT. https://chatgpt.com (accessed January 23, 2025).
[71] P. K. Dutta, S. M. El-kenawy, G. Ali, and K. Dhoska, "An Energy Consumption Monitoring and Control System in Buildings using Internet of Things," *Babylonian Journal of Internet of Things,* vol. 2023, pp. 38–47, 2023. https://doi.org/10.58496/BJIoT/2023/006
[72] M. M. Mijwil, I. Bala, G. Ali, M. Aljanabi, M. Abotaleb, R. Doshi, . . . E.-S. M. El-Kenawy, "Sensing of Type 2 Diabetes Patients Based on Internet of Things Solutions: An Extensive Survey," In K. K. Hiran, R. Doshi, & M. Patel (Eds.), *Modern Technology in Healthcare and Medical Education: Blockchain, IoT, AR, and VR* (pp. 34-46). IGI Global, 2024. doi:10.4018/979-8-3693-5493-3.ch003
[73] A. Sakhri, A. Ahmed, M. Maimour, M. Kherbache, E. Rondeau, and N. Doghmane, "A digital twin-based energy-efficient wireless multimedia sensor network for waterbirds monitoring," *Future Generation Computer Systems*, vol. 155, pp. 146-163, 2024. https://doi.org/10.1016/j.future.2024.02.011
[74] J. Howard, A. E. Sutton-Grier, L. S. Smart, C. C. Lopes, J. Hamilton, J. Kleypas, S. Simpson, J. McGowan, A. Pessarrodona, H. K. Alleway, and E. Landis, "Blue carbon pathways for climate mitigation: Known, emerging and unlikely," *Marine Policy*, vol. *156,* pp. 1-15, 2023. https://doi.org/10.1016/j.marpol.2023.105788
[75] S. Chakraborty, P. H. Mallick, and S. Kundu, "Participatory Rural Appraisal for Assessing Freshwater Wetland Status and Fishery Potential in West Midnapore, West Bengal, India," *Proceedings of the Zoological Society*, vol. *76*, no. 2, pp. 134–145, 2023. https://doi.org/10.1007/s12595-023-00477-2
[76] G. Zare, B. Malekmohammadi, H. Jafari, A. R. Yavari, and A. Nohegar, "Management of socio-ecological wetland systems using mulino decision support system and analytic network process," *International Journal of Environmental Science and Technology*, vol. *19*, no. 4, pp. 2559–2572, 2022. https://doi.org/10.1007/s13762-021-03368-1
[77] Z. Hassan, B. Shahbaz, and F. G. Lopez, "Enhancing Blue/Green Infrastructure for Resilient Urban Environments: Smart Solutions and Nature-Based Strategies," *3rd International Congress on Engineering and Life Science (ICELIS)*, Trabzon, Turkiye, 20-22 September 2023, pp. 1-50. https://doi.org/10.61326/icelis.2023.18

[78] S. L. Chen, H. S. Chou, C. H. Huang, C. Y. Chen, L. Y. Li, C. H. Huang, Y. Y. Chen, J. H. Tang, W. H. Chang, and J. S. Huang, "An Intelligent Water Monitoring IoT System for Ecological Environment and Smart Cities," *Sensors*, vol. *23*, no. 20, pp. 1-16, 2023. https://doi.org/10.3390/s23208540
[79] Krismadinata, A. Sakinah, A. Razak, and W. Purwanto, "Development of An IoT-Based Ecological Aspect Monitoring System for Tor Douronensis Farming," *SSRG International Journal of Electronics and Communication Engineering*, vol. *11*, no. 2, pp. 24-32, 2024. https://doi.org/10.14445/23488549/IJECE-V11I2P103
[80] S. LaFond-Hudson, and B. Sulman, "Modeling strategies and data needs for representing coastal wetland vegetation in land surface models," *New Phytologist*, vol. *238*, no. 3, pp. 938-951, 2023. https://doi.org/10.1111/nph.18760
[81] S. Gopalakrishnan, S. Nejati, S. Sedaghat, K. Gupta, R. K. Mishra, and R. Rahimi, "Electronic-free and low-cost wireless sensor tag for monitoring fish freshness," *Sensors and Actuators B: Chemical*, vol. *381*, pp. 133398, 2023. https://doi.org/10.1016/j.snb.2023.133398
[82] X. Guan, L. Zwaigenbaum, and L. K. Sonnenberg, "Building Capacity for Community Pediatric Autism Diagnosis: A Systemic Review of Physician Training Programs," *Journal of Developmental and Behavioral Pediatrics*, vol. 43, no. 1, pp. 44-54, 2022. https://doi.org/10.1097/DBP.0000000000001042
[83] Y. A. Abid, J. Wu, M. Farhan, and T. Ahmad, "ECMT Framework for Internet of Things: An Integrative Approach Employing In-Memory Attribute Examination and Sophisticated Neural Network Architectures in Conjunction with Hybridized Machine Learning Methodologies," *IEEE Internet of Things Journal*, vol. *11*, no. 4, pp. 5867-5886, 2024. https://doi.org/10.1109/JIOT.2023.3312152
[84] E. M. Brice, M. Halabisky, and A. M. Ray, "Making the leap from ponds to landscapes: Integrating field-based monitoring of amphibians and wetlands with satellite observations," *Ecological Indicators*, vol. *135*, pp. 1-15, 2022. https://doi.org/10.1016/j.ecolind.2022.108559
[85] N. T. K. Dung, B. K. Veettil, D. Q. Bao, and T. Tran, "Environmental management in Ramsar designated wetland areas in Vietnam: studies from U Minh Thuong and Tram Chim national parks (Mekong Delta)," *Environmental Monitoring and Assessment*, vol. *194,* no. 777, 2022. https://doi.org/10.1007/s10661-022-10178-6
[86] L. S. A. Nayak, K. Das, S. Hota, B. J. R. Sahu, and D. A. Mishra, "Implementation of Data Warehouse: An Improved Data-Driven Decision-Making Approach," In: D. Mishra, R. Buyya, P. Mohapatra, S. Patnaik, (eds) *Intelligent and Cloud Computing. Smart Innovation, Systems and Technologies*, (vol. 286). Springer, 2022. https://doi.org/10.1007/978-981-16-9873-6_38
[87] A. T. M. Fisch, L. Bardwell, and I. A. Eckley, "Real time anomaly detection and categorization," *Statistics and Computing*, vol. *32*, no. 55, pp. 1-15, 2022. https://doi.org/10.1007/s11222-022-10112-3
[88] J. Gillespie, T. P. da Costa, X. Cama-Moncunill, T. Cadden, J. Condell, T. Cowderoy, E. Ramsey, F. Murphy, M. Kull, R. Gallagher, and R. Ramanathan, "Real-Time Anomaly Detection in Cold Chain Transportation Using IoT Technology," *Sustainability*, vol. *15*, no. 3, pp. 1-24, 2023. https://doi.org/10.3390/su15032255
[89] N. W. Jeffery, S. J. Lehnert, T. Kess, K. K. S. Layton, B. F. Wringe, and R. R. E. Stanley, "Application of Omics Tools in Designing and Monitoring Marine Protected Areas For a Sustainable Blue Economy," *Frontiers in Genetics*, vol. *13*, pp. 1-10, 2022. https://doi.org/10.3389/fgene.2022.886494
[90] B. M. Yakubu, R. Latif, A. Yakubu, M. I. Khan, and A. I. Magashi, "Rice Chain: secure and traceable rice supply chain framework using blockchain technology," *PeerJ Computer Science*, vol. *8,* pp. 1-24, 2022. https://doi.org/10.7717/PEERJ-CS.801
[91] S. M. Solanki, "Industry 4.0 and Smart Manufacturing: Exploring the integration of advanced technologies in manufacturing," *Revista Review Index Journal of Multidisciplinary*, vol. *3*, no. 2, pp. 36-46, 2023. https://doi.org/10.31305/rrijm2023.v03.n02.005
[92] M. H. Alsharif, A. Jahid, R. Kannadasan, and M. K. Kim, "Unleashing the potential of sixth generation (6G) wireless networks in smart energy grid management: A comprehensive review," *Energy Reports*, vol. *11*, pp. 1376-1398, 2024. https://doi.org/10.1016/j.egyr.2024.01.011
[93] M. A. Ditmer, R. M. Niemiec, G. Wittemyer, and K. R. Crooks, "Socio-ecological drivers of public conservation voting: Restoring gray wolves to Colorado, USA," *Ecological Applications*, vol. *32*, no. 3, pp. 1-10, 2022. https://doi.org/10.1002/eap.2532
[94] A. R. Rissman, A. Fochesatto, E. B. Lowe, Y. Lu, R. M. Hirsch, and R. D. Jackson, "Grassland and managed grazing policy review," *Frontiers in Sustainable Food Systems*, vol. *7*, pp. 1-19, 2023. https://doi.org/10.3389/fsufs.2023.1010441
[95] D. J. Johnson, M. F. Brunette, D. J. Goodman, M. Adams, C. Bryer, J. R. Doherty, V. Flanagan, J. R. Frew, S. Mullins, F. Sheehan, A. Tobar-Santamaria, S. Whitney, and S. Lord, "Promoting community stakeholder engagement in research on treatment for pregnant women with opioid use disorder," *Journal of Comparative Effectiveness Research*, vol. *11*, no. 15, pp. 1085-1094, 2022. https://doi.org/10.2217/cer-2022-0090
[96] K. S. K. Chung, P. Eskerod, A. L. Jepsen, and J. Zhang, "Response strategies for community stakeholder engagement on social media: A case study of a large infrastructure project," *International Journal of Project Management*, vol. *41*, no. 5, pp. 1-13, 2023. https://doi.org/10.1016/j.ijproman.2023.102495
[97] J. Jahangeer, L. Zhang, and Z. Tang, "Evaluating wetland hydrological performance under three different conservation programs in Nebraska, United States, during 2018–2021," *Journal of the American Water Resources Association*, vol. *60*, no. 1, pp. 132-147, 2024. https://doi.org/10.1111/1752-1688.13160
[98] D. J. Mehta, S. Eslamian, and K. Prajapati, "Flood modelling for a data-scare semi-arid region using 1-D hydrodynamic model: a case study of Navsari Region," *Modeling Earth Systems and Environment*, vol. *8*, no. 2, pp. 2675–2685, 2022. https://doi.org/10.1007/s40808-021-01259-5
[99] D. Feng, H. Beck, K. Lawson, and C. Shen, "The suitability of differentiable, physics-informed machine learning hydrologic models for ungauged regions and climate change impact assessment," *Hydrology and Earth System Sciences*, vol. *27*, no. 12, pp. 2357–2373, 2023. https://doi.org/10.5194/hess-27-2357-2023
[100] R. McGeady, R. M. Runya, J. S. G. Dooley, J. A. Howe, C. J. Fox, A. J. Wheeler, G. Summers, A. Callaway, S. Beck, L. S. Brown, G. Dooly, and C. McGonigle, "A review of new and existing non-extractive techniques for monitoring marine protected areas," *Frontiers in Marine Science*, vol. 10, pp. 1-22, 2023. https://doi.org/10.3389/fmars.2023.1126301

[101] M. J. Keyhanpour, S. H. Musavi Jahromi, and H. Ebrahimi, "System dynamics model of sustainable water resources management using the Nexus Water-Food-Energy approach," *Ain Shams Engineering Journal*, vol. *12*, no. 2, pp. 1267-1281, 2021. https://doi.org/10.1016/j.asej.2020.07.029
[102] S. Chen, K. Tamilmani, K. T. Tran, D. Waseem, and V. Weerakkody, "How privacy practices affect customer commitment in the sharing economy: A study of Airbnb through an institutional perspective," *Industrial Marketing Management*, vol. *107*, pp. 161-175, 2022. https://doi.org/10.1016/j.indmarman.2022.08.020
[103] V. S. Narwane, R. D. Raut, S. K. Mangla, M. Dora, and B. E. Narkhede, "Risks to Big Data Analytics and Blockchain Technology Adoption in Supply Chains," *Annals of Operations Research*, vol. *327*, no. 1, pp. 339–374, 2023. https://doi.org/10.1007/s10479-021-04396-3
[104] N. P., Owoh, and M. M. Singh, "Security analysis of mobile crowd sensing applications," *Applied Computing and Informatics*, vol. *18, no.* 1–2, pp. 1-20, 2022. https://doi.org/10.1016/j.aci.2018.10.002
[105] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, and S. A. Bahaj, "Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)," *Electronics*, vol. *11, no.* 3, pp. 1-18, 2022. https://doi.org/10.3390/electronics11030494
[106] U. Islam, A. Muhammad, R. Mansoor, M. S. Hossain, I. Ahmad, E. T. Eldin, J. A. Khan, A. U. Rehman, and M. Shafiq, "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models," *Sustainability*, vol. *14*, no. 14, pp. 1-18, 2022. https://doi.org/10.3390/su14148374
[107] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Sensors*, vol. 22, no. 3, pp. 1-26, 2022. https://doi.org/10.3390/s22031094
[108] R. Khatoun, Cybersecurity in Smart Homes: Architectures, Solutions and Technologies. John Wiley & Son, 2022, pp. 1-304. https://doi.org/10.1002/9781119987451
[109] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications*, vol. 209, pp. 103540, 2023. https://doi.org/10.1016/j.jnca.2022.103540
[110] D. Esenarro, J. Vilchez, M. Adrianzen, V. Raymundo, A. Gómez, and Cobeñas, P. "Management Techniques of Ancestral Hydraulic Systems, Nasca, Peru; Marrakech, Morocco; and Tabriz, Iran in Different Civilizations with Arid Climates," *Water*, vol. *15*, no. 19, pp. 1-24, 2023. https://doi.org/10.3390/w15193407
[111] O. S. Faragallah, A. Afifi, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, F. E. Abd El-Samie, and W. El-Shafai, "Efficient HEVC Integrity Verification Scheme for Multimedia Cybersecurity Applications," *IEEE Access*, vol. *8*, pp. 167069-167089, 2020. https://doi.org/10.1109/ACCESS.2020.3019840
[112] L. Fan, L. He, E. Dong, J. Yang, C. Li, J. Lin, and Z. Wang, "EvoIoT: An evolutionary IoT and non-IoT classification model in open environments," *Computer Networks*, vol. *219*, pp. 109450, 2022. https://doi.org/10.1016/j.comnet.2022.109450
[113] S. A. Bhat, N. F. Huang, I. B. Sofi, and M. Sultan, "Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability," *Agriculture*, vol. 12, no. 1, pp. 1-25, 2022. https://doi.org/10.3390/agriculture12010040
[114] G. Jeon, H. Jin, J.H. Lee, S. Jeon, and J.T. Seo, "IWTW: A Framework for IoWT Cyber Threat Analysis," *Computer Modeling in Engineering & Sciences*, vol. 141, no. 2, pp. 1575-1622, 2024. https://doi.org/10.32604/cmes.2024.053465
[115] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," *IEEE Access*, vol. *9*, pp. 107200-107223, 2021. https://doi.org/10.1109/ACCESS.2021.3101218
[116] Y. Qiao, Q. Lan, Z. Zhou, and C. Ma, "Privacy-preserving credit evaluation system based on blockchain," *Expert Systems with Applications*, vol. *188,* pp. 115989, 2022. https://doi.org/10.1016/j.eswa.2021.115989
[117] A. Qasem, P. Shirani, M. Debbabi, L. Wang, B. Lebel, and B. L. Agba, "Automatic Vulnerability Detection in Embedded Devices and Firmware: Survey and Layered Taxonomies," *ACM Computing Surveys*, vol. *54*, no. 2, pp. 1-42, 2022. https://doi.org/10.1145/3432893
[118] T. J. Mason, M. Krogh, G. C. Popovic, W. Glamore, and D. A. Keith, "Persistent effects of underground longwall coal mining on freshwater wetland hydrology," *Science of the Total Environment*, vol. *772,* pp. 144772, 2021. https://doi.org/10.1016/j.scitotenv.2020.144772
[119] M. Farghali, A. I. Osman, I. M. A. Mohamed, Z. Chen, L. Chen, I. Ihara, P. S. Yap, and D. W. Rooney, "Strategies to save energy in the context of the energy crisis: a review," *Environmental Chemistry Letters*, vol. 21, no. 4, pp. 2003–2039, 2023. https://doi.org/10.1007/s10311-023-01591-5
[120] A. E. Peng DiGiacomo, R. Giannelli, B. Puckett, E. Smith, J. T. Ridge, and J. Davis, "Considerations and trade-offs of UAS-based coastal wetland monitoring in the Southeastern United States," *Frontiers in Remote Sensing*, vol. *3*, pp. 1-20, 2022. https://doi.org/10.3389/frsen.2022.924969
[121] Y. Tan, J. Dai, X. Wu, S. Wu, and J. Zhang, "Characteristics, occurrence and fate of non-point source microplastic pollution in aquatic environments," *Journal of Cleaner Production,* vol. 341, pp. 130766, 2022. https://doi.org/10.1016/j.jclepro.2022.130766
[122] J. P. Donnelly, S. L. King, J. Knetter, J. H. Gammonley, V. J. Dreitz, B. A. Grisham, M. C. Nowak, and D. P. Collins, "Migration efficiency sustains connectivity across agroecological networks supporting sandhill crane migration," *Ecosphere*, vol. *12*, no. 6, pp. 1-22, 2021. https://doi.org/10.1002/ecs2.3543
[123] K. Wright, P. Passalacqua, M. Simard, and C. E. Jones, "Integrating Connectivity Into Hydrodynamic Models: An Automated Open-Source Method to Refine an Unstructured Mesh Using Remote Sensing," *Journal of Advances in Modeling Earth Systems*, vol. *14*, no. 8, pp. 1-23, 2022. https://doi.org/10.1029/2022MS003025
[124] M. Pan, H. Yan, Z. Zhang, and K. Chen, "A Study on the Impact of Big Data Complexity Technostress on Data Management Capabilities," *2023 6th International Conference on Artificial Intelligence and Big Data, ICAIBD,* Chengdu, China, 26-29 May 2023. https://doi.org/10.1109/ICAIBD57115.2023.10206411

[125] T. Yang, R. Sun, R. S. Rathore, and I. Baig, "Enhancing cybersecurity and privacy protection for Cloud Computing-Assisted Vehicular Network of Autonomous Electric Vehicles: Applications of Machine Learning," *World Electric Vehicle Journal,* vol. 16, no. 1, pp. 1–32, 2024. https://doi.org/10.3390/wevj16010014
[126] G. Ali, M. M. Mijwil, I. Adamopoulos, and J. Ayad, "Leveraging the Internet of Things, Remote Sensing, and Artificial Intelligence for Sustainable Forest Management," *Babylonian Journal of Internet of Things*, vol. 2025, pp. 1–65, 2025. https://doi.org/10.58496/BJIoT/2025/001
[127] M. M. Mijwil, G. Ali, and E. Sadıkoğlu, "The Evolving Role of Artificial Intelligence in the Future of Distance Learning: Exploring the Next Frontier," *Mesopotamian Journal of Computer Science*, vol. 2023, pp. 98–105, 2023. https://doi.org/10.58496/mjcsc/2023/012
[128] G. Ali, M. M. Mijwil, I. Adamopoulos, B. A. Buruga, M. Gök, and M. Sallam, "Harnessing the Potential of Artificial Intelligence in Managing Viral Hepatitis," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 128–163, 2024. https://doi.org/10.58496/MJBD/2024/010
[129] M. M. Mijwil, O. Adelaja, A. Badr, G. Ali, B. A. Buruga, and P. Pudasaini, "Innovative Livestock: A Survey of Artificial Intelligence Techniques in Livestock Farming Management," *Wasit Journal of Computer and Mathematics Science*, vol. 2(4), pp. 99–106, 2023. https://doi.org/10.31185/wjcms.206
[130] H. Meziane, and N. Ouerdi, "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems," *Scientific Reports*, vol. 13, no. 1, pp. 1–31, 2023. https://doi.org/10.1038/s41598-023-46640-9
[131] B. Bokolo, R. Jinad, and Q. Liu, "A Comparison Study to Detect Malware using Deep Learning and Machine learning Techniques," *2023 IEEE 6th International Conference on Big Data and Artificial Intelligence (BDAI),* Jiaxing, China, 07-09 July 2023, PP. 1–6. https://doi.org/10.1109/bdai59165.2023.10256957
[132] A. Setiyaji, K. Ramli, Z. Y. Hidayatulloh, and G. B. Dharmawan, "A technique utilizing Machine Learning and Convolutional Neural Networks (CNN) for the identification of SQL Injection Attacks," *2024 4th International Conference of Science and Information Technology in Smart Administration (ICSINTESA),* Balikpapan, Indonesia, 12-12 July 2024, pp. 1–6. https://doi.org/10.1109/icsintesa62455.2024.10748116
[133] R. Bukhowah, A. Aljughaiman, and M. M. H. Rahman, "Detection of DOS attacks for IoT in Information-Centric Networks using Machine Learning: Opportunities, challenges, and future research directions," *Electronics*, vol. 13, no. 6, pp. 1–25, 2024. https://doi.org/10.3390/electronics13061031
[134] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," *Scientific Reports*, vol. 15, no. 1, pp. 1–22, 2025. https://doi.org/10.1038/s41598-025-85248-z
[135] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," *Cluster Computing*, vol. 27, no. 7, pp. 9065–9089, 2024. https://doi.org/10.1007/s10586-024-04509-0
[136] H. A. Alamri, V. Thayananthan, and J. Yazdani, "Machine Learning for Securing SDN based 5G Network," *International Journal of Computer Applications*, vol. *174*, no. 14, pp. 9-16, 2021. https://doi.org/10.5120/ijca2021921027
[137] E. El-Shafeiy, W. M. Elsayed, H. Elwahsh, M. Alsabaan, M. I. Ibrahem, and G. F. Elhady, "Deep Complex Gated Recurrent Networks-Based IoT Network intrusion detection Systems," *Sensors*, vol. 24, no. 18, pp. 1–22, 2024. https://doi.org/10.3390/s24185933
[138] D. Thakur, J. K. Saini, and S. Srinivasan, "DeepThink IOT: The strength of deep learning in Internet of Things," *Artificial Intelligence Review*, vol. 56, no. 12, pp. 14663–14730, 2023. https://doi.org/10.1007/s10462-023-10513-4
[139] S. Gaba, I. Budhiraja, V. Kumar, S. Martha, J. Khurmi, A. Singh, K. K. Singh, S. S. Askar, and M. Abouhawwash, "A systematic analysis of enhancing cyber security using deep learning for cyber physical systems," *IEEE Access*, vol. 12, pp. 6017–6035, 2024. https://doi.org/10.1109/access.2023.3349022
[140] Q. A. Al-Haija, and A. Droos, "A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT)," *Expert Systems*, vol. 42, no. 2, pp. 1–46, 2024. https://doi.org/10.1111/exsy.13726
[141] T. Al-Shurbaji, M. Anbar, S. Manickam, I. H. Hasbullah, N. ALfriehate, B. A. Alabsi, A. R. Alzighaibi, and H. Hashim, "Deep Learning-Based Intrusion Detection System for Detecting IoT botnet Attacks: A review," IEEE Access, pp. 1–32, 2025. https://doi.org/10.1109/access.2025.3526711
[142] T. Rehman, N. Tariq, F. A. Khan, and S. U. Rehman, "FFL-IDS: a FOG-Enabled Federated Learning-Based Intrusion Detection System to counter jamming and spoofing attacks for the industrial internet of things," *Sensors*, vol. 25, no. 1, pp. 1–34, 2024. https://doi.org/10.3390/s25010010
[143] D. Arnold, M. Gromov, and J. Saniie, "Network Traffic Visualization Coupled with Convolutional Neural Networks for Enhanced IoT Botnet Detection," *IEEE Access*, vol. 12, pp. 73547–73560, 2024. https://doi.org/10.1109/access.2024.3404270
[144] N. K. Sah, M. Kolli, K. P. Dharmaraj, and H. Vishwas, "Comparative Deep Learning approach for intrusion detection," *2024 13th International Conference on Computing Communication and Networking Technologies (ICCCNT),* Kamand, India, 24-28 June 2024, pp. 1–6. https://doi.org/10.1109/icccnt61001.2024.10724847
[145] S. Yaras, and M. Dener, "IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm," *Electronics*, vol. 13, no. 6, pp. 1-28, 2024. https://doi.org/10.3390/electronics13061053
[146] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, and R. Canal, "Deep-Learning Based Detection for Cyber-Attacks in IoT networks: a Distributed Attack Detection framework," *Journal of Network and Systems Management*, vol. 31, no. 2, pp. 1–24, 2023. https://doi.org/10.1007/s10922-023-09722-7
[147] N. Imtiaz, A. Wahid, S. Z. Ul Abideen, M. Muhammad Kamal, N. Sehito, S. Khan, B. S. Virdee, L. Kouhalvandi, and M. Alibakhshikenari, "A Deep Learning-Based Approach for the Detection of Various Internet of Things Intrusion Attacks Through Optical Networks," *Photonics*, 1vol. 2, no.1), pp. 1-39, 2025. https://doi.org/10.3390/photonics12010035
[148] S. Chowdhury, R. Gill, H. S. Pokhariya, and A. Shrivastava, "A machine learning approach for adversarial attack detection and mitigation in cybersecurity," *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS),* Coimbatore, India, 14-15 March 2024, pp. 2650–2654. https://doi.org/10.1109/icaccs60874.2024.10717164

[149] A. Deshmukh, and K. Ravulakollu, "An efficient CNN-Based Intrusion Detection System for IoT: Use case towards Cybersecurity," *Technologies*, vol. 12, no. 10, pp. 1–21, 2024. https://doi.org/10.3390/technologies12100203
[150] B. Taşcı, "Deep-Learning-Based approach for IoT attack and malware detection," *Applied Sciences,* vol. 14. No. 18, pp. 1–21, 2024. https://doi.org/10.3390/app14188505
[151] F. L. Becerra-Suarez, V. A. Tuesta-Monteza, H. I. Mejia-Cabrera, and J. Arcila-Diaz, "Performance evaluation of deep learning models for classifying cybersecurity attacks in IoT networks," *Informatics*, vol. 11, no. 2, pp. 1–13, 2024. https://doi.org/10.3390/informatics11020032
[152] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports,* vol. 14, no. 1, pp. 1–19, 2024. https://doi.org/10.1038/s41598-024-62861-y
[153] J. A. Parra-Jiménez, S. A. Gutiérrez-Betancur, and J. W. Branch-Bedoya, "A Method Based on Deep Learning for the Detection and Characterization of Cybersecurity Incidents in Internet of Things Devices," *2024 IEEE Colombian Conference on Communications and Computing (COLCOM),* Barranquilla, Colombia, 21-23 August 2024, pp. 1–6. https://doi.org/10.1109/colcom62950.2024.10720315
[154] S. Szymoniak, J. Piątkowski, and M. Kurkowski, "Defense and Security Mechanisms in the Internet of Things: A review," *Applied Sciences,* vol. 15, no. 2, pp. 1–36, 2025. https://doi.org/10.3390/app15020499
[155] E. Dritsas, and M. Trigka, "Machine Learning in Information and Communications Technology: a survey," *Information*, vol. 16, no. 1, pp. 1–26, 2025. https://doi.org/10.3390/info16010008
[156] S. Ness, V. Eswarakrishnan, H. Sridharan, V. Shinde, N. V. P. Janapareddy, and V. Dhanawat, "Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques," *IEEE Access*, pp. 1–18, 2025. https://doi.org/10.1109/access.2025.3526988
[157] A. G. Ayad, M. M. El-Gayar, N. A. Hikal, and N. A. Sakr, "Efficient Real-Time anomaly detection in IoT networks using One-Class autoencoder and deep neural network," *Electronics*, vol. 14, no. 1, pp. 1–25, 2024. https://doi.org/10.3390/electronics14010104
[158] J. Simon, N. Kapileswar, R. Vani, N. M. Reddy, D. Moulali, and A. R. N. Reddy, "Enhanced Network Anomaly Detection Using Autoencoders: A Deep Learning Approach for Proactive Cybersecurity," *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI),* Coimbatore, India, 28-30 August 2024, pp. 90–96. https://doi.org/10.1109/icoici62503.2024.10696845
[159] T. Rajendran, N. M. Imtiaz, K. Jagadeesh, and B. Sampathkumar, "Cybersecurity Threat Detection Using Deep Learning and Anomaly Detection Techniques," *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS),* Chikkaballapur, India, 18-19 April 2024, pp. 1–7. https://doi.org/10.1109/ickecs61492.2024.10617347
[160] M. S. Mohammed, and H. A. Talib, "Using Machine Learning Algorithms in Intrusion Detection Systems: A review," *Tikrit Journal of Pure Science*, vol. 29, no. 3, pp. 63–74, 2024. https://doi.org/10.25130/tjps.v29i3.1553
[161] M. Kolhar, and S. M. Aldossary, "A Deep Learning Approach for Securing IoT Infrastructure with Emphasis on Smart Vertical Networks," *Designs,* vol. 7, no. 6, pp. 1–17, 2023. https://doi.org/10.3390/designs7060139
[162] U. Ahmed, M. Nazir, A. Sarwar, T. Ali, E. M. Aggoune, T. Shahzad, and M. A. Khan, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports,* vol. 15, no. 1, pp. 1–33, 2025. https://doi.org/10.1038/s41598-025-85866-7
[163] E. V. N. Jyothi, M. Kranthi, S. Sailaja, U. Sesadri, S. N. Koka, and P. C. S. Reddy, "An Adaptive Intrusion Detection System in Industrial Internet of Things(IIoT) using Deep Learning," *2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS),* Dehradun, India, 26-27 April 2024, pp. 1–6. https://doi.org/10.1109/istems60181.2024.10560245
[164] C. Du, Y. Guo, and Y. Zhang, "A Deep Learning-Based Intrusion Detection Model Integrating Convolutional Neural Network and Vision Transformer for Network Traffic Attack in the Internet of Things," *Electronics*, vol. 13, no. 14, pp. 1-15, 2024. https://doi.org/10.3390/electronics13142685
[165] M. Maaz, G. Ahmed, A. S. Al-Shamayleh, A. Akhunzada, S. Siddiqui, and A. H. Al-Ghushami, "Empowering IoT resilience: hybrid deep learning techniques for enhanced security," *IEEE Access,* vol. 12, pp. 180597–180618, 2024. https://doi.org/10.1109/access.2024.3482005
[166] F. Al-Quayed, Z. Ahmad, and M. Humayun, "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0," *IEEE Access*, vol. 12, pp. 34800–34819, 2024. https://doi.org/10.1109/access.2024.3372187
[167] M. Udurume, V. Shakhov, and I. Koo, "Comparative Evaluation of Network-Based Intrusion Detection: Deep Learning vs Traditional Machine Learning Approach," *2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN),* Budapest, Hungary, 02-05 July 2024, pp. 520–525. https://doi.org/10.1109/icufn61752.2024.10625037
[168] G. Kumar, P. Gupta, G. K. Yadav, R. Verma, J. P. Bhati, and V. S. Bhakuni, "Evaluating the Effectiveness of Deep Learning Models in Network Intrusion Detection," *2024 International Conference on Cybernation and Computation (CYBERCOM),* Dehradun, India, 15-16 November 2024, pp. 766–771. https://doi.org/10.1109/cybercom63683.2024.10803243
[169] H. R. Sayegh, W. Dong, and A. M. Al-Madani, "Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data," *Applied Sciences,* vol. 14, no. 2, pp. 1–20, 2024. https://doi.org/10.3390/app14020479
[170] B. Cui, Y. Chai, Z. Yang, and K. Li, "Intrusion Detection in IoT Using Deep Residual Networks with Attention Mechanisms," *Future Internet,* vol. 16, no. 7, pp. 1–15, 2024. https://doi.org/10.3390/fi16070255
[171] M. S. Ataa, E. E. Sanad, and R. A. El-Khoribi, "Intrusion detection in software defined network using deep learning approaches," *Scientific Reports,* vol. 14, no. 1, pp. 1–15, 2024. https://doi.org/10.1038/s41598-024-79001-1
[172] V. Kantharaju, H. Suresh, M. Niranjanamurthy, S. I. Ansarullah, F. Amin, and A. Alabrah, "Machine learning based intrusion detection framework for detecting security attacks in internet of things," *Scientific Reports,* vol. 14, no. 1, pp. 1–10, 2024. https://doi.org/10.1038/s41598-024-81535-3
[173] V. Kandasamy, and A. A. Roseline, "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks," *Scientific Reports,* vol. 15, no. 1, pp. 1–26, 2025. https://doi.org/10.1038/s41598-025-85547-5

[174] T. Mahmud, M. A. H. Prince, M. H. Ali, M. S. Hossain, and K. Andersson, "Enhancing Cybersecurity: Hybrid deep learning approaches to smishing attack detection," *Systems*, vol. 12, no. 11, pp. 1–21, 2024. https://doi.org/10.3390/systems12110490
[175] B. B. Gupta, A. Gaurav, V. Arya, R. W. Attar, S. Bansal, A. Alhomoud, and K. T. Chui, "Advanced BERT and CNN-Based computational model for phishing detection in enterprise systems," *Computer Modeling in Engineering & Sciences,* vol. 141, no. 3, pp. 2165-2183, 2024. https://doi.org/10.32604/cmes.2024.056473
[176] M. Taha, H. D. A. Jabar, and W. Mohammed, "A Machine Learning Algorithms for Detecting Phishing Websites: A Comparative study," *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 3, pp. 275–286, 2024. https://doi.org/10.52866/ijcsm.2024.05.03.015
[177] O. K. Sahingoz, E. BUBEr, and E. Kugu, "DEPHIDES: Deep Learning based Phishing Detection System," *IEEE Access,* vol. 12, pp. 8052–8070, 2024. https://doi.org/10.1109/access.2024.3352629
[178] M. Patil, N. Shivsharan, Y. Naik, H. Yeram, and A. Gawade, "Enhancing Cybersecurity: A Comprehensive Analysis of Machine Learning Techniques in Detecting and Preventing Phishing Attacks with a Focus on Xgboost Algorithm," *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS),* Gurugram, India, 03-04 May 2024, pp. 01–06. https://doi.org/10.1109/iscs61804.2024.10581237
[179] M. S. Akter, H. Shahriar, S. I. Ahamed, K. D. Gupta, M. Rahman, A. Mohamed, M. Rahman, A. Rahman, and F. Wu, "Case Study-Based Approach of Quantum Machine Learning in Cybersecurity: Quantum Support Vector Machine for malware classification and protection," *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC),* Torino, Italy, 26-30 June 2023, pp. 1057–1063. https://doi.org/10.1109/compsac57700.2023.00161
[180] N. Attila, A. Szilvia, H. Anikó, F. Beatrix, and R. Zoltán, "Machine Learning Used in Cyber Security," *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI),* Timisoara, Romania, 23-25 May 2024, pp. 000297–000302. https://doi.org/10.1109/saci60582.2024.10619896
[181] A. A. Almazroi, and N. Ayub, "Deep learning hybridization for improved malware detection in smart Internet of Things," *Scientific Reports,* vol. 14, no. 1, pp. 1–18, 2024. https://doi.org/10.1038/s41598-024-57864-8
[182] A. E. Hariri, M. Mouiti, and M. Lazaar, "Real-time ransomware process detection using an advanced hybrid approach with machine learning within IoT Ecosystems," *Engineering Research Express,* vol. 7, no. 1, pp. 1–24, 2025. https://doi.org/10.1088/2631-8695/ada3b3
[183] M. R. Jeebodh, and N. Baliyan, "IoT malware detection using deep learning," *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT),* Kamand, India, 24-28 June 2024, pp. 1–6. https://doi.org/10.1109/icccnt61001.2024.10724403
[184] N. Charoenwong, S. Kosolsombat, and C. Ratanavilisagul, "Classification Attack on IoT Devices with Machine Learning," *2024 IEEE 9th International Conference on Computational Intelligence and Applications (ICCIA),* Haikou, China, 09-11 August 2024, pp. 11–17. https://doi.org/10.1109/iccia62557.2024.10719134
[185] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, "A deep learning methodology for predicting cybersecurity attacks on the internet of things," *Information*, vol. 14, no. 10, pp. 1–19, 2023. https://doi.org/10.3390/info14100550
[186] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for detecting DOS attacks in IoT networks based on machine learning algorithms," *Sensors*, vol. 24, no. 2, pp. 1–30, 2024. https://doi.org/10.3390/s24020713
[187] M. Ragab, S. M. Alshammari, L. A. Maghrabi, D. Alsalman, T. Althaqafi, and A. A. Al-Ghamdi, "Robust DDoS Attack Detection Using Piecewise Harris Hawks Optimizer with Deep Learning for a Secure Internet of Things Environment," *Mathematics*, vol. 11, no. 21, pp. 1-18, 2023. https://doi.org/10.3390/math11214448
[188] H. A. Sakr, M. M. Fouda, A. F. Ashour, A. Abdelhafeez, M. I. El-Afifi, and M. R. Abdellah, "Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems," *Egyptian Informatics Journal,* vol. 28, pp. 1–22, 2024. https://doi.org/10.1016/j.eij.2024.100540
[189] A. A. Alshdadi, A. A. Almazroi, N. Ayub, M. D. Lytras, E. Alsolami, and F. S. Alsubaei, "Big Data-Driven Deep Learning ensembler for DDOS attack detection," *Future Internet*, vol. 16, no. 12, pp. 1–26, 2024. https://doi.org/10.3390/fi16120458
[190] A. Almadhor, A. Altalbe, I. Bouazzi, A. A. Hejaili, and N. Kryvinska, "Strengthening network DDOS attack detection in heterogeneous IoT environment with federated XAI learning approach," *Scientific Reports,* vol. 14, no. 1, pp. 1–16, 2024. https://doi.org/10.1038/s41598-024-76016-6
[191] A. Berqia, H. Bouijij, A. Merimi, and A. Ouaggane, "Detecting DDoS Attacks using Machine Learning in IoT Environment," *2024 International Conference on Intelligent Systems and Computer Vision (ISCV),* Fez, Morocco, 08-10 May 2024, PP. 1–8. https://doi.org/10.1109/iscv60512.2024.10620122
[192] İ. Avcı, and M. Koca, "Predicting DDOS attacks using machine learning algorithms in building management systems," *Electronics*, vol. 12, no. 19, pp. 1–13, 2023. https://doi.org/10.3390/electronics12194142
[193] D. Sridevi, L. Kannagi, G. Vivekanandan, and S. Revathi, "Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques," *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI),* Greater Noida, India, 23-25 November 2023, pp. 871–875. https://doi.org/10.1109/iccsai59793.2023.10421133
[194] K. Selvaraj, and M. M. Singh, "APT Attack Detection Using Packet Flow and Optimized Ensemble Machine Learning with Low Time Complexity," *2024 IEEE Symposium on Wireless Technology & Applications (ISWTA),* Kuala Lumpur, Malaysia, 20-21 July 2024, pp. 229–234. https://doi.org/10.1109/iswta62130.2024.10652055
[195] N. Mohamed, "Artificial Intelligence in Cybersecurity: A Review of solutions for APT-Exploited Vulnerabilities," *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT),* Kamand, India, 24-28 June 2024, pp. 1–7. https://doi.org/10.1109/icccnt61001.2024.10724084
[196] R. Jain, and N. Nihalani, "Botnet Detection in Distributed Network Using Machine Learning- A Detailed Review," *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE),* Gautam Buddha Nagar, India, 09-11 May 2024, pp. 888–895. https://doi.org/10.1109/ic3se62002.2024.10593476
[197] N. Mohamed, "Botnet Detection: A review of machine learning and AI strategies," *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT),* Kamand, India, 24-28 June 2024, pp. 1–6. https://doi.org/10.1109/icccnt61001.2024.10724496

[198] A. A. Wardana, G. Kołaczek, A. Warzyński, and P. Sukarno, “Ensemble averaging deep neural network for botnet detection in heterogeneous Internet of Things devices,” *Scientific Reports,* vol. 14, no. 1, pp. 1–18, 2024. https://doi.org/10.1038/s41598-024-54438-6
[199] M. Saied, S. Guirguis, and M. Madbouly, “A comparative analysis of using ensemble trees for botnet detection and classification in IoT,” *Scientific Reports*, vol. 13, no. 1, pp. 1–15, 2023. https://doi.org/10.1038/s41598-023-48681-6
[200] J. R. Tadhani, V. Vekariya, V. Sorathiya, S. Alshathri, and W. El-Shafai, “Securing web applications against XSS and SQLi attacks using a novel deep learning approach,” *Scientific Reports*, vol. 14, no. 1, pp. 1–17, 2024. https://doi.org/10.1038/s41598-023-48845-4
[201] R. Kumar, and S. Yadav, "ML-Driven Cyberattack Prevention in Wetland IoT Networks," *Journal of Cybersecurity in Environmental IoT Systems,* vol. 14, no. 1, pp. 77-88, 2025.
[202] P. Reddy, and S. Raj, "Predictive Analytics for Wetland Ecosystem Monitoring and Security," *Environmental Systems Security Journal,* vol. 7, no. 2, pp. 154-168, 2025.
[203] S. Mahamud, and M. Alam, "An IoT-based Smart Wetland Monitoring System with Machine Learning for Environmental Security," *Environmental Monitoring and Protection Journal*, vol. 45, no. 3, pp. 302-318, 2023.
[204] R. Sharma, et al. "Deep Learning for Real-Time Intrusion Detection in Wetland IoT Networks," *Journal of Cybersecurity and IoT*, vol. 39, no. 5, pp. 450-464, 2024.
[205] N. Ansar, M. S. Ansari, M. Sharique, A. Khatoon, M. A. Malik, and M. M. Siddiqui, “A Cutting-Edge deep learning method for enhancing IoT security,” *arXiv (Cornell University),* pp. 1–15, 2024. https://doi.org/10.48550/arxiv.2406.12400
[206] N. Patel, et al. “AI-Based Anomaly Detection for Secure Wetland IoT Systems," *Journal of Environmental Security and AI,* vol. 12, no. 1, pp. 98-113, 2023.
[207] L. Wu, and X. Zhang, “Deep Learning for Securing Communication in Wetland IoT Networks," *International Journal of IoT Security,* vol. 18, no. 2, pp. 85-97, 2023.
[208] M. Hamidouche, E. Popko, and B. Ouni, “Enhancing IoT Security via Automatic Network Traffic Analysis: The Transition from Machine Learning to Deep Learning,” *arXiv (Cornell University),* pp. 1–8, 2023. https://doi.org/10.48550/arxiv.2312.00034
[209] A. Khan, et al. “Deep Learning for Enhancing Cybersecurity of Wetland IoT Devices," *Journal of Secure Computing,* vol. 33, no. 3, pp. 215-227, 2024.
[210] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, “Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends,” *Sensors*, vol. 24, no. 6, pp. 1–32, 2024. https://doi.org/10.3390/s24061968
[211] X. Zhang, and Y. Liu, “Federated Learning for Privacy-Preserving Wetland IoT Systems,” *International Journal of Environmental Data Science,* vol. 10, no. 2, pp. 152-168, 2023.
[212] Yuan, S., and Wu, X. “Deep learning for insider threat detection: Review, challenges and opportunities,” *Computers and Security*, vol. 104, pp. 102221, 2021. https://doi.org/10.1016/j.cose.2021.102221
[213] L. Blöbaum, L. Torello Pianale, L. Olsson, and A. Grünberger, “Quantifying microbial robustness in dynamic environments using microfluidic single-cell cultivation,” *Microbial Cell Factories*, vol. *23*, no. 1, pp. 1-20, 2024. https://doi.org/10.1186/s12934-024-02318-z
[214] E. Irshad, and A. Basit Siddiqui, “Cyber threat attribution using unstructured reports in cyber threat intelligence,” *Egyptian Informatics Journal*, vol. *24*, no. 1, pp. 43-59, 2023. https://doi.org/10.1016/j.eij.2022.11.001
[215] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, “Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey,” *IEEE Access*, vol. *10,* pp. 121173-121192, 2022. https://doi.org/10.1109/ACCESS.2022.3220622
[216] J. A. Abraham, and V. R. Bindu, “Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review,” *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation, ICAECA 2021*, Coimbatore, India, 08-09 October 2021. https://doi.org/10.1109/ICAECA52838.2021.9675595
[217] T. Saba, K. Haseeb, A. A. Shah, A. Rehman, U. Tariq, and Z. Mehmood, “A Machine-Learning-Based Approach for Autonomous IoT Security,” *IT Professional*, vol. *23*, no. 3, pp. 69-75, 2021. https://doi.org/10.1109/MITP.2020.3031358
[218] A. L. Guillou, S. Niculescu, and C. Schmullius, “Machine and deep learning methods for detection and mapping of coastal wetlands of Crozon Peninsula (Brittany, France) used metric and sub-metric spatial resolution,” *Proceedings of SPIE, the International Society for Optical Engineering, 2023, Earth Resources and Environmental Remote Sensing/GIS Applications XIV,* Amsterdam, Netherlands, 19 October 2023, pp. 1–21. https://doi.org/10.1117/12.2678006
[219] M. A. Günen, “Performance Comparison of Deep Learning and Machine Learning Methods in Determining Wetland Water Areas Using EuroSAT Dataset,” *Environmental Science and Pollution Research,* vol. 28, no. 44, pp. 62556–62571, 2022. https://doi.org/10.1007/s11356-021-17177-z
[220] V. Verma, K. S. Vutukuru, S. S. Divvela, and S. S. Sirigineedi, “Internet of things and machine learning application for a remotely operated Wetland siphon system during hurricanes,” In *Advances in geographical and environmental sciences* (pp. 443–462). Springer, 2022. https://doi.org/10.1007/978-981-16-6573-8_21
[221] G. F. Gemechu, X. Rui, and H. Lu, “Wetland Change Mapping Using Machine Learning Algorithms, and Their Link with Climate Variation and Economic Growth: A Case Study of Guangling County, China,” *Sustainability*, vol. 14, no. 1, pp. 1–25, 2022. https://doi.org/10.3390/su14010439
[222] I. H. Sarker, “Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective,” *SN Computer Science*, vol. *2*, no. 154, 2021. https://doi.org/10.1007/s42979-021-00535-6
[223] D. Dasgupta, Z. Akhtar, and S. Sen, “Machine learning in cybersecurity: a comprehensive survey,” *Journal of Defense Modeling and Simulation*, vol. *19*, no. 1, pp. 57-106, 2022. https://doi.org/10.1177/1548512920951275
[224] J. Vynikal, J. Müllerová, and J. Pacina, “Deep learning approaches for delineating wetlands on historical topographic maps,” *Transactions in GIS,* vol. 28, no. 5, pp. 1400–1411, 2024. https://doi.org/10.1111/tgis.13193
[225] S. R. Mamidi, “Deep learning applications in cloud Security: Challenges and opportunities,” *Journal of Artificial Intelligence General Science (JAIGS),* vol. 4, no. 1, pp. 310–318, 2024. https://doi.org/10.60087/jaigs.v4i1.165

[226] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of IoT security challenges and its solutions using artificial intelligence," *Brain Sciences,* vol. 13, no. 4, pp. 1-30, 2023. https://doi.org/10.3390/brainsci13040683
[227] G. Gök, O. Salor, and M. C. Taplamacıoğlu, "Transient event classification using pmu data with deep learning techniques and synthetically supported training-set," *IET Generation, Transmission and Distribution*, vol. *17*, no. 6, pp. 1287-1297, 2023. https://doi.org/10.1049/gtd2.12734
[228] G. Andresini, A. Appice, F. P. Caforio, D. Malerba, and G. Vessio, "ROULETTE: A neural attention multi-output model for explainable Network Intrusion Detection," *Expert Systems with Applications*, vol. *201*, pp. 117144, 2022. https://doi.org/10.1016/j.eswa.2022.117144
[229] P. Kühn, D. N. Relke, and C. Reuter, "Common vulnerability scoring system prediction based on open source intelligence information sources," *Computers and Security*, vol. *131*, pp. 103286, 2023. https://doi.org/10.1016/j.cose.2023.103286
[230] Y. I. Alzoubi, A. Mishra, and A. E. Topcu, "Research trends in deep learning and machine learning for cloud computing security," *Artificial Intelligence Review,* vol. 57, no. 5, pp. 1–43, 2024. https://doi.org/10.1007/s10462-024-10776-5
[231] K. Boikanyo, A. M. Zungeru, B. Sigweni, A. Yahya, and C. Lebekwe, "Remote patient monitoring systems: Applications, architecture, and challenges," *Scientific African*, vol. 20, pp. 1-28, 2023. https://doi.org/10.1016/j.sciaf.2023.e01638