http://dx.doi.org/10.14500/aro.12365

Navigating Cyber Threats: The Role of Machine Learning and Deep Learning in Fifth-Generation Internet of Things Security

Umed H. Jader†, Reben Kurda and Sara R. Muhamad

Department of Information System Engineering, Technical College of Computer and Informatic Engineering, Erbil Polytechnic University, Erbil, Kurdistan Region – F.R. Iraq

***Abstract*—The high-speed development of Fifth Generation technologies announces a new era for the internet of things (IoT), distinguished by high-rate connectivity, speed, and low latency. However, this advancement also opens doors to major security challenges and expands the attack surface. Existing general IoT surveys do not systematically analyze Fifth Generation-enabled IoT concerns, which creates a clear need for a focused synthesis of machine learning and deep learning (DL) defenses tailored to Fifth Generation-IoT constraints and threat models. To address this gap, this survey conducts a preferred reporting items for systematic reviews and meta-analyses-guided analysis of recent studies published in the past 5 years, extracting methodologies, results, datasets, metrics, tools, and reported limitations to answer explicit research questions about which approaches work, under which conditions, and with what deployment implications for Fifth Generation IoT threat detection and mitigation. The results show that DL families and hybrid deep models dominate intrusion, anomaly, and malicious traffic detection, while research overemphasizes denial-of-service attacks relative to Replay, Ransomware, Sybil, Man-in-the-Middle, and Phishing attacks. The recommendations, which come from comparative evidence across datasets, attack categories, and model performance limitations, emphasize the need for more diverse and realistic Fifth Generation IoT datasets as well as for understudied learning paradigms, such as continual learning, federated learning, meta-learning, and self-supervised learning. These insights highlight clear research directions toward adaptive, privacy-preserving, and generalizable intrusion detection in Fifth Generation-IoT systems.**

***Index Terms*—5G, Attacks, Deep learning, Internet of things, Machine learning.**

I. Introduction

The integration of Fifth Generation (5G) and Internet of Things (IoT) together forms a mutual relationship that builds on the strengths of both to establish further connected and intelligent worlds. Advanced high reliability, low latency, and extensive connectivity in 5G are considerably important for the diverse and high demanding needs of different IoT applications (Chettri and Bera, 2020, Ahad, et al., 2020). Such a fusion deploys IoT devices easily in diverse environments, such as urban and remote regions, preparing for flexible and scalable connectivity solutions. However, all this rapid growth in connected devices also introduces many different security vulnerabilities, and IoT networks are considered the main target for various cyber-attacks, such as Man-in-the-Middle (MitM), denial of service (DoS), and botnet attacks (Alfaw and Al-Omary, 2022, Prasad and Bharathi, 2023, Wazid, et al., 2021). According to GSMA Intelligence, the number of global IoT connections is expected to exceed 38 billion by 2030, while cellular IoT connections will surpass 7 billion (Gsma, 2023; Ericsson, 2025). The IoT devices market is projected to grow from $70 billion in 2024 to $181 billion by 2030, representing an annual growth rate above 16% (GrandViewResearch, 2025b). Despite this exponential rise, the attack surface of IoT and 5G systems is also expanding rapidly, with global reports estimating that 5G-related security breaches could cost industries over 27% billion annually by 2030 (GrandViewResearch, 2025a).

In recent years, the use of machine learning (ML) and deep learning (DL) has been greatly increased to develop various new forms of security by researchers to fight against different cyber-attacks. These methods can be used to enhance the efficiency of detection and mitigating cyber-attacks using efficient data analysis and identification of various data patterns. Some very recent studies have revealed the performance of hybrid feature selection with DL-based architectures that have shown excellent performance in detecting cyber-attacks in IoT networks with very high accuracy (Kim, Kim and Kim, 2022b; Lv, Singh and Li, 2021; Bharati and Podder, 2022).

A closer look at the literature reveals that most existing surveys focus on either 5G or IoT security separately, rarely examining their joint vulnerabilities, ML/DL solutions, datasets, and performance trends in an integrated way. Some studies are outdated (before 2021) or lack a systematic methodology, while others overlook comparative analyses of

ARO-The Scientific Journal of Koya University
Vol. XIV, No. 1 (2026), Article ID: ARO.12365. 17 pages
DOI: 10.14500/aro.12365
Received: 20 June 2025; Accepted: 04 December 2025
Regular review paper; Published: 05 February 2026
†Corresponding author's e-mail: omid.jader@epu.edu.iq

datasets and learning approaches. Therefore, a comprehensive and up-to-date review is needed to consolidate recent progress and identify gaps in 5G-enabled IoT attack detection using ML/DL methods. Table I compares this study with the related works.

Furthermore, to address these deficiencies, this work provides a systematic literature review guided by the Preferred Reporting Items for Sstematic reviews and Meta-Analyses (PRISMA) framework. Our review contributes by:

1. Providing a structured analysis of recent ML/DL-based approaches for 5G-enabled IoT security
2. Highlighting dominant attack categories, such as DDoS and underexplored threats, such as Ransomware, Sybil, and MitM
3. Identifying research gaps in datasets, evaluation metrics, and model generalization
4. Suggesting advanced learning paradigms, including continual learning, reinforcement learning, graph neural networks, meta learning, and self-supervised learning, for future adaptive and privacy-aware intrusion detection.

To make sure our review is thorough and can be easily replicated, we framed a set of key research questions:

1. What are the primary security threats, vulnerabilities, and attack methods targeting 5G-enabled IoT systems?
2. Which DL and ML algorithms, including hybrid models, have been applied to detect and counter these attacks, and how well do they perform?
3. What are the datasets and their impact on the real-world deployment?
4. What challenges remain, and what promising directions should future research take to develop adaptive and privacy-focused intrusion detection for 5G-IoT environments?

II. Methodology

This survey aims at the comprehensive review of the literature related to the role of ML and DL in 5G-enabled IoT networks against cyber-attacks. It is worth noting that this study adheres to the PRISMA framework to ensure transparency and structural process in the paper selections.

A. Search Strategy

A systematic exploration is conducted across five reputable scientific databases, such as IEEE Xplore, Science Direct, Google Scholar, Link Springer, and PubMed. Papers published between January 1, 2020, and December 31, 2024, are searched to capture recent advancements in ML/DL approaches for attack detection in 5G-enabled IoT networks. Search strings combined Boolean operators: (“5G” OR “5G-enabled”) AND (“IoT” OR “Internet of Things”) AND (“machine learning” OR “ML” OR “deep learning” OR “DL” OR “artificial intelligence” OR “AI”) AND (“security” OR “cybersecurity” OR “threat detection” OR “intrusion detection” OR “anomaly detection” OR “attack mitigation”).

B. Inclusion and Exclusion

In the paper selection process, the criteria to include papers are:

1. Papers published in peer-reviewed journals or conferences based on the aforementioned date range
2. Focus on ML/DL-based attack detection or mitigation within 5G-IoT systems
3. Papers providing methodology, dataset, and evaluation metrics.

Furthermore, the excluded criteria are:

1. Non-English or non-peer-reviewed papers
2. Articles focusing solely on hardware, physical-layer security, or theoretical modeling without ML/DL implementation
3. Inaccessible full texts or duplicates.

C. Screening and Eligibility Process

The PRISMA flow chart (Fig. 1) depicts the selection steps:

1. Identification: 2885 records are initially retrieved (IEEE Xplore = 526, ScienceDirect = 996, SpringerLink = 631, Google Scholar = 697, PubMed = 35).
2. Screening: After duplicate removal (n = 874), the remaining studies underwent title and abstract screening to exclude papers that are not relevant to the topic, not written in English, not peer-reviewed, not full-text availablity, or not ML/DL-based methodologies. Only studies that aligned with the review’s focus are retained for full-text assessment.
3. Eligibility: 83 full-text papers are assessed; 26 are excluded for the reason of not focusing on 5G-IoT (they are IoT or 5G individually), 30 studies for the reason of not attack-related as well.
4. Included: 27 studies were included for qualitative and quantitative synthesis.

TABLE I
Comparison of The Related Works

References	Scope	ML/DL coverage	Dataset discussion	Key limitation
(Chettri and Bera, 2020)	5G-IoT architecture	Traditional ML only	None	No 5G security, dataset, or metric analysis
(Shafique, et al., 2020)	5G-IoT challenges and trends	Partial	None	No 5G-IoT security, dataset, or metric analysis
(Ahad, et al., 2020)	IoT applications	No DL coverage	None	No 5G-IoT security, dataset, or metric analysis
(Wazid, et al., 2021)	5G-IoT security	None	None	No dataset or metric analysis
(Hasan, et al., 2022)	5G-IoT security	None	None	No ML/DL, dataset, or metric analysis
(Rafique, et al., 2024)	IoT anomaly	Yes	Yes	No 5G context
This survey	5G-IoT security	Comprehensive ML/DL	Extensive	Bridges all previous gaps

IoT: Internet of things, ML: Machine learning, DL: Deep learning

http://dx.doi.org/10.14500/aro.12365

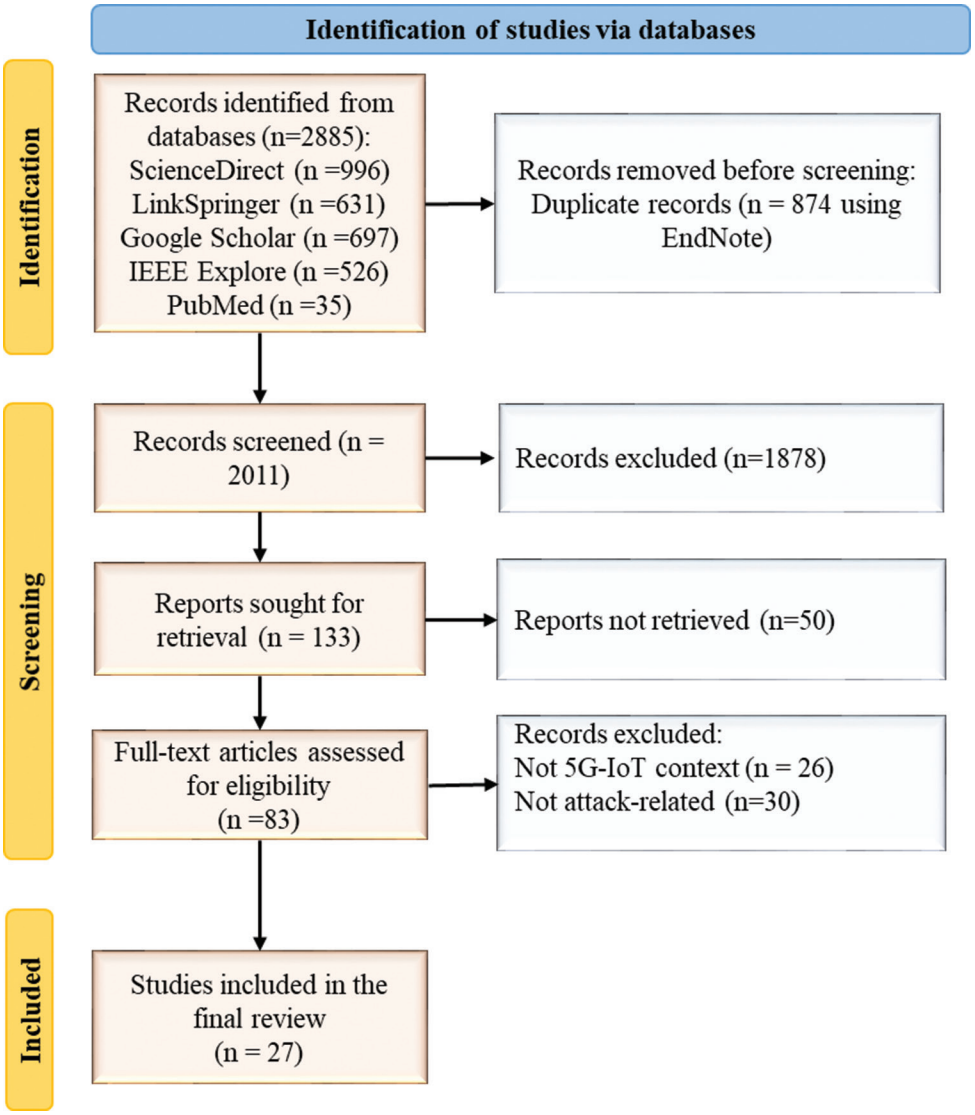

Fig. 1. Preferred reporting items for systematic reviews and meta-analyses 2020 flow diagram for the review process.

D. Data Extraction and Analysis

For data extraction, a structured framework is applied to all the included papers, focusing on the study goal, targeted attack type, methodology (DL/ML algorithms), datasets, performance metrics, and simulation tools. The data synthesis and analysis process, a thematic analysis is executed to underline the current limitations, attack categorization, dominant models, necessity of diverse and real-world datasets, challenges, and future suggestions.

III. Security Issues In 5G-Enabled IoT Systems

5G-IoT communications security refers to the set of protocols and countermeasures that are designed to ensure the security of the composite network of infrastructure, devices, and sensors that operate in the domain of 5G technology. One of the key security concerns in 5G technology-dependent IoT systems is the increased attack surface due to the sheer volume of connected devices (Alfaw and Al-Omary, 2022). The convergence of technologies, such as software-defined network (SDN), NVF, and cloud computing, complicates the security landscape that is used. While the technologies improve network efficiency and flexibility, they, at the same time, provide new entry points for vulnerabilities to be used by malicious attackers (Alfaw and Al-Omary, 2022, Prasad and Bharathi, 2023). Moreover, the real-time nature of newer technologies, such as smart warehouses and the industrial IoT makes them vulnerable to cyber-attacks and data breaches, resulting in disruption of services and potential loss of data (Das, et al., 2023). Due to their hugeness in terms of size and complexity, the integration of strong and effective security mechanisms for risk mitigation and protection of sensitive information being conveyed in the 5G-enabled IoT systems is crucial. In this section, a comprehensive list of attacks is presented, and their effects on communications within the 5G-based IoT system are described.

A. DoS and Distributed DoS

The most serious threats in the network security, which have recently attracted so much attention from the security

and threat community, are DoS and DDoS attacks. The aim of these attacks is to disable services by flooding the vulnerable target system with an unrealistic surge of fake requests. These attacks cripple network resources and prevent legitimate users from accessing them (Kumari and Jain, 2024). Within a 5G system, a large number of IoT devices interconnected with one another can be exploited to launch massive DDoS attacks (e.g., Transmission Control Protocol [TCP] resynchronization, TCP flooding, TCP synchronization flooding, and User Datagram Protocol [UDP] flooding) causing severe service degradation (Valadares, et al., 2023).

B. Eavesdropping

Eavesdropping (also called Reconnaissance, Sniffing, or Information gathering) attacks involve illegally intercepting and listening to a private communication, and they represent a serious threat to data confidentiality. Specifically, these attacks can be harmful in the involved systems in which sensitive information is communicated, for example, financial transactions or personal communications (Valadares, et al., 2023, Bahalul Haque, et al., 2023). In a 5G-IoT scenario, the combination of massive device connectivity and low-latency, high-throughput links enlarges the attack surface and enables real-time traffic interception and relay, making eavesdropping attempts more feasible and potentially more damaging.

C. MitM Attack

MitM attacks are a form of cyber-attack in which an attacker surreptitiously intercepts and may modify the communication between two parties who think they are communicating directly with each other. Such attacks can result in significant data breaches and unauthorized access to confidential information, as well as possibly modifying and even not sending data to its destination (Valadares, et al., 2023, Aoueileyine, et al., 2024). Within the 5G-IoT system, the massive connectivity and low latency features increase vulnerabilities in the attack surface, causing MitM attacks to be more active in a compromised network (Bjerre, Blomsterberg and Andersen, 2022).

D. Jamming

Jamming is a technique that disrupts communications in wireless-based networks by sending noise signals on the same frequency band (Tarannum, Usha and Ahammed, 2024). Jamming attacks, as a subset of DoS attacks, pose a significant threat to 5G and IoT environments by intentionally disrupting communication between devices through the injection of spurious packets into the wireless channel, which disrupts the normal operation of devices within the network. Furthermore, it can be unintentional due to the use of the same signals by the neighbor nodes (Zahra, Bostanci and Soyturk, 2023).

E. Injection

Injection attacks are a class of application-layer vulnerabilities where untrusted input is interpreted as code or commands by back-end engines (e.g., databases, shells, or XML parsers), allowing adversaries to manipulate queries or execute commands. In 5G-enabled IoT systems, injections manifest as structural query language injections against cloud/gateway backends, command/firmware injection on resource-constrained devices, and client-side injections, such as cross-site scripting (XSS). Injection is a logic problem at the application/firmware layer (Noman and Abu-Sharkh, 2023, Mazhar, et al., 2023).

F. Replay

This type of attack takes place when an attacker captures legitimate communications between devices in an unknown interval of time and then replays or resends those messages to trick the system (Taher, et al., 2023, Barshan, et al., 2024, Naha, et al., 2023, Xiao, et al., 2024). For example, in a 5G-IoT, an attacker intercepts the communication between a smart door lock and a user's smartphone. By capturing the signal that unlocks the door, the attacker can replay this signal at a later time to gain unauthorized access.

G. Ransomware

One of the most severe threats to 5G-IoT systems is ransomware. A ransomware attack is a type of malware that encrypts the victim's data or locks them out of their systems until a ransom is paid to the hacker for decryption or re-access to the systems. In recent years, the widespread increase of ransomware has emerged as a major cybersecurity threat, inflicting severe financial, reputational, and operational damage on individuals, organizations, and governments (Razaulla, et al., 2023, Ispahany, et al., 2024).

H. Sybil

In this technique of security threat, the attackers create several fake identities or nodes within the network systems, and these nodes seem, such as legal devices and sensors participating in the communication, data exchange, and decision-making operations. Once a sybil attack is launched in 5G-IoT environments, such as smart vehicular systems, it can easily facilitate other attacks, such as DoS (Rakhi and Shobha, 2023, Tulay and Koksal, 2024).

I. Pilot Contamination Attack

Pilot contamination attacks are a significant security threat in 5G-enabled IoT systems, particularly in massive MIMO networks. In this method, non-orthogonal pilot sequences are used to detect active users and estimate channel specifications. Then a hacker transmits the same pilot signals at the same time as legal users, thereby contaminating the channel estimation process at the base station (BSs) (Wang, et al., 2021; Taleb, et al., 2022).

J. Zero-day

A 0-day attack is discovered as a new cyber-attack that is not yet known to both the public and the cyber community, which is why it's called 0-day. Attackers use the systems' vulnerabilities or use innovative tactics to bypass existing security measures and access to their chosen targets before

a patch or solution is provided by developers (Guo, 2023; Korba, Boualouache and Ghamri-Doudane, 2024). 80% of security breaches are driven by 0-day attacks, with each attack costing an average of 1.2 million dollars. This highlights the significant threat posed by 0-day vulnerabilities (Sameera and Shashi, 2020).

K. Spoofing Attack

It refers to a malicious actor trying to be a legitimating device to deceive a system, obtain data accessibility, and alter system function through the fake identity of an authorized user, device, or network service. There are several types of this attack, Media Access Control spoofing (Rachakonda, Siddula and Sathya, 2024), Address Resolution Protocol spoofing (Patel and Shah, 2024), Global Positioning System (GPS) spoofing (Jung, et al., 2024), Email spoofing (Maroofi, et al., 2021), Domain Name System (DNS) spoofing (Trabelsi, et al., 2024), and Channel-based spoofing (Li, et al., 2021). In 5G networks, especially those utilizing millimeter Wave technology, physical-layer security has emerged as a promising countermeasure (Bahalul Haque, et al., 2023).

L. Phishing Attack

Phishing is a cyber-attack where individuals are tricked into giving up their personal and corporate information. It is the easiest form of cyberattacks for hackers to implement, and it is one of the simplest traps for victims to fall into. The anti-phishing working group (APWG) reported nearly five million phishing attacks in 2023, marking it as a record-breaking year (APWG, 2024). This tactic enables hackers to obtain the necessary details to access their targets' personal and corporate accounts (Dhanavanthini and Chakkravarthy, 2023; Malik, et al., 2023).

M. Botnet Attacks

The botnet is a network-based attack that breaches multiple computers into "bots" to launch malicious activities, such as DDoS, identify theft, DNS spoofing, spamming, and phishing. In a botnet attack, a malicious actor, "Bot master," tries to get unauthorized access to a single device and then implements botnet malware to take control of the device without alienating its legitimate users. After that, establish a connection of bots with a command and control (C&C) center owned by the attacker, and the bots remain ready to launch malicious activities under the instructions of C&C (Habibi, Chemmakha and Lazaar, 2023). There are many types of botnets, such as Mirai and Bashlite (Alshehri, et al., 2024), as well as Sality, ZeroAccess, Nullsoft Scriptable Install System (NSIS), Mozi, and Gnutella as peer-to-peer botnets (Xing, Shu and Kang, 2023).

While specific attacks exploit distinct technical weaknesses, their broader consequences for 5G-IoT networks tend to converge and are greatly intensified by fundamental aspects of 5G technology. Features, such as ultra-reliable low-latency communication, massive device connectivity, network slicing, and NFV, make these systems not only more scalable and adaptable but also more vulnerable to both rapid attack spread and resource exhaustion. For instance, disruptions, such as DoS or jamming can interrupt time-sensitive communications or overwhelm virtual network elements, while adversarial actions, such as spoofing, botnet infiltration, or forged data can move quickly between different network slices, compromising data integrity, resource allocation, and secure service isolation. As a result, the collective impact of these attacks manifests as service degradation, data confidentiality breaches, and instability of virtualized infrastructures, posing severe challenges to maintaining secure, resilient, and high-performance 5G-IoT operations. Fig. 2 illustrates the possibility of each attack occurring based on the main 5G-IoT layers, which are the physical or device, network, and application layers.

IV. ML and DL Solutions in 5G-Enabled IOT Networks

In recent years, several DL/ML-based frameworks and models have been proposed by researchers to protect and secure systems against cyber threats and attacks in various applications of 5G-enabled IoT networks. In this survey, the recent developments are reviewed, and their specifications, in terms of aim, methodology, and results, are described.

A trustworthy security solution using explainable artificial intelligence (XAI) is deployed by (Goyal, et al., 2024) to enhance security for unmanned aerial vehicles (UAVs) on 5G networks. They develop an obstacle detection and avoidance model with XAI techniques, then integrate it with a Q-learning agent to improve decision-making in cases that are critical for safety. The trained Q-learning agent, equipped with the XAI model, is tested in both simulated environments and controlled real-world settings. Their results indicate that the proposed method can locate attacking nodes at least 98.4% of the time.

(Viana, et al., 2024) propose a DL framework named deep attention recognition using two important observable parameters, signal-to-interference-plus-noise ratio and reference signal received power, to detect possible jamming attacks in 5G UAVs under different conditions, including line-of-sight (LoS) and non-LoS (NLoS). The use of the Attention and long short-term memory (LSTM) layers into the convolutional neural network (CNN) structure enables a synergistic process, in which both directions are simultaneously trained on the sets of data, which are the results of the simulation of multiple scenarios involving channel conditions and attacker actions. Additional mechanisms used in the study, Time-Series Augmentation and Majority Voting Algorithm, are used to enhance the accuracy of classification with low possibilities of false alarms. The findings demonstrate that the presented framework, including an Attention layer, is better at performing attack detection, as it is more accurate by 4% in the case of LoS and approximately 3% in a situation where the distance is short and in NLoS.

A model named enhanced dwarf mongoose optimization algorithm with DL based attack detection (EDMOA-DLAD) is proposed by (Alsariera, et al., 2024) for attack detection

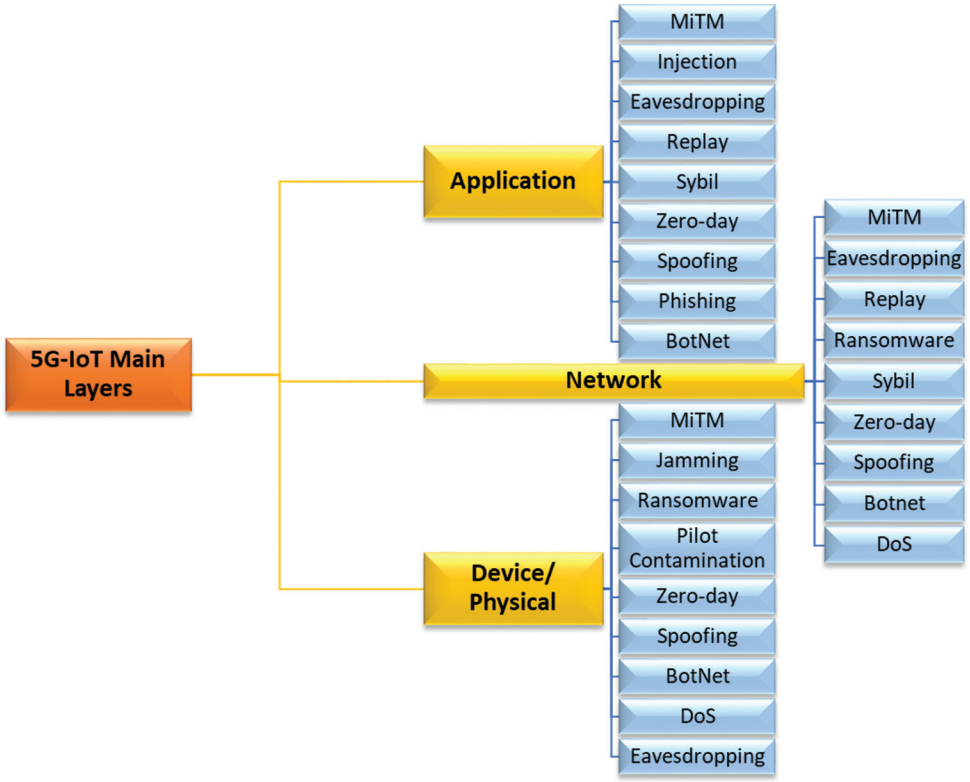

Fig. 2. Attacks related to each 5G-internet of things layer.

in drone networks. The paper consists of three sections, in the first of which, a part of feature selection, the Dwarf Mongoose optimization algorithm was used, and the second section was a deep variational autoencoder to classify attacks, and the third section was a beetle antenna search algorithm to optimize the hyperparameters of the deep model. The model is tested by simulation on benchmark data. The obtained findings indicate that the suggested EDMOA-DLAD approach has a very good performance of 99.79% on identifying and categorizing attacks, which is superior to other comparison classification methods, such as support vector machine (SVM), and decision tree (DT). (Viana, et al., 2022) proposes a hybrid convolutional attention-based DL model that leverages the LSTM attention mechanism to enhance the detection of attacks in UAV networks operating under 5G conditions, utilizing Orthogonal Frequency Division Multiplexing receivers on Clustered Delay Line. The research addresses complex situations where legitimate ground users are present alongside attackers whose locations are unknown. Their approach focuses on two key parameters existing in 5G UAV connections, the Signal to Interference plus Noise Ratio and the Received Signal Strength Indicator. The total accuracy of the developed algorithm was about 76% in all the used scenarios and it is able to detect all attackers in an environment with 20 legitimated users. The minimum time required to detect an attack is 100 ms, with a significant attack power that matches the power level used by the legitimate UAV. In addition, the algorithm can identify moving attackers from a distance of up to 500 m.

Dang, et al., 2022 develop a deep ensemble learning method to detect GPS spoofing attacks, which pose a significant issue to UAVs in mobile networks. The detection process of GPS spoofing is designed as a non-linear optimization problem. Moments, quartiles, and probability distributions are employed as statistical analysis methods to analyze the path loss properties that exist between BSs and UAVs in a cellular network. Furthermore, a multi-access edge computing (MEC) framework is proposed to enhance GPS spoofing detection using deep ensemble learning methodologies. In the MEC servers, all multi-layer perceptrons (MLPs) make independent predictions to forecast the percentage of GPS spoofing for places advertised by every BS. The edge cloud server utilizes six ML models for determining whether a GPS location is spoofed or not to aggregate individual predictions from the MLPs. The findings of the research prove that the suggested deep ensemble learning strategy efficiently detects GPS spoofing attacks with a 97% accuracy for 2 BSs and is resilient to environmental changes while minimizing the computational load on UAVs, especially in the 5G and IoT scenarios.

An adaptive information security system is constructed by (Jiang, et al., 2022) for 5G-enabled smart grids. The artificial neural network (ANN) is employed to train a model that determines the most appropriate data transmission path in the 5G power communication network. Then, they integrate a zero-trust architecture, with case-based learning algorithms being used to evaluate the trustworthiness of access entities continuously. The results prove that the security framework put forth significantly improves 5G-IoT security in smart grid systems. It effectively deters different types of attacks, including unauthorized access and data manipulation. The framework also proves to have enhanced efficiency

of data transmission, thus proving to be a good method of implementing enhanced security into existing smart grid systems.

A method is presented by (Martinez Quintero, et al., 2023) to detect and identify replay attacks on vehicles, specifically targeting Remote Keyless Entry systems by utilizing software-defined radio (SDR) technology. They propose a method that integrates SVM as ML and Visual Geometry Group 16 (VGG16) as CNN-based DL techniques to improve the accuracy of signal classification and transmitter identification. Realtek-SDR device was used to capture key-fog signals and the GNU Radio software to process the received signals, as well as HackRF-SDR utilize to create fake signals by retransmitting the original signals. The mentioned models are designed and then trained through the Kaggle platform. The results demonstrate that the proposed method significantly improves the identification and classification of radio frequency signals, showcasing an increase in accuracy of approximately 3–6% compared to previous studies.

(Sousa, Magaia and Silva, 2023) Focus on developing an IDS based on ML algorithms for flood attack detection in 5G-enabled Internet of Vehicles systems. Four distinct datasets, each representing different scenarios with different sender, receiver, and attacker vehicles, are generated through simulation using network simulator 3. Initially, simple ML techniques, specifically DT, were employed to establish baseline results, then methods, such as random forest (RF) and MLP, were explored. For better generalization, each algorithm was trained on one dataset with several varying parameters and tested on the other three datasets. It was found that while complex models, such as MLP, do not perform well; RF provides consistent results comparable to DT, with the added benefit of stability across different test sets.

The security vulnerabilities in automated vehicles operating on advanced 5G networks are addressed by (Korba, et al., 2023). They propose federated-based learning integrated with a deep Autoencoder intrusion detection system for identifying 0-day attacks and preserving user privacy and communication load. The relevant features are extracted from packet headers of the network traffic created by the participating automated vehicles using Trananalyzer and then utilized to train the deep Autoencoder model. By employing federated learning (FL), the system allows multiple automated vehicles to collaboratively train the detection model. The training is orchestrated by a MEC server, which aggregates the updates from the participating vehicles. The performance of the proposed model surpasses other centralized algorithms, such as DT. (Alferaidi, et al., 2022) introduce a distributed hybrid CNN-LSTM model for vehicular IoT networks operating over 5G connectivity. It is implemented on the Apache Spark framework to handle large-scale streaming data; the pipeline exploited CNN layers for spatial feature abstraction and LSTM modules for sequential temporal learning. The model is evaluated on both the NSL-KDD and UNSW-NB15 datasets, the model achieves 99.7% accuracy for attack classification while reducing training and testing times significantly compared with standalone CNN or LSTM baselines.

Furthermore, another study by (Verma, et al., 2024) proposes a dual Autoencoder model based on FL to enhance the detection of 0-day attacks in 5G-enabled Industrial IoT. The framework operates by having individual industrial units, equipped with various intelligent devices, collect and store data locally. Each unit has been used to train the two independent AE models, each associated with a one-class SVM classifier, one for normal traffic and another for attack traffic. Then, these models share their parameters with a central server via 5G network capabilities, allowing for the creation of global models that can effectively identify anomalies without sharing sensitive raw data. The results surpass the other traditional ML-based models' accuracy, detection rate, and F1-score, besides memory usage and computing time are evaluated as the server-side scalability.

Anand, et al., 2021 develop a CNN model to detect malware attacks in 5G-IoT healthcare applications, aiming to improve cybersecurity issues in the healthcare services that utilize 5G and IoT technologies. The model uses three layers and provides significant results with 99% accuracy compared to the state-of-the-art methods. As well as, the 5G-SIID model is designed by (Sadhwani, et al., 2024) as a hybrid and scalable IDS against DDoS attacks in 5G-IoT networks. Both CNN and LSTM methods are integrated in the model. They performed the F1-score feature selection method to extract the most significant attributes from the dataset, ultimately narrowing it down to 10 key features from an initial set of 52. The proposed technique outperforms the other 7 state-of-the-art ML and DL classifiers with an accuracy of 99.99 and 99.98% for binary and multiclass classification scenarios, respectively.

Another study proposes a distributed malicious traffic detection scheme exploiting transformer-based models to construct a resilient framework for malicious traffic detection in 5G and beyond IoT networks. In this scheme, transformer models are trained locally at edge servers as detection points and share their model parameters with the main server for parameter aggregation to create a general model utilizing FL. The approach is collaborative between different edge servers and a central cloud server to improve the detection capabilities in unknown IoT devices. The proposed collaborative scheme achieves up to 99.2% average detection accuracy and F1-score, which exceeds the state-of-the-art non-collaborative approaches (Luo, et al., 2024).

The research of (Alqura'n, et al., 2024) investigates the improvement of detection in ANNs and promotes the use of a forward-looking mechanism to detect XSS attacks in IoT networks, especially those hosted in 5G networks. A bilayered neural network (BLNN) and a trilayered neural network (TLNN) are integrated into the proposed model. The mutual information and recursive feature elimination methods of feature selection have been used to optimize this model to have a smaller computational budget while delivering results close at hand in terms of accuracy. Findings indicate that the detection accuracy of BLNN is approximately 99.84% and for TLNN is around 99.79%. (Ferrag, Debbah and Al-

Hawawreh, 2023) offers a model that incorporates generative adversarial networks (GAN) and transformer-based architectures for the enhancement of cyber threat detection in 5G beyond IoT networks. The GAN part of the model, which consists of a generator and a discriminator, is charged with the responsibility of creating artificial data that is similar to the pre-existing dataset of the IoT. In addition, the generated data are analyzed with the Transformer model with the help of an attention mechanism that puts more weight to the significance of various components of the input data. The study outcomes reveal that the proposed security model, which utilizes the Transformer, can identify IoT attacks with an impressive accuracy of 95%.

(Naik, et al., 2024) Combine attention-based techniques with LSTM for forecasting network traffic and optimizing resources. As well as for attack detection, an Autoencoder mechanism is developed to address security and management issues in 5G-enabled IoT networks. This research emphasizes on error analysis and performance indicators statistically, which proves the efficiency of the proposed models in predicting the behavior of networks and detecting attacks. The results show the performance of the proposed Autoencoder attack detection with respect to the existing ML models, and the model is able to learn non-linear data, and it is not sensitive to feature scaling.

In the study of El-Sofany, et al., 2024, a ML-based security model relying on NFV and SDN technologies is proposed, which automatically handles the security challenges faced by IoT devices. Multiple attack classes, such as Ack, UDP, Junk, and UDP plain from the balanced BoTNet-IoT-L01 dataset and U2R, DDoS, Probe, and R2L from NSL-KDD, are used to train and evaluate ML classifiers. The model's performance is tested with the UNSW_NB15 dataset using the Synthetic Minority Oversampling Technique to overcome data imbalance. The findings demonstrate that the proposed ML-based security model achieved an impressive accuracy rate of 99.9%, demonstrating its effectiveness in detecting and responding to various types of attacks. The model also shows a high detection average and a perfect area under the curve score of 1.

An Autoencoder model is presented by (Yadav, et al., 2022) to detect network intrusions like DoS attacks in 5G-enabled IoT environments. They emphasize new datasets and preprocessing techniques like encoding and normalization approaches to accurately train the proposed model. The efficacy of the proposed model is compared with existing state-of-the-art ML-based and DL-based intrusion detection systems to exhibit detection rate and accuracy improvements. (Kim, Kim and Kim, 2022b) proposes a study investigating various successful feature selection techniques, that is, feature importance evaluation, recursive feature elimination, cross-validation, and sequential feature selection, with the aim of identifying IoT DDoS attacks in the 5G core network. The authors utilize the Kitsune dataset for collecting GTP-U packets and employ different ML algorithms, that is, k-nearest neighbors (KNN), DT, RF, and stacking ensemble, for data classification. The study firmly establishes that the selection of features has the potential to improve the effectiveness along with the accuracy of classification models. In addition, to detect IoT botnet traffic in a 5G Core network path, (Kim, Kim and Kim, 2022a) evaluate several ML algorithms. The authors utilize binary classification to differentiate between benign and malicious traffic and multiclass classification to identify different types of traffic labeled in the dataset. All 5G Core GTP packets are analyzed with Open5GCore Rel.6, which is an open-source project for 5G mobile core networks, to set up the GTP tunneling testbed. Four algorithms are tested for anomaly detection: KNN, SVM, RF, and stacking. For the evaluation of the ML performance, IP + GTP packets were used in tandem for IoT botnet detection in a 5GC environment with the aim of having performance comparable to that of a wired network. The results show that the stacking algorithm achieved 99.924% accuracy in binary classification and 97.5% accuracy in multiclass classification.

Cheng, Hong and Hung, 2022 propose a MEC architecture to improve security by detecting and mitigating threats for artificial intelligence of things devices within 5G networks, particularly focusing on fake BS attacks. Generally, gathering real-time data from both legitimate and fake BSs is achieved by utilizing mobile and machine inspectors that monitor signaling messages, particularly focusing on the Attach Reject messages, which are critical for identifying fake BS activities. Both the malicious detection and the fake BS attack detection have been trained with the integrated inspectors to the MEC, utilizing the received information. When the real-time signals are greater than the determined threshold from the trained dataset, the MEC detects the signal as an attack and sends a notification to the subscribed users in a timely manner. The results present 94.8% and 91% as accuracy for malicious and fake BS attack detection, respectively, and also that the integration of AI and MEC can significantly strengthen the detection and mitigation of security threats in 5G-enabled systems, so that communication between IoT devices and users is more secure.

A pilot contamination attack detection model in grant-free mMTC networks is proposed by (Wang, et al., 2021) utilizing a single-hidden-layer multiple-measurement Siamese network. This model is trained using channel virtual representation samples, which are derived from legitimate IoT users. In addition, to enhance the training process, GANs are incorporated to generate additional dissimilar sample pairs. This allows the model to learn effectively without requiring extensive labeling of each device in the network and accurately detect the pilot contamination attack. The findings demonstrate that the detection accuracy can reach as high as 99% when utilizing 128 antennas at the BS or access point. Even in less favorable conditions, such as a Signal-to-Noise Ratio (SNR) of 0 dB, the detection accuracy remains above 95%. Fan, et al., 2020 propose IoTDefender to enhance intrusion detection in 5G-IoT environments utilizing a federated transfer learning technique. The architecture consists of several MEC platforms (4 clients) and a central security cloud (server). Each MEC platform trains its own model using local private datasets, while the cloud aggregates knowledge from all clients without accessing their data directly. A modified deep neural network (DNN) is utilized

and trained at both sides. The model performance surpasses the traditional algorithms such as KNN, adaptive boosting (AB), RF, CNN, as well as only transfer learning, and only FL, with a detection accuracy of 91.93%.

In another study, a hybrid decision-extra-trees (DET) classifier is introduced that fuses ensemble decision forests with deep architectures for adaptive 5G-IoT attack mitigation. The model is trained on the Bot-IoT dataset, featuring attacks, such as DDoS, DoS, reconnaissance, exfiltration, and theft. The DET classifier achieves the highest performance among competing models with a per-attack precision of 99.4% (DoS), 97% as recall (DDoS), and average ROC are above 0.97%, outperforming other traditional models (Kholidy, et al., 2023).

(Alzhrani and Alliheedi, 2024) design a simulated 5G-IoT environment, encompassing 100 IoT New Radio User equipment (NRUe) devices and 512,666 labeled samples (containing benign and DDoS) with 16 traffic features. The core result compares four DL models and three ML approaches for DDoS detection. CNN, Forward NN, SVM, stochastic gradient descent (SGD), and KNN achieved very high accuracy (CNN: 99.74%, FNN: 99.53%, SVM: 99.75%, KNN: 99.83%, SGD: 99.27%). LSTM and DNN performed poorly, with equal or <50% accuracy. The analysis emphasizes CNN and FNN as optimal choices for high-throughput, real-time DDoS detection in 5G-IoT networks.

Furthermore, a harmony search feature selection (HSAFS) precedes intrusion recognition with an optimal convolutional autoencoder (OCAE) is presented by Maray, et al., 2023 as a three-stage detection pipeline for SDN-based IoT networks. Artificial Fish Swarm Algorithm is utilized as hyperparameters fine-tuning. The multi-class labeled dataset comprises 84,792 instances. HSAFS-OCAE achieves an average accuracy of 99.12%.

The reviewed studies reveal a broad spectrum of ML/DL for intrusion and attack detection in 5G-enabled IoT environments. To unify these findings and enhance clarity, we introduce a taxonomy (as illustrated in Fig. 3) that organizes the reported methods along four complementary dimensions: Model family, learning paradigm, architectural integration, and deployment tier. Furthermore, model architectures are categorized using a standardized form to ensure consistency across studies. Traditional ML, Single-model DL architectures (e.g., CNN, LSTM, Transformer), which are distinguished from Composite DL architectures (e.g., CNN + LSTM, LSTM + Attention, CNN + LSTM + Attention), and Hybrid ML-DL approaches (e.g., AE + SVM, CNN + RF) are treated as a separate group.

V. Discussion and Future Trends

In this section, a deeper analysis is provided of the reviewed papers in accordance with the research question mentioned in section II. The analysis highlights dataset diversity, model trends, evaluation practices, and future challenges in applying ML/DL for cyber-attack detection within 5G-enabled IoT systems. The detailed specifications of the reviewed works and their limitations are demonstrated in Table A in the appendix section.

To synthesize the findings of this study and directly address the layered security challenges in 5G-enabled IoT, Table II provides a comprehensive mapping of threats to their corresponding countermeasures. It organizes typical attacks according to the 5G-IoT architectural layer they target (Physical/Device, Network, and Application). For each layer, we present the recommended ML/DL countermeasures identified in the literature, accompanied by a rationale that explains their suitability for handling specific threat characteristics and the resource constraints of the deployment environment. In addition, more elaborations and statistical insights are provided in the following subsections.

A. Primary Security Threats, Vulnerabilities, and Attack Methods (RQ1)

As shown in Fig. 4, DoS and DDoS attacks are highly emphasized (18.5.4%) due to their disruptive nature in IoT

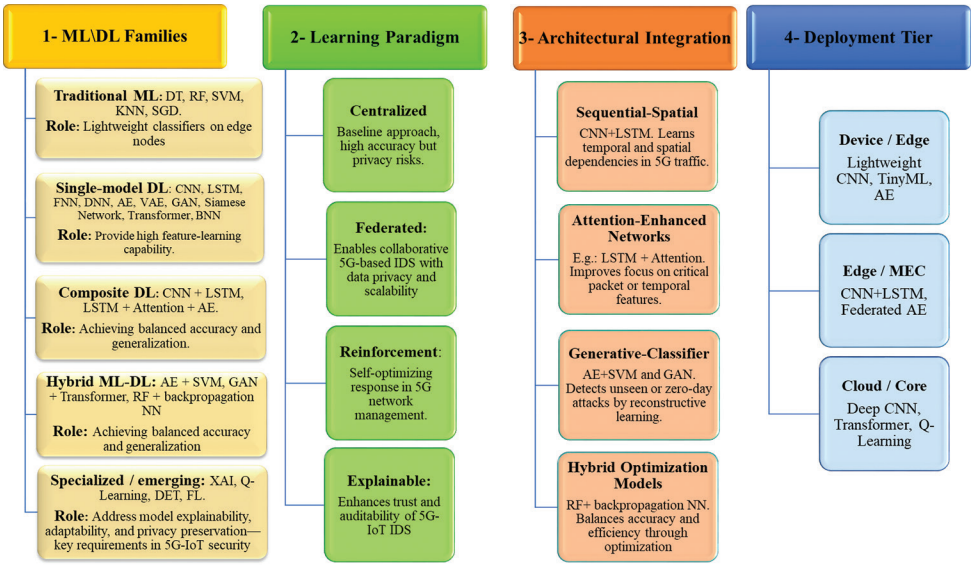

Fig. 3. Taxonomy of machine learning/deep learning for 5G-enabled internet of things security.

TABLE II
MAPPING OF ATTACKS TO ML/DL COUNTERMEASURES, PREFERABLY BY MEANS OF A LAYERED 5G-IOT ARCHITECTURE

5G-IoT layer	Attacks	Recommended ML/DL	Rationale
Physical/device	Jamming, Spoofing, Pilot Contamination, 0-day, BotNet, DoS, Eavesdropping	LSTM with Attention, Siamese+GAN, Q-Learning, XAI	Efficient at capturing temporal signal anomalies and spatial channel patterns; reinforcement and explainability improve adaptability and transparency in resource-constrained edge devices.
Network	MitM, Eavesdropping, Replay, Ransomware, Sybil, 0-day, Spoofing, Botnet, DoS	CNN, LSTM, Autoencoder, SVM, RF Ensemble Learning	Robust in modeling traffic patterns and anomalies; ensemble methods increase resilience to imbalanced datasets and novel threats across network flows.
Application	MiTM, Eavesdropping, Replay, Sybil, 0-day, Spoofing, Phishing, BotNet	VAE, One-class SVM, GAN+Transformer, FL	Strong in unsupervised anomaly detection and privacy preservation; generative techniques enable synthetic data augmentation for 0-day attacks, and FL models ensure scalability and data sovereignty.

MiTM: Man-in-the-middle, CNN: Convolutional neural network, VAE: Variational autoencoder, SVM: Support vector machine

and 5G networks. The prevalence of studies on these attacks reflects their significance and the complexity of mitigating them in high-bandwidth, low-latency environments like 5G. Furthermore, multi-attack classification, focusing on datasets encompassing multiple threat vectors (for instance, DDoS, DoS, Injection, MITM, Password, Ransomware, Mirai, BashLite, and Torii), accounts for 18.5%, emphasizing comprehensive detection frameworks. Intrusion detection studies, which address general anomalies or broad intrusions without a specific attack focus, often using multi-attack datasets for overall intrusion mitigation, comprise 14.8%. Botnet (11.1%), Spoofing, Jamming, and 0-day attacks each has a notable portion (7.4%) of research, while other types highlight minor (3.7%) research areas. This addresses the need for continued exploration of underrepresented areas to address evolving security challenges.

As well as, such distribution shows strong attention to volumetric attacks, underrepresented threats (including Ransomware, Sybil, MitM, and Phishing) remain insufficiently explored. These attacks often exhibit behavioral and identity-level deviations rather than high traffic volumes, requiring more representation-learning and behavioral modeling techniques. Approaches such as Autoencoders and GAN-based anomaly detection can effectively identify hidden deviations, while attention-driven architectures (e.g., Transformer or LSTM with Attention) capture sequential user or device behavior useful for detecting Sybil or phishing activities. Future research should focus on extending these advanced ML/DL models to such stealthy threats to improve holistic 5G-IoT protection.

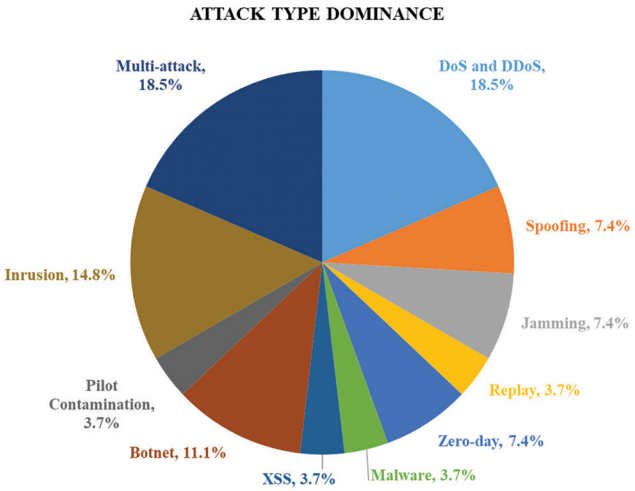

Fig. 4. Attack types percentage focused in literature.

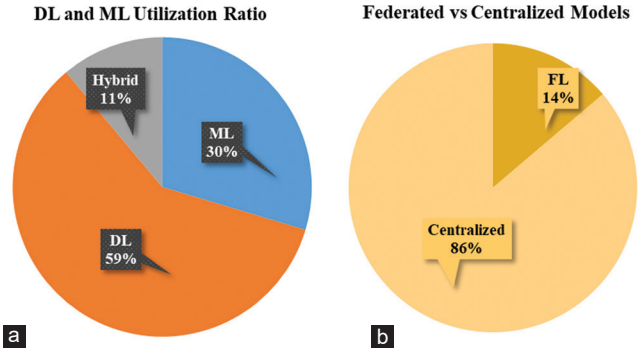

Fig. 5. (a) The ratio of deep learning, machine learning or Hybrid models and (b) Federated or Centralized structure in the reviewed studies.

B. ML/DL Model Distribution and Trends (RQ2)

Single-model DL algorithms dominated 59% (Fig. 5a) of the reviewed works, while ML algorithms presented 30%. Particularly, CNN, LSTM, and Autoencoders are the most frequently utilized DL models, respectively, reflecting their effectiveness in handling complex data and detecting a wide range of attacks (such as DoS/DDoS, MitM, Botnet, Spoofing, 0-day and anomaly-based intrusions) in 5G-IoT networks. Furthermore, the use of composite DL models (CNN + LSTM, LSTM + Autoencoder, and GAN + Transformer) are growing to combine multiple techniques to improve performance, while the models' time complexity and real-time implementation should be considered. Besides, traditional ML models like RF, DT, and SVM are still in widespread use for simpler classification tasks and baseline results.

On the other hand, a minority of studies (11%) utilized hybrid DL-ML architectures, such as Autoencoder + SVM or CNN + RF combinations. These hybrid methods were designed to leverage DL's ability to learn abstract, non-linear features automatically while employing lightweight ML classifiers for efficient classification, which is particularly valuable for resource-constrained IoT environments. In addition, as shown in Fig. 5b, FL frameworks are considered by a small subset of the studied (14%) as a plausible solution that overcomes the concern of privacy while training its models with distributed data. FL can actually put 5G-enabled

IoT security in a far better place by allowing devices to infer using locally held datasets, while keeping customers' sensitive information confidential.

However, FL's repeated exchanges of model updates across devices create communication overhead, straining 5G bandwidth and draining battery life on low-power IoT nodes. Scalability remains a major challenge due to slow aggregation in massive networks with uneven data distribution across clients. To make FL viable, use techniques like model compression and hierarchical setups at 5G edges, which reduce traffic significantly while maintaining accuracy. FL with differential privacy adds robust protection without extra bandwidth costs. These steps ensure FL scales for real 5G-IoT deployments, balancing privacy with efficiency.

Furthermore, based on the model distribution in Fig. 5a, Table III offers a concise comparative snapshot of detection accuracy, F1-score, and latency (as processing time) across the reviewed studies, drawn directly from their reported results. While direct equivalence is limited by variations in classification tasks (binary and multiclass detection), datasets (synthetic UAV simulations vs. legacy NSL-KDD traffic), environments (edge vs. cloud), and even model parameters. These insights highlight the need for standardized benchmarks in future 5G-IoT research.

C. Datasets and Experimental Contexts (RQ3)

One of the most significant aspects that contributes to the further development of the uses of ML and DL in 5G-IoT settings is high-quality and diverse datasets. The successfulness of the models relies greatly on whether they effectively reflect the reality of 5G-IoT network structures. One of the main notes made during the review is the extensive dependency on a small number of benchmark datasets. Based on the data presented in Fig. 6, NSL-KDD has the highest usage, followed by UNSW_NB15, but many studies (10 studies) also used domain-specific/synthetic datasets that were created using simulated 5G or IoT environments. The distribution suggests that while the domain-specific datasets are prevalent in recent works, they might not be a complex and heterogeneous as the actual 5G-IoT traffic. Only one dataset (5G-NIDD) incorporates realistic 5G (without IoT devices) attack behaviors. Consequently, realistic and standardized datasets remain a major research gap in 5G-IoT intrusion detection. Hence, improvement in dataset standardization and sharing is needed for better comparability, generalizability, and reproducibility in 5G-IoT threat detection. In addition, greater use of authentic, diverse, and representative 5G-IoT-era datasets will help bridge the gap to practical deployments. Besides, the integration of synthetic data generation techniques, such as those employed

TABLE III
PERFORMANCE COMPARISON OF THE REVIEWED STUDIES IN TERMS OF ACCURACY, F1-SCORE AND TIME (LATENCY), AND N/A MEANS NOT MENTIONED

References	ML/DL	Accuracy%	F1-score	Time
(Goyal, et al., 2024)	XAI, Q-learning	94.31	N/A	341 ms
(Viana, et al., 2024)	LSTM -attention	89.59	N/A	31 ms
(Alsariera, et al., 2024)	VAE	99.79	0.9419	N/A
(Luo, et al., 2024)	FL - Transformer	99.2	0.992	N/A
(Verma, et al., 2024)	AE+SVM - FL	99.32	0.9984	N/A
(Sadhwani, et al., 2024)	CNN+LSTM	99.81	0.997	N/A
(Alqura'n, et al., 2024)	Bilayered Neural Network	99.84	0.998	N/A
(Naik, et al., 2024)	LSTM+Attention mechanism and Autoencoder	96.97	0.9402	N/A
(El-Sofany, et al., 2024)	RF-backpropagation NN	99.9	0.999	230.4 s
(Martinez Quintero, et al., 2023)	SVM and VGG-16	87.27	0.8771	N/A
(Sousa, Magaia and Silva, 2023)	DT, RF, and MLP	97	0.97	N/A
(Korba, et al., 2023)	Autoencoder+FL	87.94	0.9121	30% decrease the training time
(Ferrag, Debbah and Al-Hawawreh, 2023)	GAN and Transformer	95	1 for normal and 0.32 for injection	N/A
(Viana, et al., 2022)	CNN+LSTM with self-attention layer	77.35	0.79	100 ms
(Dang, et al., 2022)	Ensemble learning with MLP	97	N/A	2700
(Jiang, et al., 2022)	ANN	95	N/A	110 s
(Kim, Kim and Kim, 2022a)	KNN, SVM, RF, and stacking algorithm	96.24	0.9651	N/A
(Yadav, et al., 2022)	Autoencoder	99.76	N/A	N/A
(Kim, Kim and Kim, 2022b)	KNN, DT, RF, and Stacking Ensemble	97.26	0.9699	25.5–109.9 s
(Cheng, Hong and Hung, 2022)	Just mentioned ML model as a tool in the structure.	94.8	N/A	N/A
(Anand, et al., 2021)	CNN	99	N/A	N/A
(Wang, et al., 2021)	Single-hidden-layer multiple measurement Siamese network and GAN	99	N/A	N/A
(Fan, et al., 2020)	Federated transfer learning	91.93	N/A	N/A
(Alferaidi, et al., 2022)	CNN+LSTM	99.8	N/A	2.2 mn
(Kholidy, et al., 2023)	DET	100	1	N/A
(Alzhrani and Alliheedi, 2024)	CNN and FNN	99.74	0.9974	N/A
(Maray, et al., 2023)	Autoencoder	99.12	0.9072	N/A

CNN: Convolutional neural network, VAE: Variational autoencoder, SVM: Support vector machine

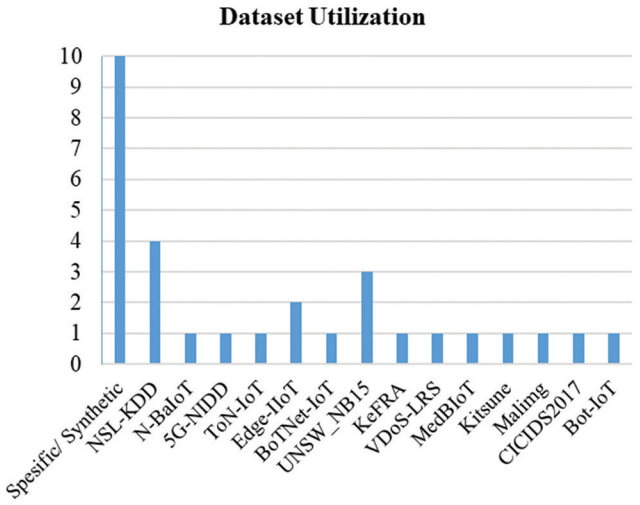

Fig. 6. Dataset distribution in the reviewed studies.

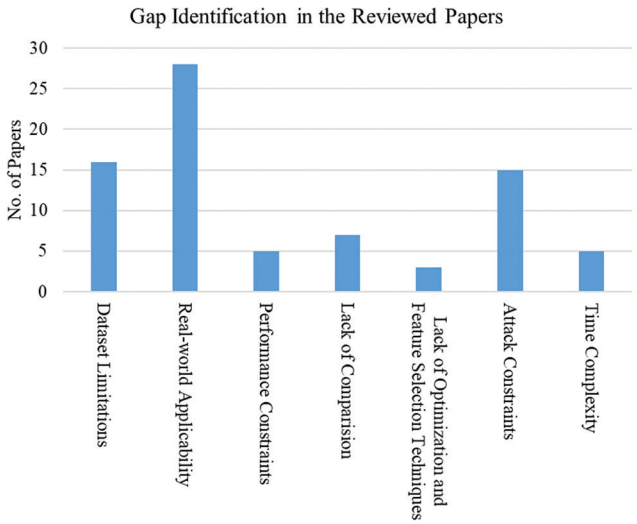

Fig. 7. Categorizing the highlighted gaps of reviewed papers.

in GANs, is able to complement existing datasets. This ensures that models are trained on a comprehensive array of conditions and threats.

In addition, analysis of the reviewed studies shows recurring dataset issues, mainly severe class imbalance, narrow device or traffic diversity, and reliance on synthetic traces that lack real 5G noise characteristics. The generalization and realistic evaluation of intrusion detection models are limited by these weaknesses. To mitigate them, future work should adopt stratified sampling to balance classes, employ realistic synthetic augmentation (e.g., CTGAN or waveform-GAN) to enrich rare attacks, and apply domain-adaptation or self-supervised pre-training to bridge gaps between simulated and real 5G-IoT data. Standardized metadata and transparent pre-processing will further enhance reproducibility and benchmarking quality.

D. Challenges and Promising Future Directions (RQ4)

Even with remarkable progress with ML and DL in 5G-IoT intrusion detection, several challenges persist. A significant proportion of recent studies still tend to use synthetic datasets because actual 5G traffic data is hard to find and share. This reliance creates an important gap, as public available datasets do not reflect what's really happening at the edge of networks or the complex mix of devices and services you see in real deployments. Addressing this limitation will require larger collaborative initiatives, particularly between telecom providers and IoT manufacturers, to develop and open up more realistic datasets. As illustrated in Fig. 7, the most frequently reported limitations across the reviewed studies include issues with dataset quality and diversity, no real-world deployment validation, underexplored attack coverage, benchmarking inconsistencies, and time or resource constraints. The review highlights that benchmarking frameworks and hybrid testbeds integrating simulated and real traffic traces (e.g., ToN-IoT, CIC-IoT-23) should be the focus in the future to examine the latency, scalability, and robustness of networks under realistic conditions. Alongside these data and validation challenges, issues of privacy and bandwidth make continuous transmission of raw data to the cloud impractical for training. That's why FL and edge intelligence (where models learn and adapt without moving sensitive data) are starting to gain attention as more practical options for building scalable and privacy-aware IDS. It's also important to consider the real-world technical demands of 5G-IoT. IDSs should run in real time with minimal delay. This creates a need for CNNs, Transformers, and other models that are optimized for both speed and efficiency, making them better suited for edge devices. Another recurring problem is that benchmarking in this field remains messy. Many groups use their own setups and datasets, making it difficult to compare or reproduce published results. There's a strong case for building standard evaluation frameworks and shared testbeds.

In addition to classical DL and FL techniques, there are a few state-of-the-art paradigms that have become more popular for improving 5G-IoT intrusion detection. Even the best DL models often struggle when deployed on different devices or in new environments, any studies have tested approaches such as continual learning to help systems keep adapting over time, without suffering from catastrophic forgetting, even as new threats appear. GNNs are able to learn the relational structure of 5G-IoT topologies and identify the collective and cross-device attacks (e.g. Botnets, Sybil activities). Using heavily annotated 5G traffic for training allows self-supervised learning methods to learn the data distribution by predicting or contrasting feature representations and thus reducing reliance on labeled data. Last but not least, meta-learning can generalize the learned model on previously unseen or low-data attacks by learning shared initializations across tasks. Looking ahead, the best path forward seems to be a hybrid one. Bringing together FL, continual learning, and perhaps even self-supervised or meta-learning techniques will help models stay up-to-date and privacy-conscious at the same time. Finally, future research should focus on solutions that are both adaptable and practical, grounded in real-world data and able to evolve with new threats as 5G-IoT continues to grow.

E. Real 5G Traffic Datasets and Limitations in 5G-Enabled IoT Studies

While there is a significant growth of research on security in 5G-enabled IoT systems, the availability of real 5G traffic data still remains extremely limited. The majority of the existing studies rely on simulated network traces, legacy IoT datasets, or synthetic 5G-like traffic generated through network emulators. This reliance stems from practical barriers, including the proprietary nature of telecom data, high costs of 5G testbeds, and privacy regulations limiting public sharing of authentic traffic. The existing sources do not fully capture the characteristics of operational 5G environments, such as dynamic network slicing, ultra-low latency communication, massive device density, or the heterogeneity of IoT deployments. Therefore, the experimental evaluation of IDS often takes place under simplified or pre-5G assumptions, potentially inflating model accuracy and limiting their generalizability to real-world 5G scenarios.

Only a small number of recent works employ datasets generated from 5G testbeds or controlled 5G core environments, and even these remain restricted in scale and diversity. This scarcity is primarily due to the proprietary nature of carrier-grade 5G infrastructure, privacy considerations, and the challenges associated with capturing and releasing real 5G traffic. Consequently, current IDS research still lacks benchmark-quality datasets that reflect authentic 5G-enabled IoT behaviors. Future efforts in dataset development and collaborative testbed initiatives are essential to support more realistic evaluation and deployment of ML/DL-based intrusion detection in next-generation IoT systems.

While DL-based models like Transformer, CNN, LSTM, and integrated CNN-based architectures obtain significant detection accuracy, their latency and memory requirements pose challenges for real-time inference on constrained IoT devices. As demonstrated by the most reviewed studies, they performed training and evaluation in centralized environments, overlooking execution overhead at the device level. Real-time IDS in practical 5G-IoT deployments can be supported through lightweight architectures (such as MobileNet), model compression techniques (such as pruning, quantization, and knowledge distillation), and edge or MEC servers for partial offloading. Dynamic adaptation of device and edge inference can balance latency, energy utilization, and detection accuracy, making DL-based security solutions practical within the tight resource limits of 5G-enabled IoT environments.

Unlike other reviews, this paper identifies the main limitations of the methodology in the field through the application of the PRISMA-based approach, which unites studies on ML, DL, and hybrid models in the context of 5G-based IoT security. The other better thing is that it considers the details, datasets, evaluation metrics, and types of cyber-attacks that are covered and the performance of models in practice, which are not always discussed in detail in other places.

VI. Conclusion

An extensive synthesis of contemporary advancements and persistent challenges in ML and DL-based IDS within 5G-enabled IoT systems is provided by this study. It also covers several key gaps overlooked by earlier reviews by combination evidences from model adoption trends, attack-type coverage, and dataset utilization. This review's key contributions are first a quantitative analysis of attack distribution and model strategies uniquely focused on 5G-IoT environments, second providing a comprehensive investigation of dataset realism and evaluation practice, based on recent and quantitatively summarized evidences from the reviewed literature, and third a critical mapping of persistent gaps (ranging from deployment feasibility to benchmarking and real-world applicability) that collectively establish a research agenda for future work.

On the other hand, the key takeaways of this review can be summarized as follows. First, it is indicated that there is persistent dependence on legacy and synthetic datasets, limiting real-world 5G-IoT deployment as well as most existing works either lack access to authentic 5G traffic or do not even use it, creating a significant challenge for both the development and evaluation of robust IDS systems. Second, although DL architectures like CNNs and Transformers show promising potential, limited studies have addressed efficiency concerns needed for edge deployment, generalization, or privacy. FL, in particular, is only beginning to be explored, and continual learning techniques notably remain absent. Finally, the absence of standardized evaluation protocols hinders consistent benchmarking. The methodological inconsistency, fragmented datasets, and a lack of cross-study comparison make it difficult to assess progress or translate findings to large-scale, operational settings.

Overall, this study presents the most comprehensive and current synthesis to date of ML/DL methods for 5G-IoT security. It highlights urgent needs for realistic datasets, reproducible benchmarks, and adaptive, privacy-preserving architectures. The fundamental advancements will rely on collaboration among researchers, industry, and policymakers to realize these foundational improvements and to ensure security systems that are both innovative and reliably deployable.

References

Ahad, A., Tahir, M., Aman Sheikh, M., Ahmed, K.I., Mughees, A., and Numani, A., 2020. Technologies trend towards 5G network for smart health-care using IoT: A review. *Sensors (Basel)*, 20, p.4047.

Alfaw, A.H., and Al-Omary, A., 2022, 5G Security Threats. In: *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, pp.196-199.

Alferaidi, A., Yadav, K., Alharbi, Y., Razmjooy, N., Viriyasitavat, W., Gulati, K., Kautish, S., and Dhiman, G., 2022. Distributed deep CNN-LSTM model for intrusion detection method in IoT-based vehicles. *Mathematical Problems in Engineering,* 2022, p.3424819.

Alqura'n, R., Aljamal, M., Al-Aiash, I., Alsarhan, A., Khassawneh, B., Aljaidi, M., and Alanazi, R., 2024. Advancing XSS detection in IoT over 5G: A cutting-edge artificial neural network approach. *IoT*, 5, pp.478-508.

Alsariera, Y.A., Awwad, W.F., Algarni, A.D., Elmannai, H., Gamarra, M., and

Escorcia-Gutierrez, J., 2024. Enhanced dwarf mongoose optimization algorithm with deep learning-based attack detection for drones. *Alexandria Engineering Journal*, 93, pp.59-66

Alshehri, M.S., Ahmad, J., Almakdi, S., Qathrady, M.A., Ghadi, Y.Y., and Buchanan, W.J., 2024. SkipGateNet: A lightweight CNN-LSTM hybrid model with learnable skip connections for efficient botnet attack detection in IoT. *IEEE Access*, 12, pp.35521-35538.

Alzhrani, R., and Alliheedi, M., 2024. Enhancing IoT security in 5G networks: Mitigating DDoS attacks with deep learning. *Journal of Information Security and Cybercrimes Research*, 7, pp.156-166.

Anand, A., Rani, S., Anand, D., Aljahdali, H.M., and Kerr, D., 2021. An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications. *Sensors*, 21, p.6346.

Aoueileyine, M.O.E., Karmous, N., Bouallegue, R., Youssef, N., and Yazidi, A., 2024. Detecting and mitigating MitM attack on IoT devices using SDN. In: Barolli, L., Ed. Advanced Information Networking and Applications. Springer Nature Switzerland, Cham, pp.320-330.

APWG, 2024. *Phishing Activity Trends Report*, *1st Quarter 2024*. APWG. Available from: https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf?_gl=1*1bft75a*_ga*mtgzodm0ntywmc4xnziymtyznzq0*_ga_55rf0rhxsr*mtcymje2mzc0nc4xljaumtcymje2mzc0nc4wljauma [Last accessed on 2024 Jul 28].

Bahalul Haque, A.K.M., Nausheen, T., Al Mahfuj Shaan, A., and Murad, S.A., 2023. Security Attacks and Countermeasures in 5G Enabled Internet of Things. In: Bhushan, B., Sharma, S.K., Kumar, R., and Priyadarshini, I., Eds. *5G and Beyond.* Singapore: Springer Nature Singapore.

Barshan, A., Mohammadi, S.M.A., Abdollahi, F., Davarani, R.Z., and Esmaeili, S., 2024. Local detection of replay attacks and data anomalies on PMU measurements of smart power grids via tracking critical dynamic modes. *International Journal of Electrical Power and Energy Systems*, 159, p.110038.

Bharati, S., and Podder, P., 2022. Machine and deep learning for IoT security and privacy: Applications, challenges, and future directions. *Security and Communication Networks*, 2022, p.8951961.

Bjerre, S.A., Blomsterberg, M.W.K., and Andersen, B., 2022. 5G Attacks and Countermeasures. In: *2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, p.285-290.

Cheng, S.M., Hong, B.K., and Hung, C.F., 2022. Attack detection and mitigation in MEC-enabled 5G networks for AIoT. *IEEE Internet of Things Magazine*, 5, pp.76-81.

Chettri, L., and Bera, R., 2020. A comprehensive survey on internet of things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal*, 7, pp.16-32.

Dang, Y., Benzaïd, C., Yang, B., Taleb, T., and Shen, Y., 2022. Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs. *IEEE Internet of Things Journal*, 9, pp.25068-25085.

Das, A.K., Roy, S., Bandara, E., and Shetty, S., 2023. Securing age-of-information (AoI)-enabled 5G smart warehouse using access control scheme. *IEEE Internet of Things Journal*, 10, pp.1358-1375.

Dhanavanthini, P., and Chakkravarthy, S.S., 2023. Phish-armour: Phishing detection using deep recurrent neural networks. *Soft Computing*, 2023, p.1-13.

El-Sofany, H., El-Seoud, S.A., Karam, O.H., and Bouallegue, B., 2024. Using machine learning algorithms to enhance IoT system security. *Scientific Reports*, 14, p.12077.

Ericsson., 2025. *IoT Connections Outlook*. Ericsson Mobility Report. Available from: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook [Last accessed on 2025 Oct 19].

Fan, Y., Li, Y., Zhan, M., Cui, H., and Zhang, Y., 2020. IoTDefender: A Federated Transfer Learning Intrusion Detection Framework for 5G IoT. In: *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, pp.88-95.

Ferrag, M.A., Debbah, M., and Al-Hawawreh, M., 2023. Generative AI for Cyber Threat-Hunting in 6G-enabled IoT Networks. In: *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW),* pp.16-25.

Goyal, S., Rajawat, A.S., Solank, R.K., Patil, D., and Potgantwar, A., 2024. A trustable security solutions using XAI for 5G-enabled UAV. *Journal of Logistics, Informatics and Service Science*, 11, pp.73-86.

Grandviewresearch, 2025a. *5G Security Market*. Available from: https://www.grandviewresearch.com/industry-analysis/5g-security-market-report [Last accessed on 2025 Oct 20].

Grandviewresearch, 2025b. *IoT Devices Market*. Available from: https://www.grandviewresearch.com/industry-analysis/iot-devices-market-report [Last accessed on 2025 Oct 20].

Gsma, I., 2023. *IoT Connections Forecast to 2030*. Available from: https://www.gsmaintelligence.com/research/iot-connections-forecast-to-2030 [Last accessed on 2025 Oct 19].

Guo, Y., 2023. A review of machine learning-based zero-day attack detection: Challenges and future directions. *Computer Communications*, 198, pp.175-185.

Habibi, O., Chemmakha, M., and Lazaar, M., 2023. Imbalanced tabular data modelization using CTGAN and machine learning to improve IoT Botnet attacks detection. *Engineering Applications of Artificial Intelligence*, 118, p.105669.

Hasan, M.K., Ghazal, T.M., Saeed, R.A., Pandey, B., Gohel, H., Eshmawi, A.A., Abdel-Khalek, S., and Alkhassawneh, H.M., 2022. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Communications*, 16, p.421-432.

Ispahany, J., Islam, M.R., Islam, M.Z., and Khan, M.A., 2024. Ransomware detection using machine learning: A review, research limitations and future directions. *IEEE Access*, 12, pp.68785-68813

Jiang, C., Xu, H., Huang, C., and Huang, Q., 2022. An adaptive information security system for 5g-enabled smart grid based on artificial neural network and case-based learning algorithms. *Frontiers in Computational Neuroscience*, 16, p.872978.

Jung, J.H., Hong, M.Y., Choi, H., and Yoon, J.W., 2024. An analysis of GPS spoofing attack and efficient approach to spoofing detection in PX4. *IEEE Access*, 12, pp.46668-46677.

Kholidy, H.A., Berrouachedi, A., Benkhelifa, E., and Jaziri, R. Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification. In: *2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*, p.1-8.

Kim, Y.E., Kim, M.G., and Kim, H., 2022a. Detecting IoT botnet in 5G core network using machine learning. *Computers Materials Continua*, 72, pp.4467-4488.

Kim, Y.E., Kim, Y.S., and Kim, H., 2022b. Effective feature selection methods to detect IoT DDoS attack in 5G core network. *Sensors*, 22, p.3819.

Korba, A.A., Boualouache, A., and Ghamri-Doudane, Y., 2024. Zero-X: A blockchain-enabled open-set federated learning framework for zero-day attack detection in IoV. In: *IEEE Transactions on Vehicular Technology*, pp.1-16.

Korba, A.A., Boualouache, A., Brik, B., Rahal, R., Ghamri-Doudane, Y., and Senouci, S.M., 2023. Federated learning for zero-day attack detection in 5G and beyond V2X networks. In: *ICC 2023 - IEEE International Conference on Communications*, pp.1137-1142.

Kumari, P., and Jain, A.K., 2024. Timely detection of DDoS attacks in IoT with dimensionality reduction. *Cluster Computing*, 27, pp.7869-7887.

Li, W., Wang, N., Jiao, L., and Zeng, K., 2021. Physical layer spoofing attack detection in MmWave massive MIMO 5G networks. *IEEE Access*, 9, pp.60419-60432.

Luo, Y., Chen, X., Sun, H., Li, X., Ge, N., Feng, W., and Lu, J., 2024. Securing 5G/6G IoT using transformer and personalized federated learning: An access-side distributed malicious traffic detection framework. *IEEE Open Journal of the Communications Society*, 5, pp.1325-1339.

Lv, Z., Singh, A.K., and Li, J., 2021. Deep learning for security problems in 5G heterogeneous networks. *IEEE Network*, 35, pp.67-73.

Malik, A., Bhushan, B., Bhatia Khan, S., Kashyap, R., Chaganti, R., and Rakesh, N., 2023. Security Attacks and vulnerability analysis in mobile wireless networking. In: Bhushan, B., Sharma, S.K., Kumar, R., and Priyadarshini, I., Eds. *5G and Beyond.* Springer Nature Singapore, Singapore.

Maray, M., Alshahrani, H.M., Alissa, K.A., Alotaibi, N., Gaddah, A., Meree, A., Othman, M., and Hamza, M.A., 2023. Optimal deep learning driven intrusion detection in SDN-enabled IoT environment. *Computers, Materials and Continua*, 74, pp.6587-6604.

Maroofi, S., Korczyński, M., Hölzel, A., and Duda, A., 2021. Adoption of email anti-spoofing schemes: A large scale analysis. *IEEE Transactions on Network and Service Management*, 18, pp.3184-3196.

Martinez Quintero, J.C., Estupiñan Cuesta, E.P., and Ramirez Lopez, L.J., 2023. A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms. *Results in Engineering*, 19, p.101243

Mazhar, T., Talpur, D.B., Shloul, T.A., Ghadi, Y.Y., Haq, I., Ullah, I., Ouahada, K., and Hamam, H. 2023. Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain Sci*., 13, pp.683.

Naha, A., Teixeira, A., Ahlén, A., and Dey, S., 2023. Sequential detection of replay attacks. *IEEE Transactions on Automatic Control*, 68, pp.1941-1948.

Naik, S., Thippeswamy, P., Raghavan, A., Rajgopal, M., and Sujith, A., 2024. Efficient network management and security in 5G enabled internet of things using deep learning algorithms. *International Journal of Electrical and Computer Engineering*, 14, pp.1058-1070.

Noman, H.A., and Abu-Sharkh, O.M.F., 2023. Code injection attacks in wireless-based internet of things (IoT): A comprehensive review and practical implementations. *Sensors (Basel)*, 23, p.6067.

Patel, D., and Shah, D., 2024. Combating ARP Spoofing: Detection and Analysis Techniques. In: *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp.543-547.

Prasad, V.M., and Bharathi, B., 2023. Security in 5G networks: A systematic analysis of high-speed data connections. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11, p.216-222.

Rachakonda, L.P., Siddula, M., and Sathya, V., 2024. A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing*, 4, p.100220.

Rafique, W., Barai, J., Fapojuwo, A.O., and Krishnamurthy, D., 2024. A survey on beyond 5G network slicing for smart cities applications. *IEEE Communications Surveys and Tutorials*, 27, pp.595-628.

Rakhi, S., and Shobha, K.R., 2023. LCSS based sybil attack detection and avoidance in clustered vehicular networks. *IEEE Access*, 11, pp.75179-75190.

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B.C.M., and Assi, C., 2023. The age of ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access*, 11, pp.40698-40723.

Sadhwani, S., Mathur, A., Muthalagu, R., and Pawar, P.M., 2024. 5G-SIID: An intelligent hybrid DDoS intrusion detector for 5G IoT networks. *International Journal of Machine Learning and Cybernetics*, 16, pp.1243-1263.

Sameera, N., and Shashi, M., 2020. Deep transductive transfer learning framework for zero-day attack detection. *ICT Express,* 6, pp.361-367.

Shafique, K., Khawaja, B.A., Sabir, F., Qazi, S., and Mustaqim, M., 2020. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access*, 8, pp.23022-23040.

Sousa, B., Magaia, N., and Silva, S., 2023. An intelligent intrusion detection system for 5G-enabled internet of vehicles. *Electronics*, 12, p.1757.

Taher, M.A., Tariq, M., Behnamfar, M., and Sarwat, A.I., 2023. Analyzing replay attack impact in DC microgrid consensus control: Detection and mitigation by kalman-filter-based observer. *IEEE Access*, 11, pp.121368-121378.

Taleb, H., Khawam, K., Lahoud, S., Helou, M.E., and Martin, S., 2022. Pilot Contamination mitigation in massive MIMO Cloud Radio Access Networks. *IEEE Access*, 10, pp.58212-58224.

Tarannum, S., Usha, S.M., and Ahammed, G.F.A., 2024. A comprehensive study of LPWAN, LoRaWAN for IoT: Background, related research, performance, potential challenges and proposed methodology. *AIP Conference Proceedings*, 3122, p.080001.

Trabelsi, Z., Parambil, M.M.A., Qayyum, T., and Alomar, B., 2024. Teaching DNS Spoofing Attack Using a Hands-on Cybersecurity Approach Based on Virtual Kali Linux Platform. In: *2024 IEEE Global Engineering Education Conference (EDUCON)*, p.1-8.

Tulay, H.B., and Koksal, C.E., 2024. Sybil attack detection based on signal clustering in vehicular networks. In: *IEEE Transactions on Machine Learning in Communications and Networking*, 2, pp.753-765.

Valadares, D.C.G., Will, N.C., Sobrinho, Á.Á.C.C., Lima, A.C.D., Morais, I.S., and Santos, D.F.S., 2023. Security Challenges and Recommendations in 5G-IoT Scenarios. In: Barolli, L., Ed. *Advanced Information Networking and Applications*. Springer International Publishing, Cham, pp.558-573.

Verma, P., Bharot, N., Breslin, J.G., Shea, D.O., Vidyarthi, A., and Gupta, D., 2024. Zero-day guardian: A dual model enabled federated learning framework for handling zero-day attacks in 5G enabled IIoT. *IEEE Transactions on Consumer Electronics*, 70, pp.3856-3866.

Viana, J., Farkhari, H., Campos, L.M., Sebastião, P., Koutlia, K., Lagén, S., Bernardo, L., and Dinis, R., 2022. A Convolutional Attention Based Deep Learning Solution for 5G UAV Network Attack Recognition over Fading Channels and Interference. In: *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, pp.1-5.

Viana, J., Farkhari, H., Sebastião, P., Campos, L.M., Koutlia, K., Bojovic, B., Lagén, S., and Dinis, R., 2024. Deep attention recognition for attack identification in 5G UAV scenarios: Novel architecture and end-to-end evaluation. *IEEE Transactions on Vehicular Technology*, 73, pp.131-146.

Wang, N., Li, W., Alipour-Fanid, A., Jiao, L., Dabaghchian, M., and Zeng, K., 2021. Pilot contamination attack detection for 5G MmWave grant-free IoT networks. *IEEE Transactions on Information Forensics and Security*, 16, pp.658-670.

Wazid, M., Das, A.K., Shetty, S., Gope, P., and Rodrigues, J.J.P.C., 2021. Security in 5G-enabled internet of things communication: Issues, challenges, and future research roadmap. *IEEE Access*, 9, pp.4466-4489.

Xiao, S., Wang, Z., Si, X., and Liu, G., 2024. Mean-square exponential stabilization of memristive neural networks: Dealing with replay attacks and communication interruptions. *Communications in Nonlinear Science and Numerical Simulation*, 138, p.108188.

Xing, Y., Shu, H., and Kang, F., 2023. PeerRemove: An adaptive node removal strategy for P2P botnet based on deep reinforcement learning. *Computers and Security*, 128, p.103129.

Yadav, N., Pande, S., Khamparia, A., and Gupta, D., 2022. Intrusion detection system on IoT with 5G network using deep learning. *Wireless Communications and Mobile Computing*, 2022, p.9304689.

Zahra, F.T., Bostanci, Y.S., and Soyturk, M., 2023. Real-time jamming detection in wireless IoT networks. *IEEE Access*, 11, pp.70425-70442.

Appendix

TABLE A
Comparison Table of the Reviewed Papers

References	Dataset	Attack type	ML/DL	Limitations
(Goyal, et al., 2024)	Data are collected from actual field deployments of 5G-enabled UAVs, also simulations are conducted to generate synthetic datasets.	Intrusion	XAI, Q-learning	The study may not account for the rapidly evolving nature of cybersecurity threats, besides, the attack types are not discussed and the model is not evaluated on specialized UAV attack-based datasets.
(Viana, et al., 2024)	Synthetic Jamming Dataset for UAVs that contained 2400 folders, each containing RSSI and SINR data files, and categorized into Yes Jamming, No Jamming, Moving Jamming, and Fixed Jamming.	Jamming	DNN with attention layer	Need for extensive and large datasets to train the model containing diverse attacks. Moreover, due to the resource limitations of UAVs, utilizing optimization algorithms is required to improve DL complexity. Lack of comparison to the state-of-the-art models.
(Alsariera, et al., 2024)	NSL-KDD	Multi-attack classification (DoS, R2l, Probe, and U2r attacks)	VAE	Evaluation of the model performance with other related datasets is crucial to indicate the model's generalization. Furthermore, its results are not compared to the related works' results, they are just compared with some existing classifiers.
(Luo, et al., 2024)	N-BaIoT	Botnet	FL-transformer	Limited dataset diversity, which causes model generalization. Moreover, a combination of a transformer and personalized FL may be complex and require significant computational resources.
(Verma, et al., 2024)	A local dataset collects data from several industrial IoT devices.	0-day	AE+SVM-FL	The model increased complexity, which may cause challenges in resource-constrained environments. Evaluating the model on other related datasets is required to ensure the model's generalization and robustness in real-world applications.
(Sadhwani, et al., 2024)	5G-NIDD	DDoS	CNN and LSTM	The dataset has minor classes, and they did not use balancing techniques; also, advanced feature selections can be used to obtain better performance. Only a DDoS attack is considered in the study. The computational time of the model is not considered.
(Alqura'n, et al., 2024)	NF-ToN-IoT-v2 and Edge-IIoTset	XSS	Bilayered Neural Network	The model's computational time is not considered, and the focus is only on one type of attack.
(Naik, et al., 2024)	The raw TCP/IP dump data with 41 features are collected for a network by simulating a typical US Air Force LAN	Intrusion	LSTM+Attention mechanism and Autoencoder	The utilized database for attack detection is outdated and is not well suited to 5G- IoT environments, this causes overfitting and inaccurate prediction in noisy traffic, as well as the position of the proposed attack detection not being determined in the 5G infrastructure.
(El-Sofany, et al., 2024)	BoTNet-IoT-L01, NSL-KDD, and UNSW_ NB15	Multi-attack	RF-backpropagation NN	Using a mix of various optimization techniques, like preparing data, adjusting hyperparameters, and applying ensemble methods, can create combined benefits that enhance both the speed of execution and the accuracy of the model.
(Martinez Quintero, et al., 2023)	KeFRA	Replay	SVM and VGG-16	Focus on a specific attack type (replay attack). The utilized dataset contains only 240 images, and this may not be sufficient to cover all the variability of RF signals in real-world scenarios.
(Sousa Magaia and Silva, 2023)	They created their dataset through simulations.	DDoS (Flooding)	DT, RF, and MLP	Focus on a specific attack type, scalability, which is critical in urban environments, is not considered, and model evaluation on existing datasets is required for generalization.
(Korba, et al., 2023)	VDoS-LRS	0-day	Autoencoder	They should focus on diverse attack datasets to propose a robust zero-attack detection model. The models relied on only DDoS attacks for training the model, which caused generalization.
(Ferrag, Debbah and Al-Hawawreh, 2023)	Edge-IIoT	Multi-attack (DoS/ DDoS, Information Gathering (Reconnaissance), MITM, Injection, and Malware)	GAN and Transformer	Generative AI models bring challenges related to cost, latency, and memory requirements, making it difficult to deploy on devices with limited resources. Lack of comparison with the other state-of-the-art advanced techniques.
(Viana, et al., 2022)	Synthetic Jamming Dataset for UAVs that contained 2400 folders each containing RSSI and SINR data files.	Jamming	Integration of CNN and LSTM with self-attention layer	The minimum time required to detect an attack is 100 ms, which is critical for real-time applications. And the utilized dataset only contained jamming attack scenarios, thus more assessment processes with other datasets are required to improve the versatility of the proposed algorithm.
(Dang, et al., 2022)	Not mentioned	Spoofing	Ensemble learning with MLP	The study relies on only GPS spoofing attacks, and the dataset specifications are not mentioned and they did not utilize another related dataset. These cause model generalization and robustness. Comparison with related works will provide better improvements to the study.

(Contd...)

TABLE A
(Continued)

References	Dataset	Attack type	ML/DL	Limitations
(Jiang, et al., 2022)	The dataset was acquired from an experimental 5G power IoT scenario over a period of 2 days, specifically from Friday to Saturday.	Intrusion	ANN	The dataset used for training and testing the model is derived from a specific experimental scenario over a short period (2 days). The study did not provide detailed methodologies on how the various attacks were simulated or created. The study does not provide a comparative analysis with existing security solutions or frameworks.
(Kim, Kim and Kim, 2022a)	MedBIoT	Botnet	KNN, SVM, RF, and stacking algorithm	Additional evaluation is required to tackle the generalizability of the findings to other datasets or real-world scenarios. A specific focus on botnet attacks may overlook other significant threats.
(Yadav, et al., 2022)	NSW-NB15	DoS	Autoencoder	They focus on DoS attack, and farther assessment is required to achieve globalization and real-world capability.
(Kim, Kim and Kim, 2022b)	Kitsune	DDoS	KNN, DT, RF, and Stacking Ensemble	Limited dataset due to the lack of diverse and various types of attacks. Lack of comparison with state-of-the-art solutions.
(Cheng, Hong and Hung, 2022)	Gathering real-time data from both legitimate and fake BSs	Spoofing	Just mentioned the ML model as a tool in the structure.	The research primarily focuses on BS attacks and may not comprehensively address other potential security threats that IoT devices could face in a 5G environment. Lack of comprehensive evaluation of the existing solutions.
(Anand, et al., 2021)	Malimg	Malware	CNN	The proposed model is not trained with normal traffic and not validated with other famous datasets to be suitable for real-world healthcare environments.
(Wang, et al., 2021)	They use stored data in base stations, which are derived from legitimate IoT users.	Pilot contamination	Single-hidden-layer multiple measurement Siamese network and GAN	The model's performance may be affected if the training dataset does not adequately represent the various scenarios. The proposed model relies heavily on accurate channel models, if the channel characteristics are not well-represented, the detection performance may degrade.
(Fan, et al., 2020)	Private datasets are used in each MEC clients (C), C1-C3: Each has a Wi-fi IoT network and C4 has NSL-KDD dataset. The public dataset is CICIDS2017	Multi-attack	Federated transfer learning	The study does not fully explore how to effectively manage and select clients in larger and more complex networks.
(Alferaidi, et al., 2022)	NSL-KDD and UNSW-NB15	Intrusion	CNN+LSTM	The authors claim to have proposed an intrusion detection model for in-vehicle (car) networks; therefore, they should evaluate their model using real-world data collected from actual automotive networks rather than relying on public datasets.
(Kholidy, et al., 2023)	Bot-IoT	Botnet	DET	Limited to one dataset, which may cause model generalization, and only 10 out of 43 features are selected.
(Alzhrani and Alliheedi, 2024)	They created their own dataset, containing 512,666 samples (normal and DDoS) and 16 features.	DDoS	CNN and FNN	They perform a specific 5G-IoT scenario, which may suffer generalization issues. It lacks comparison with state-of-the-art approaches and is limited to a binary classification.
(Maray, et al., 2023)	A dataset with 84,792 samples under six class labels (benign, bot, brute-force FTP, DDoS-Loic-UDP, DDoS-Hoic, infiltration)	Multi-attack	Autoencoder	The dataset details are not presented. Data are categorized into classes, and then each class is trained and tested individually. To validate the robustness of the proposed model, an evaluation using combined classes is necessary.

MiTM: Man-in-the-Middle, TCP: Transmission control protocol, IoT: Internet of things, DoS: Denial of service, ML: Machine learning, DL: Deep learning, AI: Artificial intelligence, UDP: User datagram protocol, XAI: Explainable artificial intelligence, UAVs: Unmanned aerial vehicles, CNN: Convolutional neural network, VAE: Variational autoencoder, SVM: Support vector machine, GPS: Global positioning system, DNN: Deep neural network