Artificial Intelligence Review (2025) 58:340
https://doi.org/10.1007/s10462-025-11346-z

Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives

Euclides Carlos Pinto Neto[1] · **Shahrear Iqbal**[1] · **Scott Buffett**[1] · **Madeena Sultana**[2] · **Adrian Taylor**[2]

Accepted: 29 July 2025 / Published online: 20 August 2025

Abstract
Intrusion Detection Systems (IDS) can help cybersecurity analysts detect malicious activities in computational environments. Recently, Deep Learning (DL) methods in IDS have demonstrated notable performance, revealing new underlying cybersecurity patterns in systems' operations. Conversely, issues such as low performance in real systems, high false positive rates, and lack of explainability hinder its real-world deployment. In addition, the adoption of many new emerging technologies, such as cloud, edge computing, and the Internet of Things (IoT) introduces new forms of vulnerabilities. Therefore, the improvement of intrusion detection in emerging technologies depends on the clear definitions of challenging security problems and the limitations of existing solutions. The main goal of this research is to conduct a literature review of DL solutions for intrusion detection in emerging technologies to understand the state-of-the-art solutions and their limitations. Specifically, we conduct a comprehensive review of IDS-based automated threat defense methods, with the objective of identifying the landscape of, and opportunities for, incorporating DL methods into IDS. To accomplish this, a thorough review of IDS methods is conducted for multiple platforms and technologies, focusing on the use of common DL techniques. To expand on the study, several widely used IDS datasets are evaluated to assess their ability to train DL models and support researchers in understanding their characteristics and limitations. The analysis of attack vectors in emerging technologies is conducted, enabling an in-depth evaluation of security solutions in the future. Our findings show many clear opportunities for future research, including addressing the gap between solutions for controlled/simulated environments versus real systems, overcoming trustworthiness issues, including lack of explainability, and further exploring operationalization issues such as deployable solutions and continuous detection. Our analysis highlights that the operationalization of DL for intrusion detection in emerging technologies represents a key challenge to be addressed in the next few years.

Keywords Deep learning · Intrusion detection systems · Cybersecurity · Emerging technologies · Datasets

Extended author information available on the last page of the article

1 Introduction

The negative impacts of cyberattacks can affect a wide variety of functionalities in business and industry, from disrupting daily operations to compromising safety-critical systems. Organizations acknowledge the importance of establishing effective security countermeasures. In fact, such defenses require different resources depending on the potential impacts, secrecy, and safety aspects. The constant development of new threats highlights the need to enhance existing protection mechanisms. Making matters worse, detecting and mitigating such attacks have become more challenging in the past few years. In addition, in the last decade, many advanced technologies have been created to address complex business issues, enable new business opportunities, and improve the efficiency of existing operations, thus increasing the attack surface and introducing new vulnerabilities, making the act of cyber defense even more challenging.

The development of Information and Communication Technologies (ICT) has enabled new business paradigms and the design of new solutions to serve society. In this context, computer networks connect systems and backbones, offering distributed solutions that comprise infrastructure innovations, protocols, applications, and context-specific solutions (Tanenbaum (2003)). Considering Confidentiality, Integrity, and Availability (CIA) as a critical triad in any network interaction, the presence of malicious actors aiming at compromising communications is an increasing concern to the business world. Apart from the impressive evolution of computer networks' capabilities, modern society demands a continuously optimized environment and resources for demanding applications. Each new computing paradigm presents its specific networking requirements and challenges, including cybersecurity.

These emerging technologies comprise computing paradigms (e.g., cloud computing, edge computing, and Multi-access Edge Computing - MEC), ubiquitous applications (e.g., Internet of Things - IoT, Internet of Vehicles - IoV, Internet of Medical Things - IoMT, and Industrial Internet of Things - IIoT), networking innovations (e.g., Software-Defined Networking - SDN) and safety-critical applications (e.g., Industrial Control Systems - ICS). These new technologies require specialized cybersecurity methods to detect and mitigate attacks while adhering to many constraints. The number of annual attacks launched against these systems is substantial, preventing humans from analyzing every single incident. This problem is exacerbated by the shortage of experts in cybersecurity (Ramezan (2023)). Organizations of all sizes face challenges in recruiting, training, and retaining talent. This overwhelming landscape defines an unsustainable environment for manual attack detection and mitigation and emphasizes the need for automated capabilities.

The adoption of advanced technologies to overcome these obstacles is complex given the constrained dynamics of real business operations. Such solutions need to be environmentally aware, i.e., demonstrate that automated capabilities comply with organizational policies while defining a holistic approach. Besides, cybersecurity decisions need to be transparent, explainable, and robust in challenging scenarios. Finally, operationalization is pivotal since it represents the actual deployment of such tools in the business environment, considering a continuous improvement process and a generalized discovery of malicious activities.

Intrusion Detection Systems (IDS) act as augmentation platforms for cybersecurity analysts by automatically detecting malicious activities in computational environments (Ald-

weesh et al. (2020); Gümüşbaş et al. (2020)). These systems can analyze data at scale and automate specific parts of incident analysis. Although IDS have been successful in many applications, the current sophistication of cyberattacks sheds light on the importance of adopting advanced capabilities beyond the countermeasures used in the past. In this sense, traditional IDS present critical shortcomings that can be exploited by threat actors, preventing their adoption in real-world systems. As a result, novel techniques have been adapted to support IDS, and one of the most prominent classes is the use of Deep Learning (DL).

DL is an area of Machine Learning (ML) and Artificial Intelligence (AI) focused on the use of neural architectures to solve complex tasks (Goodfellow et al. (2016)). This class of algorithms reveals underlying patterns in large amounts of data and has presented remarkable success in various application areas, ranging from deep fake detection (Altamimi and Salameh (2024)) to cloud failure prediction (Tengku Asmawi et al. (2022)). Examples of DL techniques are Deep Feed Forward Networks (DNN)(Cybenko (1989) Goodfellow et al. (2016)), Convolutional Neural Networks (CNNs) (Li et al. (2021); Gu et al. (2018); Hijazi et al. (2015)), Recurrent Neural Networks (RNNs) (Lipton et al. (2015); Salehinejad et al. (2017); Bullinaria (2013)), Federated Deep Learning (FDL) (Li et al. (2020); Kairouz et al. (2021); Li et al. (2019)), Generative Adversarial Networks (GANs) (Goodfellow et al. (2020); Pan et al. (2019); Saxena and Cao (2021)), Autoencoders (AE) (Bank et al. (2023); Doersch (2016)), and Transformer-based Methods (TF) (Vaswani (2017); Islam et al. (2024); Adjewa et al. (2024)). In recent years, scientific works have proposed DL methods to detect cyberattacks in controlled environments, outperforming traditional techniques by a wide margin in some cases. Conversely, this success comes from experiments in controlled environments. DL-empowered IDS still present critical limitations that prevent their wide adoption in real systems, such as high false positives that overwhelm analysts. Also, generalization is a major issue in intrusion detection since models perform well in one environment may present a decrease in performance in different systems.

The main goal of this research is to conduct a literature review of DL solutions for IDS in emerging technologies to understand the state-of-the-art IDS solutions and their limitations. The main purpose of this effort is to define a baseline of state-of-the-art solutions to protect emerging technologies and identify their respective limitations. This comprehensive investigation intends to support cybersecurity researchers in identifying challenging problems and promising research opportunities based on the characteristics of existing solutions. Therefore, we aim to advance IDS capabilities by highlighting research pathways for more secure applications. We categorize state-of-the-art efforts according to the DL technique adopted. Also, we analyze and compare popular IDS datasets to highlight current states of advancements and identify gaps for future developments. Finally, we highlight immediate research directions in protecting emerging technologies (e.g., IoT, SDN, and ICS).

1.1 Related work

In the past few years, there have been efforts to identify open challenges in using DL for IDS. Hodo et al. (2017) present a survey and taxonomy on using DL for intrusion detection. This work introduces a detailed IDS classification and a review of papers in different applications (e.g., cloud computing and IoT), considering specific DL techniques (e.g., DNN, CNN, and RNN). Similarly, Liu and Lang (2019) review solutions that use ML and DL for IDS. In addition to Hodo et al., the authors consider Generative Adversarial Net-

works (GANs) and evaluate multiple datasets. Aldweesh et al. (2020) discuss the conceptual structure of different DL techniques and their differences while analyzing IDS applications. Multiple works are reviewed in application areas such as cloud computing and IoT. Additionally, Asharf et al. (2020) focus on reviewing IDS solutions for IoT operations based on DL. Another in-depth analysis of the state-of-the-art IDS initiatives is presented by Ahmad et al. (2021). Gamage and Samarabandu (2020) and Gümüşbaş et al. (2020) evaluate datasets and consider several DL architectures. Lansky et al. (2021) present a review that encompasses the application of Federated Deep Learning (FDL), not focusing on Transformers (TF). Three other works published recently also focus on reviewing the application of DL in IDS. Al-Shurbaji et al. (2025) analyze existing approaches for botnet detection in IoT, listing several related technologies (such as WiFi, ZigBee, and WiiMax) and applications (such as transportation, smart home, smart cities, and manufacturing). The authors also present a taxonomy of IoT security comprising data, communication, architecture, and application. Although a taxonomy of attack surface is not presented, a discussion on IoT device vulnerabilities is conducted. Liao et al. (2024) also focus on the applications of DL to IoT. This work brings important insights regarding the reviewed papers, including data processing techniques, feature extraction, and classification process. However, the authors do not present an analysis of state-of-the-art IoT datasets. Finally, Muneer et al. (2024) target a more general objective by reviewing Artificial Intelligence (AI) approaches to IDS. The authors list the strengths and weaknesses of DL methods, Machine Learning (ML), and Federated Learning (FL). This paper also focuses on explainability. However, it does not present an in-depth analysis of emerging technologies, their attack surfaces, and the applicability of DL to their protection. Compared to all these works, we focus on emerging technologies, their attack vectors, relevant datasets for each application, and the difficulties each technology faces regarding intrusion detection. Table 1 compares our work with the related efforts and highlights that proposing a taxonomy for attack surface in emerging technologies is not considered by other works. Also, the classification of efforts and datasets based on the applicability in emerging technologies and an analysis of future directions based on individual technologies are not in the scope of the related work. Conversely, all works

Table 1 Comparison of this work with previous efforts

Work	Emerging Technologies	DL	Taxonomy of Attack Surface	Dataset Analysis	Dataset and Work Classification	Open Challenges Categorization
Hodo et al. (2017)	✓	✓				
Liu and Lang (2019)	✓	✓		✓		
Aldweesh et al. (2020)	✓	✓		✓		
Asharf et al. (2020)	✓	✓		✓		
Gamage and Samarabandu (2020)	✓	✓		✓		
Gümüşbaş et al. (2020)	✓	✓		✓		
Ahmad et al. (2021)	✓	✓		✓		
Lansky et al. (2021)	✓	✓		✓		
Liao et al. (2024)	✓	✓		✓		
Muneer et al. (2024)	✓	✓				
Al-Shurbaji et al. (2025)	✓	✓				
This work	✓	✓	✓	✓	✓	✓

focus on emerging technologies and the application of Deep Learning (DL) for intrusion detection. To clarify the novelty of our approach, Table 2 shows the emerging technologies and DL models considered in all works. Therefore, our review investigates the application of multiple DL models in different emerging technologies not covered by existing works. Finally, there has been an increase in insightful reviews related to our study. These works help researchers identify new directions, but cover different technologies and techniques in a more general sense. For example, with a focus on IoT, Saied et al. (2023c, 2023b) analyze the application of Artificial Intelligence (AI) to improve intrusion detection, while Saied Essa and Kamal Guirguis (2023) focus on boosting-based machine learning. Other examples are Thakur and Kumar (2021) and Hu et al. (2024), in which the review targets the use of nature-inspired methods. These works bring important insights that support the definition of our contributions, described in the following section.

1.2 Contributions

The main contributions of this research are:

- **A comprehensive review of state-of-the-art intrusion detection solutions:** We analyze several research efforts to define a baseline of solutions to protect emerging technologies and identify their respective limitations. Ultimately, we aim to advance IDS capabilities by highlighting research pathways for more secure applications. Our focus is on emerging technologies, including cloud computing, edge computing, IoT, IoV, IoMT, IIoT, Software-Defined Networking (SDN), Multi-access Edge Computing (MEC), and Industrial Control Systems (ICS). We consider methods that consolidate the use of Deep Learning (DL) techniques, i.e., Deep Feed Forward Networks (DNN), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Federated Deep Learning (FDL), Generative Adversarial Networks (GANs), Autoencoders (AE), and Transformers (TF) in intrusion detection systems for emerging technologies.
- **A comprehensive analysis of recent IDS datasets:** We review widely used IDS datasets to help researchers understand their characteristics and limitations, and make an informed decision regarding which dataset to use based on their needs. This detailed evaluation focuses on the support for the development and deployment of DL models and considers a temporal evaluation from 1999. We also list the attacks executed in each scenario and the topological configuration, and categorize each work based on its application to emerging technologies.
- **An identification of attack surfaces for each emerging technology:** to pinpoint the areas targeted by attackers when launching malicious activities, we present a taxonomy of attack surfaces in each emerging technology, comprising high-level components such as applications and low-level resources such as infrastructure. This investigation offers researchers new perspectives regarding how these systems can be compromised and, consequently, how security countermeasures can be effectively designed.
- **A thorough investigation of research gaps and open challenges:** We identify critical and immediate future directions stemming from open challenges in the context of using DL for intrusion detection in emerging technologies. This analysis provides clear research pathways for future work to address current shortcomings of state-of-the-art approaches and reveal the current and future horizons for automating threat defense by

Table 2 Comparison of this work with previous efforts regarding the emerging technologies and Deep Learning (DL) techniques evaluated

	Emerging Technologies						Deep Learning						
Work	Cloud	Edge	IoT	SDN	MEC	ICS	DNN	CNN	RNN	FDL	GAN	AE	TF
Hodo et al. (2017)	✓		✓				✓	✓	✓			✓	
Liu and Lang (2019)			✓				✓	✓	✓		✓	✓	
Aldweesh et al. (2020)	✓		✓				✓	✓	✓		✓	✓	
Asharf et al. (2020)	✓		✓				✓	✓	✓		✓	✓	
Gamage and Samarabandu (2020)			✓				✓	✓	✓			✓	
Gümüşbaş et al. (2020)							✓	✓	✓		✓	✓	
Ahmad et al. (2021)	✓		✓				✓	✓	✓			✓	
Lansky et al. (2021)	✓		✓				✓	✓	✓	✓	✓	✓	
Liao et al. (2024)			✓				✓	✓	✓			✓	
Muneer et al. (2024)			✓				✓	✓	✓	✓		✓	
Al-Shurbaji et al. (2025)			✓				✓	✓	✓		✓	✓	
This Research	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

adopting DL in IDS.

1.3 Research methodology

In order to identify and select papers relevant to our review, we considered a sequence of actions (Abdulganiyu et al. (2023), Saied et al. (2023a)). First, we identified the main research questions for our investigation. Then, we defined the search strategy. After that, we established the criteria for the inclusion of papers.

1.3.1 Research questions

In this research, we aim to answer these Research Questions (RQ):

- **RQ1:** What are the main characteristics and limitations of DL techniques used in the intrusion detection process for each emerging technology?
- **RQ2:** What are the main open challenges in the use of DL for intrusion detection in emerging technologies?

1.3.2 Search strategy

Our goals comprise the solutions developed for multiple emerging technologies. We used Google Scholar as our search engine and multiple combinations of strings. Figure 1 illustrates the approach adopted in this search and the main strings used, i.e., the emerging technology term was followed by the IDS term and the Deep Learning (DL) term.

1.3.3 Selection of papers

The inclusion criteria to select papers incorporate:

- Research articles dated after 2016.
- Research articles that are relevant to the context of IDS;
- Research articles that are relevant to the context of applied Deep Learning (DL);
- Research articles focused on specific emerging technologies;
- Research articles that present a similar style to enable comparison;
- Research articles that present a relevant aspect of the emerging technology considered and can represent other similar works that cover the same topic.
- Research articles that present a novel contribution to emerging technologies protection and can represent other similar works that focus on similar problems;
- Research articles that present consistency and specific similarities with other articles selected.

1.4 Outline

This paper is organized as follows: Sect. 2 describes the main concepts of intrusion detection and emerging technologies. Then, sections 3 and 4 review state-of-the-art datasets and DL solutions for intrusion detection, respectively. Finally, section 5 discusses the open chal-

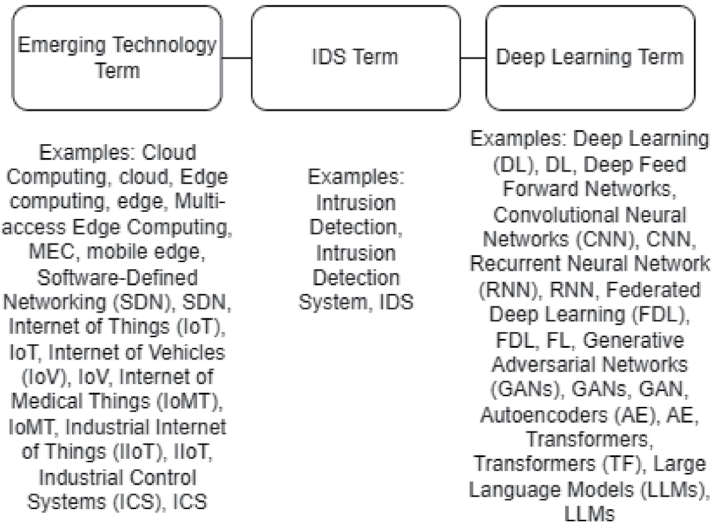

Fig. 1 Approach adopted to search for relevant papers on Google Scholar

lenges of this research field, while section 6 presents the conclusion of this research. Table 3 lists the acronyms used in this research.

2 Intrusion detection in emerging technologies

Intrusion detection refers to the ability to identify abnormal, unauthorized, and malicious activities in computational systems (Aldweesh et al. (2020); Gümüşbaş et al. (2020)). The demand for new technologies poses a challenge in detecting intrusions, emphasizing the need for advanced analytical solutions. This section introduces the concepts of intrusion detection and emerging technologies.

2.1 Intrusion detection systems (IDS)

The current cyberattack landscape threatens the secure operation of businesses and enterprises. A standard practice is to deploy security solutions that prevent invasions and block unwanted traffic from external networks. However, these preventive measures are limited and cannot completely avoid malicious activities (e.g., through the exploitation of unknown vulnerabilities by attackers or malicious activities of legitimate users). In this context, detecting intrusion represents another layer of security based on the analysis of the topology behavior (Patel et al. (2010)).

Intrusion Detection Systems (IDS) represent a class of methods and solutions focused on detecting malicious and unwanted activities in a particular system (Bace et al. (2001)). IDS can present several configurations and have drastically evolved over the last few decades. Threat actors aim to disrupt applications' availability, compromise privacy, and disrupt confidentiality. Malicious activities present characteristics that can be detected by different methods, e.g., statistical, distance-based, rule-based, profile-based, Machine Learning

Table 3 List of Acronyms

Acronym	Meaning	Acronym	Meaning
AE	Autoencoder	**IoT**	Internet of Things
AI	Artificial Intelligence	IoV	Internet of Vehicles
APSO	Adaptive Particle Swarm Optimization	IT	Information Technology
BiLSTM	Bidirectional Long Short-Term Memory	LIME	Local Interpretable Model-agnostic Explanations
CAN	Controller Area Network	LSTM	Long Short-Term Memory
CIA	Confidentiality, Integrity, and Availability	MEC	Multi-access Edge Computing
CNN	Convolutional Neural Network	ML	Machine Learning
DDoS	Distributed Denial of Service	MAE	Mean Absolute Error
DL	Deep Learning	MQTT	Message Queuing Telemetry Transport
DNN	Deep Neural Network	MSE	Mean Squared Error
DNS	Domain Name System	NGN	Next Generation Network
DoS	Denial of Service	NSAI	Neurosymbolic Artificial Intelligence
ELU	Exponential Linear Unit	PaaS	Platform as a Service
FDL	Federated Deep Learning	PCA	Principal Component Analysis
FL	Federated Learning	R2L	Remote to Local
GAN	Generative Adversarial Network	ReLU	Rectified Linear Unit
GRU	Gated Recurrent Unit	RNN	Recurrent Neural Network
ICS	Industrial Control Systems	RQ	Research Question
IDS	Intrusion Detection System	SaaS	Software as a Service
IIoT	Industrial Internet of Things	SDN	Software-Defined Networking
IaaS	Infrastructure as a Service	SHAP	SHapley Additive exPlanations
IF	Isolation Forest	TF	Transformers
IoMT	Internet of Medical Things	U2R	User to Root

(ML), and Deep Learning (DL) methods (Sabahi and Movaghar (2008)). This section presents the main aspects of each approach, illustrated in Fig. 2.

Distance-based methods focus on the spatial similarities between a new traffic pattern and a historical database (Said et al. (2011)). The main goal is to identify unusual features in a multidimensional space that may indicate a malicious activity (Verma and Ranga (2018)). In rule-based methods, users predefined a knowledge base to determine if a given traffic pattern pertains to normal behavior or a malicious activity (Lunt et al. (1989)). Although these methods were widely used in the past, the limited autonomous adaptability to new attacks and zero-day attacks are major shortcomings in system protection (Sabahi and Movaghar (2008)).

The dynamic topologies of current business operations involve the continuous adoption of new devices. In some applications, devices constantly change their local network connection (e.g., IoV). Profile-based methods identify characteristics and communication patterns of individual devices to establish a baseline for normal network behavior and malicious activities (Dadkhah et al. (2022)). In addition to that, statistical methods focus on the statistical aspects of normal operations and how they differ from malicious activities. The statistical models built can detect abnormal activities using univariate, multivariate, and temporal analysis (Khraisat et al. (2019)).

In recent years, the success achieved by ML models in multiple fields has motivated their use in the context of IDS. These techniques are used in different systems and leverage historical data to reveal underlying patterns in malicious traffic (Liu and Lang (2019)). In this context, Deep Learning (DL) represents a class of ML algorithms focused on complex classification problems with outstanding performance in several areas (Vinayakumar et al. (2019)). This research focuses on DL methods since they have enormous potential to solve critical cybersecurity issues while presenting major limitations in protecting real operations. The main focus of this research is to investigate state-of-the-art DL solutions that can be used in several emerging technologies, which are introduced in the next section.

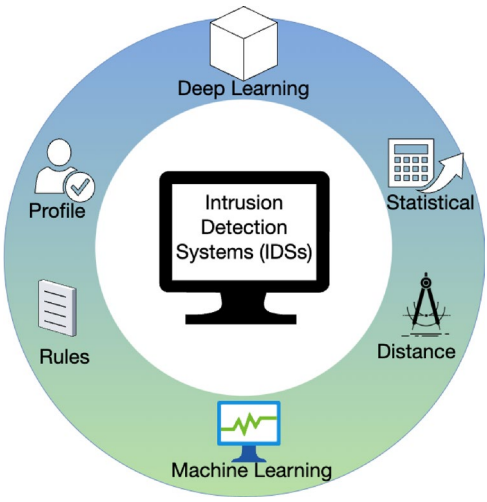

Fig. 2 Detection methods used in Intrusion Detection Systems (IDS)

2.2 Emerging technologies

The constant need for optimized services in different industries establishes the requirement for continuous technological improvement and the creation of new computing methods. Emerging technologies represent technological concepts adopted by various organizations or present in their near-future strategic roadmap. These new business enablers bring connectivity, increased efficiency, and personalized user experience, and help define new business opportunities. This section presents prominent emerging technologies for modern enterprise infrastructures.

2.2.1 Cloud computing

This technology comprises resources (e.g., applications, servers, networks, storage) accessible over a remote and distributed topology (Gong et al. (2010)). It enables distributed applications to rely on a centralized computing pool that empowers advanced analytics, real-time solutions, and ubiquitous computing (Jadeja and Modi (2012)). Although researchers have been working to develop cloud concepts for many years, there is still a transition of business operations from local applications to cloud environments (e.g., government agencies and large corporations). In fact, cloud computing is user-centric, task-centric, and programmable (Mirashe and Kalyankar (2010)). In this context, Software-as-a-Service (SaaS) enables users to access software applications remotely with different purchasing methods (e.g., on-demand). Platforms-as-a-service (PaaS) refers to establishing technologies that can be used to develop solutions while simplifying the environment setup. Finally, Infrastructure-as-a-Service (IaaS) relies on enabling users to remotely access virtualized computing resources (e.g., storage) (Mahmood (2011); Stanoevska-Slabeva and Wozniak (2010)). In this context, DL can improve the protection of cloud environments through the analysis of large-scale traffic and user connections to reveal underlying patterns of complex attacks (e.g., ATPs). Figure 3 shows the cloud computing architecture.

Alongside the benefits cloud computing offers to end users, there are several security challenges to consider. The attack surface comprises SaaS, PaaS, and IaaS. SaaS presents application-level security concerns, including injection, cross-site scripting, and internal APIs' vulnerabilities. PaaS includes different potential vulnerabilities stemming from

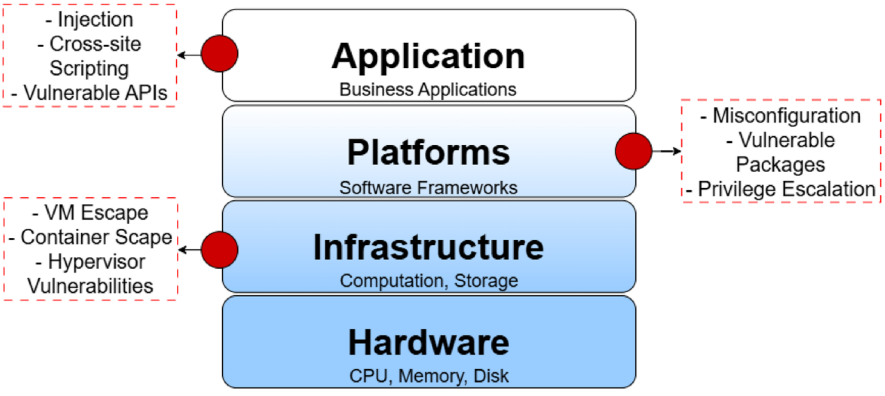

Fig. 3 Cloud Computing Architecture (Zhang et al. (2010)) and attack surface

misconfiguration, unsecured packets installed and deployed, and potential unauthorized privilege escalation. Finally, attackers target IaaS in different ways, including escaping virtualized resources and exploiting vulnerable hypervisors.

2.2.2 Edge computing

Edge computing represents a novel approach to remote computing by deploying computational resources closer to the end users (Cao et al. (2020); Mao et al. (2017)). The edge computing concept relies on placing solutions in between the centralized cloud architecture and the end users (Chen and Ran (2019)), reducing response time (Tang et al. (2021)) and increasing scalability (Satyanarayanan (2017)). This simplified access to computational resources empowers advanced analytics solutions in many areas, e.g., healthcare (Abdellatif et al. (2019)) and transportation (Lin et al. (2020)). Although edge computing has been a trending research topic for over a decade, there are still several challenges in its efficient deployment and adoption. However, there are challenges to be addressed to ensure efficient edge operations, including offloading and resource allocation (Mach and Becvar (2017); Tran and Pompili (2018)), security and privacy (Ranaweera et al. (2021)), and load balancing (Zhang et al. (2019)). Figure 4 illustrates the general edge computing architecture. In terms of cybersecurity, the edge computing attack surface comprises northbound communication vulnerabilities, southbound communication vulnerabilities, and edge core (including misconfiguration and unpatched software). Northbound communication is susceptible to attacks that target the exchange between edge and cloud servers, whereas in southbound communication, attackers target weaknesses in the data exchange between edge servers and end users.

2.2.3 Internet of things (IoT)

The current society's demand for optimized services requires deploying sensors and actuators across smart cities (Zanella et al. (2014)). These devices enable advanced analytics to leverage computing resources to provide solutions in different areas (e.g., healthcare and transportation) (Talari et al. (2017)). The Internet of Things (IoT) relies on empowering general devices (e.g., sensors and actuators) to produce, share, and consume information from multiple sources and devices (Atzori et al. (2010); Wu et al. (2010)). IoT has been adopted in several areas, including the Internet of Vehicles (IoV), the Internet of Medical

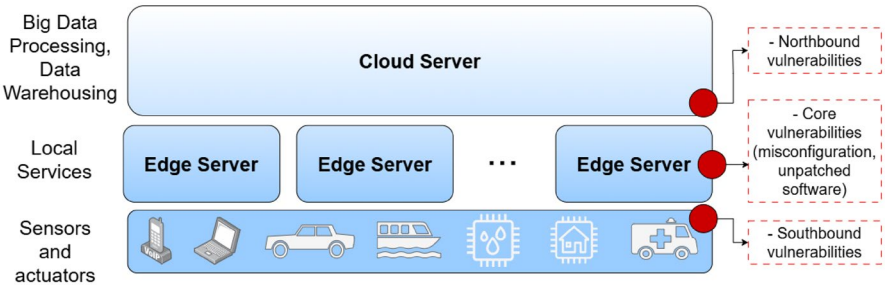

Fig. 4 Edge Computing Architecture (Cao et al. (2020); Kong et al. (2020); Kadhum et al. (2019)) and attack surface

Things (IoMT), and the Internet of Industrial Things (IIoT). In healthcare, IoMT deploys devices across hospitals and remote treatment facilities that simplify continuous health measurements, infusion, and medication control (Ghubaish et al. (2020)). In transportation, IoV allows motorized vehicles to improve the driving experience and safety levels by collecting operational data, establishing intra- and inter-vehicle communication, and enabling the interaction of vehicles, pedestrians, and Roadside Units (RSU) (Ji et al. (2020); Contreras-Castillo et al. (2017)). In industrial settings, IIoT enables various devices to support industrial processes while maintaining awareness and integration across multiple devices (Boyes et al. (2018)). Hence, although DL has successfully detected intrusion in IoT environments in the past few years, the development of new devices and complex topologies (e.g., cyber-physical applications) paves the way for new DL applications. Figure 5 illustrates devices adopted in IoT, IoV, IoMT, and IIoT solutions. Regarding areas that attackers can exploit, IoT presents vulnerabilities in the communication in the network and in the devices' characteristics. In terms of communication, IoT may adopt protocols with inappropriate security mechanisms, be susceptible to flooding attacks, and rely on vulnerable bridge components (for example, Zigbee and Z-Wave). Also, some devices present a reproducible pattern that enables impersonation in an IoT environment.

2.2.4 Software-defined networking (SDN)

This novel networking paradigm focuses on separating network control from network packet forwarding, establishing an environment that can be programmed and adapted to the business need (Kreutz et al. (2014); Xia et al. (2014)). This architecture establishes three main layers. The first includes the application layer and allows organizations to programmatically deploy solutions, policies, and flexible rules to orchestrate the network operation (Jarraya et al. (2014)). These applications communicate with the next layer, the control layer. In this process, the controller receives the inputs provided by the applications and performs the actual changes in the topology based on the business requirements (Medved et al. (2014); Berde et al. (2014); Gude et al. (2008)). Finally, the infrastructure layer integrates the network devices and is responsible for the network operations. DL can overcome security challenges by capturing abnormal patterns in multidimensional spaces while relying on temporal and generative capabilities (Novaes et al. (2021); Tang et al. (2020)). Figure 6

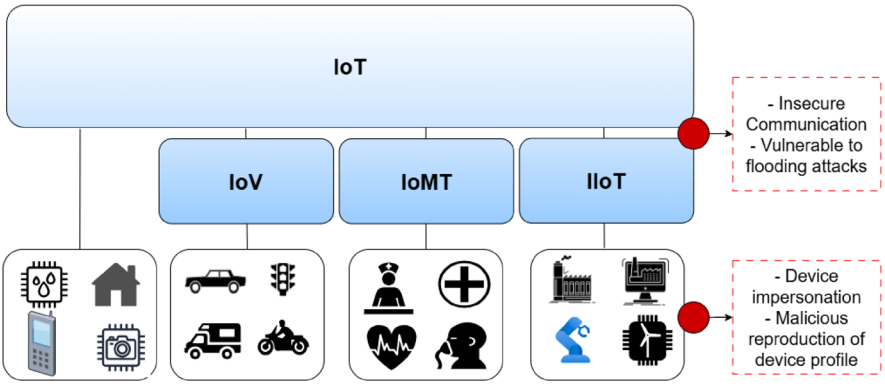

Fig. 5 Devices adopted in IoT, IoV, IoMT, and IIoT solutions, and attack surface

illustrates the SDN technology architecture, highlighting the main layers and their purposes. The exploitation of this technology could happen in any layer. The application layer may present high-level application vulnerabilities. The control layer may present insecure communication with applications and devices, as well as a lack of authentication mechanisms. Finally, the infrastructure layer is susceptible to physical access and spoofing attacks.

2.2.5 Muti-access edge computing (MEC)

Nowadays, several applications are used on mobile devices daily. The amount of traffic generated increases rapidly (Mejia et al. (2020)) and results in the requirement for more robust topologies that can handle such a volume of data. Moreover, mobile networks represent an important wireless means through which mobile devices exchange data. In this context, Multi-access Edge Computing (MEC) represents an edge technology that enables providers to extend their topologies to attend to new networking and application demands (Filali et al. (2020)). In the context of this research, although MEC and edge computing present many similarities, MEC focuses on cellular networks and mobile devices with specific protocols and technologies (e.g., 4 G and 5 G) (Shahzadi et al. (2017)). This concept relies on improving networking operations and user experience by moving cloud-based solutions closer to cellular networks and their applications (Porambage et al. (2018)). Thus, DL plays a major role in the protection of MEC given the dynamic and continuously evolving topologies, the complexity of MEC applications, and the real-time requirements. Figure 7 shows the general MEC architecture. Similarly to edge computing, the MEC architecture may present vulnerabilities in different layers. Attacks could exploit the communication between MEC and core servers as well as the communication between MEC servers and end users. Also, the application vulnerabilities inside MEC server can also be exploited, emphasizing the importance of adopting a holistic detection approach to ensure secure operations.

2.2.6 Industrial control systems (ICS)

The need for more efficient solutions in the industrial setting has motivated the development of more efficient technologies to control such environments (Kriaa et al. (2015)). In this sense, Industrial Control Systems (ICS) represent the new industrial paradigm in which Information and Communication Technology (ICT) is integrated into industrial processes (McLaughlin et al. (2016)), enabling more granular control over multiple industrial com-

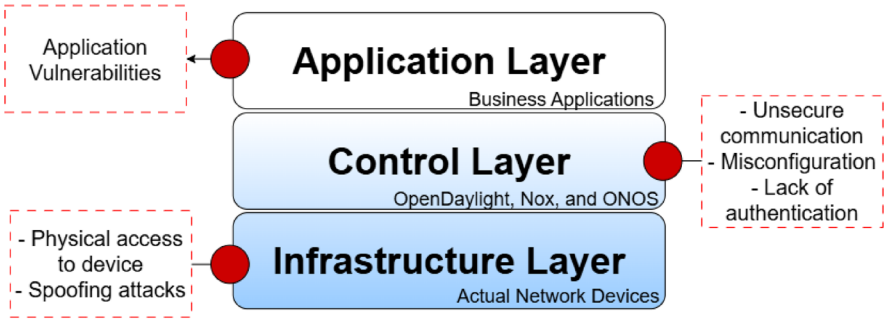

Fig. 6 SDN Architecture (Kreutz et al. (2014); Xia et al. (2014)) and attack surface

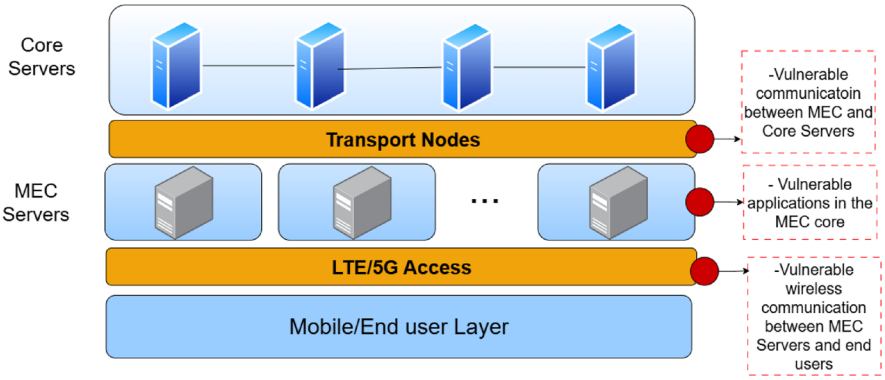

Fig. 7 Multi-Access Edge Computing (MEC) Architecture (Filali et al. (2020); Porambage et al. (2018); Liyanage et al. (2021)) and attack surface

ponents. In fact, ICS supervises industrial processes leveraging different technologies (e.g., Programmable Logic Controllers - PLCs - and Supervisory Control and Data Acquisition - SCADA) (Alladi et al. (2020)). In the past few years, there has been an increasing concern regarding the cybersecurity aspects of ICS and a growing demand for advanced cybersecurity solutions (Bhamare et al. (2020); Knowles et al. (2015)). The critical operations considered in ICS can be further protected using DL. The challenges of combining operational data (e.g., sensors) with network traffic can be tackled by multiple DL models to identify anomalous behaviors at scale. Figure 8 shows the general ICS architecture. All the layers depicted present vulnerabilities that can be exploited by malicious actors. The control center may present a lack of authentication and inappropriate network segmentation, exposing critical systems. The communication layer may suffer from weak encryption and vulnerable protocols. Finally, the devices can also be targeted by attackers since they can be physically accessed and present unpatched firmware.

All these emerging technologies enhance business operations and bring new opportunities to tackle real-world problems. Figure 9 presents the taxonomy of attack surface for emerging technologies explained in this section. The following sections introduce datasets and DL solutions for intrusion detection in emerging technologies.

3 State-of-the-art intrusion detection datasets

The development of advanced intrusion detection capabilities is a major requirement for modern business operations. This section reviews intrusion detection datasets that could empower DL models for intrusion detection in emerging technologies (i.e., cloud computing, edge computing, Internet of Things, Software-Defined Networking, Multi-Access Edge Computing, and Industrial Control Systems).

3.1 Cloud, edge, and multi-access edge computing

The development of realistic cybersecurity benchmark datasets for cloud, edge, and multi-access computing is complex and requires extensive topologies. Although there is a lack

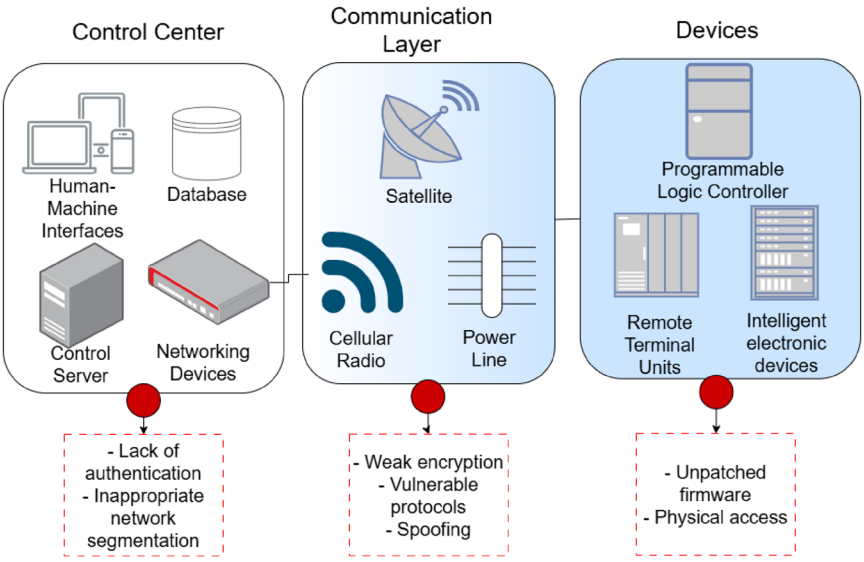

Fig. 8 General ICS architecture introduced by McLaughlin et al. (2016) and attack surface

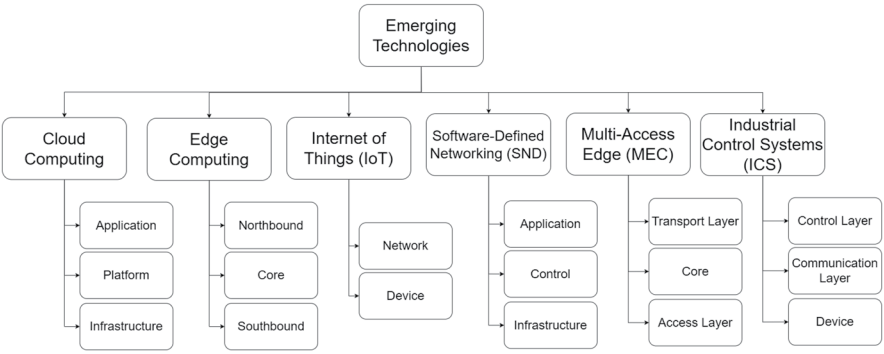

Fig. 9 Taxonomy of attack surface for emerging technologies

of security benchmarking resources for these technologies, some datasets published can be used to model specific areas and guide the development of new datasets. KDD Cup 99 (Tavallaee et al. (2009)) is one of the first IDS datasets. Based on the traffic capture at the DARPA'98 project (McHugh (2000)), this dataset has been widely used for IDS development and adapted to different environments. By adopting a simulated topology, the KDD Cup 99 presents 41 features and four attacks (i.e., DoS, User to Root (U2R), Remote to Local (R2L), and Probing). Furthermore, NSL-KDD is proposed as a way of addressing the limitations of the KDD Cup 99, e.g., the lack of realism in the simulated traffic and definition of attack scenarios.

Sharafaldin et al. (2018) introduce the CICIDS2017 dataset as an up-to-date benchmark for IDS solutions. To accomplish this, a topology of real devices was adopted and several attacks were launched following a pre-defined schedule. The authors used multiple tools to

generate, capture, and process the network traffic, and the data can be accessed in different formats. The CIDDS dataset (Ring et al. (2017)) aims to propose a new method to leverage OpenStack for producing realistic IDS data. The authors rely on the use of virtual environments to connect hosts and conduct attacks. This research allows the reproduction of new attacks, considering topology definition, labeling, and data collection.

Maciá-Fernández et al. (2018) present a new IDS dataset based on the shortcomings of existing solutions using real traffic and recent threats. The main aspect that distinguishes the UGR '16 dataset from others is the temporal evaluation. The authors state the clear goal of enabling the long-term evaluation of IDS solutions that comprise periodicity. Creech and Hu (2013) present the ADFA Linux dataset (LD) as an effort to support the development of host-based IDS based on system call patterns. The main goal is to use low-level metrics (e.g., kernel-level calls) to enhance the detection capabilities of high-level malicious activities.

The Kyoto 2006+ dataset (Song et al. (2011)) contains three years of network traffic and extends KDD Cup 99 dataset in different ways. The main goal of this research is to provide IDS researchers with practical and realistic data for the rigorous evaluation of IDS solutions. The topology comprises multiple computers (e.g., Windows and MAC) and attacks (e.g., malicious P2P connection requests, SYN scanning, SYN flooding, backscatters). Kolias et al. (2015) introduce the Aegean WiFi Intrusion Dataset (AWID) to support the development of IDS solutions for wireless networks considering 802.11 traffic. This dataset comprises 15 attacks, namely fragmentation and ARP injection, probe request, deauthentication, ChopChop, malicious request, RTS, disassociation, beacon, flooding, evil twin and caffe latte impersonation, CTS, fake power saving, and hirte attacks.

Sharafaldin et al. (2019) propose a new dataset, named CICDDoS2019, focused on reproducing realistic Distributed Denial of Service (DDoS) attacks in traditional networks. The authors present an agenda of attack execution against a real testbed composed of computers, servers, and networking devices. Several attacks are launched and the data for different attack times is collected. A correlated work is presented by Shiravi et al. (2012), where the authors target the generation of a realistic IDS dataset called ISCXIDS2012. The authors highlight important features present, including labeling, captures of complete interactions, and diversity in the intrusion approaches.

Some efforts focus on generating IDS datasets for 5 G networks, highlighting their relevance in the context of MEC. Coldwell et al. (2022) present the 5GAD-2022 dataset to support the development of next-gen IDS solutions. Relying on a simulated topology, the experiments consider the execution of multiple attacks. In Samarakoon et al. (2022), the 5 G-NIDD dataset is presented as an IDS benchmark for 5 G networking based on a real topology. The authors present an in-depth description of how the data is captured, the attacks performed, and the details of the topology.

In Moustafa and Slay (2015), the authors combine existing attacks and approaches with novel trends to generate a realistic IDS dataset named UNSW-NB15. The simulated topology adopted contains 45 distinct IP addresses and the traffic collected is stored in PCAP files. In addition, the WUSTL IDS dataset results from network traffic of benign and malicious activities in an industrial environment (Teixeira et al. (2018)). The authors replicate an industrial topology by adopting a water storage tank infrastructure.

Table 4 depicts in chronological order the datasets used to train DL solutions for cloud computing, edge computing, and MEC. We specify the goal of each dataset, the number

of features extracted, the testbed used, the attacks performed, and whether the topology is simulated or comprises real devices. This table offers insights on how the datasets could be effectively used in real scenarios. KDD Cup 99, NSL-KDD, and Kyoto 2006+ represent traditional datasets, developed several years ago and used by many researchers. However, they present limitations regarding the types of attacks and the characteristics of the environment deployed. ISCXIDS2012, UNSW-NB15, and CIC-DDoS2019 are subsequent efforts that allow the evaluation of flooding detection and mitigation studies. To address the need for datasets with specific technology constraints, ADFA-LD and AWID enable the evaluation of host-specific and wireless intrusion detection. After these datasets were published, the protection of other types of attacks gained importance and fostered the production of new solutions. Therefore, UGR'16, CICIDS2017, CIDDS-001, WUSTL IDS were designed to meet the demand for the evaluation of solutions for multiple attacks, comprising a plurality of recent threats. In the past few years, new technologies have offered improved communication and computational capabilities. WUSTL EHMS, 5GAD-2022, and 5 G-NIDD are datasets focused on next-gen systems, acting on the forefront of cybersecurity aspects and enabling the development of novel solutions. Figure 10 categorizes these datasets in terms of their applicability, providing a path to select the dataset to use and to evaluate generalization depending on the research goals. Finally, similar efforts have targeted IoT and ICS, which are the focus of the next section.

3.2 Internet of things (IoT) and industrial control systems (ICS)

Many research projects have targeted the development of realistic datasets in the context of IoT. Regarding cybersecurity, works are focused on healthcare, transportation, and industrial operations, also relevant to ICS research. Koroniotis et al. (2019), the Bot-IoT dataset is introduced as an effort to generate malicious network traffic in an IoT environment. The authors rely on a combination of real and simulated devices and execute several attacks against the topology. This dataset is widely used for developing IDS solutions in the IoT context. Similarly, given that many research efforts focus on outdated datasets that do not entail trending technologies and cyberattacks, Gad et al. (2021) introduce ToN-IoT to enable the evaluation of IDS solutions in the context of IoT and IIoT. To accomplish this, a large IoT network is adopted and several attacks are executed.

The Edge-IIoTset (Ferrag et al. (2022)) is an IDS dataset for IoT and IIoT applications. The attacks executed include DoS, DDoS, Information gathering, Man-in-the-middle, Injection, and Malware. The main objective is to support IDS solutions in this environment by deploying a large representative group of IoT and IIoT devices. Meidan et al. (2018) introduce a novel IoT dataset using real devices called N-BaIoT. By adopting a real topology, this effort motivated other initiatives in the IoT IDS domain while focusing on the execution of Mirai and BASHLITE. However, the real topology is composed of a limited number of devices, which differs from real IoT deployments. Dadkhah et al. (2022) focus on interactions among IoT devices to profile the overall network behavior. The CICIoT2022 relies on the use of a real IoT network with devices of different categories. The main goal is to foster the development of IDS solutions from a behavioral standpoint by creating profiles and detecting unusual patterns in the IoT traffic. Furthermore, Neto et al. (2023) present the CICIoT2023 as an extensive IoT security dataset comprising 105 IoT devices and launching 33 attacks grouped into DoS, DDoS, Recon, Web-based, brute force, spoofing, and mirai.

In terms of Internet of Vehicles (IoV), IDS datasets were also proposed. The CICIoV2024 (Neto et al. (2024)) is a dataset developed to support the evaluation of IoV IDS solutions. The authors use a real testbed composed of the internal components of a 2019 Ford car. Several attacks are launched against the vehicle considering the CAN protocol. The attacks are categorized into spoofing and DoS and were executed via CAN Bus. Another effort is the car hacking dataset (Seo et al. (2018)), which adopts a Hyundai YF Sonata as a testbed. The authors execute a different group of attacks (i.e., DoS, fuzzing, and spoofing) and evaluate their effect on the vehicle while capturing the network traffic. This contribution sheds light on the vulnerabilities of a specific model to foster the development of appropriate security mechanisms. Besides, Lee et al. (2017) use a KIA Soul to produce an IDS dataset for IoV called CAN Dataset for intrusion detection (OTIDS). In terms of attacks, DoS, fuzzing, and impersonation are performed against the vehicle's internal components. Similarly, this contribution targets the development of new IDS solutions for in-vehicle networks. Furthermore, the Real ORNL Automotive Dynamometer (ROAD) CAN Intrusion dataset is presented by Verma et al. (2020). The approach considers a similar testbed but includes new attacks that are executed against the vehicle units. Finally, Kim et al. (2023) propose a dataset comprising DDoS attacks against Electric Vehicle (EV) authentication in the charging infrastructure. The data is collected based on a simulation of different components in the EV operation.

Dadkhah et al. (2024) present an extensive security dataset focused on IoMT operations. In this effort, 18 attacks (categorized into DDoS, DoS, Recon, MQTT, and spoofing) are performed against the IoMT network. In fact, the topology is composed of 40 IoMT devices, of which 25 are real and 15 are simulated. The goal of this research is to propose a multi-protocol dataset to mimic real IoMT operations (i.e., Wi-Fi, Bluetooth, and MQTT). Besides, the authors introduce IoMT profiling focused on detecting anomalies in the network. The WUSTL-EHMS-2020 dataset (Hady et al. (2020)) is an effort to improve the protection of medical systems and focuses on collecting network flows and biometrics. The authors employ a testbed composed of real devices and emphasize the importance of providing IDS solutions with domain-specific information to identify anomalies in medical systems. Ahmed et al. (2021) present a security dataset for the Internet of Medical Things (IoMT) called ECU-IoHT. The main focus is on supporting the development of robust countermeasures for cyber attacks against IoMT deployments. However, a limited topology based on real devices is considered. In Zubair et al. (2022), BlueTack is introduced as the first dataset to support Bluetooth-based IDS solutions in IoMT environments. This study brings important insights into the importance of Bluetooth protection in the medical space and how such systems can be replicated in a controlled environment. The increasing complexity of system operations creates the need for advanced solutions to detect abnormal activities. Conversely, although the topology adopted includes real IoMT devices, the types of devices considered are limited and do not represent a realistic medical system. The ICU dataset (Hussain et al. (2021)) is another project to enable IDS development in the medical space. The authors rely on the use of IoTFlock to generate IoMT traffic while adopting several devices in the testbed. This study not only fosters security solutions but also sheds light on how simulation can be useful for IoT security.

Moreover, there are applications in enterprise networks that rely on specific protocols. Radoglou-Grammatikis et al. (2021) target the development of a security dataset for the IEC 60 870-5-104 protocol, which is designed for industrial healthcare systems. This dataset

Table 4 Summary of widely used IDS datasets in the context of Cloud, Edge, and MEC

Dataset	Year	Goal	# Features	Testbed	Attacks	Topology
KDD Cup 99 Tavallaee et al. (2009)	1999	One of the first datasets for general IDS	41	Enterprise Network	DoS, User to Root (U2R), Remote to Local (R2L), Probing	Simulated
NSL-KDD Tavallaee et al. (2009)	2009	Extension of KDD Cup 99	42	Enterprise Network	DoS, User to Root (U2R), Remote to Local (R2L), Probing	Simulated
Kyoto 2006+ Song et al. (2011)	2011	Provide IDS researchers with practical and realistic data for rigorous evaluation of IDS solutions	24	Enterprise Network	Malicious P2P connection requests, SYN scanning, SYN flooding, backscatters	Real Devices
ISCXIDS2012 Shiravi et al. (2012)	2012	Provide an up-to-date benchmark for IDS solutions	21	Enterprise Network	Infiltrating, DoS, DDoS, and bruteforce	Real Devices
ADFA-LD Creech and Hu (2013)	2013	Uses low-level metrics (e.g., kernel-level calls) to enhance host-based detection capabilities of high-level malicious activities	Raw system call traces	Linux Host	Password Brute Force, OS attack, Application attack, Web attack	Real Device
UNSW-NB15 Moustafa and Slay (2015)	2015	Foster the development of IDS solutions combining existing attacks with novel trends	49	Enterprise Network	Fuzzing, DoS, Backdoor, and information gathering	Simulated
AWID Kolias et al. (2015)	2015	Support the development of IDS solutions for wireless networks considering 802.11 traffic	155	Wireless	fragmentation and ARP injection, probe request, deauthentication, ChopChop, malicious request, RTS, disassociation, beacon, flooding, evil twin and caffe latte impersonation, CTS, fake power saving, and hirte attacks	Real Devices
UGR'16 Maciá-Fernández et al. (2018)	2016	Enabling the long-term evaluation of IDS solutions that comprise periodicity	13	Enterprise Network	Low-rate DoS, Port scanning, Botnet traffic	Real/ simulated Devices
CICIDS2017 Sharafaldin et al. (2018)	2017	Develop a up-to-date benchmark for IDS solutions	85	Enterprise Network	Brute Force, Heartbleed, Botnet, DoS, DDoS, Web Attack, Infiltration	Real Devices
CIDDS-001 Ring et al. (2017)	2017	Novel approach to use OpenStack for generating realistic IDS data	14	Enterprise Network	Denial of Service, Brute Force, Ping Scans, and Port Scans	Simulated

Table 4 (continued)

Dataset	Year	Goal	# Features	Testbed	Attacks	Topology
WUSTL IDS Teixeira et al. (2018)	2018	Enable the development of IDS solutions In industrial environments (SCADA)	6	Enterprise Network	Port Scan, Address Scan, Device Identification, Exploitation	Real Devices
CIC-DDoS2019 Sharafaldin et al. (2019)	2019	Enable the development of IDS solutions specialized in different types of DDoS	80	Enterprise Network	DDoS (PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, SNMP, SSDP, Web, TFTP)	Real Devices
WUSTL EHMS Hady et al. (2020)	2020	Enabling the development of medical IDS based on both network and biometric metrics in IDS solutions	44	Enterprise Network	Data Alteration and Spoofing Attacks	Real Devices
5GAD-2022 Coldwell et al. (2022)	2022	Enable the development of Next-Gen IDS solutions using a simulated topology	PCAPNG	5 G Networks	5 G attacks - Reconnaissance, Network Reconfiguration, DoS	Simu-lated
5 G-NIDD Samarakoon et al. (2022)	2022	Enable the development of Next-Gen IDS solutions using a real topology	112	5 G Networks	ICMP flood, UDP flood, SYN flood, HTTP flood, Slowloris, Torshammer, Scanning, SYN Scan, TCP Connect Scan, UDP Scan	Real Devices

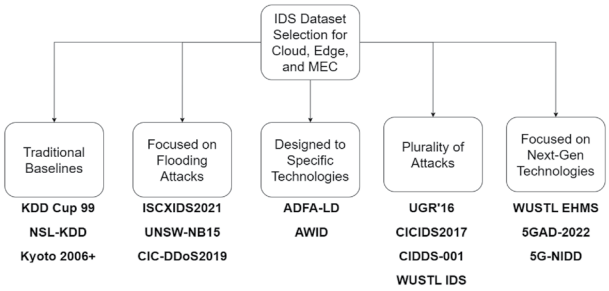

Fig. 10 Datasets applications in the context of Cloud, Edge, and MEC

observes the network requirements and security aspects of such an environment and presents traffic captured from attacks tailored to the IEC 60 870-5-104 operation. Mirsky et al. (2018) introduce Kitsune as a network IDS dataset using multiple IoT devices. This research targets the replication of a real IoT topology considering both scenarios a surveillance and an IoT network. This dataset is a precursor for many other IoT security efforts and highlights the importance of using real devices to capture realistic network traffic and device behavior. In Kang et al. (2019), a similar study is presented in which the authors use a real and small IoT topology to produce an IoT security dataset named IoTNIDS.

The MedBIoT dataset (Guerra-Manzanares et al. (2020)) consists of a collection of network traffic under normal and malicious circumstances using an IoT network of 83 IoT real and simulated devices. The topology is composed of a monitoring network, an Internet gateway, and the local IoT LAN network. The main focus of this initiative is to reproduce the behavior of botnet malware in a controlled environment (i.e., Mirai, Bashlite, Torii). Similarly, the authors in Garcia et al. (2020) introduce the IoT-23 dataset targeting the generation of an IoT security dataset based on malware execution and malicious traffic. The authors launched several IoT malware-based attacks, including Mirai, Trojan, Hajime, and Muhstik. In this case, IDS researchers can focus on up-to-date IoT threats when developing security solutions. In addition to that, MQTT-IoT-IDS dataset is presented by Hindy et al. (2020) with a special focus on the MQTT protocol. The authors adopt a simulated topology to generate and capture data and emphasize the benefits of having an MQTT-based benchmark for IDS solutions.

Table 5 presents the datasets designed and used to develop and evaluate IoT and ICS solutions. In these environments, Bot-IoT, N-BaIoT, Kitsune, and IoTNIDS represent the initial works in the field and traditional baselines used by several researchers, enabling a comparison of new solutions with multiple efforts. Some datasets are focused on threats and technologies specific to this environment. This is the case of MedBIoT, IoT-23, and MQTT-IoT-IDS. In the past few years, there has been an increasing demand for datasets with extensive testbeds and multiple attacks. The CICIoT2022 and the CICIoT2023 were designed for this purpose. Regarding IoV, OTIDS and the Car Hacking dataset are referred to as the baselines in this field. A few years after that, extensions to new environments have been developed, including new attacks and testbeds, e.g., ORNL and CICIoV2024. In recent years, the popularity of Electric Vehicles (EVs) has motivated the development of the CICEV2023 dataset.

The development of solutions for IoMT can also focus on traditional baselines that represent initial proposal in the area (i.e., ECU-IoHT and ICU), target problems involving medical-specific technologies (i.e., IEC and BlueTack), or consider an extensive testbed

Table 5 Summary of widely used IDS datasets in the context of IoT and ICS

Dataset	Year	Goal	# Features	Testbed	Attacks	Topology
OTIDS Lee et al. (2017)	2017	Support of new IDS solutions for specific vehicle models	12	IoV	DoS, Fuzzying, and impersonation	Real Car
Car Hacking Seo et al. (2018)	2018	Support of new IDS solutions for specific vehicle models	12	IoV	DoS, Fuzzying, and spoofing	Real Car
Bot-IoT Koroniotis et al. (2019)	2018	Generation of legitimate and simulated malicious IoT network traffic	46	IoT	Port Scanning, OS fingerprinting, DoS, DDoS, Data theft, keylogging	Real Devices
N-BaIoT Meidan et al. (2018)	2018	One of the first efforts regarding IDS for IoT	115	IoT	Mirai and BASHLITE	Real Devices
Kitsune Mirsky et al. (2018)	2019	Support the development of IDS solutions in surveillance and home automation network	115	IoT	OS Scan, Fuzzing, Video Injection, ARP MITM, Active Wiretap, SSDP Flood, SYN DoS, SSL Renegotiation, Mirai	Real
IoTNIDS Kang et al. (2019)	2019	Support the development of IoT IDS solutions with a small topology	PCAP	IoT	Multiple mirai attacks, Host Discovery, ARP Spoofing, SYN flooding, port scan, OS scan	Real
MedBIoT Guerra-Manzanares et al. (2020)	2020	Evaluation of security solutions for IoT botnet malware	100	IoT	Mirai, Bashlite, Torii	Real/ simu-lated
IoT-23 Garcia et al. (2020)	2020	Enable the development of up-to-date IoT security solutions for malware	21	IoT	Mirai, Torii, Trojan, Gagfyt, Kenjiro, Okiru, Hakai, IRCBot, Linux Hajime, Muhstik, Hide&Seek	Real
MQTT-IoT-IDS Hindy et al. (2020)	2020	Enable the development of MQTT IDS solutions in IoT	44	IoT	Aggressive Scan, UDP scan, SSH Brute Force, MQTT brute force	Simu-lated
ORNL Verma et al. (2020)	2020	Support of new IDS solutions for specific vehicle models	25	IoV	Fuzzing, Targeted ID fabrication, and accelerator	Real Car
ECU-IoHT Ahmed et al. (2021)	2021	Support the development of robust countermeasures for cyber attacks against IoMT deployments	9	IoMT	Scanning, ARP poisoning, DoS, Smurf, and Script Injection	Real Devices
ICU Hussain et al. (2021)	2021	Enable IDS development for IoMT using simulated traffic	52	IoMT	MQTT Publish Flood, MQTT Authentication Bypass, MQTT Packet Crafting, and COAP Replay	Simu-lated

Table 5 (continued)

Dataset	Year	Goal	# Features	Testbed	Attacks	Topology
IEC Radoglou-Grammatikis et al. (2021)	2021	Support security solutions focussed on the IEC 60 870-5-104 protocol	203	IoMT	MITM, Traffic Sniffing, DoS, Unauthorized Access	Simulated
TON_IoT Gad et al. (2021)	2021	Establishing a realistic IoT and IIoT security dataset based on a heterogeneous network	7	IoT/IIoT	Scanning, Cross-Site Scripting, DoS, DDoS, Backdoor, Injection, Password Cracking, Man-In-the-Middle (MITM), Ransomware	Real Devices
Edge-IIoT Ferrag et al. (2022)	2022	Support IDS solutions in IoT and IIoT by deploying a large and representative topology	61	IoT/IIoT	DoS, DDoS, Information gathering, Man-in-the-middle, Injection, and Malware	Real Devices
CICIoT2022 Dadkhah et al. (2022)	2022	Enabling profiling-based IDS solutions	48	IoT	Flood and RTSP Brute Force	Real Devices
BlueTack Zubair et al. (2022)	2022	First dataset to support Bluetooth-based IDS solutions in IoMT environments	21	IoMT	DDoS, Bluesmack, MITM, and DoS	Real Devices
CICIoT2023 Neto et al. (2023)	2023	Extensive IDS dataset with 103 devices and 33 attacks	47	IoT	DoS, DDoS, Recon, Web-based, brute force, spoofing, and mirai	Real Devices
CICEV2023 Kim et al. (2023)	2023	Support IDS solutions for Electric Vehicles (EVs)	7	IoV	EV authentication DDoS	Simulated
CICIoMT2024 Dadkhah et al. (2024)	2024	Evaluation of IDS solution in IoMT environment using different Protocol and Profiling	44	IoMT	DDoS, DoS, Recon, MQTT, and spoofing	Real Devices
CICIoV2024 Neto et al. (2024)	2024	Support of new IDS solutions for specific vehicle models	12	IoV	Spoofing and DoS	Real Car

with multiple attacks (i.e., CICIoMT2024). In the case of IIoT, there is still a gap in the development of datasets that cover specific applications. However, existing high-quality efforts can be used as baselines - the TON IoT and Edge-IIoT datasets. Figure 11 categorizes these datasets in terms of their applicability based on the research goals. Finally, researchers have also focused on SDN initiatives, which are presented in the next section.

3.3 Software-defined networking (SDN)

Regarding Software-Defined Networking (SDN), the development of new cybersecurity datasets requires the deployment of a specific networking paradigm (e.g., separation of infrastructure, control, and application layers). The authors in Yungaicela-Naula et al. (2023) introduce a dataset composed of network traffic of SDN-SlowRate-DDoS attacks against an SDN topology called SDN-SlowRate-DDoS dataset. By adopting real devices in an SDN topology, the main focus of this work is to enable security researchers to develop solutions for SDN-SlowRate-DDoS attacks as well as to motivate the evaluation of solutions for similar threats. A similar effort is presented by Ahuja et al. (2020), in which the authors use a simulated topology to generate a security dataset focused on DDoS (DSAD). The authors define simulated scenarios and an execution plan and collect the network traffic generated in the process.

InSDN (Elsayed et al. (2020)) is one of the first comprehensive efforts toward producing an IDS dataset for SDN. The authors focus on presenting an in-depth description of the process followed to establish the SDN topology, attack planning and execution, and data analysis. This dataset is widely used by the SDN community and can be used as a benchmark for security solutions in this domain.

Table 6 presents the datasets dedicated to capturing malicious behaviours in the context of SDN. As illustrated in Fig. 12, the DDoS SDN Attack Dataset and the SDN-SLOW-

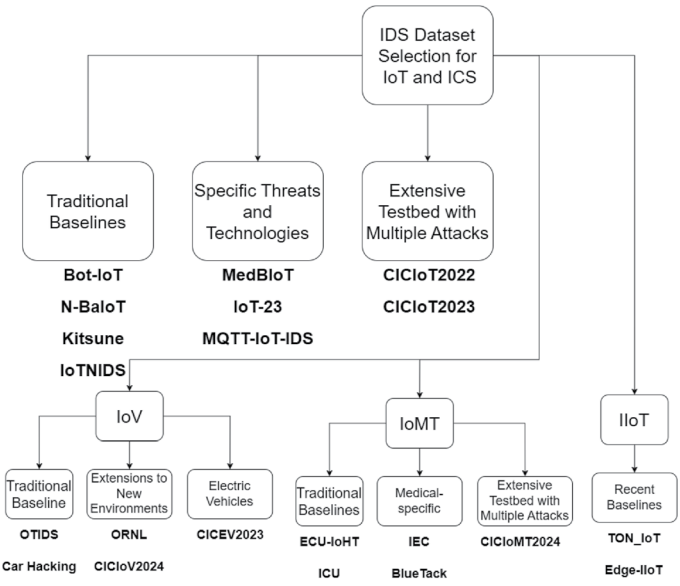

Fig. 11 Datasets applications in the context of IoT and ICS

Table 6 Summary of widely used IDS datasets in the context of SDN

Dataset	Year	Goal	# Features	Testbed	Attacks	Topology
DSAS Ahuja et al. (2020)	2020	Support the development of SDN security solutions using simulated topologies	26	SDN	TCP SYN flood, UDP Flood, ICMP flood	Simulated
InSDN Elsayed et al. (2020)	2020	Extensive IDS dataset for SDN	37	SDN	DoS, DDoS, Web Attacks, R2L, Malware, Probe, U2R (exploitation), and SDN attacks (e.g., LFA)	Simulated
SDN-SLOW-RATE-DDOS Yungaicela-Naula et al. (2023)	2023	Enable security researchers to develop SDN-based IDS solutions for DDoS attacks	13	SDN	DDoS	Real SDN Topology

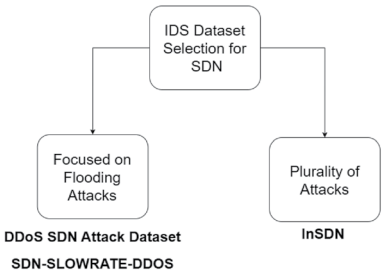

Fig. 12 Datasets applications in the context of SDN

RATE-DDOS dataset are designed to enable the evaluation of flooding attacks against these topologies. The InSDN dataset presents more attacks and can be used for other purposes.

Figure 13 presents the years in which these datasets have been released. Each white circle represents one year, and the elevation of the inclination of edges represents the time between the release of two distinct datasets. For example, KDD Cup 99 was published ten years before the NSL-KDD dataset. On the other hand, ISCXIDS2021 was released one year before ADFA-LD. As a result, these examples present different edge inclinations. Although these datasets enable IDS research to evaluate their solutions, there is still a need for new IDS datasets that target specific issues in network operations. For example, there is a lack of datasets that combine network and device behavior with business logic in specific domains. Finally, these datasets contribute to the development of new DL solutions, which is the focus of the next section.

4 State-of-the-art DL solutions for intrusion detection in emerging technologies

The remarkable success of DL techniques highlights their capabilities to solve complex problems. Detecting intrusion in emerging technologies is laborious and erroneous for several reasons (e.g., data complexity, the volume of benign and malicious traffic, and the con-

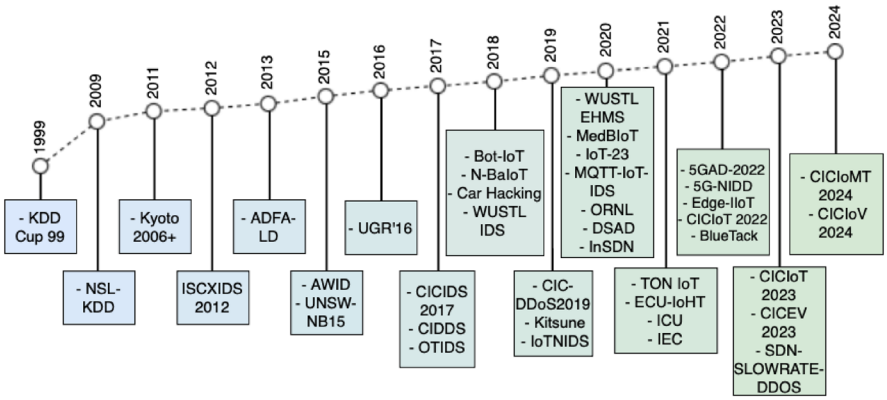

Fig. 13 Temporal evolution of IDS datasets

tinuous improvement of tailored attacks). In the past few years, research efforts addressed multiple intrusion detection limitations using DL. This section reviews such proposals while considering the aspects of each trending technological paradigm. For each category, we present a table depicting the characteristics of each contribution and highlight its immediate future directions.

4.1 Cloud computing

Many works focus on enhancing the protection of cloud computing. Abusitta et al. (2019) introduce a method for cooperation in IDS that leverages past outcomes to enable proactive decision-making in cloud environments. The authors adopt a Denoising Autoencoder to build a deep neural network and address the delay issues related to the aggregation of distributed feedback provided by multiple IDS. In fact, this approach enables the estimation of IDS feedback based on incomplete feedback. Archana et al. (2021) introduce a scalable strategy to reduce the False Positive Rate (FPR) in the context of intrusion detection. In fact, this is a major issue in the context of IDS since high false positives hinder the adoption of automated tools. The authors deploy this solution to the cloud with the ultimate goal of increasing availability and simplifying access for different users. Multiple DL methods are also evaluated, including DNN and RNN. Wang et al. (2020b) focus on optimizing intrusion detection based on the extraction of feature representations. As Deep Learning (DL) has presented outstanding capabilities regarding reframing input vectors to new representations that can yield important insights to classification problems, the authors leverage the power of autoencoders (i.e., Stacked Contractive Autoencoder - SCAE) to enable such insights to be discovered in the context of cloud intrusion detection.

Gao et al. (2022) introduces a technique to classify malicious network traffic in a cloud environment. A combination of CNN and BiLSTM is adopted after converting the KDD CUP 99 data to images. The author integrates a decision tree in the classification process and explains the main contributions in detail by demonstrating the superiority of the proposed technique over other state-of-the-art methods (i.e., AE-AlexNet and SGM-CNN). Alzughaibi and El Khediri (2023) rely on the combination of a DNN and Particle Swarm Optimization (PSO) to identify abnormal cloud activities using the CSE-CIC-IDS2018

dataset. The use of an evolutionary algorithm demonstrated efficiency improvements in the detection performance. In addition to this investigation, the authors in RM and MK (2023) utilize the same dataset to evaluate the performance of a stack of advanced algorithms for intrusion detection. The use of Principal Component Analysis (PCA), Smart Monkey Optimized Fuzzy C-Means algorithm (SMO-FCM), and an AutoEncoder enables the efficient classification of attacks.

Vu et al. (2022) present a strategy to improve the robustness of cloud IDS using generative models. The authors adopt the Conditional Denoising Adversarial Autoencoder (CDAAE) to produce malicious samples of multiple types and a combination of CDAAE and the k-NN to produce borderline instances. Another generative study is presented by Chkirbene et al. (2021), where the authors augment IDS data in the context of cloud computing. More precisely, an optimized GAN is adopted to produce trustworthy samples of minority classes to enhance the overall classification performance, which is verified in the experiments using the UNSW and NSL-KDD datasets. Finally, Long et al. (2024) introduce a cloud IDS solution based on a Transformer (TF) model, underlying the relationships between input features and intrusion types through the use of attention mechanisms. As a future direction, the authors indicate the extension of proposed capabilities to other systems (e.g., edge computing).

Table 7 compares solutions for cloud computing protection in terms of goal, DL techniques adopted, dataset used, attacks covered, limitations, future directions, and open challenges, in a chronological order. Table 8 compares the results obtained in each study. Although our focus is on capturing the accuracy, precision, and F1-score reported in the analysis tables of each work and presenting them succinctly, some papers adopt different metrics or do not directly present them in evaluation tables. In this case, the values are denoted by $*$. Also, the values presented are the highest results achieved in the multiple experiments researchers describe.

4.2 Edge computing

Edge computing is also a major target of attackers and requires advanced intrusion detection capabilities. Neto et al. (2022) focus on DDoS detection by adopting a federated approach. This collaborative solution targets the aggregation of multiple inputs to build a unified global model capable of classifying multiple threats. Also, the authors consider a multi-tenant IoT environment, which reflects the topology adopted by organizations in distributed regions. Sadaf and Sultana (2020) present an approach to detect intrusion in fog computing. This solution is empowered by combining Autoencoder (AE) and Isolation Forest (IF) to provide real-time binary classification capabilities. The experiments considered the NSL-KDD dataset and demonstrated the effectiveness of the proposed approach. Similarly, Yuan et al. (2020) propose an IDS with a focus on edge computing. This approach reframes network traffic into images and feeds them to CNNs to identify malicious activities. Although the main focus of this research is on home security, the strategy of converting packets to new representations can be used in different applications. Besides, the authors adopt an Auxiliary Classifier Generative Adversarial Network (AC-GAN) to expand the dataset used, i.e., the UNSW-NB15 dataset. Hamidpour and Bushehrian (2023) introduce an intrusion detection mechanism that evolves as new training rounds are established. The ultimate goal of this work is to demonstrate how IDS can be developed and enhanced even

with a shortage of training resources (e.g., datasets). The authors adopt an autoencoder and evaluate the effectiveness of this strategy using the N-BaIoT dataset. Zhang et al. (2022b) introduce a DDoS detection solution focused on edge computing. Adopting a BiLSTM model, the authors face the flooding issue in the context of power IoT and demonstrate the performance of this recurrent approach. In addition to detection, Myneni et al. (2022) focus on mitigating flooding attacks against edge infrastructures. This strategy enables the identification of the source of incoming packets to limit its available bandwidth. Zhang et al. (2020) investigate the impacts of poisoning attacks in the context of edge computing. The authors introduce a mechanism to poison data dedicated to federated learning using GANs. The experiments showed that label flipping and backdoor attacks successfully compromise the centralized model when the proposed approach is adopted. Ezeme et al. (2019) tackle the anomaly detection problem from a distributed standpoint. This solution relies on an offloading mechanism that provides detection capabilities, achieving reduced latency and increased throughput in Wi-Fi ad-hoc networks. Similarly, the authors in Lee et al. (2020) build upon previous projects (Aminanto et al. (2017); Parker et al. (2019)) to propose an efficient IDS for lightweight devices in an edge environment using an autoencoder. The focus is on extracting abstract features to be used by an SVM-enabled pipeline. Although efficient in experiments conducted, the authors state that this strategy needs to be evaluated in more extensive scenarios comprising other benchmark datasets. Bhutto et al. (2022) present a method to detect DDoS attacks using a transformer architecture. More specifically, the authors detect VeryShort Intermittent Distributed Denial of Service (VSI-DDoS) through reinforced transformer learning, mitigating problems in edge operations. This work creates multiple opportunities for future directions, including the evaluation of security capabilities in critical edge topologies. Finally, some recent works also focus on applying CNNs to protect edge operations (Hinojosa and Majd (2024)).

Table 9 lists the main aspects of these proposals, while Table 10 depicts the accuracy, precision, recall, and F1-score of the highest results of the experiments conducted in each work. The metrics not considered or not directly presented in the evaluation tables are denoted by the $*$ symbol.

4.3 Internet of things (IoT)

The diversity of IoT applications challenges existing security countermeasures due to their dynamic operation (e.g., constant topology change and multi-protocol interactions). Singh et al. (2021) aims to develop a lightweight solution to tackle the intrusion detection problem in resource-constrained edge environments. The authors develop a stack based on LSTM and GRU to represent sequential data. The use of lightweight models can empower IoT applications in several ways, and making these detection systems more accessible enhances the overall cybersecurity practice. Furthermore, RNNs can be used in different ways to protect IoT operations. Almiani et al. (2020) present an investigation focused on IDS automation using RNNs in a layered approach that brings protection capabilities close to the end user. Finally, the authors also state that the proposed approach can be used in real-time applications. The authors in Kan et al. (2021) introduce an IDS for IoT that uses a combination of Adaptive Particle Swarm Optimization (APSO) and CNN. This approach measures individual loss for particles during the evolution procedure. The one-dimensional architecture adopted outperformed other state-of-the-art methods in the experiments and is

Table 7 DL Solutions for Intrusion Detection in Cloud Computing. These contributions train DL models using network traffic data to detect multiple attack types

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Abusitta et al. (2019)	Enable proactive decision making based on IDS cooperation using past feedbacks	AE	KDD Cup 99	DoS, Probe, R2L, U2R	Integration of explainability mechanisms to justify the decision made	Development of explainable IDS for cloud security (Explainable Identification)
Wang et al. (2020b)	Optimization of intrusion detection based on the extraction of feature representations	AE	KDD Cup 99 and NSL-KDD	DoS, R2L, Probe, U2R	Evaluation of how representations can be enhanced with domain knowledge	Knowledge-Infused Learning (Continuous Detection Improvement)
Archana et al. (2021)	Scalable cloud-based IDS to reduce the False Positive Rate (FPR)	FF, RNN, CNN	UNSW-NB15	Reconnaissance, Shellcode, Backdoors, Analysis, DoS, Exploits, Generic, and Worm	Adoption of datasets that reflect modern cloud operations	Alignment with modern cloud technologies (Deployable Countermeasures)
Chkirbene et al. (2021)	Generation of realistic data to improve cloud-based IDS	GAN	UNSW, NSL-KDD	DOS, PROBE, R2L, U2R	Evaluation of generative capabilities for different attack phases (e.g., APT)	Multi-phase protection (Holistic Intrusion Detection)
Gao et al. (2022)	Identification of malicious activities in cloud environments	CNN, BiLSTM	KDD CUP 99	DoS, R2L, scanning and probing	Adoption of datasets that reflect modern cloud operations	Development of cloud datasets (Deployable Countermeasures)

Table 7 (continued)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Vu et al. (2022)	Robustness improvement for Cloud IDS	CDAEE, CDAEE-KNN	Cloud IDS dataset, CIC-IDS 2017, NSL-KDD, UNSW-NB15	TCP Land, PingOfDeath, SlowLoris, SlowHTTP, BruteForce, Botnet, SSH-Patator, DoS, DDoS, U2L, R2L, Probing, Exploits, Fuzzers, Reconnaissance, Backdoor, Shellcode, Worms	Development of extensions for zero-day attacks	Detection of Unknown Threats (Recognition Robustness)
Alzughaibi and El Khediri (2023)	Identification of malicious activities in cloud environments	DNN, PSO	CSE-CIC-IDS2018	DDoS, DoS, BruteForce, Bot, Infiltration, Web	Adoption of different metaheuristics and deployment to real environments	Readiness for complex operations (Continuous Detection Improvement)
RM and MK (2023)	Hybrid approach to detect AWS malicious activities	PCA, SMO-FCM, AE	CSE-CIC-IDS2018	DDoS, DoS, Brute Force, botnet	Evaluation of the proposed solution in real environments with similar constraints	Adaptability to real systems (Generalized Discovery)
Long et al. (2024)	Development of cloud IDS using attention mechanisms	TF	CIC-IDS 2018	Botnet, Infiltration, DoS, DDoS, Web Attack, Brute-force Attack	Extension of proposed capabilities to other systems (e.g., edge computing)	Integration with IDS solutions for other systems (Holistic Intrusion Detection)

Table 7 (continued)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Sanagana and Tummalach-ervu (2024)	Optimization of LSTM to improve detection performance	LSTM	ID Dataset	DoS, R2l, Probe, U2r	"Evaluation of detection method in real cloud environments (e.g., kubernetes)"	"Alignment with modern cloud technologies (Deployable Countermeasures)"

Table 8 Results obtained in the application of DL for intrusion detection in cloud computing

Paper	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Abusitta et al. (2019)	95	*	*	*
Wang et al. (2020b)	87.33	87.96	87.33	85.01
Archana et al. (2021)	95.02	85.02	74.45	79.78
Chkirbene et al. (2021)	86	*	*	*
Gao et al. (2022)	95.4	*	*	*
Vu et al. (2022)	*	*	*	*
Alzughaibi and El Khediri (2023)	98.97	99.98	98.8	99.38
RM and MK (2023)	95.3	94.7	47.8	63.5
Long et al. (2024)	99.98	99.72	99.36	99.54
Sanagana and Tummalachervu (2024)	99.71	94.94	94.36	94.57

related to other optimization proposals. For example, Lahasan and Samma (2022) present a fast autoencoder strategy optimized by a two-layer mechanism responsible for selecting training and operational constraints, guided by the permutation of input features (F), training instances (I), and architecture (M). This proposal outperformed traditional optimization algorithms in the context of this investigation. A work focused on IIoT security is presented by Zhang et al. (2022a). The authors introduce an autoencoder mechanism that enhances intrusion detection capabilities by tackling the problem of imbalanced class representation. Thus, this is another application of AE that can be further extended with additional resources (e.g., domain knowledge). A related proposal is presented by Hasan et al. (2023), where the authors introduce an explainable IDS focused on transparency and robustness in IIoT environments using LIME (Ribeiro et al. (2016)) and SHAP (Lundberg and Lee (2017)). Firstly, the data is preprocessed and fed to an ensemble of CNN models. Then, each instance of the testing set is evaluated regarding the rationale behind each classification. Future directions include the evaluation of the explainability strategy in real deployments and constrained operations. In the past few years, some efforts have focused on the protection of vehicular systems. Song et al. (2020) focus on in-vehicle applications of IoT and present an IDS solution for IoV. More specifically, the authors focus on using CNN to detect malicious behaviors in intra-vehicle communications, which are based on the Controller Area Network (CAN) protocol. Besides, the authors generate an IoV security dataset to support the development of new security solutions based on the injection and control of CAN messages. Yang and Shami (2022) rely on transfer learning and optimization to detect abnormal activities in IoV using a CNN. In this study, the authors infuse CAN bus and network traffic into the pipeline and generate images. Then, CNNs are used and optimized using PSO. Finally, the output provides the classification of the attack type with high accuracy. Finally, the Internet of Medical Things (IoMT) is an emerging application area given its benefits to society. Faruqui et al. (2023) combine a CNN and an LSTM to build an IoMT IDS that optimizes the relationship between Detection Rate (DR) and False Positive Rate (FPR) for images and non-images data classification. However, this method presents a complex architecture with heavy computational resource demands. Alongside the challenges regarding explainability, the future directions of this research also include robustness. Ravi et al. (2023) adopt network and biometric features to detect abnormal behaviors in IoMT. The combination of communication and application-specific features yields expressive rep-

Table 9 DL Solutions for Intrusion Detection for Edge Computing

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Ezeme et al. (2019)	Distributed anomaly detection in edge computing	LSTM	Original traffic	DoS and Random attacks	Evaluation of proposed strategy in real systems	Readiness for real systems' constraints (Deployable Countermeasures)
Lee et al. (2020)	Intrusion detection for constrained networks	AE	AWID	Caffe Latte, Evil Twin, and Hirte attack	Extensive evaluation in environments of different constraints	Readiness for real systems' constraints (Deployable Countermeasures)
Sadaf and Sultana (2020)	Real-time intrusion detect in fog computing	AE	NSL-KDD	DoS, R2L, Probe, U2R	Use of AE solutions in resource-constrained environments (e.g., IoT)	Awareness of the System's constraints in intrusion detection (Environmental Awareness)
Yuan et al. (2020)	Intrusion detection based on new network traffic representation	AE, GAN	UNSW-NB15	Reconnaissance, Shellcode, Backdoors, Analysis, DoS, Exploits, Generic, and Worm	Use of AE solutions in resource-constrained environments (e.g., IoT)	Awareness of the System's constraints in intrusion detection (Environmental Awareness)
Zhang et al. (2020)	Investigate how generative approaches can compromise the performance of edge computing solutions	GAN	Non-IDS datasets	Data Poisoning	Development of Robust solutions for edge computing	Detection of Unknown Threats (Recognition Robustness)
Myneni et al. (2022)	Mitigation of flooding attacks	DN, LSTM	CICDDoS2019	DDoS (DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, SYN, TFTP, UDP, UDPLag, and Web)	Development of robust flooding protection for zero-day attacks	Detection of Unknown Threats (Recognition Robustness)
Zhang et al. (2022b)	Flooding detection based on contextual information	BiLSTM	Original traffic	DDoS	Extension of capabilities for scalable deployments	Readiness for real systems' constraints (Deployable Countermeasures)
Neto et al. (2022)	Distributed DDoS detection	DNN	CICDDoS2019	DDoS	Evaluation of RNNs in distributed solutions	Evaluation of other DL architectures (Continuous Detection Improvement)

Table 9 (continued)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Bhutto et al. (2022)	Detection of flooding attacks tailored to edge computing	TF	CIC-DDoS2019, UNSW- NB15	DDoS	Evaluation of detection mechanism in critical edge topologies	Readiness for real systems' constraints (Deployable Countermeasures)
Hamidpour and Bushehrian (2023)	Intrusion detection mechanism that evolves with training rounds	AE	N-BaIoT	Ack, COMBO, Junk, Scan, Syn, TCP, UDP, and UDPplain	Use of AE solutions in resource-constrained environments (e.g., IoT)	Awareness of the System's constraints in intrusion detection (Environmental Awareness)
Hinojosa and Majd (2024)	Development of pipeline to process data and detect malicious activities	CNN	CICIoT2023	Reconnaissance, DoS, Brute Force, Spoofing, DDoS, Web, Mirai	Assessment of performance in different environment and performance comparison with state-of-the-art methods	Readiness for real systems' constraints (Deployable Countermeasures)

Table 10 Results obtained in the application of DL for intrusion detection in edge computing

Paper	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Ezeme et al. (2019)	*	*	*	*
Lee et al. (2020)	98.22	*	97.64	98.21
Sadaf and Sultana (2020)	95.4	94.81	97.25	96.01
Yuan et al. (2020)	96	96	98	97
Zhang et al. (2020)	*	*	*	*
Myneni et al. (2022)	90.87	*	*	*
Zhang et al. (2022b)	95.96	*	*	*
Neto et al. (2022)	84.8	*	*	*
Bhutto et al. (2022)	98.74	100	98.73	*
Hamidpour and Bushehrian (2023)	*	*	*	86.12
Hinojosa and Majd (2024)	*	99.79	99.79	99.79

resentations to empower deep learning architecture (e.g., through the use of attention mechanisms). The authors also integrate CNN and LSTM to outperform several other methods. Li et al. (2024) present an intrusion detection method for IoT using Large Language Models (LLMs). The authors aim to produce a cybersecurity agent that detects malicious activities while providing explanations for the decisions made, whereas Yaras and Dener (2024) classify attacks against IoT in a big data environment using a hybrid DL method. Finally, Table 11 summarizes DL applications for intrusion detection in IoT, while Table 12 presents the metrics obtained in each study.

4.4 Software-defined networking (SDN)

Novel networking capabilities are required in business operations to enable new services with optimized performance. Although Software-Defined Networking (SDN) establishes new networking capabilities, DL solutions enhance network orchestration and security. Novaes et al. (2021) presents an SDN-based intrusion detection mechanism focused on DDoS attacks while observing and addressing vulnerabilities regarding adversarial examples. The authors employ a GAN pipeline in which mitigation mechanisms are integrated into the SDN stack. Similarly, Hussain and Hnamte (2021) use DL to detect intrusion in SDN operations. The topology adopted contains multiple open-flow devices and integrates the intelligent detection mechanism alongside the controller. The results achieved using multiple datasets suggest that the adoption of DL can yield a better security posture, although the application to real topologies can present shortcomings (e.g., limited domain knowledge integration). Furthermore, advanced techniques can be combined in a way to provide better insights and enhance SDN security countermeasures. Said et al. (2023) combine CNN and RNN with the ultimate goal of detecting malicious behavior in the context of SDN. Using multiple datasets, the authors investigate the importance of several features and conduct an extensive evaluation of the proposed approach. A similar combined approach is presented by Yang et al. (2022), in which the authors use an ensemble of autoencoders to extract and represent features to enable the detection of zero-day attacks in the context of SDN. The authors adopt multiple unsupervised methods after reducing the dimensionality of the input vector. The authors in Cui et al. (2023) propose a collaborative and federated approach

Table 11 DL solutions for intrusion detection in the internet of things (IoT)

Paper	Goal	DL Model	Dataset	Application	Attacks	Limitations and Future Work	Open Challenge
Almiani et al. (2020)	IDS automation brought close to the end user	RNN	NSL-KDD	IoT	DoS, Probe, R2L, U2R	Evaluation of the proposed method in highly imbalanced datasets	Alignment with modern security data trends (Continuous Detection Improvement)
Song et al. (2020)	Detection of malicious behaviors in intra-vehicle communications	CNN	Car-hacking	IoV	DoS, Fuzzy, Spoofing	Evaluation of protocols used in different transportation systems	Development of IoT IDS for multimodal transportation (Holistic Intrusion Detection)
Singh et al. (2021)	Lightweight intrusion detection for resource-constrained systems	RNN	UNSW2015	IoT	DDoS	Evaluation of the proposed method in different IoT areas (e.g., healthcare)	Security of multiple IoT applications (Generalized Discovery)
Kan et al. (2021)	Intrusion detection using evolutionary architectures	CNN	N-BaIoT	IoT	Ack, COMBO, Junk, Scan, Syn, TCP, UDP, and UDPplain	Evaluation of evolutionary architectures for individual classes of cyber attacks	Integrated evaluation of the attack phases (Holistic Intrusion Detection)
Lahasan and Samma (2022)	Intrusion detection using evolutionary architectures	AE	N-BaIoT	IoT	Gafgyt and Mirai	Investigation towards the benefits of optimization methods in IDS explainability	Adoption of methods optimized for explainability (Explainable Identification)
Zhang et al. (2022a)	Intrusion detection in imbalanced scenarios	AE	NSL-KDD	IIoT	DoS, Probe, R2L, U2R	Development of similar approach in other IoT contexts	Security of multiple IoT applications (Generalized Discovery)
Yang and Shami (2022)	Transfer learning application to IoV IDS	CNN	Car Hacking, CICIDS2017	IoV	DoS, fuzzy, gear spoofing, RPM spoofing, DoS, port scan, brute-force, web attacks, and botnets	Evaluation of how transfer learning supports the development of transparent and robust IDS solutions	Integration of multiple models to detect unknown attacks (Recognition Robustness)

Table 11 (continued)

Paper	Goal	DL Model	Dataset	Application	Attacks	Limitations and Future Work	Open Challenge
Faruqui et al. (2023)	Intrusion detection using hybrid models	CNN, LSTM	CIC-IDS2017	IoMT	Brute force, DoS, DDoS, infiltration, portscan, botnet	Evaluation of robustness and explanability	Development of explainable IDS for IoT security (Explainable Identification)
Ravi et al. (2023)	Intrusion detection using hybrid models	CNN, LSTM	WUST EHMS 2020, SDN-IoT, KDDCup-99	IoMT	General Attacks	Granular performance evaluation for specific IoMT attacks	Development of multi-stage IDS for IoMT (Holistic Intrusion Detection)
Hasan et al. (2023)	Transparent intrusion detection in IIoT	CNN	TON_IoT	IIoT	Scanning, DoS, Injection, DDoS, Password cracking, XSS, ransomware, backdoor, MITM	Multi-modal intrusion detection, extending explainability across different networks	Align Explainability with Business requirements (Continuous Detection Improvement)
Li et al. (2024)	Explainable IoT IDS using Large Language Models (LLMs)	TF	ACI-IoT'23, CIC-IoT 2023	IoT	Reconnaissance, DoS, Brute Force, Spoofing, DDoS, Web, Mirai	Deployment in real topologies with limited processing capabilities	Performance Evaluation considering real systems' constraints (Deployable Countermeasures)
Yaras and Dener (2024)	Classification of attacks against IoT in a big data environment using a hybrid DL method(LLMs)	CNN, LSTM	CIC-IoT 2023, TON_IoT	IoT	Reconnaissance, DoS, Brute Force, Spoofing, DDoS, Web, Mirai	Assessment of detection capabilities in zero-day attacks	Align Explainability with Business requirements (Continuous Detection Improvement)

Table 12 Results obtained in the application of DL for intrusion detection in the Internet of Things (IoT)

Paper	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Almiani et al. (2020)	91.69	49.97	47.81	48.87
Song et al. (2020)	*	100	99.89	99.95
Singh et al. (2021)	99.5	99.5	99.55	99.7
Kan et al. (2021)	*	*	*	*
Lahasan and Samma (2022)	99.75	99.11	99.77	99.44
Zhang et al. (2022a)	95.42	93.14	90.29	92.35
Yang and Shami (2022)	100	100	100	100
Faruqui et al. (2023)	97.63	98.47	97	97.73
Ravi et al. (2023)	95	94	85	88
Hasan et al. (2023)	99.63	99.8	99.2	99.5
Li et al. (2024)	98	98.2	97.2	97.5
Yaras and Dener (2024)	99.99	99.99	99.99	99.99

to intrusion detection. While targeting Software-Defined VANETs (SDVN), this strategy aggregates security insights from local networks by sharing local CNNs parameters to empower a centralized model. The experiments demonstrate that this approach outperforms existing solutions. Janabi et al. (2022) use a CNN to detect abnormal activities in SDN. This proposal relies on the use of OpenFlow channel so that flow statistics are shared and classified as benign or attack. The experiments showed that CNN presents high accuracy in this classification task. Besides, the authors evaluate this method's impacts on throughput and latency, revealing low implications with degradation rates of 2.3% and 1.8%, respectively. Tang et al. (2018) use a GRU model to detect malicious activities in SDN. Given the traffic going through an SDN switch, the detection mechanism is deployed to the SDN controller, which supports the switch regarding anomaly mitigation. Three components are adopted to collect flows (flow collector), detect abnormal patterns (anomaly detector), and mitigate potential impacts (anomaly mitigator). The experiments demonstrated high accuracy with low impact on the network operation. Similarly, Tang et al. (2020) implement a GRU model in a POX controller to detect malicious activities. Without extensive degradation of the network performance, this evaluation demonstrated the effectiveness of neural networks and GRU models. In Tang et al. (2016), a DL model is used to detect malicious behaviors in SDN flows, using a reduced set of features and achieving high accuracy. Additionally, Makuvaza et al. (2021) focus on real-time detection of distributed flooding attacks against SDN infrastructures. These efforts present insight regarding how DL can be used in real-world environments by considering different constraints (e.g., response time) and characteristics of deployed security analytics solutions. Finally, Ahsan et al. (2024) adopt a transformer-based approach to protect SDN topologies in the context of Vehicle ad-hoc Networks (VANETS). This intrusion detection initiative combines Federated Learning (FL) with the Bidirectional Encoder Representations from Transformers (BERT), targeting a privacy-preserving and attention-based strategy. The evaluation conducted with the VeReMi dataset (Van Der Heijden et al. (2018)) demonstrated that the proposed approach is promising in future deployments. The main aspects of these contributions are presented and compared in Table 13 and their experimental results are described in Table 14.

4.5 Multi-access edge (MEC)

Some research investigations focus on utilizing DL to improve the Multi-Access Edge (MEC) security. Liu et al. (2021) improves intrusion detection in MEC using an RNN. The authors use a GRU supported by a decision tree, responsible for TCP protocol extraction. This platform is intended to interact with the security engineer while communicating with edge servers. In this case, the edge server interacts with the network data, extracts TCP data, and provides it to the analysis cluster. The evaluation is conducted by multiple neural networks and the outputs are provided to the security engineer. The experiments showed the efficiency of this strategy while not requiring changes in network topology. Abou El Houda et al. (2023) introduce a federated approach to protect IoT solutions in MEC environments. This collaborative strategy aims at detecting and mitigating threats while preserving privacy through the parameter aggregation supported by the MEC orchestrator. Another work that proposes a federated approach is presented by Sedjelmaci and Ansari (2022), where the Federated Generative Adversarial Network (FedGAN) algorithm is introduced as an initial combination with game theory to improve MEC security through attack classification - leveraging a Gathering Agent (GA) and a Detection Agent (DA). Wang et al. (2023) employ an LSTM autoencoder to detect anomalies in MEC operations. Relying on a special sampling mechanism that enables the parallel training of multiple detectors and the selection of the best-performing model, the authors demonstrated the superiority of this method compared to existing solutions. Rather than focus on attacks, the authors evaluate operational anomalies using the serviceSurvey dataset (Jiang et al. (2012)). Adeniyi et al. (2024) combine an autoencoder with a feed-forward model to detect DDoS attacks in MEC topologies. The first phase in the detection problem relies on creating informative representations conducted by the autoencoder. Then, underlying patterns are revealed and used by the feed-forward network to detect attacks. This integrated solution presents improvements in classification results compared to existing methods. Flooding attacks are also the target of Gyamfi and Jurcut (2022). This strategy aims to detect DoS attacks in MEC-enabled IIoT operations based on operational Key Performance Indicators (KPIs). A recurrent approach is adopted to evaluate sequential aspects with a personalized filter, which achieves high performance. Fernando et al. (2023) detect abnormal MEC activities using a CNN using a novel method to represent the traffic while minimizing loss. Moreover, other approaches adopt the traditional feed-forward solutions to protect MEC operations. Hilal et al. (2023) rely on Deep Learning (DL) to detect cyberattacks in MEC, focusing on the Quality of Experience (QoE). Table 15 depicts the main aspects of DL applications for intrusion detection in MEC, while Table 16 presents the results obtained.

4.6 Industrial control systems (ICS)

The detection of threats in ICS can adopt multiple DL techniques to address operational issues while meeting industrial requirements. Ling et al. (2021) adopt a recurrent approach to identify malicious activities in ICS using a Bidirectional Simple Recurrent Unit (BiSRU). The authors emphasize the impact of vanishing gradients and develop a strategy based on adaptable connectivity as a mitigation procedure, demonstrating improved performance compared to other methods on ICS-specific datasets (Morris and Gao (2014)). Similarly, the authors in Khan et al. (2022) protect IoT-based ICS using a federated and recurrent

model to mitigate the vanishing gradients problem. A federated system model is proposed comprising local training and testing, and updates of local and global models. The evaluation demonstrated the high performance achieved using the gas pipeline dataset (Morris and Gao (2014)). Jahromi et al. (2021) also adopt a federated strategy for ICS intrusion detection, but consider the use of autoencoders. The centralized parameter aggregation employed enables the integration of multiple trained architectures. There is also a research line in the use of CNNs to enhance ICS security operations. Wang et al. (2020a) also adopt an autoencoder to protect ICS, but consider training and threshold definitions, which leads to data prediction and recovery and, ultimately, anomaly detection. The authors in Jin et al. (2023) combine a BiLSTM and a CNN with efficient channel attention to foster intrusion detection capabilities in ICS. A procedure that incorporates sequence evaluation and oversampling, and presents a convolution module, attention module, and BiLSTM module is developed, outperforming existing solutions for ICS security solutions. Another successful CNN adoption is described by Kravchik and Shabtai (2018), where the authors rely on the difference in estimated and measured values in the anomaly detection pipeline. This method successfully detected 31 out of the 36 attacks investigated. Finally, Cai et al. (2023) present a generative approach for intrusion detection in ICS that combines CNN and GAN. This adversarial approach adopts a Wasserstein Generative Adversarial Network (WGAN) and sheds light on how generative AI can be helpful for the security of ICS operations. Table 17 presents the characteristics of these research endeavors and highlights their future directions, followed by the metrics of each research effort presented in Table 18. Finally, some TF-based efforts have been published as a preliminary investigation in different fields. Ann et al. (2024) focus on investigating how Large Language Models (LLMs) can be used to detect intrusions in ICS. Using the MITRE ATT&CK framework knowledge, the authors present a preliminary study by highlighting data collection, pre-processing, and modeling.

4.7 Discussion

Based on the results obtained in each work, important insights are found in the numerical experimental results. Figure 14 illustrates the average results obtained for each emerging technology. These four graphs show the results of accuracy, precision, recall, and F1-score. In terms of accuracy, recall, and F1-score, the average results indicates that efforts designed for MEC present a higher performance. However, DL techniques used to detect intrusion in edge computing presented a higher precision. On the other hand, SDN and cloud computing are among the technologies with the lowest average performance in the context of DL applied to detect intrusion. Although these results demonstrate the individual performance, it is important to note that all the overall values are above 90% with a few exceptions. In other words, this high performance is difficult to reproduce in the real world due to several operational factors. Figure 15 presents a different angle to this analysis by presenting the average performance obtained by each DL technique. Once again, the values are mostly above 90%, with a remarkable accuracy, precision, recall, and F1-score achieved by Transformers (TF).

These efforts present important insights to mitigate threats in emerging technologies. However, there are several limitations to be dealt with in the next few years. The upcoming section presents a detailed discussion on open challenges and highlights lines of investigation in the use of DL to protect emerging technologies.

Table 13 DL Solutions for Intrusion Detection for Software Defined Networking (SDN)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Tang et al. (2016)	Detection of intrusion in SDN using DL	FFN	NSL-KDD	DoS, R2L, U2R, Probe	Integration of security evaluation techniques across multiple networking paradigms	Development of SDN IDS that integrates features of other systems (Holistic Intrusion Detection)
Tang et al. (2018)	Detection of intrusion in SDN using RNN	GRU	NSL-KDD	17 attacks (KDDTest+) and 22 attacks (KDDTrain+)	Architectural optimization and evaluation of large-scale deployments	Performance evaluation In real SDN deployments (Deployable Countermeasures)
Tang et al. (2020)	Implementation of IDS solution in a SDN controller	GRU	NSL-KDD	DoS, R2L, U2R, Probe	Evaluation of large-scale deployments	Development of SDN solutions based on the operational network traffic and logs (Deployable Countermeasures)
Hussain and Hnamte (2021)	Detection of intrusion in SDN using DL	FFN	KDD-CUP99, NSL-KDD	Several attacks from both datasets	Development of solutions for real topologies	Performance evaluation In real SDN deployments (Deployable Countermeasures)
Novaes et al. (2021)	Robust Intrusion detection mechanism for DDoS attacks	GAN	CICDDoS 2019	DDoS (NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, TFTP)	Robustness evaluation for other attack types (e.g., spoofing)	Detection of Unknown Threats in the context of SDN (Recognition Robustness)
Makuvaza et al. (2021)	Real-time detection of flooding attacks in SDN	FNN	CICIDS2017	DDoS	Robustness evaluation for DDoS protection in other environments (e.g., IoT)	Development of robust solutions that consider the interoperability of SDN with other technologies (Recognition Robustness)
Yang et al. (2022)	Detection of zero-day attacks based on new feature representations	AE	Open Datasets	Mirai, SYN DDoS, SSL Renegotiation, SSDP Flood, Fuzzing, Active Wiretap	Extrapolate the dimensionality reduction capabilities to enable real-time applications in different contexts	Development of similar methods to protect different SDN topologies with different constraints (Generalized Discovery)
Janabi et al. (2022)	Detection of intrusion in SDN using CNN	CNN	InSDN	DoS, DDoS, Probe, U2R, R2L, and Portscan	Deployment in real SDN devices and evaluation in large topologies	Performance evaluation In real SDN deployments (Deployable Countermeasures)

Table 13 (continued)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Said et al. (2023)	Combine CNN and RNN to detect malicious behavior in SDN	CNN, RNN	UNSW-NB15, NSL-KDD, InSDN	BFA, U2R, DDoS, DoS, R2L, Botnet, Web Attack, Probe	Extend solution for real-time applications	Evaluation of real-time intrusion detection for SDN (Deployable Countermeasures)
Cui et al. (2023)	Collaborative IDS in VANETs	CNN, FL	KDD99, NSL-KDD	Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probe	Evaluation of semi-supervised learning to address the lack of labeled data	Assessment of new capabilities and further evaluation in real topologies (Continuous Detection Improvement)
Ahsan et al. (2024)	Combination of FL and BERT to protect SDN topologies in the context of Vehicle ad-hoc Networks (VANETS)	FL, TF	VeReMi	Eventual stop Attack, Random Attack, Constant Offset Attack, Constant Attack, Random Offset Attack	Evaluation of detection capabilities in rel operations and in constrained scenarios	Development of SD-VANETs solutions based on the operational network traffic and logs (Deployable Countermeasures)

Table 14 Results obtained in the application of DL for intrusion detection in Software-Defined Networking (SDN)

Paper	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Tang et al. (2016)	75.75	83	76	75
Tang et al. (2018)	89	87.91	89.90	88.90
Tang et al. (2020)	80.7	85	81	81
Hussain and Hnamte (2021)	99.61	99.37	99.61	99.48
Novaes et al. (2021)	99.78	99.76	99.99	99.87
Makuvaza et al. (2021)	2	2	2	2
Yang et al. (2022)	99.99	*	*	*
Janabi et al. (2022)	100	100	100	100
Said et al. (2023)	97.77	99.85	95.28	97.51
Cui et al. (2023)	99.12	*	*	99.2
Ahsan et al. (2024)	84	79	95	86

5 Open challenges

The development of DL strategies for IDS and the promising results achieved in the past few years demonstrate their effectiveness in supporting advanced cybersecurity solutions. However, there is still a group of critical shortcomings that prevent their wide adoption in real systems. This section presents the limitations of intrusion detection for emerging technologies and the adoption of DL in real applications. We shed light on future research direction, illustrated in Fig. 16, and consider business adaptability, trustworthiness, and operationalization of protection mechanisms.

5.1 Business adaptability

This category refers to the gap between controlled environments and real systems. The papers reviewed in this research describe the use of datasets and models and report high achievements in the results, not considering an extensive investigation of how such solutions can be widely adopted in real systems (e.g., under restrictive constraints). Deploying such techniques in real infrastructures brings environmental awareness and holistic requirements challenges.

5.1.1 Environmental awareness

In many cases, the outputs provided by DL models do not comply with the policies and regulations in place due to the lack of operational awareness (e.g., characteristics of internal network procedures, seasonal events, and special operations). This misalignment can have minor implications (e.g., rare and uncritical misclassification), but can also substantially compromise the system's operations (e.g., erroneous prioritization and unauthorized procedures recommended in actionable reports). For example, in cloud and edge computing, misleading cybersecurity insights can result in faulty privilege management, reducing intrusion detection performance. This also affects IoT operations, since attacks tailored for safety-critical devices (e.g., infusion pumps in IoMT) may remain undetected due to the lack of contextual awareness of DL models. Regarding DL models, this problem leads DNNs, CNNs, and RNNs to output vectors that yield infeasible procedures. Another major issue refers to the use of federated approaches. This problem may lead organizations to

Table 15 DL Solutions for Intrusion Detection for Multi-access Edge Computing (MEC)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Liu et al. (2021)	Intrusion detection in MEC using a TCP protocol extractor	GRU	CSIC2010	SQL injection, CRLF injection, XSS, buffer overflow	Evaluation of GRU in the detection of recent attacks	Leverage recurrent capabilities to detect recent and unknown MEC threats (Continuous Detection Improvement)
Sedjelmaci and Ansari (2022)	Detection of malicious behavior in MEC operations using game theory	FL, GAN	UNSW	Backdoors, DoS, Exploits, Generic, Fuzzers, Analysis, Reconnaissance, Shellcode and Worms	Incorporation of other AI algorithms and extension to different networking paradigms	Adoption of other DL models for IDS considering different MEC configurations (Continuous Detection Improvement)
Gyamfi and Jurcut (2022)	Flooding detection in MEC-enabled IIoT	LSTM	Experimental Testbed	DoS	Evaluation of DoS detection in large-scale MEC-enabled IIoT	Performance evaluation In real MEC deployments (Deployable Countermeasures)
Abou El Houda et al. (2023)	Federated protection of IoT applications in MEC environments	FL	NSL-KDD, Edge-IIoTset	SQL injection, DDoS, Password, vulnerability scan, backdoors, probe	Evaluation of privacy-preserving IDS solutions in constrained environments (e.g., IoMT)	Development of MEC solutions that aggregate knowledge while maintaining privacy (Continuous Detection mprovement)
Wang et al. (2023)	Anomaly detection in MEC operations	LSTM, AE	serviceSurvey	Anomalies	Refinement of the anomaly detection mechanism to evaluate multiple types of cyberattacks	Optimize IDS for multi-phase attacks against MEC topologies (Holistic Intrusion Detection)
Fernando et al. (2023)	Image-based IDS in 5 G-MEC environments	CNN	UNSW-NB15	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms	Deployment of 5 G-MEC for more realistic performance assessment	Performance evaluation In real MEC deployments (Deployable Countermeasures)

Table 15 (continued)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Hilal et al. (2023)	Enhancement of QoE in MEC, including attack detection	GRU	Experimental Testbed	General MEC attacks	Performance evaluation considering specific attacks and real deployments	Performance evaluation In real MEC deployments (Deployable Countermeasures)
Adeniyi et al. (2024)	Intrusion detection based on improved features representation	AE, FF	UNSW-NB15, BoT-IoT, ToN-IoT, CSE-CIC-IDS2018	DDoS	Collaboration among different networking technologies (e.g., cloud and edge) to improve intrusion detection capabilities	Development of integrated solutions that combine operational features of multiple technologies (Environmental Awareness)

Table 16 Results obtained in the application of DL for intrusion detection in Multi-access Edge Computing (MEC)

Paper	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Liu et al. (2021)	99.73	100	100	100
Sedjelmaci and Ansari (2022)	*	*	*	*
Gyamfi and Jurcut (2022)	95	93	92	91
Abou El Houda et al. (2023)	99	99	99	99
Wang et al. (2023)	*	95.56	93.83	94.69
Fernando et al. (2023)	96	95	97	95
Hilal et al. (2023)	99.2	*	99.8	99.6
Adeniyi et al. (2024)	99.98	98.92	94.24	96.52

provide undesired data samples to the distributed training process, affecting overall performance and privacy. For GANs and AEs, the representation created during training can diverge from the desired outcome, ultimately impacting the detection of abnormal activities in the network. To address this issue of existing solutions, Neurosymbolic AI (NSAI) (Garcez and Lamb (2023)) stands out as an efficient pathway to establish context-aware DL solutions for IDS. NSAI relies on the combination of symbolic AI and neural models in a way that the traditional encoding of knowledge can boost the representational power of DL. This new research direction enables the definition of context (e.g., topological details, policies in use, priorities, and strategic roadmaps) to be infused in DL models to facilitate deployment in real systems.

We envision three areas IDS researchers could consider in the application of DL:

1. **Development of simulation tools and datasets:** Most of the public datasets try to reproduce a realistic environment. However, there is a current demand for training resources that capture the real business operations in different industrial sectors (e.g., finance, healthcare, and transportation).
2. **Design of metrics and benchmark frameworks:** There is a current need for metrics that evaluate how DL-based IDS would fit in a realistic environment. Beyond their detection capabilities, these metrics would allow business owners to evaluate how aligned a given technology is with their specific daily operations.
3. **Combining cybersecurity and business operations:** New datasets and training resources need to provide insights regarding the network operation alongside business metrics. For example, a healthcare dataset could include unique medical-based features not present in an industrial dataset and vice versa.

5.1.2 Holistic intrusion detection

The survey presented in this paper reveals that several approaches are dedicated to specific technologies or even isolated areas of different emerging technologies. Although this separation is important to clearly define the scope of the investigation, a critical limitation refers to the interoperability of security mechanisms across the entire topological spectrum. Large organizations have extensive topologies and adopt multiple emerging technologies simultaneously. Hence, the analysis of malicious activities needs to go beyond specific architectural islands and encompass a wider environment. For example, multinational organizations may offer SDN services in a particular region while offering IoT solutions in others. Adopting a

Table 17 DL solutions for intrusion detection in industrial control systems (ICS)

Paper	Goal	DL Model	Dataset	Attacks	Limitations and Future Work	Open Challenge
Kravchik and Shabtai (2018)	Anomaly detection based on estimation error	CNN	SWaT	36 attacks	Evaluation of explainability aspects of ICS security solutions	Development of explainable IDS for ICS security (Explainable Identification)
Wang et al. (2020a)	Anomaly detection based on advanced representations	AE	SWaT	SSSP, SSMP, MSSP, MSMP	Performance improvement and evaluation in dynamic environments	Performance evaluation In real ICS deployments (Deployable Countermeasures)
Ling et al. (2021)	Identification of malicious activities in IDS observing the vanishing gradient problem	BiSRU	Gas Pipeline and Water Storage Tank	NMRI, CMRI, MSCI, MPCI, MFCI, DoS, RECO	Identification of zero-day attacks	Development of IDS for unknown ICS attacks (Recognition Robustness)
Jahromi et al. (2021)	Federated IDS using unsupervised learning	AE	SWaT	SSSP, SSMP, MSSP, MSMP	Integration with other ICS systems	Development of a multi-phase IDS solution focused on different ICS systems (Holistic Intrusion Detection)
Khan et al. (2022)	Federated Identification of malicious activities in IDS observing the vanishing gradient problem	FL, SRU	Gas Pipeline	DoS, Reconn, NMRI, MFCI, MSCI, CMRI	Gradual improvement of attack detection in ICS for future deployments	Development of privacy-preserving IDS for different ICS systems (Continuous Detection Improvement)
Jin et al. (2023)	Combination of a recurrent and a convolutional model to protect ICS	BiLSTM, CNN	Original Traffic	Spoofing, detection attack, socket attack, DDoS	Detection of unknown attacks	Recognition Robustness
Cai et al. (2023)	Detection of ICS attacks using generative AI	CNN, GAN	Gas Pipeline, TON_IOT	Injection, DoS, Reconnaissance	Development of efficient training strategies for large-scale applications	Optimization of models developed to meet the requirements of real ICS systems (Deployable Countermeasures)

narrow detection approach limits the defense systems of different sites from sharing valuable insights and improving detection performance. Besides, the shortened interoperability of multiple DL architectures results in a reduced sharing practice, impacting detection performance. In this context, several possible research lines exist to establish a holistic intrusion detection practice. First, the integration of DL models trained for different tasks or paradigms is a major line of investigation. It relies on understanding how insights that be shared across multiple cybersecurity tasks. Also, a similar combination of insights is needed for different emerging technologies, e.g., identifying how attacks against SDN controllers can affect IoT operations. Developing these capabilities simplifies the deployment of DL solutions for IDS in real-world systems.

Researchers in this field could consider these two main lines of investigation:

1. **Development of datasets that incorporate multiple emerging technologies:** Existing datasets focus on specific environments and lack a comprehensive collection of the integration of multiple technologies. The future dataset will explore the intersection of emerging technologies and their challenges and benefits for business operations.
2. **Collaboration of IDS approaches:** There is a current need for the integration and operationalization of solutions that protect different parts of a system of different systems. The design of effective collaborative approaches will empower DL-based IDS to enhance systems' protection.

5.2 Trustworthiness

To ensure the efficient adoption of DL in real IDS systems, trustworthiness refers to the reliability upon which users can deploy their services. This category emphasizes the importance of transparency of the models and decisions to maintain business alignment and feasibility. The studies reviewed in this research present a limited perspective of explainable identification and recognition robustness.

5.2.1 Explainable identification

The impressive results DL has achieved in the past few years have attracted much attention from the research community and industrial practitioners. Conversely, understanding the reasons why decisions are made remains a critical shortcoming in IDS. Without a clear description of the rationale employed, analysts need to trust a complex model that can make mistakes. Such a scenario can result in substantial problems for the CIA triad and disrupt the system's operation. For example, in ICS routines, erroneous classifications can affect productivity and lead to safety problems. Albeit accurate, the lack of transparency of DL architectures prevents their adoption in real ICS operations due to the uncertainty involved. To address this shortcoming, future research directions involve the development of strategies that are integrated into or interact with DL models to understand the decisions made for IDS. Although in the past few years, there have been efforts to explain advanced models, not understanding the decisions made still prevents DL deployment in real cybersecurity applications.

The main research directions are:

Table 18 Results obtained in the application of DL for intrusion detection in Industrial Control Systems (ICS)

Paper	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Kravchik and Shabtai (2018)	*	96.8	79.1	287.1
Wang et al. (2020a)	*	85.59	88.52	89.97
Ling et al. (2021)	96.23	*	97.28	*
Jahromi et al. (2021)	90.83	90.98	90.83	90.9
Khan et al. (2022)	99.89	99.9	99.83	99.91
Jin et al. (2023)	97.04	97.17	97.05	97.03
Cai et al. (2023)	99	97.9	93.9	95.9

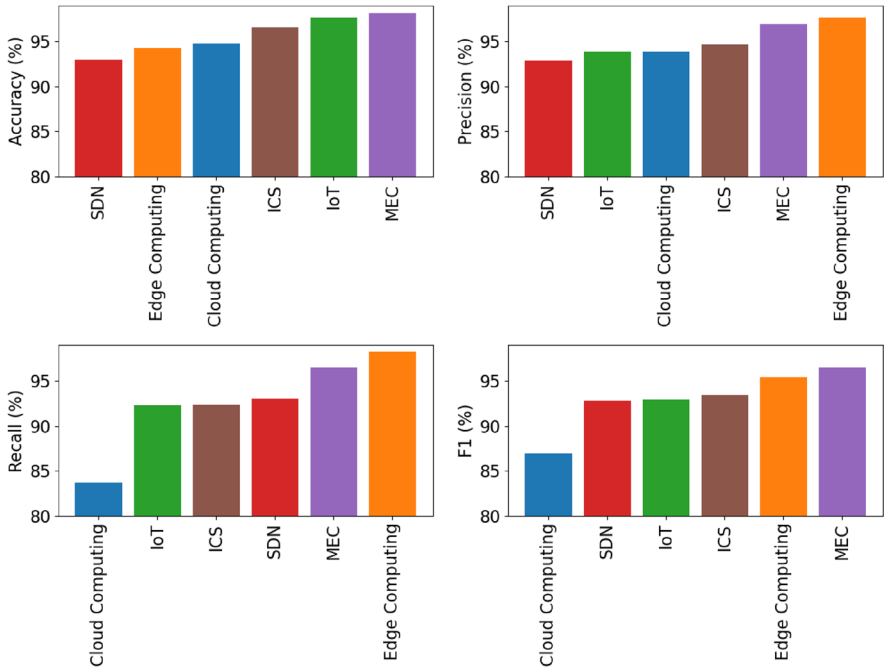

Fig. 14 Average performance achieved in each category by emerging technologies

1. Human-Computer Interaction (HCI) aspects of DL-based IDS: Effective intrusion detection methods need to be efficiently used in the real world. This research line will investigate how DL-based solutions could help security analysts by providing business-tailored explanations for outputs.
2. Reverse engineering of malicious behaviors: Explanations can offer the reasons why a model classifies a network traffic instance as an attack. For attacks that present limited information and exploit specific business characteristics, explanations represent a way to understand malicious behaviors better and improve detection capabilities.

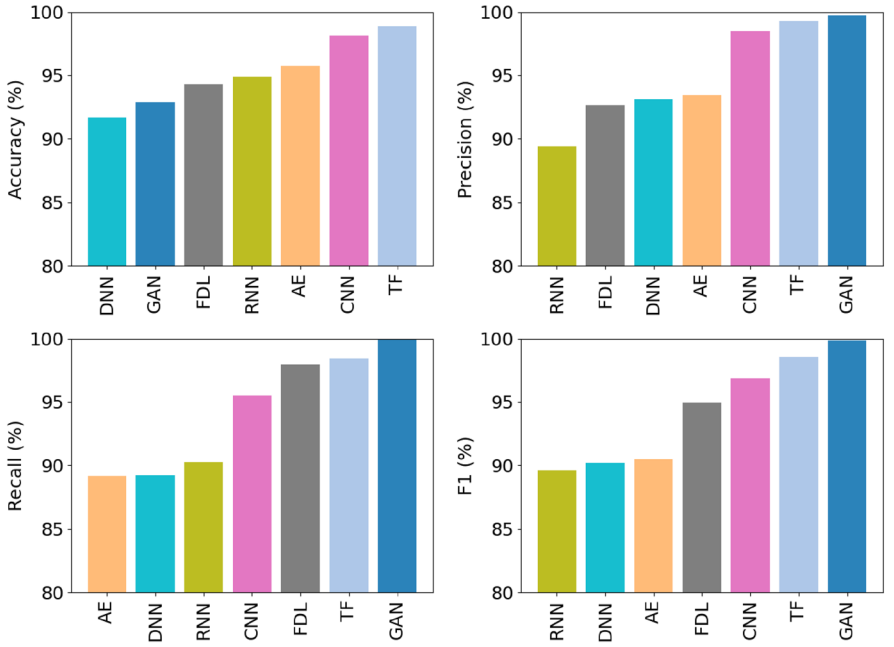

Fig. 15 Average performance achieved in each category by DL techniques

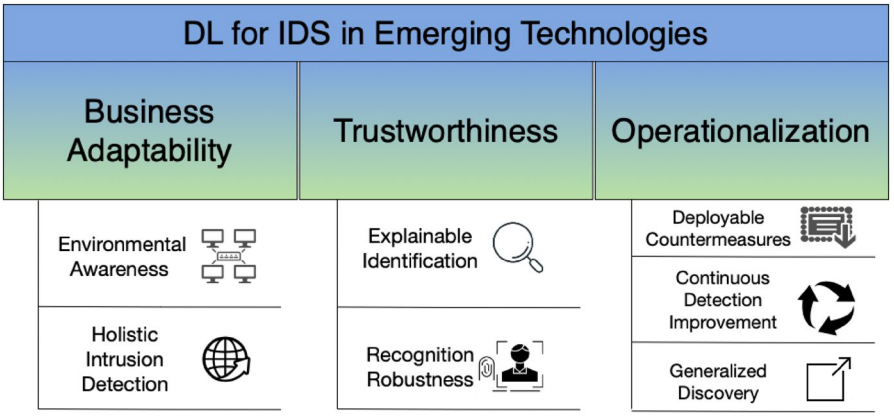

Fig. 16 Open Challenges: DL for IDS in Emerging Technologies

5.2.2 Recognition robustness

The adoption of DL-based IDS depends on leveraging training resources to achieve acceptable deployable performance. Hence, threat actors target potential vulnerabilities stemming from the particular instance to remain undetected. For example, a model can accurately detect conventional DDoS attacks, but present a poor performance if some attack is launched with a small variation in its data fields. Future work will address this issue by proposing

models capable of achieving high accuracy while observing potential adversarial attacks. In fact, this represents another pivotal enabler for using DL-based IDS in real systems. Another example refers to poisoned gradients in FL architectures. Environments with multiple devices (e.g., MEC and IoT) can be affected by such malicious activities, emphasizing the importance of robustness as an open challenge.

Two immediate research lines are:

1. **Continuous update and correction:** New DL-based IDS systems need to adapt to business changes, concept drifting requirements, and continuously learn from the interaction of business and cybersecurity operational features.
2. **Strategies to gradually integrate and evaluate models:** Considering that models can be attacked, the design of gradual integration and evaluation is critical to the success of DL-based IDS in the real world. Therefore, a future research investigation line refers to the proposal of methods that could evaluate if a model behaves as expected by security analysts (e.g., making the right decision for the right reasons and aligning with business requirements).

5.3 Operationalization

Finally, once we achieve the capabilities necessary for producing trustworthiness, future work will introduce mechanisms that maintain defensive resources active, updated, and operational. These areas comprise deployable countermeasures, continuous detection improvement, and generalized discovery.

5.3.1 Deployable countermeasures

The creation and training of DL methods can be challenging and require powerful setups. Nevertheless, their deployment can be difficult for several reasons. Monitoring represents an obstacle alongside the flexibility for scalability. The isolation of these services is also paramount to ensure data privacy and overall security. Finally, the continuous evaluation needs to integrate performance assessment and compliance with the organization's policies. Such obstacles impact all the emerging technologies discussed in this paper. Ranging from the wide variety of IoT topologies to the safety-critical aspects of ICS, controlling and assessing cybersecurity capabilities are pivotal. The scope of future research includes strategies to simplify the deployment of advanced IDS solutions regarding monitoring, flexibility, scalability, and compliance with established policies. For instance, the generative capabilities of GANs can enhance continuous evolution by identifying new attacking trends. However, although useful for detection mechanisms, such methods are still limited and require resources not commonly available (e.g., massive and high-quality data).

Two research lines relevant to the DL application to IDS are identified:

1. Prioritization and business-aware IDS: The deployment of DL-based IDS requires a solid and effective approach that does not affect operations. The development of gradual methods based on technology readiness and flexibility is a major research direction.
2. Performance evaluation: Beyond the detection capabilities, DL-based IDS need to adapt to the environmental constraints. In this context, benchmarks are needed to

evaluate whether such solutions are appropriate for specific environments. Examples are the lack of computational resources in IoT and the privacy requirements of medical applications.

5.3.2 Continuous detection improvement

Cyberattacks are in constant evolution. Ensuring appropriate defenses against cutting-edge threats requires a cyclical enhancement of detection and mitigation mechanisms. This operational shift involves changes in the data ingested, services adopted, seasonal nuances, and unknown vulnerabilities. However, existing proposals design efficient approaches with limited evolutionary components. Future work includes creating methods that continuously adapt to environmental changes throughout their lifecycles. For example, RNNs can be used to identify evolutionary patterns in the data and provide generative models (e.g., GANs) with new trends to estimate what zero-day attacks can be launched. For example, several IoT devices are designed and commercialized annually, and the readiness to protect critical infrastructures regardless of the new vulnerabilities they might contain represents an open challenge. As the rapid pace of the cybersecurity landscape challenges the deployment of rigid solutions, evolutionary IDS based on DL is a key challenge to address in the next few years.

Two research lines are identified for the continuous detection improvement:

1. **Threat modeling:** As technology evolves, new vulnerabilities are added to the systems. Therefore, it is vital to understand malicious behavior to effectively improve the detection capabilities of DL-based IDS. An important research line is the design of strategies to model threats and to use this knowledge in order to provide awareness to the classification models.
2. **Autonomous evolution:** The recent developments of AI agents can empower DL-based IDS. A research line in this context reflects the use of agents to autonomously evolve DL solutions and continuously improve detection capabilities.

5.3.3 Generalized discovery

One of the most critical gaps between controlled environments and real operations is the diversity of attacks that can be launched. Even if a DL model is trained to detect specific attacks (e.g., DDoS), unseen variations of these threats can remain undetected. For example, new IoV components (e.g., infotainment systems) commonly released annually may introduce communication patterns not presented before. The same applies to ICS, in which new automation capabilities are frequently introduced. As it represents unknown scenarios to rigid IDS, exploiting zero-day vulnerabilities can result in undetected malicious activities. Hence, there is a need for models capable of learning general patterns that can identify abnormal behaviors in new datasets and adapt to concept shifting.

Two main research directions are stated in regard to generalized discovery:

1. Generalization evaluation platforms: This research line focuses on establishing platforms that can be used to evaluate how prepared a given DL-based IDS is to operate in environments with different characteristics. Such platforms would enable the

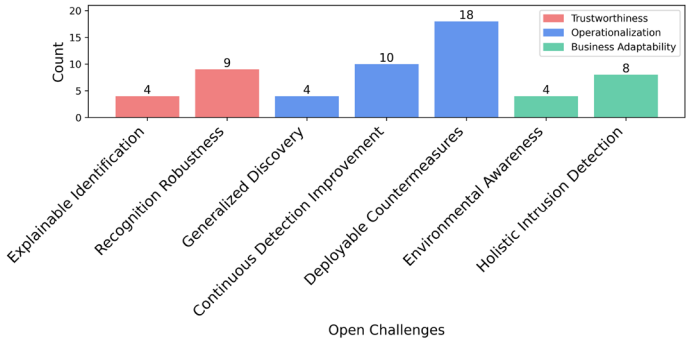

Fig. 17 "Main open challenges for research efforts reviewed in this paper (Tables 7-17)"

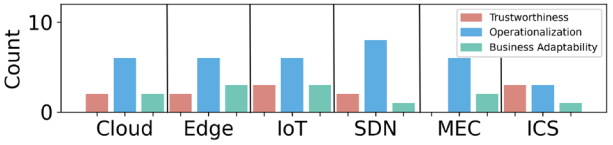

Fig. 18 Open challenges count for each emerging technology

assessment of generalization capabilities, improve existing evaluation frameworks, and align with business requirements regarding the deployment of solutions.

2. Extensive evaluation of zero-day attacks: Attacks that are unknown to organizations remain a major challenge nowadays. A future investigation line relies on the extensive evaluation of such threats by the design and continuous update of assessment resources.

Figure 17 presents the number of main open challenges for the research projects reviewed in this paper. This analysis shows that operationalization remains the most common gap in the use of DL for intrusion detection. Furthermore, robust and holistic security solutions represent major challenges to be addressed in future work. Finally, Fig. 18 illustrates the open challenges count for each emerging technology. Once again, operationalization represents a major aspect for all paradigms, although other aspects remain relevant.

6 Conclusion

The rise of cyber threats has fueled the development of advanced methods to enhance the protection of organizational resources. This complex horizon becomes even more critical due to the extensive shortage of specialized cybersecurity professionals, the evolution of attacking frameworks, and the high number of malicious activities recorded daily. This research evaluated the use of Deep Learning (DL) applications for Intrusion Detection Systems (IDS) in the context of emerging technologies. In total, 59 scientific papers and 39 datasets were reviewed, covering areas such as cloud computing, edge computing, Internet of Things (IoT), Multi-access Edge Computing (MEC), and Industrial Control Systems (ICS). This analysis considered the evaluation of contributions, attacks, characteristics, DL techniques adopted, and future work. Besides, we evaluated and compared popular datasets used in the context of IDS with a categorization that helps researchers choose the most

appropriate dataset depending on their goals. We also presented a taxonomy of attack surfaces for each technology, highlighting aspects that need to be considered in future intrusion detection works. The numerical evaluation conducted demonstrated that existing solutions present high performance in a controlled environment, which differs from real-world applications, given the inherent complexity of business operations. The insights unveiled led to the identification of immediate open challenges, including environmental awareness, holistic intrusion detection, explainable identification, recognition robustness, deployable countermeasures, continuous detection improvement, and generalized discovery. In an individual evaluation, we discovered that operationalization remains a major issue and represents a challenging research direction for the next few years. Finally, future work also includes investigating other Machine Learning (ML) models applied to IDS in emerging technologies. Also, the investigation of interpretability mechanisms and their limitations is of vital importance to improve cyber defenses. Finally, a review of operationalization methods is in the scope of promising future work, paving the way for models to be effectively used in read business operations.

Author contributions E.C.P.N.: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Writing – original draft. S.I.: Conceptualization, Formal analysis, Funding acquisition, Investigation, Project administration, Supervision, Writing – original draft. S.B.: Investigation, Supervision, Writing – review and editing. M.S.: Investigation, Writing – review and editing. A.T.: Investigation, Writing – review and editing. All authors reviewed the manuscript.

Funding Open access funding provided by National Research Council Canada library. Open access funding provided by the National Research Council Canada.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

Abdellatif AA, Mohamed A, Chiasserini CF et al (2019) Edge computing for smart health: context-aware approaches, opportunities, and challenges. IEEE Netw 33(3):196–203

Abdulganiyu OH, Ait Tchakoucht T, Saheed YK (2023) A systematic literature review for network intrusion detection system (ids). Int J Inf Secur 22(5):1125–1162

Abou El Houda Z, Brik B, Ksentini A et al (2023) A mec-based architecture to secure iot applications using federated deep learning. IEEE Internet Things Mag 6(1):60–63

Abusitta A, Bellaiche M, Dagenais M et al (2019) A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Futur Gener Comput Syst 98:308–318

Adeniyi O, Sadiq AS, Pillai P et al (2024) Securing mobile edge computing using hybrid deep learning method. Computers 13(1):25

Adjewa F, Esseghir M, Merghem-Boulahia L (2024) Llm-based continuous intrusion detection framework for next-gen networks. arXiv preprint arXiv:2411.03354
Ahmad Z, Shahid Khan A, Wai Shiang C et al (2021) Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol 32(1):e4150
Ahmed M, Byreddy S, Nutakki A et al (2021) Ecu-ioht: a dataset for analyzing cyberattacks in internet of health things. Ad Hoc Netw 122:102621
Ahsan SI, Legg P, Alam S (2024) Privacy-preserving intrusion detection in software-defined vanet using federated learning with bert. arXiv preprint arXiv:2401.07343
Ahuja N, Singal G, Mukhopadhyay D (2020) Ddos attack sdn dataset Mendeley Data 1:17632
Al-Shurbaji T, Anbar M, Manickam S et al (2025) Deep learning-based intrusion detection system for detecting iot botnet attacks: A review. IEEE Access, New York
Aldweesh A, Derhab A, Emam AZ (2020) Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues. Knowl-Based Syst 189:105124
Alladi T, Chamola V, Zeadally S (2020) Industrial control systems: cyberattack trends and countermeasures. Comput Commun 155:1–8
Almiani M, AbuGhazleh A, Al-Rahayfeh A et al (2020) Deep recurrent neural network for iot intrusion detection system. Simul Model Pract Theory 101:102031
Altamimi S, Salameh W (2024) Deepfake video detection: Analysis for deep learning models using transfer learning. In: 2024 25th International Arab Conference on Information Technology (ACIT), IEEE, pp 1–9
Alzughaibi S, El Khediri S (2023) A cloud intrusion detection systems based on dnn using backpropagation and pso on the cse-cic-ids2018 dataset. Appl Sci 13(4):2276
Aminanto ME, Choi R, Tanuwidjaja HC et al (2017) Deep abstraction and weighted feature selection for wi-fi impersonation detection. IEEE Trans Inf Forensics Secur 13(3):621–636
Ann S, Cho SJ, Kim H (2024) A preliminary study on an intrusion detection method using large language models in industrial control systems. In: 2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, pp 600–602
Archana, HP C, Khushi et al (2021) Cloud-based network intrusion detection system using deep learning. In: The 7th Annual International Conference on Arab Women in Computing in Conjunction with the 2nd Forum of Women in Research, pp 1–6
Asharf J, Moustafa N, Khurshid H et al (2020) A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions. Electronics 9(7):1177
Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805
Bace RG, Mell P et al (2001) Intrusion detection systems. US Department of Commerce, Technology Administration, National Institute
Bank D, Koenigstein N, Giryes R (2023) Autoencoders. Machine learning for data science handbook: data mining and knowledge discovery handbook pp 353–374
Berde P, Gerola M, Hart J et al (2014) Onos: towards an open, distributed sdn os. In: Proceedings of the third workshop on Hot topics in software defined networking, pp 1–6
Bhamare D, Zolanvari M, Erbad A et al (2020) Cybersecurity for industrial control systems a survey. Comput Secur 89:101677
Bhutto AB, Vu XS, Elmroth E et al (2022) Reinforced transformer learning for vsi-ddos detection in edge clouds. IEEE Access 10:94677–94690
Boyes H, Hallaq B, Cunningham J et al (2018) The industrial internet of things (iiot): An analysis framework. Comput Ind 101:1–12
Bullinaria JA (2013) Recurrent neural networks. Neural Comput Lect 12:1–20
Cai Z, Du H, Wang H et al (2023) One-dimensional convolutional wasserstein generative adversarial network based intrusion detection method for industrial control systems. Electronics 12(22):4653
Cao K, Liu Y, Meng G et al (2020) An overview on edge computing research. IEEE Access 8:85714–85728
Chen J, Ran X (2019) Deep learning with edge computing: a review. Proc IEEE 107(8):1655–1674
Chkirbene Z, Abdallah HB, Hassine K et al (2021) Data augmentation for intrusion detection and classification in cloud networks. In: 2021 International Wireless Communications and Mobile Computing (IWCMC), IEEE, pp 831–836
Coldwell C, Conger D, Goodell E et al (2022) Machine learning 5g attack detection in programmable logic. In: 2022 IEEE Globecom Workshops (GC Wkshps), pp 1365–1370, https://doi.org/10.11578/dc.20220811.1
Contreras-Castillo J, Zeadally S, Guerrero-Ibañez JA (2017) Internet of vehicles: architecture, protocols, and security. IEEE Internet Things J 5(5):3701–3709
Creech G, Hu J (2013) A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Trans Comput 63(4):807–819

Cui J, Sun H, Zhong H et al (2023) Collaborative intrusion detection system for sdvn: A fairness federated deep learning approach. IEEE Transactions on Parallel and Distributed Systems
Cybenko G (1989) Approximation by superpositions of a sigmoidal function. Math Control Signals Syst 2(4):303–314
Dadkhah S, Mahdikhani H, Danso PK et al (2022) Towards the development of a realistic multidimensional iot profiling dataset. 2022 19th Annual International Conference on Privacy, Security & Trust (PST). IEEE, New York, pp 1–11
Dadkhah S, Carlos Pinto Neto E, Ferreira R et al (2024) Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing iomt device security. Raphael and Chukwuka Molokwu, Reginald and Sadeghi, Somayeh and Ghorbani, Ali, CiCIoMT2024: Attack Vectors in Healthcare Devices-A Multi-Protocol Dataset for Assessing IoMT Device Security
Doersch C (2016) Tutorial on variational autoencoders. arXiv preprint arXiv:1606.05908
Elsayed MS, Le-Khac NA, Jurcut AD (2020) Insdn: a novel sdn intrusion dataset. Ieee Access 8:165263–165284
Ezeme OM, Mahmoud QH, Azim A (2019) A deep learning approach to distributed anomaly detection for edge computing. In: 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), IEEE, pp 992–999
Faruqui N, Yousuf MA, Whaiduzzaman M et al (2023) Safetymed: a novel iomt intrusion detection system using cnn-lstm hybridization. Electronics 12(17):3541
Fernando OA, Xiao H, Spring J (2023) New algorithms for the detection of malicious traffic in 5g-mec. In: 2023 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, pp 1–6
Ferrag MA, Friha O, Hamouda D et al (2022) Edge-iiotset: a new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning. IEEE Access 10:40281–40306
Filali A, Abouaomar A, Cherkaoui S et al (2020) Multi-access edge computing: a survey. IEEE Access 8:197017–197046
Gad AR, Nashat AA, Barkat TM (2021) Intrusion detection system using machine learning for vehicular ad hoc networks based on ton-iot dataset. IEEE Access 9:142206–142217
Gamage S, Samarabandu J (2020) Deep learning methods in network intrusion detection: a survey and an objective comparison. J Netw Comput Appl 169:102767
Gao J et al (2022) Network intrusion detection method combining cnn and bilstm in cloud computing environment. Computational intelligence and neuroscience 2022
Garcez A, Lamb LC (2023) Neurosymbolic ai: the 3rd wave. Artif Intell Rev 56(11):12387–12406
Garcia S, Parmisano A, Erquiaga MJ (2020) Iot-23: A labeled dataset with malicious and benign iot network traffic. Praha, Czech Republic, Tech Rep, Stratosphere Lab
Ghubaish A, Salman T, Zolanvari M et al (2020) Recent advances in the internet-of-medical-things (iomt) systems security. IEEE Internet Things J 8(11):8707–8718
Gong C, Liu J, Zhang Q et al (2010) The characteristics of cloud computing. In: 2010 39th International Conference on Parallel Processing Workshops, IEEE, pp 275–279
Goodfellow I, Bengio Y, Courville A et al (2016) Deep learning
Goodfellow I, Pouget-Abadie J, Mirza M et al (2020) Generative adversarial networks. Commun ACM 63(11):139–144
Gu J, Wang Z, Kuen J et al (2018) Recent advances in convolutional neural networks. Pattern Recogn 77:354–377
Gude N, Koponen T, Pettit J et al (2008) Nox: towards an operating system for networks. ACM SIGCOMM Comput Commun Rev 38(3):105–110
Guerra-Manzanares A, Medina-Galindo J, Bahsi H et al (2020) Medbiot: Generation of an iot botnet dataset in a medium-sized iot network. In: ICISSP, pp 207–218
Gümüşbaş D, Yıldırım T, Genovese A et al (2020) A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. IEEE Syst J 15(2):1717–1731
Gyamfi E, Jurcut A (2022) M-tads: A multi-trust dos attack detection system for mec-enabled industrial Iot. In: 2022 IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, pp 166–172
Hady AA, Ghubaish A, Salman T et al (2020) Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access 8:106576–106584
Hamidpour H, Bushehrian O (2023) A round-based network attack detection model using auto-encoder in iot-edge computing. In: 2023 7th International Conference on Internet of Things and Applications (IoT), IEEE, pp 1–6
Hasan MK, Sulaiman R, Islam S et al (2023) An explainable ensemble deep learning approach for intrusion detection in industrial internet of things. IEEE Access
Hijazi S, Kumar R, Rowen C et al (2015) Using convolutional neural networks for image recognition. Cadence Des Syst Inc San Jose CA USA 9(1):39

Hilal AM, Alohali MA, Al-Wesabi FN et al (2023) Enhancing quality of experience in mobile edge computing using deep learning based data offloading and cyberattack detection technique. Clust Comput 10:1–12
Hindy H, Bayne E, Bures M et al (2020) Machine learning based iot intrusion detection system: An mqtt case study (mqtt-iot-ids2020 dataset). In: International networking conference, Springer, pp 73–84
Hinojosa A, Majd NE (2024) Edge computing network intrusion detection system in iot using deep learning. In: 2024 33rd International Conference on Computer Communications and Networks (ICCCN), IEEE, pp 1–6
Hodo E, Bellekens X, Hamilton A et al (2017) Shallow and deep networks intrusion detection system: A taxonomy and survey. arXiv preprint arXiv:1701.02145
Hu W, Cao Q, Darbandi M et al (2024) A deep analysis of nature-inspired and meta-heuristic algorithms for designing intrusion detection systems in cloud/edge and iot: state-of-the-art techniques, challenges, and future directions. Clust Comput 27(7):8789–8815
Hussain F, Abbas SG, Shah GA et al (2021) A framework for malicious traffic detection in iot healthcare environment. Sensors 21(9):3025
Hussain J, Hnamte V (2021) Deep learning based intrusion detection system: Software defined network. In: 2021 Asian Conference on Innovation in Technology (ASIANCON), IEEE, pp 1–6
Islam S, Elmekki H, Elsebai A et al (2024) A comprehensive survey on applications of transformers for deep learning tasks. Exp Syst Appl 241:122666
Jadeja Y, Modi K (2012) Cloud computing-concepts, architecture and challenges. In: 2012 international conference on computing, electronics and electrical technologies (ICCEET), IEEE, pp 877–880
Jahromi AN, Karimipour H, Dehghantanha A (2021) Deep federated learning-based cyber-attack detection in industrial control systems. 2021 18th International Conference on Privacy. IEEE, Security and Trust (PST), pp 1–6
Janabi AH, Kanakis T, Johnson M (2022) Convolutional neural network based algorithm for early warning proactive system security in software defined networks. IEEE Access 10:14301–14310
Jarraya Y, Madi T, Debbabi M (2014) A survey and a layered taxonomy of software-defined networking. IEEE Commun Surv Tutor 16(4):1955–1980
Ji B, Zhang X, Mumtaz S et al (2020) Survey on the internet of vehicles: network architectures and applications. IEEE Commun Stand Mag 4(1):34–41
Jiang W, Lee D, Hu S (2012) Large-scale longitudinal analysis of soap-based and restful web services. In: 2012 ieee 19th international conference on web services, IEEE, pp 218–225
Jin K, Zhang L, Zhang Y et al (2023) A network traffic intrusion detection method for industrial control systems based on deep learning. Electronics 12(20):4329
Kadhum M, Manaseer S, Dalhoum ALA (2019) Cloud-edge network data processing based on user requirements using modify mapreduce algorithm and machine learning techniques. Int J Adv Comput Sci Appl 10(12):1
Kairouz P, McMahan HB, Avent B et al (2021) Advances and open problems in federated learning. Found Trends ® Mach Learn 14(1–2):1–210
Kan X, Fan Y, Fang Z et al (2021) A novel iot network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network. Inf Sci 568:147–162
Kang H, Ahn DH, Lee GM et al (2019) Iot network intrusion dataset IEEE Dataport 10:q70p–q449
Khan IA, Pi D, Abbas MZ et al (2022) Federated-srus: a federated simple recurrent units-based ids for accurate detection of cyber attacks against iot-augmented industrial control systems. IEEE Internet Things J 10(10):8467–8476
Khraisat A, Gondal I, Vamplew P et al (2019) Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity 2(1):1–22
Kim Y, Hakak S, Ghorbani A (2023) Ddos attack dataset (cicev2023) against ev authentication in charging infrastructure. 2023 20th Annual International Conference on Privacy. IEEE, Security and Trust (PST), pp 1–9
Knowles W, Prince D, Hutchison D et al (2015) A survey of cyber security management in industrial control systems. Int J Crit Infrastruct Prot 9:52–80
Kolias C, Kambourakis G, Stavrou A et al (2015) Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Commun Surv Tutor 18(1):184–208
Kong W, Li X, Hou L et al (2020) An efficient and credible multi-source trust fusion mechanism based on time decay for edge computing. Electronics 9(3):502
Koroniotis N, Moustafa N, Sitnikova E et al (2019) Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Futur Gener Comput Syst 100:779–796
Kravchik M, Shabtai A (2018) Detecting cyber attacks in industrial control systems using convolutional neural networks. In: Proceedings of the 2018 workshop on cyber-physical systems security and privacy, pp 72–83

Kreutz D, Ramos FM, Verissimo PE et al (2014) Software-defined networking: a comprehensive survey. Proc IEEE 103(1):14–76
Kriaa S, Pietre-Cambacedes L, Bouissou M et al (2015) A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst safe 139:156–178
Lahasan B, Samma H (2022) Optimized deep autoencoder model for internet of things intruder detection. IEEE Access 10:8434–8448
Lansky J, Ali S, Mohammadi M et al (2021) Deep learning-based intrusion detection systems: a systematic review. IEEE Access 9:101574–101599
Lee H, Jeong SH, Kim HK (2017) Otids: A novel intrusion detection system for in-vehicle network by using remote frame. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), pp 57–570. https://doi.org/10.1109/PST.2017.00017
Lee SJ, Yoo PD, Asyhari AT et al (2020) Impact: impersonation attack detection via edge computing using deep autoencoder and feature abstraction. IEEE Access 8:65520–65529
Li T, Sahu AK, Talwalkar A et al (2020) Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag 37(3):50–60
Li X, Huang K, Yang W et al (2019) On the convergence of fedavg on non-iid data. arXiv preprint arXiv:1907.02189
Li Y, Xiang Z, Bastian ND et al (2024) Ids-agent: An llm agent for explainable intrusion detection in iot networks. In: NeurIPS 2024 Workshop on Open-World Agents
Li Z, Liu F, Yang W et al (2021) A survey of convolutional neural networks: analysis, applications, and prospects. IEEE Trans Neural Netw Learn Syst 33(12):6999–7019
Liao H, Murah MZ, Hasan MK et al (2024) A survey of deep learning technologies for intrusion detection in internet of things. IEEe Access 12:4745–4761
Lin J, Yu W, Yang X et al (2020) An edge computing based public vehicle system for smart transportation. IEEE Trans Veh Technol 69(11):12635–12651
Ling J, Zhu Z, Luo Y et al (2021) An intrusion detection method for industrial control systems based on bidirectional simple recurrent unit. Comput Electr Eng 91:107049
Lipton ZC, Berkowitz J, Elkan C (2015) A critical review of recurrent neural networks for sequence learning. arXiv preprint arXiv:1506.00019
Liu H, Lang B (2019) Machine learning and deep learning methods for intrusion detection systems: a survey. Appl Sci 9(20):4396
Liu X, Zhang W, Zhou X et al (2021) Mecguard: Gru enhanced attack detection in mobile edge computing environment. Comput Commun 172:1–9
Liyanage M, Porambage P, Ding AY et al (2021) Driving forces for multi-access edge computing (mec) iot integration in 5g. ICT Express 7(2):127–137
Long Z, Yan H, Shen G et al (2024) A transformer-based network intrusion detection approach for cloud security. J Cloud Comput 13(1):5
Lundberg SM, Lee SI (2017) A unified approach to interpreting model predictions. Adv Neural Inf Process Syst 30:12
Lunt TF, Jagannathan R, Lee R et al (1989) Knowledge based intrusion detection. In: Proceedings of the Annual AI Systems in Government Conference, Washington, DC
Mach P, Becvar Z (2017) Mobile edge computing: a survey on architecture and computation offloading. IEEE Commun Surv Tutor 19(3):1628–1656
Maciá-Fernández G, Camacho J, Magán-Carrión R et al (2018) Ugr '16: a new dataset for the evaluation of cyclostationarity-based network idss. Comput Secur 73:411–424
Mahmood Z (2011) Cloud computing for enterprise architectures: concepts, principles and approaches
Makuvaza A, Jat DS, Gamundani AM (2021) Deep neural network (dnn) solution for real-time detection of distributed denial of service (ddos) attacks in software defined networks (sdns). SN Comput Sci 2(2):107
Mao Y, You C, Zhang J et al (2017) A survey on mobile edge computing: the communication perspective. IEEE Commun Surv Tutor 19(4):2322–2358
McHugh J (2000) Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Trans Inf Syst Secur (TISSEC) 3(4):262–294
McLaughlin S, Konstantinou C, Wang X et al (2016) The cybersecurity landscape in industrial control systems. Proc IEEE 104(5):1039–1057
Medved J, Varga R, Tkacik A et al (2014) Opendaylight: Towards a model-driven sdn controller architecture. In: Proceeding of IEEE international symposium on a world of wireless, mobile and multimedia networks 2014, IEEE, pp 1–6
Meidan Y, Bohadana M, Mathov Y et al (2018) N-baiot-network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Comput 17(3):12–22

Mejia J, Ochoa-Zezzati A, Cruz-Mejía O (2020) Traffic forecasting on mobile networks using 3d convolutional layers. Mobile Netw Appl 25:2134–2140
Mirashe SP, Kalyankar NV (2010) Cloud computing. arXiv preprint arXiv:1003.4074
Mirsky Y, Doitshman T, Elovici Y et al (2018) Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint arXiv:1802.09089
Morris T, Gao W (2014) Industrial control system traffic data sets for intrusion detection research. In: Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference, ICCIP 2014, Arlington, VA, USA, March 17-19, 2014, Revised Selected Papers 8, Springer, pp 65–78
Moustafa N, Slay J (2015) Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 military communications and information systems conference (MilCIS), IEEE, pp 1–6
Muneer S, Farooq U, Athar A et al (2024) A critical review of artificial intelligence based approaches in intrusion detection: a comprehensive analysis. J Eng 1:3909173
Myneni S, Chowdhary A, Huang D et al (2022) Smartdefense: a distributed deep defense against ddos attacks with edge computing. Comput Netw 209:108874
Neto ECP, Dadkhah S, Ghorbani AA (2022) Collaborative ddos detection in distributed multi-tenant iot using federated learning. In: 2022 19th Annual International Conference on Privacy, Security & Trust (PST), IEEE, pp 1–10
Neto ECP, Dadkhah S, Ferreira R et al (2023) Ciciot 2023: a real-time dataset and benchmark for large-scale attacks in iot environment. Sensors 23(13):5941
Neto ECP, Taslimasa H, Dadkhah S et al (2024) Ciciov 2024: advancing realistic ids approaches against dos and spoofing attack in iov can bus. Internet Things 26:101209
Novaes MP, Carvalho LF, Lloret J et al (2021) Adversarial deep learning approach detection and defense against ddos attacks in sdn environments. Futur Gener Comput Syst 125:156–167
Pan Z, Yu W, Yi X et al (2019) Recent progress on generative adversarial networks (gans): a survey. IEEE Access 7:36322–36333
Parker LR, Yoo PD, Asyhari TA et al (2019) Demise: Interpretable deep extraction and mutual information selection techniques for iot intrusion detection. In: Proceedings of the 14th international conference on availability, reliability and security, pp 1–10
Patel A, Qassim Q, Wills C (2010) A survey of intrusion detection and prevention systems. Inf Manag Comput Secur 18(4):277–290
Porambage P, Okwuibe J, Liyanage M et al (2018) Survey on multi-access edge computing for internet of things realization. IEEE Commun Surv Tutor 20(4):2961–2991
Radoglou-Grammatikis P, Rompolos K, Sarigiannidis P et al (2021) Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach. IEEE Trans Industr Inf 18(3):2041–2052
Ramezan CA (2023) Examining the cyber skills gap: an analysis of cybersecurity positions by sub-field. J Inf Syst Educ 34(1):94–105
Ranaweera P, Jurcut AD, Liyanage M (2021) Survey on multi-access edge computing security and privacy. IEEE Commun Surv Tutor 23(2):1078–1124
Ravi V, Pham TD, Alazab M (2023) Deep learning-based network intrusion detection system for internet of medical things. IEEE Internet Things Mag 6(2):50–54
Ribeiro MT, Singh S, Guestrin C (2016) " why should i trust you?" explaining the predictions of any classifier. In: Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, pp 1135–1144
Ring M, Wunderlich S, Grüdl D et al (2017) Flow-based benchmark data sets for intrusion detection. In: Proceedings of the 16th European conference on cyber warfare and security. ACPI, pp 361–369
Rm B, MK JK (2023) Intrusion detection on aws cloud through hybrid deep learning algorithm. Electronics 12(6):1423
Sabahi F, Movaghar A (2008) Intrusion detection: A survey. In: 2008 Third International Conference on Systems and Networks Communications, IEEE, pp 23–26
Sadaf K, Sultana J (2020) Intrusion detection based on autoencoder and isolation forest in fog computing. IEEE Access 8:167059–167068
Said D, Stirling L, Federolf P et al (2011) Data preprocessing for distance-based unsupervised intrusion detection. 2011 Ninth Annual International Conference on Privacy. IEEE, Security and Trust, pp 181–188
Said RB, Sabir Z, Askerzade I (2023) Cnn-bilstm: a hybrid deep learning approach for network intrusion detection system in software defined networking with hybrid feature selection. IEEE Access, New York
Saied M, Adjogble F, Guirguis S et al (2023a) A framework for systematic scientific research management. In: 2023 Portland International Conference on Management of Engineering and Technology (PICMET), IEEE, pp 1–16

Saied M, Guirguis S, Madbouly M (2023) A comparative analysis of using ensemble trees for botnet detection and classification in iot. Sci Rep 13(1):21632
Saied M, Guirguis S, Madbouly M (2023) A comparative study of using boosting-based machine learning algorithms for iot network intrusion detection. Int J Comput Intel Syst 16(1):177
Saied Essa M, Kamal Guirguis S (2023) Evaluation of tree-based machine learning algorithms for network intrusion detection in the internet of things. IT Profession 25(5):45–56
Salehinejad H, Sankar S, Barfett J et al (2017) Recent advances in recurrent neural networks. arXiv preprint arXiv:1801.01078
Samarakoon S, Siriwardhana Y, Porambage P et al (2022) 5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network. arXiv preprint arXiv:2212.01298
Sanagana DPR, Tummalachervu CK (2024) Securing cloud computing environment via optimal deep learning-based intrusion detection systems. In: 2024 Second International Conference on Data Science and Information System (ICDSIS), IEEE, pp 1–6
Satyanarayanan M (2017) The emergence of edge computing. Computer 50(1):30–39
Saxena D, Cao J (2021) Generative adversarial networks (gans) challenges, solutions, and future directions. ACM Comput Surv (CSUR) 54(3):1–42
Sedjelmaci H, Ansari N (2022) On cooperative federated defense to secure multi-access edge computing. IEEE Consumer Electronics Magazine
Seo E, Song HM, Kim HK (2018) Gids: Gan based intrusion detection system for in-vehicle network. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp 1–https://doi.org/10.1109/PST.2018.8514157
Shahzadi S, Iqbal M, Dagiuklas T et al (2017) Multi-access edge computing: open issues, challenges and future perspectives. J Cloud Comput 6:1–13
Sharafaldin I, Lashkari AH, Ghorbani AA (2018) Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp 1:108–116
Sharafaldin I, Lashkari AH, Hakak S et al (2019) Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In: 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, pp 1–8
Shiravi A, Shiravi H, Tavallaee M et al (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput Secur 31(3):357–374
Singh P, Pankaj A, Mitra R et al (2021) Edge-detect: edge-centric network intrusion detection using deep neural network. In: 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), IEEE, pp 1–6
Song HM, Woo J, Kim HK (2020) In-vehicle network intrusion detection using deep convolutional neural network. Vehic Commun 21:100198
Song J, Takakura H, Okabe Y et al (2011) Statistical analysis of honeypot data and building of kyoto 2006+ dataset for nids evaluation. In: Proceedings of the first workshop on building analysis datasets and gathering experience returns for security, pp 29–36
Stanoevska-Slabeva K, Wozniak T (2010) Cloud basics - an introduction to cloud computing. Springer, Berlin
Talari S, Shafie-Khah M, Siano P et al (2017) A review of smart cities based on the internet of things concept. Energies 10(4):421
Tanenbaum AS (2003) Computer networks. Pearson Education India
Tang C, Zhu C, Wu H et al (2021) Toward response time minimization considering energy consumption in caching-assisted vehicular edge computing. IEEE Internet Things J 9(7):5051–5064
Tang TA, Mhamdi L, McLernon D et al (2016) Deep learning approach for network intrusion detection in software defined networking. In: 2016 international conference on wireless networks and mobile communications (WINCOM), IEEE, pp 258–263
Tang TA, Mhamdi L, McLernon D et al (2018) Deep recurrent neural network for intrusion detection in sdn-based networks. In: 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), IEEE, pp 202–206
Tang TA, Mhamdi L, McLernon D et al (2020) Deepids: deep learning approach for intrusion detection in software defined networking. Electronics 9(9):1533
Tavallaee M, Bagheri E, Lu W et al (2009) A detailed analysis of the kdd cup 99 data set. In: 2009 IEEE symposium on computational intelligence for security and defense applications, Ieee, pp 1–6
Teixeira MA, Salman T, Zolanvari M et al (2018) Scada system testbed for cybersecurity research using machine learning approach. Future Internet 10(8):76
Tengku Asmawi TN, Ismail A, Shen J (2022) Cloud failure prediction based on traditional machine learning and deep learning. J Cloud Comput 11(1):47
Thakur K, Kumar G (2021) Nature inspired techniques and applications in intrusion detection systems: Recent progress and updated perspective. Arch Comput Methods Eng 28(4):2897–2919

Tran TX, Pompili D (2018) Joint task offloading and resource allocation for multi-server mobile-edge computing networks. IEEE Trans Veh Technol 68(1):856–868
Van Der Heijden RW, Lukaseder T, Kargl F (2018) Veremi: A dataset for comparable evaluation of misbehavior detection in vanets. In: Security and Privacy in Communication Networks: 14th International Conference, SecureComm 2018, Singapore, Singapore, August 8-10, 2018, Proceedings, Part I, Springer, pp 318–337
Vaswani A (2017) Attention is all you need. Adv Neural Inf Process Syst 10:7
Verma A, Ranga V (2018) Statistical analysis of cidds-001 dataset for network intrusion detection systems using distance-based machine learning. Proc Comput Sci 125:709–716
Verma ME, Iannacone MD, Bridges RA et al (2020) Road: The real ornl automotive dynamometer controller area network intrusion detection dataset (with a comprehensive can ids dataset survey & guide). arXiv preprint arXiv:2012.14600
Vinayakumar R, Alazab M, Soman KP et al (2019) Deep learning approach for intelligent intrusion detection system. Ieee Access 7:41525–41550
Vu L, Nguyen QU, Nguyen DN et al (2022) Deep generative learning models for cloud intrusion detection systems. IEEE Trans Cybern 53(1):565–577
Wang C, Wang B, Liu H et al (2020) Anomaly detection for industrial control system based on autoencoder neural network. Wirel Commun Mob Comput 1:8897926
Wang L, Chen S, Chen F et al (2023) B-detection: Runtime reliability anomaly detection for mec services with boosting lstm autoencoder. IEEE Transactions on Mobile Computing
Wang W, Du X, Shan D et al (2020) Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE Trans Cloud Comput 10(3):1634–1646
Wu M, Lu TJ, Ling FY et al (2010) Research on the architecture of internet of things. In: 2010 3rd international conference on advanced computer theory and engineering (ICACTE), IEEE, pp V5–484
Xia W, Wen Y, Foh CH et al (2014) A survey on software-defined networking. IEEE Commun Surv Tutor 17(1):27–51
Yang L, Shami A (2022) A transfer learning and optimized cnn based intrusion detection system for internet of vehicles. In: ICC 2022-IEEE International Conference on Communications, IEEE, pp 2774–2779
Yang L, Song Y, Gao S et al (2022) Griffin: Real-time network intrusion detection system via ensemble of autoencoder in sdn. IEEE Trans Netw Serv Manage 19(3):2269–2281
Yaras S, Dener M (2024) Iot-based intrusion detection system using new hybrid deep learning algorithm. Electronics 13(6):1053
Yuan D, Ota K, Dong M et al (2020) Intrusion detection for smart home security based on data augmentation with edge computing. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, pp 1–6
Yungaicela-Naula NM, Vargas-Rosales C, Perez-Diaz JA et al (2023) Physical assessment of an sdn-based security framework for ddos attack mitigation: Introducing the sdn-slowrate-ddos dataset. IEEE Access
Zanella A, Bui N, Castellani A et al (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
Zhang J, Guo H, Liu J et al (2019) Task offloading in vehicular edge computing networks: A load-balancing solution. IEEE Trans Veh Technol 69(2):2092–2104
Zhang J, Chen B, Cheng X et al (2020) Poisongan: Generative poisoning attacks against federated learning in edge computing systems. IEEE Internet Things J 8(5):3310–3322
Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1:7–18
Zhang W, Zhang Y et al (2022) Intrusion detection model for industrial internet of things based on improved autoencoder. Comput Intell Neurosci 2022:10
Zhang Y, Liu Y, Guo X et al (2022) A bilstm-based ddos attack detection method for edge computing. Energies 15(21):7882
Zubair M, Ghubaish A, Unal D et al (2022) Secure bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. Sensors 22(21):8280

Authors and Affiliations

Euclides Carlos Pinto Neto[1] · Shahrear Iqbal[1] · Scott Buffett[1] · Madeena Sultana[2] · Adrian Taylor[2]

✉ Shahrear Iqbal
Shahrear.Iqbal@nrc-cnrc.gc.ca

Euclides Carlos Pinto Neto
EuclidesCarlos.PintoNeto@nrc-cnrc.gc.ca

Scott Buffett
Scott.Buffett@nrc-cnrc.gc.ca

Madeena Sultana
Madeena.Sultana@ecn.forces.gc.ca

Adrian Taylor
Adrian.Taylor@forces.gc.ca

[1] National Research Council Canada, Fredericton, NB, Canada

[2] Defence Research and Development Canada (DRDC), Ottawa, ON, Canada