Cluster Computing (2024) 27:9065–9089
https://doi.org/10.1007/s10586-024-04509-0

Securing internet of things using machine and deep learning methods: a survey

Ali Ghaffari[1,2,3] · Nasim Jelodari[1] · Samira pouralish[1] · Nahide derakhshanfard[1] · Bahman Arasteh[2]

Received: 10 December 2023 / Revised: 20 March 2024 / Accepted: 5 April 2024 / Published online: 16 April 2024

Abstract
The Internet of Things (IoT) is a vast network of devices with sensors or actuators connected through wired or wireless networks. It has a transformative effect on integrating technology into people's daily lives. IoT covers essential areas such as smart cities, smart homes, and health-based industries. However, security and privacy challenges arise with the rapid growth of IoT devices and applications. Vulnerabilities such as node spoofing, unauthorized access to data, and cyberattacks such as denial of service (DoS), eavesdropping, and intrusion detection have emerged as significant concerns. Recently, machine learning (ML) and deep learning (DL) methods have significantly progressed and are robust solutions to address these security issues in IoT devices. This paper comprehensively reviews IoT security research focusing on ML/DL approaches. It also categorizes recent studies on security issues based on ML/DL solutions and highlights their opportunities, advantages, and limitations. These insights provide potential directions for future research challenges.

Keywords Internet of things · Machine learning · Deep learning · Security

1 Introduction

The Internet of Things (IoT) is a network where various intelligent objects and devices communicate over the Internet [1, 2]. The total number of connected devices globally is approximately 17 billion, and IoT devices make up 7 billion of that number (excluding smartphones, tablets, and laptops). Projections indicate that this number will reach 75.44 billion devices worldwide by 2025 [3, 4]. IoT technologies are critical in advancing various applications in healthcare [5], home automation, agriculture, transportation [6, 7], and education [8, 9]. With ongoing technological advancements and expanding application domains [10], IoT has evolved into a collection of customized solutions designed for specific purposes [11, 12].

The IoT architecture consists of three layers: the terminal perception layer, the network layer, and the application layer. IoT systems' complexity and limited resources expose them to various security risks and dynamic and diverse threats [13–16]. Ensuring the security of these systems is a highly intricate and demanding task [17]. The expansion of IoT also brings forth numerous challenges in various IoT applications, including standardization, interoperability, data storage, processing, trust management, identity, and privacy [18–20]. These challenges encompass a broad spectrum of concerns that must be addressed to foster a secure and reliable IoT ecosystem [21–23].

The potential attack surface has expanded significantly with IoT devices' rapid growth and integration into various sectors [24]. This increased attack surface threatens the individual devices and the overall network infrastructure to which they are connected [25, 26]. DoS attacks, spoofing, jamming, eavesdropping, data manipulation, and malicious attacks are the most common IoT attacks. Attackers can exploit vulnerabilities within IoT systems to gain unauthorized access, manipulate data, disrupt services, or compromise privacy [27, 28]. Standardized protocols and interfaces are required to ensure seamless communication

✉ Ali Ghaffari
A.Ghaffari@iaut.ac.ir

[1] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

[2] Department of Computer Engineering, Faculty of Engineering and Natural Science, Istinye University, Istanbul, Türkiye

[3] Department of Computer Science, Khazar University, Baku, Azerbaijan

and collaboration among IoT devices and platforms [29, 30]. This can lead to compatibility issues, data fragmentation, and difficulties in managing and securing heterogeneous IoT environments.

Moreover, the large amount of data generated by IoT devices poses challenges for storage, processing, and analysis. Efficient data management strategies, including secure storage and effective processing mechanisms, are essential to derive meaningful insights from the vast amounts of data generated by IoT systems while ensuring privacy and protecting sensitive information. Trust management is another crucial aspect in the IoT domain. Establishing trust among various entities, such as devices, applications, and users, is necessary to ensure secure interactions and data exchange. Building robust trust models to authenticate and authorize entities is vital for maintaining the integrity and security of IoT systems. Confidentiality, integrity, and availability of data and services are paramount concerns in the IoT landscape [31]. Safeguarding confidentiality, ensuring the integrity of transmitted and stored information, and guaranteeing the availability of critical services require robust security measures, including encryption, access control mechanisms, intrusion detection systems, and redundancy planning. In addition to security, privacy is a fundamental right that must be preserved in the IoT ecosystem [32]. Collecting and processing vast amounts of personal data through IoT devices can lead to privacy breaches and expose individuals to various risks. Implementing privacy-by-design principles, ensuring user consent, and adopting privacy-enhancing technologies are crucial to protecting individuals' privacy within the IoT framework [33]. Addressing these multifaceted challenges and developing comprehensive solutions are imperative for the sustainable growth and secure deployment of IoT systems. Collaboration among industry stakeholders, policymakers, and researchers is crucial to establishing best practices, regulations, and standards that promote the security, privacy, and reliability of IoT [34].

Therefore, appropriate security techniques are proposed depending on the particular security concerns. The focus of this paper is specifically on the use of ML/DL techniques. These techniques significantly address security issues and find applications in various domains, including speech recognition and image processing [35]. Their versatility and effectiveness make them valuable tools for enhancing security and enabling advancements in multiple fields. ML is a method that autonomously and intelligently performs computational tasks that require careful design and testing using different approaches [36]. ML requires an efficient process for computing and storing vast data. In contrast, DL is a type of ML that is computationally complex and expensive. It can automatically extract high-level features from surface features, making it an ideal solution to address security concerns in IoT. In addition, DL has made significant advances in training complex deep neural network structures [37], leading to improved decision-making capabilities for a wide range of detection, classification, and prediction tasks [38].

This paper reviewed the recently presented survey papers based on ML/DL and compared them with this paper. However, this paper aims to identify the security challenges and threats hamper IoT applications. We analyze many research models related to the main threats and present a new taxonomy in the field of artificial intelligence. This survey thoroughly examines recent literature concerning deep learning and machine learning techniques applied to IoT security, constituting a substantial contribution to the field. The main contributions of this paper are as follows:

- This paper comprehensively discusses the security challenges of the IoT.
- This paper examines the inherent vulnerability and cyber threats associated with IoT systems and emphasizes the critical role of ML/DL techniques in reducing these risks.
- This paper addresses state-of-the-art IoT-specific challenges, including cyberattacks, eavesdropping, DoS, unauthorized data access, and intrusion detection.
- The main objective of this paper is to comprehensively analyze and classify the various ML/DL methods proposed for IoT security and to evaluate their strengths and weaknesses accurately.
- This paper expresses various prospective research challenges and future pathways for the application of ML/DL to ensure the security of IoT.

The next sections of this article are as follows: Sect. 2 discusses the historical background of the field and reviews the relevant literature. Section 3 focuses on the IoT system architecture, which includes various layers, and explains the security concerns associated with each layer. In Sect. 4, security challenges in the IoT are examined. Part 5 presents a range of security solutions based on machine learning and deep learning in IoT environments. Section 6 emphasizes the challenges ahead, potential areas for further research, and future perspectives. Finally, Sect. 7 concludes the paper.

Table 1 shows the acronyms and abbreviations.

2 Related works

In [39], the authors examined the IoT paradigm, focusing on intelligent environments that utilize the Internet of Things. The authors also address security issues concerning machine learning solutions. Furthermore, the article

Table 1 Acronyms and abbreviations

Abbreviation	Term
AI	Artificial intelligence
ANN	Artificial Neural Network
CNN	Convolutional Neural Network
DT	Decision Tree
DL	Deep Learning
DoS	Denial of Service
DDoS	Distributed Denial of Service
GSM	Global System for Mobile
5G	5th Generation
NT-GNN	Network Traffic NN
IoT	Internet of Things
IF	Isolation Forest
IDS	Intrusion Detection Systems
IPv4	Internet Protocol Version 4
MAC	Medium Access Control
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
SDN	Software Defined Network
SVM	Support Vector Machine
SLR	Systematic Literature Review
GNN	Graph Neural Network
LSTM	Long-Short-Term Memory
LDoS	Low-Rate Denial of Service
GRU	Gated Recurrent Unit
MDE	Model-Driven Engineering
MitM	Man-in-the-Middle
RBF	Radial Basis Function
RFID	Radio Frequency Identification
RMC-CNN	robust multi-cascade CNN
SLR	Systematic Literature Review
WiFi	Wireless Fidelity
WiMax	World Interoperability for Microwave Access

highlights the importance of security and explores diverse deep and machine-learning methods that can be applied to enhance security within the IoT domain. Additionally, the authors discuss and investigate potential future approaches centered around advanced learning techniques.

In [40], the authors provided an in-depth analysis of security concepts within the IoT domain, explicitly focusing on cyber security. The article explores integrating artificial intelligence models to address security concerns from various angles in IoT applications. Moreover, the authors emphasize incorporating deep learning approaches to strengthen security measures further.

In [41], the authors briefly introduce the IoT and its applications while addressing security concerns such as confidentiality, integrity, and availability across different layers. The primary focus of this article lies in conducting an extensive evaluation of machine learning (ML), artificial intelligence (AI), and blockchain methods aimed at resolving security challenges arising in the realm of IoT. Furthermore, the article also highlights additional security issues that can be effectively tackled by implementing ML, AI, and blockchain technologies.

In [42], the authors encompassed an in-depth analysis of current IoT security studies. The authors give particular attention to examining intrusion detection systems, emphasizing those that utilize deep learning techniques. Furthermore, they contribute a comprehensive classification system, aligning specific security threats with the corresponding components of the Cisco IoT reference model to provide a holistic understanding of the potential vulnerabilities in the IoT ecosystem. The progress in machine learning and deep learning has opened up new possibilities for creating potent techniques to enhance Internet of Things security. The primary objective of [43] is to conduct an in-depth review of comprehensive studies in this domain. Additionally, it furnishes an extensive compilation of the attributes and obstacles associated with utilizing machine learning and deep learning to secure the Internet of Things frameworks. These insights will contribute to a better understanding of how these advanced technologies can safeguard IoT systems.

In [44], the authors provided a comprehensive overview of the context of the security of the Internet of Things. They also presented a detailed classification of deep learning techniques, followed by an extensive systematic review focusing on three key aspects: security considerations, the implementation of DL architectures, and their application areas, along with the datasets employed. This article primarily focused on the deep learning approaches proposed to address security challenges within the Internet of Things. By focusing solely on these tactics, the authors aimed to offer valuable insights into the effective use of DL in bolstering IoT security.

In [45], the authors initially present an overview of the existing research, offering a classification based on IoT vulnerabilities, the types of attackers involved, and the effects and threats. The analysis delves into weak links, practical solutions, and enterprise authentication technologies deployed to detect and address these vulnerabilities. Moreover, the paper encompasses real-time strategies to identify and manage large-scale malicious IoT devices. Additionally, it delves into observational literature to investigate and categorize network load generated by vulnerable sensors. Lastly, the paper reviews systematic treatment methodologies, culminating in well-informed conclusions. In [46], the authors comprehensively analyze IoT security measures, thoroughly examining four critical security threats concerning device authentication, DoS, and defenses against DDoS attacks. The paper focuses on intrusion detection and malware detection techniques while exploring the application of artificial intelligence (AI) methods, including ML and

DL, which are proposed to tackle these security challenges in IoT. Additionally, the authors shed light on the specific challenges of implementing these AI techniques within the IoT architecture.

The interconnected nature of the Internet of Things and the communication capabilities between devices give rise to security concerns within IoT networks. An intrusion detection system (IDS) is proposed to address this as an effective security mechanism for safeguarding IoT networks and devices. In [47], the authors comprehensively examined IDS, encompassing the classification of different IDS placement strategies and IDS analysis strategies within the IoT architecture. Furthermore, the study discusses various categories of intrusions that can occur in IoT. The paper explores utilizing machine learning (ML) and deep learning (DL) techniques to detect attacks within IoT networks. Additionally, security issues and challenges in the IoT ecosystem are thoroughly explored. The paper's conclusion emphasizes that current detection methods for IoT fall short of adequately addressing a wide range of attacks.

In [48], the authors thoroughly explored the primary security concerns and existing open challenges encountered in IoT infrastructure. Additionally, it conducts an in-depth examination and analysis of advanced ML-based approaches employed to secure IoT domains. The paper sheds light on the security demands and challenges within IoT-based systems while emphasizing the supportive role of ML in enhancing security measures in this domain. Despite the high accuracy achieved by ML-based solutions, they also introduce specific issues. Consequently, the study advocates for developing lightweight ML-based security solutions that operate efficiently within such frameworks. Alternatively, a layered approach may prove beneficial in this context. To this end, the analysis also delves into common limitations of ML security techniques.

In [49], the authors offered a comprehensive evaluation of ML and DL techniques proposed for enhancing security measures within IoT systems and securing the fundamental layers of IoT, namely the perception, network, and application layers. This article delves into the various IoT security threats, encompassing inherent and newly introduced risks. It explores potential attack levels within the IoT system and the associated threats at each level. Subsequently, the paper outlines the potential applications of ML and DL methods in IoT security, highlighting each approach's advantages, disadvantages, and opportunities. Furthermore, it addresses the opportunities and challenges of integrating ML/DL within IoT security practices. By delving into these aspects, the article aims to provide valuable insights into strengthening the security of IoT ecosystems.

In [50], the authors conducted an extensive survey on implementing deep learning in the context of security and privacy concerns within IoT. The main emphasis lies in utilizing deep learning techniques to address these security issues. To achieve this, the paper initially examines deep learning applications in IoT security from the perspectives of system architecture and the employed methods. Subsequently, it conducts a thorough analysis and evaluation of the effectiveness of deep learning in enhancing security measures. Additionally, the paper introduces a novel approach involving a functional layer to facilitate meaningful device modeling, thus improving feature mapping for precise device identification. In [51], the primary emphasis of the authors lies in conducting a Systematic Literature Review (SLR) that explores diverse research areas related to IoT, cyber security, machine Learning, and big data. This review article briefly covers three main topics: (i) Machine learning algorithms commonly employed for enhancing IoT security, (ii) the susceptibility of large-scale IoT attacks, and (iii) various machine learning approaches and techniques utilized to detect and mitigate such attacks.

In [52], a novel and optimized architecture for IoT is introduced, consisting of five distinct layers. A fresh classification of threats and security attacks targeting IoT devices is presented based on the newly proposed architecture. These layers encompass a physical understanding layer a network and protocol layer, a transmission layer, an application layer, a data layer, and cloud services. The paper also highlights several open research topics, such as the need for standardized encryption algorithms, the potential of machine learning algorithms to strengthen security and the accompanying challenges, the application of blockchain for resolving security issues in the IoT domain, and the considerations surrounding deploying IoT systems.

In [53], the authors explore the most recent advancements in intrusion detection and intelligent methods employed in IoT to ensure data security. Furthermore, the study delves into recent research concerning various intelligent techniques and their implementation in intrusion detection architectures within computer networks, specifically focusing on the Internet of Things and machine learning applications. In [54], the authors extensively examined the hurdles linked to security and sources of threats in IoT applications. After addressing the security concerns, the paper explores emerging and established technologies like blockchain, fog computing, edge computing, and machine learning, aiming to bolster IoT security. Moreover, the article discusses challenges concerning various layers, such as the measurement, network, middleware, gateways, and application layers. In addition, the paper outlines future research directions geared toward elevating the security standards of IoT systems.

In [55], the authors explore improving IoT security, focusing on network- and host-level improvements through machine learning techniques. These techniques encompass

supervised, unsupervised, and reinforcement learning approaches. Additionally, the paper investigates the challenges encountered by machine learning methods when striving to provide better protection for IoT devices.

In [27, 31], the authors have examined IoT architecture and explored various threats, security attacks, and their impact on IoT systems. This article investigates the application of machine learning, a subset of artificial intelligence, to tackle these attacks in the IoT domain. Furthermore, the paper delves into different categories of machine learning-based algorithms studied for this purpose. In [56], the researchers examined the existing literature on various machine learning and deep learning techniques applied to cyber security attacks. They explored utilizing these methods to detect diverse types of attacks and presented a thorough classification of the different algorithms employed in the domain of DL/ML.

In [57], the authors explain the complexities and issues related to security, privacy, confidentiality, and reliability concerning computer networks and IoT. The primary emphasis of this research centers on multiple intrusion detection systems, which are thoroughly analyzed from various perspectives. Furthermore, the study evaluates public network-based data intrusion detection systems. It explores the application of deep learning techniques for IDS, assessing their performance based on criteria such as accuracy, recall, f1 score, false alarm rate, and detection rate. Another obstacle encountered within the realm of IoT is cybersecurity. Therefore, it becomes essential to establish a robust cybersecurity framework to detect diverse forms of attacks effectively. In [58], the authors examined a dataset comprising cyber security attacks and underscored the significance of employing machine learning and deep learning methodologies in cybersecurity.

In [59], the authors offered a comprehensive examination of IoT, delving into its various security challenges. The survey investigates security concerns and potential attack risks at every level of IoT. Furthermore, the utilization of deep learning to enhance the security of IoT has been thoroughly explored. The author also discusses the merits and drawbacks of employing deep learning techniques in IoT security.

A thorough investigation has been conducted encompassing cutting-edge deep learning methodologies and technologies related to IoT security and big data. Furthermore, this paper explores a comparative evaluation, thematic categorization, and the interconnections among deep learning, IoT security, and big data technologies. Ultimately, the obstacles encountered within these three domains have been pinpointed and deliberated upon [60]. In [61] offers an exhaustive examination of security vulnerabilities within Machine Learning enabled IoT. It underscores the significance of collaborative endeavors, privacy-preserving strategies, resilient models, ethical benchmarks, and ongoing scholarly investigation for societal progress. On the other hand [62], provides an in-depth review of the integration of IoT and Wireless Sensor Networks (WSN) with a federated learning (FL) machine learning approach. It addresses challenges related to heterogeneity, security, and privacy while outlining achievements and suggesting future research directions.

[53] thoroughly categorizes IIoT networks empowered by blockchain technology, assesses existing centralized systems, and underscores blockchain's significance and potential applications in the industrial Internet of Things (IIoT) [63]. The paper delves into an examination of different consensus mechanisms and approaches within the scope of IoT applications, tackles security challenges within IoT networks, and investigates forthcoming endeavors associated with IoT systems built on blockchain. It also underscores the significance of robust cybersecurity measures within the IoT sector. It explores how integrating ML and AI algorithms with blockchain technology can bolster detection, prevention, and secure data storage in IoT systems. The passage further delves into diverse machine learning methodologies, including decision trees, artificial neural networks, support vector machines, and deep learning strategies to enhance security solutions for advancing IoT devices [64].

In contrast to the previously cited works, our survey presents a distinctive contribution to the field, comprehensively encompassing all three dimensions of IoT research: ML methods, DL methods, and the associated challenges. Previous papers [27, 31, 39, 47, 49, 57] and [61] collectively present a comprehensive review of machine learning methodologies in IoT security. Their investigation focuses on the challenges inherent on the Internet of Things. Alternatively, as demonstrated in [41, 64, 65], and [66], there has been a focus on the intersection of machine learning, artificial intelligence, and blockchain technology. However, a standard limitation of these studies is the need for increased practical application and empirical testing of the proposed solutions. While the potential of these technologies are deliberated in each study, empirical evidence and case studies showcasing the efficacy of machine learning and deep learning in fortifying IoT devices exist in the literature.

Our survey bridges this gap by integrating these aspects, introducing novel depth to the existing literature, and paving the way to explore new research trajectories. Notably, our survey stands out by encompassing a review of the most recent articles in the field, spanning publications up to 2024. Therefore, our analysis and conclusions are based on the latest trends and advancements in the IoT landscape. Consequently, our work furnishes an up-to-date portrayal of state-of-the-art research, encapsulating recent articles that have

leveraged machine learning and deep learning methodologies within this domain.

In Table 2, the surveys mentioned in the related work are briefly stated, along with their primary objectives and limitations.

3 IoT architecture and applications

This section will thoroughly examine and explain IoT's different applications and architecture, consisting of three main layers: the application, network, and perception.

3.1 IoT architecture

The architecture of IoT comprises three layers: the application layer, the perception layer, and the network layer. These layers collaborate to facilitate the operation of IoT systems. Figure 1 shows the architecture of IoT. In the following, each of the layers is briefly described.

3.1.1 Application layer

The application layer is where data from IoT devices undergoes processing, analysis, and triggering of actions. It encompasses applications, services, and software that leverage data gathered from IoT devices to offer insights, make informed choices, and execute operations. This layer can be tailored to suit diverse applications, ranging from smart homes and industrial automation to healthcare. Additionally, this layer encompasses security concerns, including DoS attacks, which may involve program-related attacks, injection attacks, tampering, and scripting attacks [67, 68].

3.1.2 Network layer

The network layer facilitates data transmission from IoT devices to the network. Objects can exchange data with connected devices through the network layer, which is essential for intelligent event management and processing in IoT [69]. This layer's role is to receive valuable digital data. Extracting data from the perception layer and transmitting it to processing systems in the middleware layer involves employing diverse communication technologies like WiFi, Bluetooth, WiMax, Zigbee, GSM, 5G [70], etc., in conjunction with protocols such as IPv4, IPv6, MQTT, and others [71, 72]. Given the substantial volume of data IoT sensors collect [73], efficient middleware is essential for managing this data. In this regard, cloud computing [74, 75] plays a central role in this layer.

3.1.3 Perception layer

The IoT comprehension layer is a crucial bridge connecting the IoT to the physical world. The perception layer is a self-organizing network system consisting of sensor nodes with varying resource limitations, communicating wirelessly. The perception layer establishes a physical connection with 'objects' and transmits their data to a sink or gateway. This layer encompasses a range of devices such as sensors, RFID readers, webcams, and smartphones, all employed for sensing and data collection purposes, including information about objects and the environment. However, it is worth noting that this layer is susceptible to significant security challenges [76, 77].

3.2 IoT applications

IoT applications are expanded daily and consist of different applications [78–80]. These applications include home automation, smart city, military applications, industries automation [81–83], security applications, healthcare applications, and target tracking [84]. Security is one of the most critical challenges in all applications. Figure 2 indicates different applications of IoT.

4 IoT Security challenges

The Internet of Things has significantly influenced industries and people's daily lives. IoT aims to integrate the physical and digital worlds as a bridge between them. By utilizing the Internet of Things, people aim to enhance their lives, seeking simplicity, comfort, and well-being [49, 85, 86].

As the Internet of Things continues to gain prominence and expand usage, there is a concurrent escalation in security and cyber-related challenges. These challenges significantly impact the efficacy and functionality of IoT systems [87]. IoT devices present a range of intricate security concerns due to the open nature of the IoT ecosystem, which operates over the Internet. Consequently, these devices are frequently exposed to damage and attacks from various agents and external factors. Hence, there is a critical need for the early detection of security vulnerabilities within the IoT environment [88]. IoT devices and ecosystems face a wide range of threats and vulnerabilities. A threat is an activity that exploits security flaws in a system that can compromise its security and performance. These threats can have severe consequences for individuals and organizations [89].

Table 2 The main object of related works

Reference	Year	Method	Focus	Limitation(s)
[27]	2020	ML	A study about the security challenges faced by IoT due to its rapid growth and the need for advanced security measures. The paper highlights the potential of machine learning in detecting attacks and abnormal behaviors in IoT devices and networks.	Examining the benefits and drawbacks of machine learning algorithms concerning IoT security without extensively exploring the specific challenges encountered by various machine learning models such as GRU or GNN within IoT security.
[41]	2020	ML/AI/ Blockchain	A systematic study of machine learning, artificial intelligence, and blockchain as primary technologies for addressing security issues in IoT also identifies and explores the primary security issues of confidentiality, integrity, and availability.	The analysis may lack thorough examination or comparison with alternative emerging technologies or conventional security approaches for securing IoT devices and networks.
[31]	2023	ML	A survey and analysis of machine learning algorithms for IoT security	not offer a comprehensive comparison or assessment of various machine learning algorithms concerning IoT security. It could not thoroughly analyze the efficacy, scalability, and practical implementation hurdles related to specific machine learning algorithms for safeguarding IoT systems.
[39]	2022	ML	A study on the security of IoT emphasizes the need for AI and ML solutions to increase the security of IoT.	---
[40]	2021	DL	proposing and assessing deep learning models aimed at improving cybersecurity in IoT and highlighting the susceptibility of IoT networks to cyber threats, particularly DDoS attacks	focus on applications of deep learning models for cybersecurity in IoT networks and does not fully explore other threats in IoT.
[42]	2020	DL	providing a systematic review of the state-of-the-art in IoT security threats and vulnerabilities, with a specific emphasis on Intrusion Detection Systems (IDS) based on DL techniques, also classify security threats according to the Cisco IoT reference model architecture	concentrates exclusively on Deep Learning-based Intrusion Detection Systems (IDS) for IoT security, neglecting alternative effective security measures or strategies. Moreover, it does not extensively examine the obstacles, constraints, or emerging developments in IoT security beyond Deep Learning-based IDS.
[43]	2021	ML/DL	exploring different approaches and techniques for detecting attacks in IoT networks using ML/DL algorithms	investigates traditional techniques and does not explore more advanced methodologies such as deep learning models like DNN, CNN, and RNN, which have demonstrated considerable potential in detecting cyberattacks within IoT environments.
[44]	2021	DL	Identifying the research gaps in the field of IoT security and examining the vulnerabilities of DL approaches in the IoT security scenario	systematic review of Deep Learning methods for IoT security is constrained by its emphasis on conventional machine learning models like SVM, MLP, CNN, and SVM. At the same time, it offers a limited examination of advanced deep learning structures such as DNN, RNN, and GAN models.
[45]	2022	ML/DL	providing a comprehensive overview of the use of AI techniques for enhancing security in IoT	the narrow focus on specific algorithms for enhancing IoT security, potentially overlooking a broader range of artificial intelligence techniques and advancements in the field, also does not provide a comprehensive overview of the full spectrum of AI applications and their effectiveness in addressing IoT security challenges, limiting the depth of insights for researchers and practitioners in the field.
[46]	2020	ML/DL	A study on the potential of artificial intelligence, specifically ML and DL, in addressing the security threats faced by the IoT also analyzes the technical feasibility of AI in solving IoT security problems.	Insufficient thoroughness in investigating particular AI methodologies and their utilization to tackle IoT security issues.
[47]	2021	ML/DL	A comprehensive review of the use of machine learning and deep learning techniques in Intrusion Detection Systems for IoT security	The limitation of this survey is the lack of in-depth examination of recent updates, security issues, and challenges related to IDS for IoT from both machine learning and deep learning perspectives, as well as the lack of examination of other types of threats in this domain.
[48]	2022	ML	A study and exploring the application of machine learning algorithms for enhancing security in the Internet of Things domain	A possible constraint arises from the emphasis on particular periods or recent advancements within the intersection of machine learning and IoT security.

Table 2 (continued)

Reference	Year	Method	Focus	Limitation(s)
[49]	2020	ML/DL	A comprehensive survey and analysis of the application of machine learning and deep learning techniques in IoT security	focus on a specific time limit, particularly within the last five years, which may restrict the coverage of historical developments or future trends in machine learning and deep learning techniques for IoT security.
[50]	2021	DL	A study into the application of deep learning algorithms in IoT security assesses the appropriateness of deep learning for enhancing security within IoT systems. It gauges the effectiveness of deep learning in bolstering security within IoT systems.	The concentration is solely on deep learning applications tailored to IoT security and privacy issues, possibly neglecting the exploration of alternative machine learning methods or hybrid strategies that could also contribute to bolstering security in IoT environments.
[51]	2021	ML	A literature survey to emphasize the importance of developing models that integrate state-of-the-art techniques from big data and machine learning to detect IoT attacks inaccurate or near real-time	One potential limitation of this survey could be its exclusive focus on machine learning approaches to IoT security, potentially overlooking other security measures or strategies that could complement or enhance the effectiveness of machine learning in securing IoT systems.
[52]	2020	-	To propose a compacted and optimized architecture for IoT based on five layers also introduces a new classification of security threats and attacks based on this architecture. It discusses the different layers of the proposed architecture. This paper highlights the security features and challenges in each layer.	The emphasis on introducing a novel, streamlined, and refined structure for IoT, consisting of five layers, might restrict the applicability of the results to alternative IoT architectures or security frameworks. Furthermore, the review centers on particular security risks and breaches within the confines of the suggested architecture, potentially neglecting broader security issues or alternative security strategies that could be pertinent across various IoT landscapes.
[53]	2019	ML	A survey of machine learning-based network intrusion detection systems	The concentration is on intrusion detection techniques based on machine learning for the Internet of Things (IoT), potentially disregarding other non-machine learning methodologies or hybrid strategies that could also prove efficacious in bolstering IoT security. Furthermore, there are constraints about the extent of analysis, the range of attacks examined, or the assessment criteria employed.
[54]	2019	ML / Blockchain	A survey of IoT security, including the analysis of security architectures, protocols, and technologies used at each layer of the IoT security architecture	not extensively examine the particular security challenges encountered across various IoT application domains or thoroughly investigate emerging security solutions and architectures.
[55]	2020	ML	A study on securing the Internet of Things using machine learning techniques	The limitation is related to memory and computational constraints. These constraints can impact the implementation and effectiveness of machine learning solutions for IoT security.
[56]	2021	ML/DL	Providing a detailed classification of various machine learning and deep learning algorithms and discusses their use in detecting various categories of cyber attacks	The limitation is related to the challenges associated with scaling detection methods to the size of the Internet in real-time.
[57]	2022	DL	A study about the use of deep learning for intrusion detection and security in the context of the Internet of Things	not thoroughly cover all the existing challenges and potential solutions concerning deep learning for intrusion detection and security within the Internet of Things (IoT) domain.
[58]	2021	ML/DL	A survey and review of the role of artificial intelligence, machine learning, and deep learning in cybersecurity attack detection	focuses on applying AI, ML, and DL to detect cybersecurity attacks without highlighting specific limitations.
[59]	2022	DL	Investigate the application of deep learning methods to improve security in IoT settings.	Not fully exploring all the security challenges in the Internet of Things (IoT) domain when utilizing deep learning techniques.
[60]	2020	DL	A comprehensive survey on deep learning, IoT security, and big data technologies, highlighting the potential of deep learning for detecting security breaches in IoT systems and the benefits of incorporating big data technologies for improved performance and data handling	The focus is exclusively on deep learning, without exploring traditional machine learning algorithms in the context of big data.

Table 2 (continued)

Reference	Year	Method	Focus	Limitation(s)
[61]	2024	ML	Provides a detailed analysis of security threats in the ML-based Internet of Things, categorizes the threats, and emphasizes the importance of protecting ML models and data.	The constraint lies in its limited scope, which concentrates solely on attacks within machine learning based IoT ecosystems. This singular focus may inadvertently neglect broader security considerations or alternative security methodologies applicable to various IoT settings.
[62]	2024	FL	A thorough examination of the significance of Federated Learning (FL) in addressing privacy and security concerns within the context of the Internet of Things (IoT) and Wireless Sensor Networks (WSN).	---
[65]	2024	FL / Blockchain	An extensive categorization of IIoT networks incorporating blockchain and addresses security challenges within IoT networks. Additionally, it outlines forthcoming endeavors and blockchain technology's applicability in the IoT context.	The limitation is related to the scope of the survey, which may limit the depth of analysis and coverage of alternative approaches beyond blockchain and federated learning for intrusion detection in IIoT.
[64]	2024	AI/ML/ Blockchain	A comprehensive review to increase security intelligence on the Internet of Things using advanced technologies such as artificial intelligence, ML, and blockchain	narrow focus on enhancing IoT security through the constructive interaction of machine learning, artificial intelligence, and blockchain technologies.
[66]	2024	ML / Blockchain	Thoroughly examine prospective measures to enhance IoT security, encompassing emerging and conventional techniques like blockchain, machine learning, cryptography, and quantum computing.	Incorporating various intricate technologies might present technical challenges and demand substantial computational resources, which should be considered as a potential limitation.

4.1 Types of threats

Several types of threats affect the Internet of Things. Figure 2 shows the taxonomy of the Internet of Things threats, divided into physical and cyber categories. In the following, we briefly describe each of them.

4.1.1 Cyber threats

IoT threats are primarily categorized into cyber and physical threats, with cyber threats encompassing passive and active threat types (Fig. 2).

Cybersecurity threats within the realm of the Internet of Things are distinct due to IoT's unique characteristics and constraints. These threats can potentially target and exploit IoT's various limitations and vulnerabilities [90, 91].

Cyber threats can be categorized into passive threats and active threats, each representing diverse types of risks and vulnerabilities:

4.1.1.1 Passive threats Passive threats involve unauthorized access or monitoring of data or IoT devices without altering or disrupting their operations. These threats focus on.

Stealing information or gathering intelligence without directly interfering with the IoT system's functionality (Fig. 3). Some examples of passive threats in IoT security include:

- *Eavesdropping*

Eavesdropping entails secretly listening to the discussions of individuals without their permission, intending to collect information [92].

In an eavesdropping threat, an attacker seeks to exploit weaknesses in security mechanisms, such as encryption or authentication, to access data in transit.

The attacker aims to collect sensitive information by transferring data, commands, or messages without the knowledge or consent of legitimate users or device owners.

- *Traffic Analysis*

This type of threat refers to monitoring and analyzing network traffic patterns and data exchange in IoT ecosystem to identify potential security threats, anomalies, or vulnerabilities. This technique helps security professionals and network administrators gain insight into IoT device behavior and data flow, effectively identifying and responding to security issues. The attacker intercepts and examines the messages and analyzes the packet traffic to obtain network information [93]. Critical aspects of traffic analysis in IoT security include Monitoring Data Flows, Anomaly Detection [94], Security Event Correlation, Identification

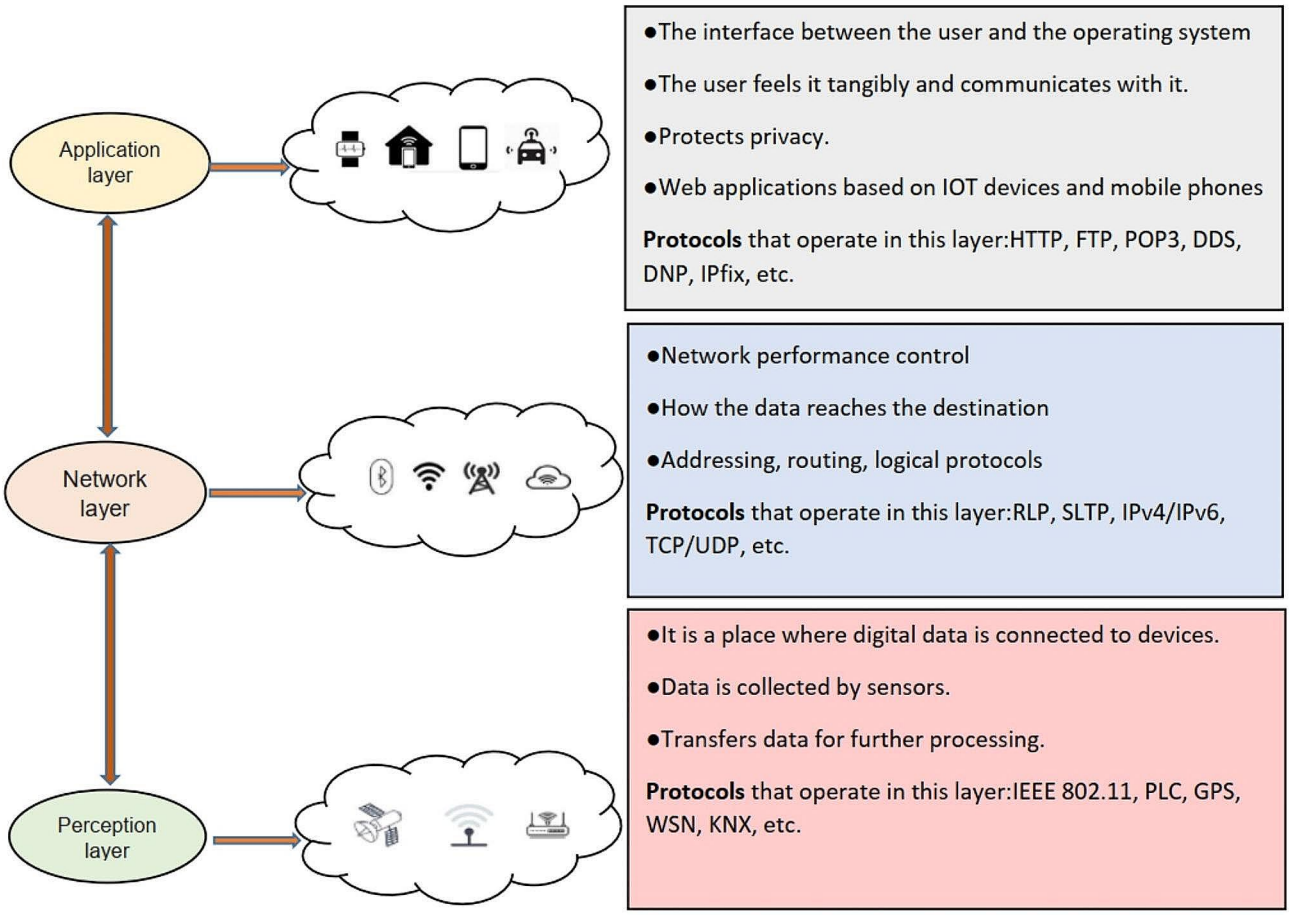


Fig. 1 IoT architecture

of Abnormal Traffic, Encryption and Decryption Analysis, Network Segmentation Analysis, IoT Device Profiling, and Real-time Monitoring.

- *Data Theft*

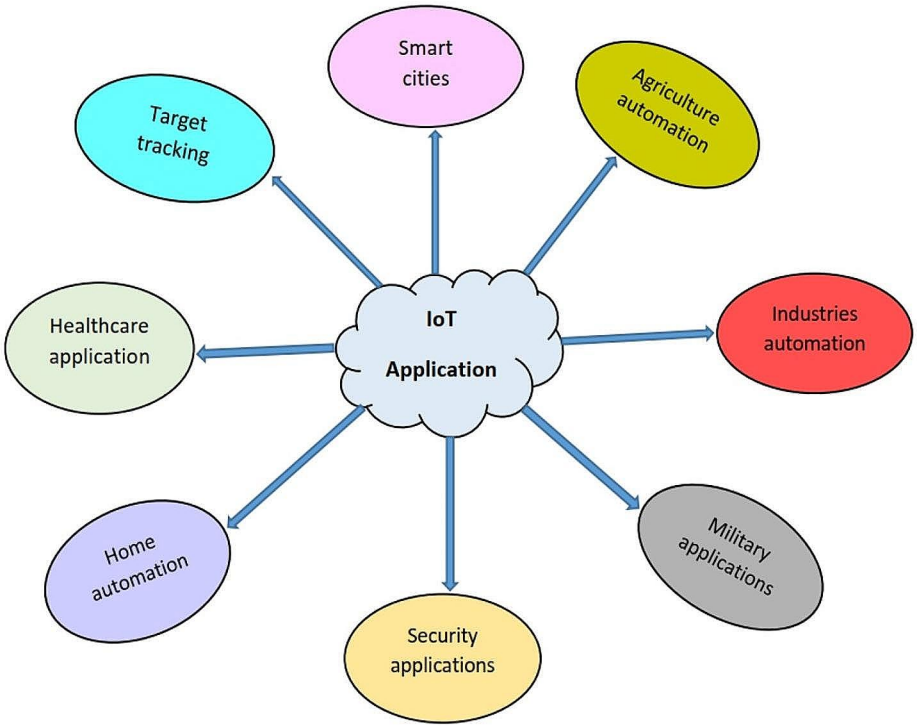
Data theft in IoT security refers to malicious actors' unauthorized acquisition, copying, or retrieval of sensitive or confidential data from IoT devices, networks, or systems. Data theft typically occurs when attackers access IoT devices or their associated networks without authorization. Once access is obtained, the attacker may exploit vulnerabilities or weaknesses in the security measures to extract data. The stolen data can be used for various malicious purposes, including identity theft, financial fraud, corporate espionage, or cyberattacks. Protecting against data theft in IoT security requires implementing robust security measures such as encryption, authentication, access controls, intrusion detection systems, and regular security updates to minimize vulnerabilities and unauthorized access. Additionally, monitoring network traffic and IoT device behavior can help detect and respond to potential data theft incidents in real-time [54].

4.1.1.2 Active threats Active threats involve direct manipulation, disruption, or interference with IoT devices, networks, or data. These threats aim to alter or compromise the functioning of the IoT system. Active threats can have more immediate and noticeable consequences (Fig. 2). Some examples of active threats in IoT security include:

- *Denial of Service (DoS) Attacks*

A DoS attack is a technique employed to disrupt a network connection, rendering it inaccessible to its intended users. Such an attack transpires when a malevolent actor inundates the central server with excessive requests, rendering legitimate users unable to access the server. The attacker persistently bombards the host with spam requests until it becomes overwhelmed and ceases to function. Typically, DoS attacks are directed at data communication systems,

Fig. 2 Applications of IoT



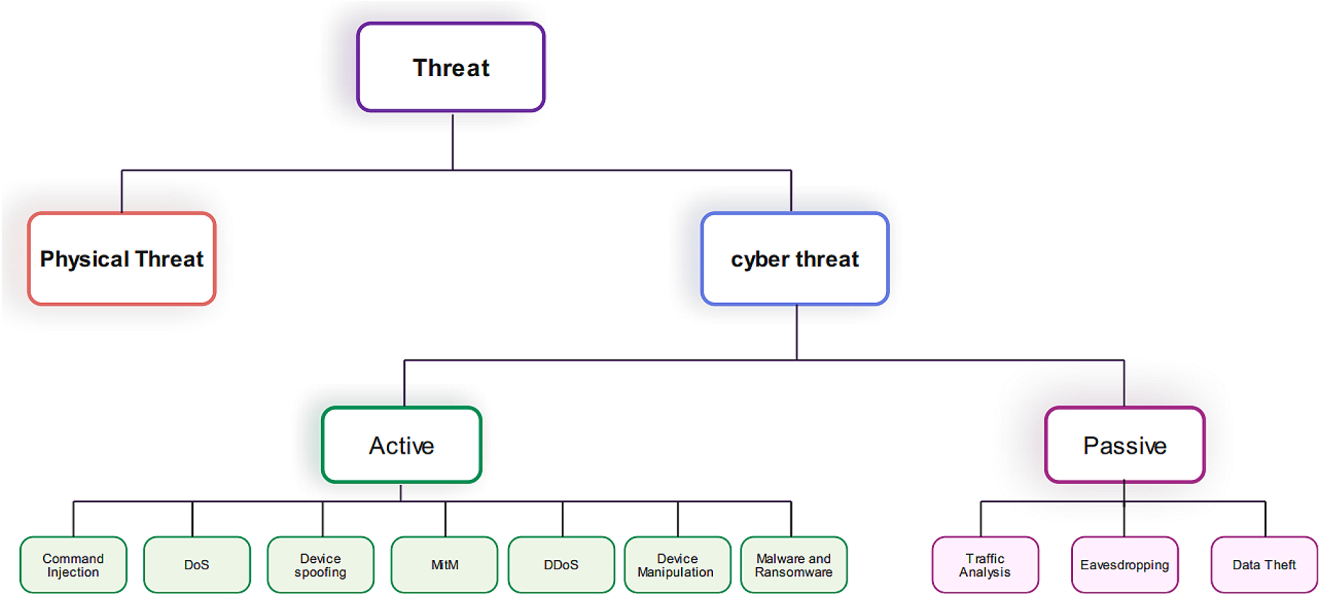


Fig. 3 Taxonomy of threats in IoT security

with web servers of prominent entities like smart homes, personal medical devices, and industrial applications often falling victim to such disruptive attacks.

- *Distributed Denial of Service (DDoS) Attacks*

DDoS is a malicious attack that aims to overwhelm a network or system by organizing a coordinated barrage of traffic from multiple compromised devices or bots. DDoS attacks are volume attacks, and compromised devices are often Also known as botnets; these devices have weak internal security and suffer from other limitations such as low computing power and battery capacity. Due to weak security, an attacker injects malware using tools such as Mirai code or the Lizards Tresser tool and takes control of the device. Mitigating DDoS attacks in IoT security usually involves implementing traffic filtering, intrusion detection systems, limiting Rates, and using content delivery networks (CDNs)

or specialized DDoS mitigation services to absorb and reduce the high volume of malicious traffic generated by the attack. In addition, IoT devices must be regularly patched and updated to reduce their susceptibility to becoming part of a botnet used in DDoS attacks [95].

- *Malware and Ransomware*

Ransomware is malicious software restricting access to critical data and demanding payment for its release. In this attack, the offender seeks to encrypt the victim's data using robust encryption techniques and requests a ransom, typically in Bitcoin, in exchange for the decryption key. The repercussions of a ransomware incident encompass temporary or permanent data loss, disruption of regular system functions, and financial setbacks. Two primary categories of ransomware exist crypto-ransomware and lock ransomware [96].

- *Device Manipulation*

Device manipulation in IoT security refers to unauthorized or malicious alteration, tampering, or interference with IoT devices, configurations, or physical components [97, 98]. This activity is typically done to compromise the IoT device's functionality, security, integrity, or broader ecosystem. Device manipulation poses significant security risks in IoT environments, as it can result in unauthorized access, data breaches, service disruptions, and privacy violations.

- *Man-in-the-Middle (MitM) Attacks*

Man-in-the-middle (MitM) attacks represent a prevalent security threat in wireless networks, enabling attackers to intercept and manipulate communication between two end devices [99]. MitM attacks have greater complexity than other attack types, making them challenging to identify [100, 101].

- *Device Spoofing*

This attack involves accessing legitimate network users' medium access control (MAC) addresses to perpetrate malicious actions [102]. Spoofing attacks can maliciously compromise both wired and wireless networks. In these attacks, the malicious actor gains access to a device, its resources, and the network by exploiting frames and fields containing address identifiers belonging to the target user. These identifiers may include the MAC address or IP address [103]. Spoofing attacks come in various forms, including email, URL, and frame spoofing, but the most prevalent ones involve either MAC address or IP address manipulation [104].

- *Command Injection*

Command injection is an attack that aims to run unauthorized commands on the host operating system by exploiting vulnerabilities in a program. These attacks become possible when an application processes insecure data from users. During this attack, the attacker's provided operating system commands are typically executed with permission from the vulnerable application. The consequences of command injection attacks can vary from compromising data confidentiality and integrity to gaining unauthorized remote access to the system that hosts the vulnerable application [105, 106].

4.1.2 Physical threats

Physical threats in IoT security refer to risks and dangers that arise from physical. Access to IoT devices, systems, or infrastructure. These physical threats are part of The foundation of IoT security includes the potential for unauthorized individuals or entities to tamper with or compromise IoT components physically, resulting in security breaches, data breaches, or operational disruptions [107].

4.2 Effects of threats

Ensuring the security of IoT systems is of utmost importance due to various potential threats and vulnerabilities. The impacts of these threats on IoT can be extensive, significantly affecting the security, functionality, and reliability of IoT ecosystems. The following section briefly outlines the various effects of these threats.

4.2.1 Integrity

Integrity concerns in IoT security pertain to the trustworthiness and precision of data and devices within the IoT environment. These concerns revolve around safeguarding information from unauthorized alterations or tampering [108, 109]. The integrity feature ensures only authorized users can modify IoT device information when utilizing wireless communication networks [110]. Weaknesses in integrity checks can open the door to data tampering within IoT device memory, potentially jeopardizing the core functionality of physical devices and persisting undetected for extended periods. Solutions for ensuring integrity in IoT encompass the generation or utilization of data through programmed methods [108].

4.2.2 Authentication

Authentication is one of the most important security parameters to IoT applications. In IoT security, concerns and challenges regarding authentication are associated with confirming the legitimacy and identity of devices, users, and entities operating within the IoT ecosystem [111]. The issues surrounding authentication and access control in IoT stem from the sheer volume of devices and the character of machine-to-machine (M2M) communication inherent to the Internet of Things [112, 113]. Hence, a well-functioning IoT system requires an authentication mechanism to effectively manage system constraints while delivering robust security measures [114] (Fig. 4).

4.2.3 Availability

To minimize the potential for operational disruptions or failures in IoT systems, it is crucial to improve the availability and continuity of security services [115]. Nevertheless, the increasing amount of data in IoT poses challenges to maintaining consistent device and data availability. Exploiting this vulnerability, attackers deploy diverse attacks that may jeopardize the overall availability of the system [116].

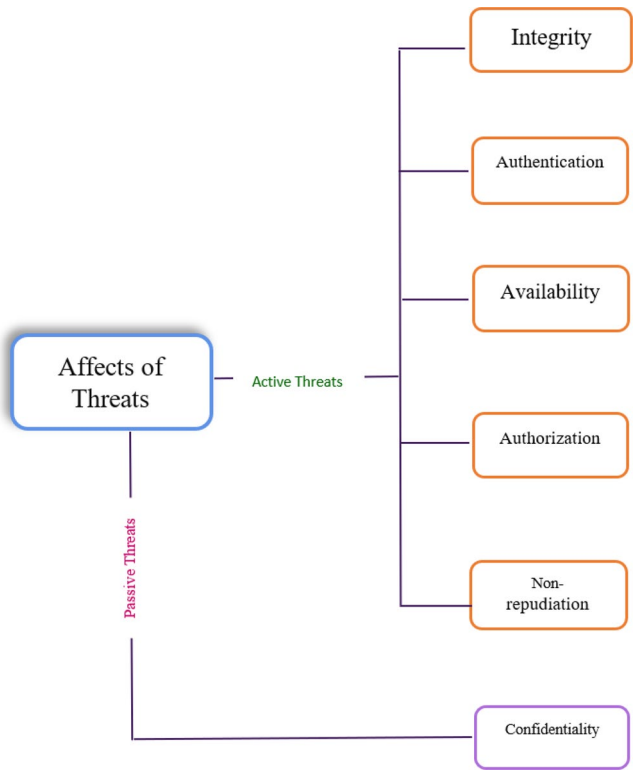


Fig. 4 Effect of threats on IoT security

4.2.4 Authorization

Authorization mechanisms are essential for security IoT ecosystems against unauthorized entry, data breaches, and security threats. These mechanisms ensure the security of valid communications by verifying the identities of all devices and confirming their entitlement to access approved resources, data, and services [117, 118]. There are two authorization processes: one for the devices and another for the users. Authorization and Authentication complement each other and have common goals [119].

4.2.5 Non-repudiation

In the IoT, non-repudiation is necessary, ensuring that services serving as a link between the smooth transmission of service/data and effective security implementation can be allowed or disowned [120, 121].

4.2.6 Confidentiality

Confidentiality within IoT security involves safeguarding sensitive information and data from unauthorized access, disclosure, or exposure. It constitutes a vital necessity, and this safeguarding can be guaranteed by implementing secure encryption methods [122, 123]. The difference between confidentiality and integrity is that Confidentiality relies on password-based encryption for protection. In contrast, integrity, specifically against memory tampering, is maintained using a message authentication code derived from the stored context [124].

5 Solutions

In this regard, several successful methods have been introduced recently. Most of them are based on Machine Learning and Deep Learning methods. Machine Learning techniques such as Support Vector Machine (SVM), Artificial Neural Net, and Linear Modeling are successful with small data sets. In big data sets, Deep Learning has higher accuracy. Graph Neural Network is an original approach in that node selection must be done carefully.

In Table 3, the studied methods are compared with each other.

5.1 Machine learning

Machine learning plays a crucial role in enhancing security in the IoT ecosystem. IoT devices are becoming increasingly prevalent and often collect and transmit sensitive data. Securing these devices and the data they manage is

Table 3 Comparison of different methods for attack detection

Method	Type	Accuracy	Advantages	Limitations
SVM	ML	High	1) robust and suitable for classification, intrusion detection, and anomaly detection tasks. 2) Exhibits reduced susceptibility to the curse of dimensionality. 3) Capable of managing non-linearly separable data using kernel functions.	1) Prone to high computational costs, particularly with extensive datasets. 2) Susceptibility to variations based on the selection of the kernel function and its parameters. 3) Vulnerability to variations depending on the selection of hyperparameters.
ANN	ML	Medium	1) Capable of adjusting to dynamic environments and emerging data patterns. 2) Proficient in assimilating vast volumes of data for learning purposes. 3) Effectively handling intricate patterns and nonlinear associations within data, particularly in intrusion and anomaly detection applications.	1) Absence of clarity in decision-making processes. 2) Diminished effectiveness in scenarios where labeled data is scarce. 3) High computational demand.
Linear Modeling	ML	Low	1)Interpretability 2)Computational Efficiency 3)Scalability	1) Limited complexity compared to non-linear models such as SVM or ANN 2) lack of proportion 3) Linear assumption
CNN	DL	High	1)Feature Extraction 2) Scalability 3)Pattern Recognition	1)Computational Complexity 2)Data Requirements 3)Interpretability
LSTM	DL	High	1)Temporal Dependencies 2)Pattern Recognition 3)Adaptability	1)Computational Complexity 2)Data Requirements 3)Interpretability
GRU	DL	High	1) handle significant noise 2) non-linearity 3) volatility of data	1) The training process can be time-consuming 2) computationally expensive 3)finding optimal hyperparameters for the model
GNN	DL	High	1) ability to model traffic flow data as a graph 2)effective in modeling and analyzing data	1) The training process can be time-consuming 2) computationally expensive 3) finding optimal hyperparameters for the model

essential. As Fig. 5 shows, we classify the IoT security in three machine learning methods. Table 4 summarizes the reviewed articles in the field of machine learning.

5.1.1 Support vector machine (SVM)

The Support Vector Machine (SVM) is a supervised machine learning algorithm with various applications [125]. It tries to find a decision boundary between different classes in the input feature space. The SVM must be trained at least once for recognition and class using one of many methods. Support Vector Machine has extremely high accuracy. The SVM is not suitable for use in big datasets. The feature selection must be used to reduce data size. Radial base Neural Net is the type of Feed Forward Neural Net. The most common transfer function in RBF [126] is Gaussian. This method needs a considerable amount of memory and is not suitable for big datasets. Generalized Regression Neural Net has the highest accuracy and is like RBF. The biggest drawback of this method is the computation complexity. Every sample of the dataset is stored in memory. The complexity of output calculation is O (N^2).

SVM has several applications for detecting Low-Rate Denial of Service (LDoS) attacks in Software Defined Networks (SDN) [127]. In the study [128], an IDS to detect low-rate distributed denial-of-service (LRDDoS) attacks in SD-IoT using an SVM algorithm along with a feature importance method, especially a logistic regression coefficient. This paper proposes different SVM kernel models. Evaluate and find that the linear kernel SVM algorithm achieves the highest accuracy. Another study [129] analyzed machine learning techniques, specifically LSTM, IF,

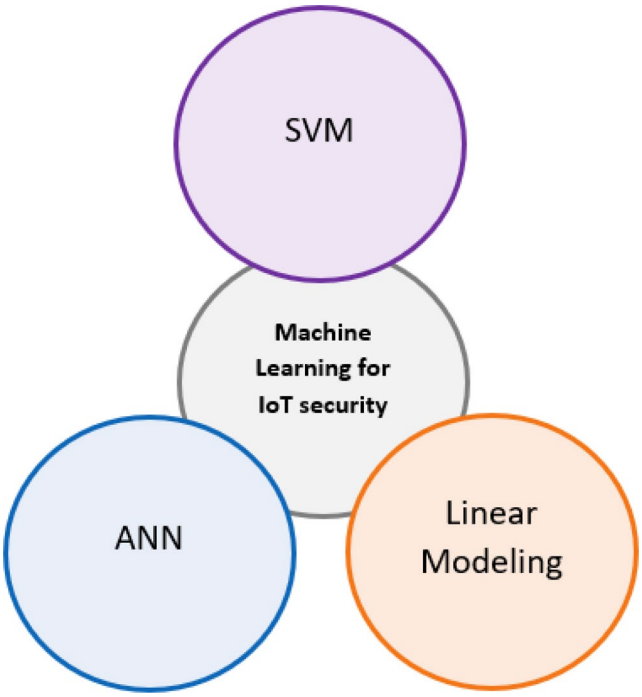


Fig. 5 Machine learning methods used in IoT security

and SVM, to detect internet threats in smart grids based on network traffic analysis. Different types of SVMs are also used to identify malware [130]. have used a decision tree based SVM to identify malware. Their experimental results prove that the proposed method efficiently identifies malware with an accuracy of 98.78%, and it takes only 42 s to process 1000 samples. A new malware detection framework is proposed for the Internet of Things using the Genetic Cascade Support Vector Machine (GC-SVM) classifier. The purpose of the proposed method is to detect and accurately identify malware in Internet of Things-based systems [131]. This study [132] investigates the utilization of support vector machines (SVM) for intrusion detection systems (IDS) deployed in the context of the Internet of Things (IoT). Specifically, two SVM techniques, C-SVM and OC-SVM, are implemented within an IDS framework to monitor and detect abnormal activities in smart node devices. The findings indicate that C-SVM attained a classification accuracy of up to 100% when assessed with unfamiliar data from the identical network topology it was trained on, achieving 81% accuracy in an unfamiliar topology. Conversely, OC-SVM achieved a maximum accuracy of 58%.

This study explores two distinct threat models: ciphertext and background models. In the ciphertext model, the IoT data analyst is restricted to accessing encrypted IoT data stored on a blockchain-based platform, with the capability to record intermediate results generated during the execution of the secure training algorithm. Conversely, in the background model, the IoT data analyst possesses additional knowledge beyond the ciphertext model, enabling collusion with one or more IoT data providers to deduce sensitive data from others. The primary objectives include safeguarding the privacy of multiple IoT providers and devising a privacy-preserving scheme for training SVM models using multiple private datasets from various IoT providers [133]. These previous papers underscore the efficacy of SVM and ML methods in bolstering IoT security by improving attack classification, safeguarding privacy, and detecting and mitigating attacks.

5.1.2 *Artificial neural networks (ANN)*

Artificial Neural Network or Feed Forward Neural Net is the most common Neural Net type and has at least one hidden layer. The most advantageous feature of this type of neural net is that output computation is high-speed. However, training time with the backpropagation algorithm could be faster. Extreme Learning Machine is another type of ANN. The training algorithm is based on a generalized matrix inverse. ANN is an imitation of a biological neural network, which is an information processing model. It can be used in the intrusion detection system between the IoT environment

Table 4 Papers use machine learning methods

Ref.	Year	SVM	ANN	Linear modeling	Threat Type	Accuracy
[128]	2022	✓	-	-	LRDDoS, IDS	99.9%
[129]	2022	✓	-	-	Cyber	-
[130]	2022	✓	-	-	Malware	98.78%
[131]	2022	✓	-	-	Malware	99.75%
[132]	2021	✓	-	-	IDS	C-SVM = 81%, OC-SVM = 58%
[133]	2019	✓	-	-	Privacy breaches, Unauthorized access	90.35% on the BCWD dataset, 93.89% on the HDD dataset
[134]	2019	-	✓	-	DoS	-
[135]	2020	-	✓	-	DDoS	95.4%
[136]	2017	-	-	✓	DDoS, Malware, Data breaches	-
[137]	2020	-	-	✓	DDoS	-

and the external network. It can also overcome traditional security methods.

There are three primary layers in the artificial neural network:

- Input layer.
- Hidden layer.
- Output layer.

Information enters the neural network through the input layer, is processed in the hidden layers, and the result can be retrieved in the output layer.

The attractiveness of artificial neural networks stems from their remarkable information-processing properties, which are related to nonlinearity, high parallelism, fault and noise tolerance, and learning and generalization capabilities. Several studies have been presented on IoT security using ANN. An ANN-based intrusion detection system for threat analysis in IoT networks, achieving 100% efficiency in detecting DoS attacks, is introduced [134].

In a different study [135], a nearly instantaneous SDN security system employs a CNN to detect DDoS attacks, demonstrating encouraging outcomes in countering advanced DDoS threats. Utilizing artificial Neural Networks in IoT security involves a variety of functions, including anomaly detection, intrusion detection, authentication, and encryption. The valuable features of adaptability and learning inherent in ANNs make them effective instruments for tackling the constantly changing and evolving security challenges in IoT environments.

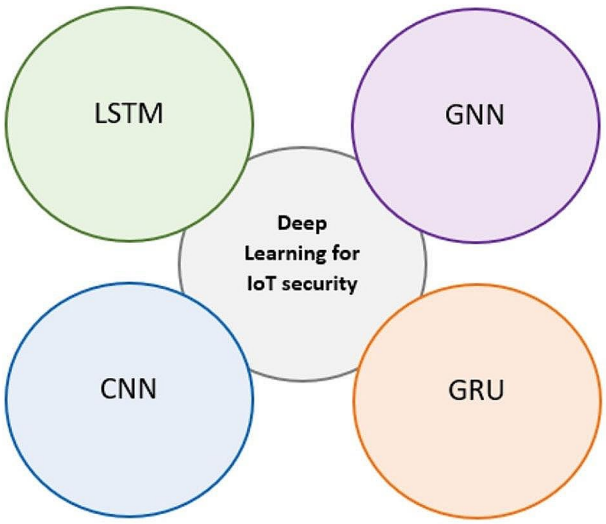


Fig. 6 Deep learning methods used in IoT security

5.1.3 Linear modeling

Linear modeling in the context of IoT security involves using linear mathematical relationships to analyze and predict security-related outcomes. Linear models are statistical models that assume a linear relationship between input variables and the target variable. These papers [136, 137] collectively explore the theme of linear modeling within the context of IoT security. While they tackle the subject from diverse perspectives, they offer insights into various facets of modeling for IoT security.

One of these papers introduces a model-driven adaptive strategy for IoT security, employing Model-Driven Engineering (MDE) to generate security services according to security requirements. This method aims to improve information management and confidentiality in IoT systems. Meanwhile [137], emphasizes the necessity for a formal IoT security model capable of assessing the security levels of different IoT systems. Their proposed model considers adversaries' actions, capabilities, and objectives, facilitating a comprehensive security evaluation based on confidentiality, integrity, availability, and soundness.

5.2 Deep learning

With the increase in data size, feature selection must be done to reduce the data size and complexity of training data. Machine learning-based methods are accurate with datasets. However, increasing the dataset size makes finding features easier. Deep Learning calculates these features using an optimization algorithm. It is very suitable for large-scale data sets and has better accuracy [138]. As depicted in Fig. 6, we explore the four deep-learning techniques in IoT security. Table 5 summarizes the reviewed articles in the field of deep learning.

5.2.1 Convolutional neural network (CNN)

Convolutional Neural Networks are used in IoT security to enhance various aspects of safeguarding IoT ecosystems. This type of DL consists of a convolution Layer, max pooling layer, softmax layer, and fully connected layer. The mammal's brain activity in object recognition is remarkable like CNN. According to the studies, CNN has higher accuracy in object detection [139, 140].

CNN-based studies have been conducted to ensure the security of the Internet of Things. In [141], the authors presented an improved CNN. The preprocessed data set of KDD99 is inserted into the intrusion detection model through edge calculation, and the enhanced CNN model is employed to achieve multi-classification of the data, utilizing the focal loss function to adjust the ratio. The precision,

Table 5 Papers based on deep learning methods

Ref.	Year	CNN	LSTM	GRU	GNN	Threat Type	Accuracy
[141]	2022	✓	-	-	-	IDS	92.14%
[142]	2023	✓	-	-	-	-	99.2% on Power dataset, 99.6% on the Loop sensor dataset, 98.6% on Land sensor
[143]	2023	✓	-	-	-	IDS	98.04%
[144]	2023	✓	-	-	-	Anomaly detection , Face recognition	94% for anomaly detection, 88% for face recognition
[145]	2024	✓	-	-	-	DDoS, IDS	99.47%on the BoNeSi-SlowHTTPtest dataset, 99.07% on the CICDDoS2019 dataset
[164]	2024	✓	✓	✓	-	IDS	100% in binary classification 97.44% in six-class classification 96.90 in fifteen-class classification
[159]	2023	-	-	-	✓	Malware	97%
[156]	2023	-	-	-	✓	IDS	96.70% on UNSW-NB15 dataset, 88.38% on the ToN-IoT dataset
[160]	2021	-	✓	-	-	Botnet, DDoS	86-90.88%
[161]	2020	-	✓	-	-	Anomaly	-
[162]	2021	-	✓	-	-	DoS, DDoS, Infiltration, Malware, Botnets, Cyber	99.92%
[163]	2021	-	✓	-	-	Anomaly, Cyber	98%
[152]	2023	-	-	✓	-	Anomaly, Cyber	99.78%
[151]	2023	-	-	✓	-	IDS	98.73%
[147]	2021	-	-	✓	-	DDoS	99.7%
[153]	2022	-	-	✓	-	Cyber, IDS	99.6%

accuracy, recall, and F1-measure values surpass those of other comparative algorithms, presenting a novel solution within intrusion detection. An attack detection in the network using a robust multi-cascade CNN (RMC-CNN) classification approach is presented to detect attack types [142]. Data is encrypted with a key generation mechanism using a dynamic honeypot encryption algorithm. Therefore, the encrypted information is transmitted securely and stored in the IoT cloud, which can be decrypted based on the user's request.

In [143], the authors proposed a CNN-CNN-based approach where the first CNN model uses raw network traffic data to select important features that help detect an IoT attack, the second CNN uses the features identified by the first CNN to build a robust detection model that Accurately identifies the Internet of Things. Furthermore, the proposed approach is compared with other deep learning algorithms and feature selection methods. The results show that it performs better than these algorithms. Also, in [144], the possibility of using logit-enhanced CNN models in smart home IoT devices for anomaly detection and face recognition is investigated. The authors have proposed six models that increase performance by combining LR (LR), gradient-boosting classifiers (XGB, GBC, CBC, HGBC, ABC, and LGBM), and CNN. These models are named LR-XGB-CNN, LR-GBC-CNN, LR-CBC-CNN, LR-HGBC-CNN and LR-LGBMCNN. The OSD-IDS mechanism serves as an optimal defense strategy targeting DDoS attacks within IoT networks. It comprises an enhanced ResNet architecture for feature extraction, an improved quantum optimization (IQQO) algorithm for feature selection, and a hybrid deep learning technique combining CNN and diagonal XG boosting (CNN-DigXG). OSD-IDS achieves accuracies of 99.476% and 99.078% in the analyzed datasets [145]. These models showed promising capabilities in anomaly detection, face recognition, and integration of these capabilities into smart home IoT devices. The findings of this study have emphasized the potential of deep learning approaches to enhance security and privacy in smart homes. A comprehensive survey on IoT security, including communication security, application interface security, and data security, is introduced to identify existing security gaps. These documents underscore the significance of tackling security issues associated with CNN in IoT settings.

5.2.2 Gate recurrent unit (GRU)

The GRU is a specialized variant of the RNN model utilized for feature extraction following dimensionality reduction preprocessing. The GRU effectively handles input sequences with temporal dependencies by introducing additional connections between hidden layer nodes, while the GRU unit governs the data output [146]. GRU is similar to LSTM in design and often yields similarly promising results in specific scenarios [147]. Nevertheless, GRU boasts a reduced node count and faster processing speed, mitigating long-term correlation issues and lowering the risk of overfitting in smaller RNN architectures [148]. In specific GRU-related tasks, it outperforms LSTM in terms of accuracy thanks to its swift training, straightforward structure, and ease of analysis [149, 150].

There are various works about GRU in IoT security. The focal point of this research involves utilizing machine learning algorithms, with a particular emphasis on deep learning techniques, to fortify security within wireless sensor networks. This article addresses the hurdles wireless sensor networks encounter concerning energy consumption and security, delving into the capabilities of algorithms. Furthermore, it underscores the significance of IDS in identifying diverse attack types, including DoS attacks. The emphasis is placed on wireless sensor networks, and the evaluation involves deep learning-based IDS models trained on specialized datasets, such as WSN-DS, for detecting various DoS attack forms [151]. In [147], the authors have developed a new approach, DIDDOS, to detect and identify DDoS cyber-attacks using GRU.in [152] focuses on enhancing cyber security in IoT networks through the use of deep learning techniques, especially the CNN-GRU model. The method used in this article includes deep learning models to develop intrusion detection systems suitable for IoT environments. The purpose of the CNN-GRU model is to improve the security performance of IoT by effectively identifying and reducing cyber threats by classifying traffic flow and analyzing network behavior. In [153], the authors concentrated on employing deep learning models, particularly CNN, LSTM, and GRUs, for crafting intrusion detection systems tailored for IoT environments. The research adopts a systematic approach, encompassing stages such as robot-IoT simulation [154], dataset preprocessing, feature selection, classification, and evaluation. This structured methodology aims to fortify the security of IoT networks by adeptly recognizing threats and cyber-attacks.

5.2.3 Graph neural network (GNN)

The latest technology is GNN, which learns from complex network structures and traffic patterns [155]. It can capture the impact of the network and has shown excellent results in detecting network attacks [156]. Also, GNNs have gained popularity due to their ability to model the underlying topology in terms of nodes and edges [157].

GNNs are crafted to account for the graph's structure, enabling the creation of efficient embeddings at both graph and node levels, exemplified in applications like graph-based

malware classification. In the context of a GNN malware classifier, node-level features are consolidated to produce graph-level features, facilitating the classification of input samples. Through message passing, the GNN model combines the features of a node with those of its neighbors, irrespective of the local structure or neighbor count. This iterative process, implemented through graph convolution layers, generates embeddings enriched with information from a broader local structure [158].

GNN is focused on several papers that solve IoT security. In [159], the authors presented the NT-GNN (Network Traffic Graph for Android 5G IoT Mobile Malware Detection) method to identify malicious code and detect malware in Android applications. In [156], the authors introduced a light graph convolutional network (GConv) called NE GConv, which addresses the challenge of limited labeled traffic flow data in IoT networks by using topological flow structure and software-defined networking technologies and intrusion detection in IoT networks.

5.2.4 Long-short-term memory (LSTM)

This type of deep Learning is very suitable for time series data and consists of remember-and-forget Gates and hidden state units [139]. In [160], the authors highlighted the importance of identifying malicious attacks in the IoT environment to minimize security risks. The proposed CNN-LSTM algorithm is applied to detect specific botnet attacks, such as BASHLITE and Mirai, on various commercial IoT devices, including doorbells, thermostats, and security cameras. The experimental results demonstrate the effectiveness of the CNN-LSTM model in detecting botnet attacks with high accuracy across different IoT devices. There are other works based on LSTM for IDS. In [161], the aim is to suggest a fresh design for an IDS tailored explicitly for IoT devices. This structure integrates the Extreme Gradient Boosting (XGBoost) model with the LSTM model to scrutinize unusual states in IoT devices. The sequence of system calls serves as markers for abnormal behaviors, and the newly proposed stacking model is utilized to detect and identify these abnormal behaviors. In [162], a framework leveraging deep learning algorithms within a fog network for devices with Software-Defined Networking (SDN) has been introduced. The system aims to enhance security by recognizing and addressing advanced cyber threats by incorporating innovative technology. A deep learning-based approach using LSTM architecture for intrusion detection in IoT device networks within smart homes is introduced. Specifically, it highlights using LSTM to predict cyberattacks on smart home IoT network devices and learn new outliers over time [163].

The primary objective and emphasis of [164] are centered on the creation and deployment of an advanced IDS specifically designed for Electric Vehicle Charging Stations (EVCS) within IoT framework [165, 166]. Moreover, the paper discusses the construction of an ensemble model that integrates CNN, LSTM, and GRU layers for intrusion detection purposes. The architecture of this model is structured to examine network traffic data, detect abnormalities, and categorize traffic into predetermined classes with notable precision.

6 Future research direction

This section presents challenges and further research directions for securing IoT applications and devices using ML and DL methods.

6.1 Implementation of ML/DL at the fog or cloud computing

The integration of blockchain technology, alongside ML/DL schemes, presents a promising approach to addressing the intricate security needs of the IoT ecosystem. The decentralized nature of blockchain can significantly enhance the security, robustness, and trustless authentication across IoT devices, ensuring a secure exchange of critical data [167]. However, it is acknowledged that blockchain's computational demands and associated overheads present challenges, including high bandwidth requirements and potential delays, critical for real-time IoT applications [168]. Numerous methodologies leveraging the integration of blockchain with ML/DL for IoT have been proposed to address these, offering innovative solutions to security and privacy challenges. For instance, the combination of Software Defined Networking (SDN) and blockchain introduces a structured framework enhancing IoT networks' performance and security, proposing a blueprint for smart, secure IoT frameworks [169].

Additionally, the critical review by Taherdoost underscores the role of ML in bolstering blockchain applications, particularly in securing data and enhancing privacy [170]. Moreover, federated learning emerges as a cutting-edge solution in this landscape, optimizing the balance between data privacy and system performance across distributed IoT devices, indicating a direction for future research and development [171]. This is further supported by the work of Ferrag et al., who highlight the effectiveness of federated deep learning approaches in enhancing IoT cybersecurity and provide a comparative analysis against traditional ML methods [172].

The converging paths of blockchain, ML/DL, and IoT technologies present a change in basic assumptions towards a more secure and private IoT ecosystem. Researchers are tasked with navigating these advancements, ensuring that the integration not only addresses current challenges but also anticipates future demands. The integration's energy and bandwidth implications, alongside the real-time processing delays, serve as critical areas for ongoing investigation, underscoring the necessity for solutions that balance efficiency with security [173–175]. As this field continues to evolve, a collaborative and multidisciplinary approach will be paramount in harnessing the full potential of these technologies, ensuring a secure, efficient, and scalable IoT ecosystem [176, 177].

6.2 Security challenge of testing datasets

Testing and training are essential for ML/DL applications, and secure and trusted datasets are needed. Providing such datasets is a significant challenge for IoT applications and can be studied as future work in this regard.

6.3 Integration of ML/DL with metaheuristic algorithms

Metaheuristic algorithms can integrate ML/DL and IoT security. These new algorithms can improve the parameter selection and tuning operations in the security of IoT devices and applications.

6.4 Data diversity

Today, with the expansion of IoT different applications, IoT heterogeneous devices produce various heterogeneous data with different scales according to the type of application. Diversity and heterogeneity of generated data with large volumes and diverse applications and managing the produced data is one of the crucial challenges.

6.5 Adaptability between ML/DL and IoT applications and devices

The IoT landscape has recently seen continuous expansion and advancement of devices and applications. Consequently, ML/DL systems must exhibit a comparable level of adaptability. Zero-day attacks are inevitable in real-world networks, and introducing new devices to the IoT system is expected. Furthermore, network traffic distribution is subject to change as these new devices join the network. A model trained statically struggles to adjust quickly to these changing conditions, potentially increasing false positives and negatives. Daily fluctuations in end-user demands also present new challenges for ML/DL applications in the IoT environment. Thus, ML/DL algorithms must effectively navigate the swiftly evolving landscape from various perspectives.

7 Conclusion

Considering that the IoT is an excellent network and has a practical impact on the daily life of today's people, but along with its advantages, there are also disadvantages such as eavesdropping, cybercrime, DoS, unauthorized access to data, node forgery, detection infiltrate. This paper reviews ML/DL-based solutions for the security of IoT. According to the studies and research done in this field, we can boldly recommend graph neural networks to detect attacks. GNN can be mixed with other data set classifiers to increase the accuracy of the operation significantly. In the meantime, the AdaBoost device significantly increases the overall accuracy in voting and classifiers. SGDM and ADAM can be used to train the weight of classifications. The size and weight of the classifiers can be quickly determined with these two, and the results are obtained. These two algorithms are based on gradient descent and chaotic behavior. According to the research done and the necessary checks on the above cases, this paper will be helpful for other researchers, and they will make effective use of it.

Author contributions "N.J., S.P. and A.G. wrote the main manuscript text and N.D. and B.A. prepared figures and tables. All authors reviewed the manuscript."

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data availability No data was used for the research described in the article.

Declarations

Conflict of interest The authors do not have a conflict of interest with anyone.

References

1. Cheng, B., Wang, M., Zhao, S., Zhai, Z., Zhu, D., Chen, J.: Situation-aware dynamic service coordination in an IoT environment. IEEE/ACM Trans. Networking. **25**(4), 2082–2095 (2017)
2. Jena, S.K., Barik, R.C., Priyadarshini, R.: A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare. Internet Things, p. 101111, (2024)
3. Rodríguez, E., Otero, B., Canal, R.: A survey of machine and deep learning methods for privacy protection in the Internet of Things, *Sensors*, vol. 23, no. 3, p. 1252, (2023)
4. Khargharia, H.S., Rehman, M.H., Banerjee, A., Montori, F., Forkan, A.R.M., Jayaraman, P.P.: Towards Marketing 4.0: Vision and Survey on the Role of IoT and Data Science, *Societies*, vol. 13, no. 4, p. 100, (2023)
5. Li, T., Zhang, M., Li, Y., Lagerspetz, E., Tarkoma, S., Hui, P.: The impact of COVID-19 on smartphone usage. IEEE Internet Things J. **8**(23), 16723–16733 (2021)
6. Luo, J., Wang, G., Li, G., Pesce, G.: Transport infrastructure connectivity and conflict resolution: A machine learning analysis. Neural Comput. Appl. **34**(9), 6585–6601 (2022)
7. Chen, J., Xu, M., Xu, W., Li, D., Peng, W., Xu, H.: A flow feedback traffic prediction based on visual quantified features. IEEE Trans. Intell. Transp. Syst., (2023)
8. Tayir, T., Li, L.: Unsupervised Multimodal Machine Translation for Low-Resource Distant Language pairs. ACM Trans. Asian Low-Resource Lang. Inform. Process., (2024)
9. Zheng, W., Lu, S., Cai, Z., Wang, R., Wang, L., Yin, L.: PALBERT: An Improved Question Answering Model, *Computer Modeling in Engineering & Sciences; Tech Science Press: Henderson, NV, USA*, (2023)
10. Zhao, L., Qu, S., Xu, H., Wei, Z., Zhang, C.: Energy-efficient trajectory design for secure SWIPT systems assisted by UAV-IRS. Veh. Commun. **45**, 100725 (2024)
11. Yin, Y., Guo, Y., Su, Q., Wang, Z.: Task allocation of multiple unmanned aerial vehicles based on deep transfer reinforcement learning, *Drones*, vol. 6, no. 8, p. 215, (2022)
12. Zhang, X., et al.: Secure Routing Strategy based on attribute-based Trust Access Control in Social-Aware Networks. J. Signal. Process. Syst. pp. 1–16, (2024)
13. Asgharzadeh, H., Ghaffari, A., Masdari, M., Gharehchopogh, F.S.: Anomaly-based intrusion detection system in the internet of things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. J. Parallel Distrib. Comput. **175**, 1–21 (2023)
14. Hanafi, A.V., Ghaffari, A., Rezaei, H., Valipour, A., arasteh, B.: Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and LSTM. Cluster Comput., pp. 1–18, (2023)
15. Mousavi, S.K., Ghaffari, A.: Data cryptography in the internet of things using the artificial bee colony algorithm in a smart irrigation system. J. Inform. Secur. Appl. **61**, 102945 (2021)
16. Mousavi, S.K., Ghaffari, A., Besharat, S., Afshari, H.: Security of internet of things using RC4 and ECC algorithms (case study: Smart irrigation systems). Wireless Pers. Commun. **116**(3), 1713–1742 (2021)
17. Shukla, P., Krishna, C.R., Patil, N.V.: SDDA-IoT: Storm-based distributed detection approach for IoT network traffic-based DDoS attacks. Cluster Comput., pp. 1–28, (2024)
18. Nematollahi, M., Ghaffari, A., Mirzaei, A.: Task and resource allocation in the internet of things based on an improved version of the moth-flame optimization algorithm. Cluster Comput., pp. 1–23, (2023)
19. Nematollahi, M., Ghaffari, A., Mirzaei, A.: Task offloading in internet of things based on the improved multi-objective aquila optimizer. Signal. Image Video Process. **18**(1), 545–552 (2024)
20. Seyfollahi, A., Abeshloo, H., Ghaffari, A.: Enhancing mobile crowdsensing in fog-based internet of things utilizing Harris hawks optimization. J. Ambient Intell. Humaniz. Comput., pp. 1–16, (2022)
21. Čolaković, A., Hadžialić, M.: Internet of things (IoT): A review of enabling technologies, challenges, and open research issues. Comput. Netw. **144**, 17–39 (2018)
22. Alotaibi, A., Barnawi, A.: Securing massive IoT in 6G: Recent solutions, architectures, future directions. Internet Things. **22**, 100715 (2023)
23. Sharma, R., Arya, R.: Secured mobile IOT ecosystem using enhanced multi-level intelligent trust scheme. Comput. Electr. Eng. **108**, 108715 (2023)
24. Kalakoti, R., Bahsi, H., Nõmm, S.: Improving IoT Security with Explainable AI: Quantitative evaluation of Explainability for IoT Botnet Detection. IEEE Internet Things J., (2024)
25. Altulaihan, E., Almaiah, M.A., Aljughaiman, A.: Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms, *Sensors*, vol. 24, no. 2, p. 713, (2024)
26. Mohy-Eddine, M., Guezzaz, A., Benkirane, S., Azrour, M.: An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. Multimedia Tools Appl. **82**(15), 23615–23633 (2023)
27. Tahsien, S.M., Karimipour, H., Spachos, P.: Machine learning based solutions for security of internet of things (IoT): A survey. J. Netw. Comput. Appl. **161**, 102630 (2020)
28. Sivasakthi, D.A., Sathiyaraj, A., Devendiran, R.: HybridRobustNet: Enhancing detection of hybrid attacks in IoT networks through advanced learning approach. Cluster Comput., pp. 1–15, (2024)
29. Alangari, S.: An unsupervised machine learning algorithm for attack and anomaly detection in IoT Sensors. Wireless Pers. Commun., pp. 1–25, (2024)
30. Indrason, N., Saha, G.: Exploring blockchain-driven security in SDN-based IoT networks. J. Netw. Comput. Appl., p. 103838, (2024)
31. Venkatesh, R., Malarvizhi, N.: IOT Security and Machine Learning Algorithms: Survey and Analysis, in *7th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2023, pp. 444–451: IEEE. (2023)
32. Truong, V.T., Le, L.B.: Security for the Metaverse: Blockchain and Machine Learning techniques for intrusion detection. IEEE Netw., (2024)
33. Braghin, C., Lilli, M., Riccobene, E.: A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study. Computers Secur. **127**, 103037 (2023)
34. Hazman, C., Guezzaz, A., Benkirane, S., Azrour, M.: lIDS-SIoEL: Intrusion detection framework for IoT-based smart environments security using ensemble learning. Cluster Comput. **26**(6), 4069–4083 (2023)
35. Khan, D., Alonazi, M., Abdelhaq, M., Algarni, A., Jalal, A., Liu, H.: Robust human locomotion and localization activity recognition over multisensory. Front. Physiol. **15**, 1344887 (2024)
36. Chen, J., Wang, Q., Peng, W., Xu, H., Li, X., Xu, W.: Disparity-based multiscale fusion network for transportation detection. IEEE Trans. Intell. Transp. Syst. **23**(10), 18855–18863 (2022)
37. Xu, Y., Wang, E., Yang, Y., Chang, Y.: A unified collaborative representation learning for neural-network based recommender systems. IEEE Trans. Knowl. Data Eng. **34**(11), 5126–5139 (2021)
38. Zhang, J., Ren, J., Cui, Y., Fu, D., Cong, J.: Multi-USV Task Planning Method based on improved deep reinforcement learning. IEEE Internet Things J., (2024)

39. Sarker, I.H., Khan, A.I., Abushark, Y.B., Alsolami, F.: Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions. Mob. Networks Appl., pp. 1–17, (2022)
40. Ahmed, K.D., Askar, S.: Deep learning models for cyber security in IoT networks: A review. Int. J. Sci. Bus. **5**(3), 61–70 (2021)
41. Mohanta, B.K., Jena, D., Satapathy, U., Patnaik, S.: Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things. **11**, 100227 (2020)
42. Idrissi, I., Azizi, M., Moussaoui, O.: IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review, in *Fourth international conference on intelligent computing in data sciences (ICDS)*, 2020, pp. 1–10: IEEE. (2020)
43. Babu, M.R., Veena, K.: A survey on attack detection methods for iot using machine learning and deep learning, in *3rd International conference on signal processing and communication (ICPSC)*, 2021, pp. 625–630: IEEE. (2021)
44. Aversano, L., Bernardi, M.L., Cimitile, M., Pecori, R.: A systematic review on Deep Learning approaches for IoT security. Comput. Sci. Rev. **40**, 100389 (2021)
45. Ahanger, T.A., Aljumah, A., Atiquzzaman, M.: State-of-the-art survey of artificial intelligent techniques for IoT security. Comput. Netw. **206**, 108771 (2022)
46. Wu, H., Han, H., Wang, X., Sun, S.: Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access. **8**, 153826–153848 (2020)
47. Thakkar, A., Lohiya, R.: A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges. Arch. Comput. Methods Eng. **28**, 3211–3243 (2021)
48. Farooq, U., Tariq, N., Asim, M., Baker, T., Al-Shamma'a, A.: Machine learning and the internet of things security: Solutions and open challenges. J. Parallel Distrib. Comput. **162**, 89–104 (2022)
49. Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M.: A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun. Surv. Tutorials. **22**(3), 1646–1685 (2020)
50. Yue, Y., Li, S., Legg, P., Li, F.: Deep learning-based security behaviour analysis in IoT environments: A survey. Secur. Communication Networks. **2021**, 1–13 (2021)
51. Ahmad, R., Alsmadi, I.: Machine learning approaches to IoT security: A systematic literature review. Internet Things. **14**, 100365 (2021)
52. Mrabet, H., Belguith, S., Alhomoud, A., Jemai, A.: A survey of IoT security based on a layered architecture of sensing and data analysis, *Sensors*, vol. 20, no. 13, p. 3625, (2020)
53. Da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque, V.H.C.: Internet of things: A survey on machine learning-based intrusion detection approaches. Comput. Netw. **151**, 147–157 (2019)
54. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access. **7**, 82721–82743 (2019)
55. Zeadally, S., Tsikerdekis, M.: Securing internet of things (IoT) with machine learning. Int. J. Commun Syst. **33**(1), e4169 (2020)
56. Geetha, R., Thilagam, T.: A review on the effectiveness of machine learning and deep learning algorithms for cyber security. Arch. Comput. Methods Eng. **28**, 2861–2879 (2021)
57. Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T., Bahaj, S.A.: Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions, *Security and Communication Networks*, vol. 2022. (2022)
58. Salih, A., Zeebaree, S.T., Ameen, S., Alkhyyat, A., Shukur, H.M.: A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection, in *7th International Engineering Conference Research & Innovation amid Global Pandemic(IEC)*, 2021, pp. 61–66: IEEE. (2021)
59. Ravikumar, K., Chiranjeevi, P., Devarajan, N.M., Kaur, C., Taloba, A.I.: Challenges in internet of things towards the security using deep learning techniques. Measurement: Sens. **24**, 100473 (2022)
60. Amanullah, M.A., et al.: Deep learning and big data technologies for IoT security. Comput. Commun. **151**, 495–517 (2020)
61. Liu, C., Chen, B., Shao, W., Zhang, C., Wong, K., Zhang, Y.: Unraveling Attacks in Machine Learning-based IoT Ecosystems: A Survey and the Open Libraries Behind Them, *arXiv preprint arXiv:2401.11723*, (2024)
62. Mengistu, T.M., Kim, T., Lin, J.-W.: A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning, *Sensors*, vol. 24, no. 3, p. 968, (2024)
63. Cao, B., Wang, X., Zhang, W., Song, H., Lv, Z.: A many-objective optimization model of industrial internet of things based on private blockchain. IEEE Netw. **34**(5), 78–83 (2020)
64. ZAINUDDIN, A.A.B.: Enhancing IoT Security: A synergy of machine learning, Artificial Intelligence, and Blockchain. Data Sci. Insights, **2**, 1, (2024)
65. Ali, S., Li, Q., Yousafzai, A.: Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. Ad Hoc Netw. **152**, 103320 (2024)
66. Cherbal, S., Zier, A., Hebal, S., Louail, L., Annane, B.: Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. J. Supercomputing. **80**(3), 3738–3816 (2024)
67. Aryavalli, S.N.G., Kumar, H.: Top 12 layer-wise security challenges and a secure architectural solution for internet of things. Comput. Electr. Eng. **105**, 108487 (2023)
68. Bertino, E., Islam, N.: Botnets and internet of things security, *Computer*, vol. 50, no. 2, pp. 76–79, (2017)
69. Gokhale, P., Bhat, O., Bhat, S.: Introduction to IOT. Int. Adv. Res. J. Sci. Eng. Technol. **5**(1), 41–44 (2018)
70. Dai, M., Sun, G., Yu, H., Niyato, D.: Maximize the Long-Term Average revenue of network slice provider via Admission Control among heterogeneous slices. IEEE/ACM Trans. Networking, (2023)
71. Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A review on internet of things (IoT). Int. J. Comput. Appl. **113**(1), 1–7 (2015)
72. Zhang, Y.: Technology framework of the Internet of Things and its application, in *International Conference on Electrical and Control Engineering*, 2011, pp. 4109–4112: IEEE. (2011)
73. Cao, B., Zhao, J., Gu, Y., Fan, S., Yang, P.: Security-aware industrial wireless sensor network deployment optimization. IEEE Trans. Industr. Inf. **16**(8), 5309–5316 (2019)
74. Sun, G., Liao, D., Zhao, D., Xu, Z., Yu, H.: Live migration for multiple correlated virtual machines in cloud-based data centers. IEEE Trans. Serv. Comput. **11**(2), 279–291 (2015)
75. Cao, B., et al.: Multiobjective 3-D topology optimization of next-generation wireless data center network. IEEE Trans. Industr. Inf. **16**(5), 3597–3605 (2019)
76. Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., Sun, J.: A new digital watermarking method for data integrity protection in the perception layer of IoT, *Security and Communication Networks*, vol. 2017. (2017)
77. Khattak, H.A., Shah, M.A., Khan, S., Ali, I., Imran, M.: Perception layer security in internet of things. Future Generation Comput. Syst. **100**, 144–164 (2019)

78. Li, J., Li, J., Wang, C., Verbeek, F.J., Schultz, T., Liu, H.: MS2OD: Outlier detection using minimum spanning tree and medoid selection. Mach. Learning: Sci. Technol. **5**(1), 015025 (2024)
79. Chen, Y., Zhu, L., Hu, Z., Chen, S., Zheng, X.: Risk propagation in multilayer heterogeneous network of coupled system of large engineering project. J. Manag. Eng. **38**(3), 04022003 (2022)
80. Wu, Z.-Y., Ismail, M., Wang, J.: Efficient exclusion strategy of shadowed RIS in dynamic indoor programmable wireless environments. IEEE Trans. Wireless Commun., (2023)
81. Lei, Y., Yanrong, C., Hai, T., Ren, G., Wenhuan, W.: DGNet: An adaptive lightweight defect detection model for New Energy Vehicle Battery Current Collector. IEEE Sens. J., (2023)
82. Xia, W., et al.: The design of fast and Lightweight Resemblance Detection for efficient Post-deduplication Delta Compression. ACM Trans. Storage. **19**(3), 1–30 (2023)
83. Yin, F., et al.: FedLoc: Federated learning framework for data-driven cooperative localization and location data processing. IEEE Open. J. Signal. Process. **1**, 187–215 (2020)
84. Liao, Q., et al.: An integrated multi-task model for fake news detection. IEEE Trans. Knowl. Data Eng. **34**(11), 5154–5165 (2021)
85. Li, Y., Zuo, Y., Song, H., Lv, Z.: Deep learning in security of internet of things. IEEE Internet Things J. **9**(22), 22133–22146 (2021)
86. Alleema, N.N., et al.: Security of Big Data over IoT Environment by Integration of Deep Learning and optimization. Int. J. Communication Networks Inform. Secur. **14**(2), 203–221 (2022)
87. Shafiq, M., Tian, Z., Bashir, A.K., Du, X., Guizani, M.: CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. IEEE Internet Things J. **8**(5), 3242–3254 (2020)
88. Lv, Z., Qiao, L., Li, J., Song, H.: Deep-learning-enabled security issues in the internet of things. IEEE Internet Things J. **8**(12), 9531–9538 (2020)
89. Krishna, R.R., Priyadarshini, A., Jha, A.V., Appasani, B., Srinivasulu, A., Bizon, N.: State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions, *Sustainability*, vol. 13, no. 16, p. 9463, (2021)
90. Altulaihan, E., Almaiah, M.A., Aljughaiman, A.: Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions, *Electronics*, vol. 11, no. 20, p. 3330, (2022)
91. Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., Elkhediri, S.: CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques, in *2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6: IEEE. (2019)
92. Kim, M., Suh, T.: Eavesdropping vulnerability and countermeasure in infrared communication for IoT devices, *Sensors*, vol. 21, no. 24, p. 8207, (2021)
93. Ahmed, H.I., Nasr, A.A., Abdel-Mageid, S., Aslan, H.K.: A survey of IoT security threats and defenses. Int. J. Adv. Comput. Res. **9**(45), 325–350 (2019)
94. Xu, H., Han, S., Li, X., Han, Z.: Anomaly Traffic Detection based on communication-efficient Federated Learning in Space-Air-Ground Integration Network. IEEE Trans. Wireless Commun. no. **99**, 1–1 (2023)
95. Salim, M.M., Rathore, S., Park, J.H.: Distributed denial of service attacks and its defenses in IoT: A survey. J. Supercomputing. no. **76**, 5320–5363 (2020)
96. Humayun, M., Jhanjhi, N., Alsayat, A., Ponnusamy, V.: Internet of things and ransomware: Evolution, mitigation and prevention. Egypt. Inf. J. no. **22**(1), 105–117 (2021)
97. Yu, J., Lu, L., Chen, Y., Zhu, Y., Kong, L.: An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing. IEEE Trans. Mob. Comput. no. **20**(2), 337–351 (2019)
98. Jiang, H., Wang, M., Zhao, P., Xiao, Z., Dustdar, S.: A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs. IEEE/ACM Trans. Networking. no. **29**(5), 2228–2241 (2021)
99. Thankappan, M., Rifà-Pous, H., Garrigues, C.: Multi-channel man-in-the-middle attacks against protected wi-fi networks: A state of the art review. Expert Syst. Appl., p. 118401, (2022)
100. Fereidouni, H., Fadeitcheva, O., Zalai, M.: IoT and Man-in-the-Middle Attacks, *arXiv preprint arXiv:2308.02479*, (2023)
101. Ma, J., Hu, J.: Safe consensus control of cooperative-competitive multi-agent systems via differential privacy, *Kybernetika*, vol. 58, no. 3, pp. 426–439, (2022)
102. Khan, F., et al.: Development of a Model for Spoofing Attacks in Internet of Things, *Mathematics*, vol. 10, no. 19, p. 3686, (2022)
103. Damghani, H., Damghani, L., Hosseinian, H., Sharifi, R.: Classification of attacks on IoT, in *4th international conference on combinatorics, cryptography, computer science and computation*, (2019)
104. Hijazi, S., Obaidat, M.S.: Address resolution protocol spoofing attacks and security approaches: A survey. Secur. Priv. no. **2**(1), e49 (2019)
105. Stasinopoulos, A., Ntantogian, C., Xenakis, C.: Commix: Detecting and exploiting command injection flaws. Dept Digit. Syst. Univ. Piraeus Piraeus Greece White Paper, (2015)
106. Zheng, W., Deng, P., Gui, K., Wu, X.: An Abstract Syntax Tree based static fuzzing mutation for vulnerability evolution analysis. Inf. Softw. Technol. no. **158**, 107194 (2023)
107. Zhang, J., Chen, H., Gong, L., Cao, J., Gu, Z.: The current research of IoT security, in *IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, 2019, pp. 346–353: IEEE. (2019)
108. Chanal, P.M., Kakkasageri, M.S.: Security and privacy in IoT: A survey. Wireless Pers. Commun. no. **115**(2), 1667–1693 (2020)
109. Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K., Kamhoua, C.: Preserving data integrity in iot networks under opportunistic data manipulation, in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, pp. 446–453: IEEE. (2017)
110. Karimipour, H., Dinavahi, V.: Robust massively parallel dynamic state estimation of power systems against cyber-attack. IEEE Access. no. **6**, 2984–2995 (2017)
111. Hameed, A., Alomary, A.: Security issues in IoT: A survey, in *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*, pp. 1–5: IEEE. (2019)
112. Ali, I., Sabir, S., Ullah, Z.: Internet of things security, device authentication and access control: a review, *arXiv preprint arXiv:07309*, 2019. (1901)
113. El-Hajj, M., Chamoun, M., Fadlallah, A., Serhrouchni, A.: Analysis of authentication techniques in Internet of Things (IoT), in *2017 1st Cyber Security in Networking Conference (CSNet)*, pp. 1–3: IEEE. (2017)
114. Yao, X., Chen, Z., Tian, Y.: A lightweight attribute-based encryption scheme for the internet of things. Future Generation Comput. Syst. no. **49**, 104–112 (2015)
115. Assiri, A., Almagwashi, H.: IoT security and privacy issues, in *1st International Conference on Computer Applications & Information Security (ICCAIS)*, 2018, pp. 1–5: IEEE. (2018)
116. Imdad, M., Jacob, D.W., Mahdin, H., Baharum, Z., Shaharudin, S.M., Azmi, M.S.: Internet of things (IoT); security requirements, attacks and counter measures. Indonesian J. Electr. Eng. Comput. Sci. no. **18**(3), 1520–1530 (2020)

117. Fang, H., Qi, A., Wang, X.: Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement. IEEE Netw. no. **34**(3), 24–29 (2020)
118. Farris, I., Taleb, T., Khettab, Y., Song, J.: A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun. Surv. Tutorials. no. **21**(1), 812–837 (2018)
119. Istiaque Ahmed, K., Tahir, M., Hadi Habaebi, M., Lun Lau, S., Ahad, A.: Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction, *Sensors*, vol. 21, no. 15, p. 5122, (2021)
120. Divya, K., Roopashree, H., Yogeesh, A.: Non-repudiation-based network security system using multiparty computation. Int. J. Adv. Comput. Sci. Appl., **13**, 3, (2022)
121. Khan, Y., Su'ud, M.B.M., Alam, M.M., Ahmad, S.F., Salim, N.A., Khan, N.: Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications, *Electronics*, vol. 12, no. 1, p. 88, (2022)
122. Hurrah, N.N., Parah, S.A., Sheikh, J.A., Al-Turjman, F., Muhammad, K.: Secure data transmission framework for confidentiality in IoTs. Ad Hoc Netw. no. **95**, 101989 (2019)
123. Khan, M.A., Salah, K.: IoT security: Review, blockchain solutions, and open challenges. Future Generation Comput. Syst. no. **82**, 395–411 (2018)
124. Valea, E., Da Silva, M., Flottes, M.-L., Di Natale, G., Dupuis, S., Rouzeyre, B.: Providing confidentiality and integrity in ultra low power iot devices, in *14th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS)*, 2019, pp. 1–6: IEEE. (2019)
125. Liu, X., et al.: Adapting feature selection algorithms for the classification of Chinese texts, *Systems*, vol. 11, no. 9, p. 483, (2023)
126. Song, Y., Xin, R., Chen, P., Zhang, R., Chen, J., Zhao, Z.: Identifying performance anomalies in fluctuating cloud environments: A robust correlative-GNN-based explainable approach. Future Generation Comput. Syst. no. **145**, 77–86 (2023)
127. Liu, B., Tang, D., Yan, Y., Zheng, Z., Zhang, S., Zhou, J.: TS-SVM: Detect LDoS attack in SDN based on two-step self-adjusting SVM, in *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021, pp. 678–685: IEEE. (2021)
128. Azmi, M.M., Sumadi, F.D.S.: Low-Rate Attack Detection on SD-IoT Using SVM Combined with Feature Importance Logistic Regression Coefficient, *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, (2022)
129. Stryczek, S., Natkaniec, M.: Internet threat detection in Smart Grids based on Network Traffic Analysis Using LSTM, IF, and SVM, *energies*, **16**, 1, p. 329, (2022)
130. Mustafa Hilal, A., et al.: Malware Detection using decision Tree Based SVM Classifier for IoT. Computers Mater. Continua, **72**, 1, (2022)
131. Gupta, S.K., Pattnaik, B., Agrawal, V., Boddu, R.S.K., Srivastava, A., Hazela, B.: Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things, in *Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 2022, pp. 1–6: IEEE. (2022)
132. Ioannou, C., Vassiliou, V.: Network attack classification in IoT using support vector machines. J. Sens. Actuator Networks. no. **10**(3), 58 (2021)
133. Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M.: Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet Things J. no. **6**(5), 7702–7712 (2019)
134. Ramadevi, R., Krishnamoorthy, N., Marshiana, D., Kumaran, S., Aarthi, N.: Development of intrusion detection system for security threats in internet of things using artificial neural network. J. Comput. Theor. Nanosci. no. **16**(8), 3242–3245 (2019)
135. de Assis, M.V., Carvalho, L.F., Rodrigues, J.J., Lloret, J., Proença, M.L. Jr.: Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. Comput. Electr. Eng. no. **86**, 106738 (2020)
136. Mozzaquatro, B.A., Agostinho, C., Melo, R., Jardim-Goncalves, R.: A model-driven adaptive approach for iot security, in *Model-Driven Engineering and Software Development: 4th International Conference, MODELSWARD* Rome, Italy, February 19–21, 2016, Revised Selected Papers 4, 2017, pp. 194–215: Springer. (2016)
137. Martin, T., Geneiatakis, D., Kounelis, I., Kerckhof, S., Nai Fovino, I.: Towards a formal IoT security model, *Symmetry*, vol. 12, no. 8, p. 1305, (2020)
138. Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., Shmatikov, V.: How to backdoor federated learning, in *International conference on artificial intelligence and statistics*, pp. 2938–2948: PMLR. (2020)
139. Tavallaee, M., Stakhanova, N., Ghorbani, A.A.: Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Trans. Syst. Man. Cybernetics Part. C (Applications Reviews). no. **40**(5), 516–524 (2010)
140. Cao, K., et al.: Achieving reliable and secure communications in wireless-powered NOMA systems. IEEE Trans. Veh. Technol. no. **70**(2), 1978–1983 (2021)
141. Wang, Y., Wang, J., Jin, H.: Network Intrusion Detection Method Based on Improved CNN in Internet of Things Environment, *Mobile Information Systems*, vol. 2022. (2022)
142. Sankaran, K.S., Kim, B.-H.: Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. Sustain. Energy Technol. Assess. no. **56**, 102983 (2023)
143. Alabsi, B.A., Anbar, M., Rihan, S.D.A.: CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks, *Sensors*, vol. 23, no. 14, p. 6507, (2023)
144. Rahim, A., Zhong, Y., Ahmad, T., Ahmad, S., Pławiak, P., Hammad, M.: Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models, *Sensors*, vol. 23, no. 15, p. 6979, (2023)
145. Prasath, J., Shyja, V.I., Chandrakanth, P., Kumar, B.K., Raja Basha, A.: An optimal secure defense mechanism for DDoS attack in IoT network using feature optimization and intrusion detection system, *Journal of Intelligent & Fuzzy Systems*, no. Preprint, pp. 1–18
146. Liu, S., Chen, X., Peng, X., Xiao, R., Networking: Network log anomaly detection based on GRU and SVDD, in *2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing &* Communications, *Social Computing &* Networking *(ISPA/BDCloud/SocialCom/SustainCom)*, pp. 1244–1249: IEEE. (2019)
147. ur Rehman, S., et al.: DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU). Future Generation Comput. Syst. no. **118**, 453–466 (2021)
148. Zhu, Z., Zhang, L., Liu, J., Ying, X.: IoT Security Detection Method Based on Multifeature and Multineural Network Fusion, *Security and Communication Networks*, vol. 2023. (2023)
149. Hochreiter, S., Schmidhuber, J.: Long short-term memory, *Neural computation*, vol. 9, no. 8, pp. 1735–1780, (1997)
150. Bokka, R., Sadasivam, T.: Securing IoT Networks: RPL Attack Detection with Deep Learning GRU Networks, (2023)
151. Sagar, A., Anushkannan, N., Indumathi, G., Muralidhar, N.V., Dhamotharan, K., Malini, P.: Wireless Sensor Network-based Intrusion Detection Technique using Deep Learning Approach of CNN-GRU, in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, pp. 1147–1152: IEEE. (2023)

152. Wang, Z., Huang, H., Du, R., Li, X., Yuan, G.: IoT Intrusion Detection Model based on CNN-GRU. Front. Comput. Intell. Syst. no. **4**(2), 90–95 (2023)
153. Banaamah, A.M., Ahmad, I.: Intrusion detection in iot using deep learning, *Sensors*, vol. 22, no. 21, p. 8417, (2022)
154. Zhou, P., et al.: Reactive human–robot collaborative manipulation of deformable linear objects using a new topological latent control model. Robot. Comput. Integr. Manuf. no. **88**, 102727 (2024)
155. Guo, Y., et al.: Traffic Shaping in IoT Networks using GNN and MAB with SDN Orchestration, (2023)
156. Altaf, T., Wang, X., Ni, W., Liu, R.P., Braun, R.: NE-GConv: A lightweight node edge graph convolutional network for intrusion detection. Computers Secur. no. **130**, 103285 (2023)
157. Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R.P., Braun, R.: A new concatenated multigraph neural network for IoT intrusion detection. Internet Things. no. **22**, 100818 (2023)
158. Esmaeili, B., Azmoodeh, A., Dehghantanha, A., Srivastava, G., Karimipour, H., Lin, J.C.-W.: A GNN-Based adversarial internet of things Malware Detection Framework for critical infrastructure: Studying Gafgyt, Mirai and Tsunami campaigns. IEEE Internet Things J., (2023)
159. Liu, T., Li, Z., Long, H., Bilal, A.: Nt-gnn: Network traffic graph for 5 g mobile iot android malware detection, *Electronics*, vol. 12, no. 4, p. 789, (2023)
160. Alkahtani, H., Aldhyani, T.H.: Botnet attack detection by using CNN-LSTM model for Internet of Things applications, *Security and Communication Networks*, vol. pp. 1–23, 2021. (2021)
161. Wang, X., Lu, X.: A host-based anomaly detection framework using XGBoost and LSTM for IoT devices, *Wireless Communications and Mobile Computing*, vol. pp. 1–13, 2020. (2020)
162. Ullah, I., Raza, B., Ali, S., Abbasi, I.A., Baseer, S., Irshad, A.: Software defined network enabled fog-to-things hybrid deep learning driven cyber threat detection system, *Security and Communication Networks*, vol. pp. 1–15, 2021. (2021)
163. Azumah, S.W., Elsayed, N., Adewopo, V., Zaghloul, Z.S., Li, C.: A deep lstm based approach for intrusion detection iot devices network in smart home. In: 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), pp. 836–841. IEEE (2021)
164. Kilichev, D., Turimov, D., Kim, W., Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and, Models, G.R.U.: *Mathematics*, vol. 12, no. 4, p. 571, (2024)
165. Yang, J., Yang, K., Xiao, Z., Jiang, H., Xu, S., Dustdar, S.: Improving commute experience for private car users via blockchain-enabled multitask learning. IEEE Internet Things J., (2023)
166. Xiao, Z., et al.: Understanding private car aggregation effect via spatio-temporal analysis of trajectory data. IEEE Trans. Cybernetics. no. **53**(4), 2346–2357 (2021)
167. Alfandi, O., Khanji, S., Ahmad, L., Khattak, A.: A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues, *Cluster Computing*, vol. 24, no. 1, pp. 37–55, (2021)
168. Jan, M.A., et al.: Security and blockchain convergence with internet of Multimedia things: Current trends, research challenges and future directions. J. Netw. Comput. Appl. no. **175**, 102918 (2021)
169. Turner, S.W., Karakus, M., Guler, E., Uludag, S.: A promising integration of sdn and blockchain for iot networks: A survey. IEEE Access., (2023)
170. Taherdoost, H.: Blockchain and machine learning: A critical review on security, *Information*, vol. 14, no. 5, p. 295, (2023)
171. Akhtarshenas, A., Vahedifar, M.A., Ayoobi, N., Maham, B., Alizadeh, T.: Federated Learning: A Cutting-Edge Survey of the Latest Advancements and Applications, *arXiv preprint arXiv:2310.05269*, (2023)
172. Ferrag, M.A., Friha, O., Maglaras, L., Janicke, H., Shu, L.: Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. IEEE Access. no. **9**, 138509–138542 (2021)
173. Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S.S., Usman, M.: Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Comput. Surv. (csur). no. **53**(6), 1–37 (2020)
174. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., Imran, M.: Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Generation Comput. Syst. no. **100**, 325–343 (2019)
175. Eghmazi, A., Ataei, M., Landry, R.J., Chevrette, G.: Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy, *IoT*, vol. 5, no. 1, pp. 20–34, (2024)
176. Baghalzadeh Shishehgarkhaneh, M., Keivani, A., Moehler, R.C., Jelodari, N., Roshdi Laleh, S.: Internet of Things (IoT), Building Information Modeling (BIM), and Digital Twin (DT) in construction industry: A review, bibliometric, and network analysis, *Buildings*, vol. 12, no. 10, p. 1503, (2022)
177. Shishehgarkhaneh, M.B., Moehler, R.C., Moradinia, S.F.: Blockchain in the Construction Industry between 2016 and 2022: A Review, Bibliometric, and Network Analysis, *Smart Cities*, vol. 6, no. 2, pp. 819–845, (2023)