

Received 17 November 2023, accepted 11 December 2023, date of publication 22 December 2023,  
date of current version 29 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3346320



## SURVEY

# Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation

MIRZA AKHI KHATUN<sup>ID 1,2</sup>, (Member, IEEE), SANOBER FARHEEN MEMON<sup>ID 1</sup>, (Member, IEEE),

CIARÁN EISING<sup>ID 1,2</sup>, (Senior Member, IEEE),

AND LUBNA LUXMI DHIRANI<sup>ID 1,2</sup>, (Senior Member, IEEE)

<sup>1</sup>Department Electronic and Computer Engineering, University of Limerick, Limerick, V94 T9PX Ireland

<sup>2</sup>SFI CRT Foundations in Data Science, University of Limerick, Limerick, V94 T9PX Ireland

Corresponding author: Mirza Akhi Khatun (Mirza.Akhi@ul.ie)

This work has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) under Grant Number 18/CRT/6049.

**ABSTRACT** The Healthcare Internet-of-Things (H-IoT), commonly known as Digital Healthcare, is a data-driven infrastructure that highly relies on smart sensing devices (i.e., blood pressure monitors, temperature sensors, etc.) for faster response time, treatments, and diagnosis. However, with the evolving cyber threat landscape, IoT devices have become more vulnerable to the broader risk surface (e.g., risks associated with generative AI, 5G-IoT, etc.), which, if exploited, may lead to data breaches, unauthorized access, and lack of command and control and potential harm. This paper reviews the fundamentals of healthcare IoT, its privacy, and data security challenges associated with machine learning and H-IoT devices. The paper further emphasizes the importance of monitoring healthcare IoT layers such as perception, network, cloud, and application. Detecting and responding to anomalies involves various cyber-attacks and protocols such as Wi-Fi 6, Narrowband Internet of Things (NB-IoT), Bluetooth, ZigBee, LoRa, and 5G New Radio (5G NR). A robust authentication mechanism based on machine learning and deep learning techniques is required to protect and mitigate H-IoT devices from increasing cybersecurity vulnerabilities. Hence, in this review paper, security and privacy challenges and risk mitigation strategies for building resilience in H-IoT are explored and reported.

**INDEX TERMS** Healthcare-IoT, generative AI, 5G-IoT, security and privacy challenges, cybersecurity, attacks, anomaly detection, machine learning, deep learning, mitigation techniques, 5G NR.

## I. INTRODUCTION

The Internet of Things (IoT) consists of interconnected physical devices exchanging data through sensors, software, and connectivity [1], [2]. The healthcare industry has undergone a significant transformation in recent years with advances in IoT, cloud, artificial intelligence (AI), and machine learning (ML). According to several experts, the expanding horizon of IoT is expected to improve healthcare. IoT can revolutionize healthcare globally by providing affordable healthcare [3], remote health monitoring [4], wellness management [5], and virtual rehabilitation [6]. Healthcare analytics can provide insight into disease and drug discovery while adding a new dimension [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Claudio Agostino Ardagna<sup>ID</sup>.

The modern world requires more efficient and timely interventions to combat escalating health issues. While traditional healthcare systems are effective, these systems are often slow and inflexible [8]. The COVID-19 pandemic has fueled the need for remote and precision healthcare, and such objectives could only be achieved using emerging technologies. Embedding an IoT-enabled architecture in a healthcare ecosystem may facilitate the collecting and processing real-time data from sensors (i.e., body sensors strategically placed on or within a patient's body, aiding real-time data collection) [9]. Different sensors are used for different applications, such as motion, flow, and biomedical. However, the ones used for healthcare applications are typically body sensor networks (BSN) [10]. In a BSN, each sensor is connected within a group, forming a network; this configuration enhances data collection and efficiency

by integrating IoT body sensors, such as brain waves, body temperature, and blood pressure sensors, as depicted in Figure 1. Moreover, the diagram also illustrates how data is stored and transmitted to the cloud via edge nodes/layers for data processing and storage. IoT devices transmit data in milliseconds and require high reliability, scalability, and end-to-end (E2E) latency connectivity networks [1]. Connecting the IoT devices with an edge-to-cloud environment is essential to facilitate the required/comprehensive health monitoring (security and reliability metrics).

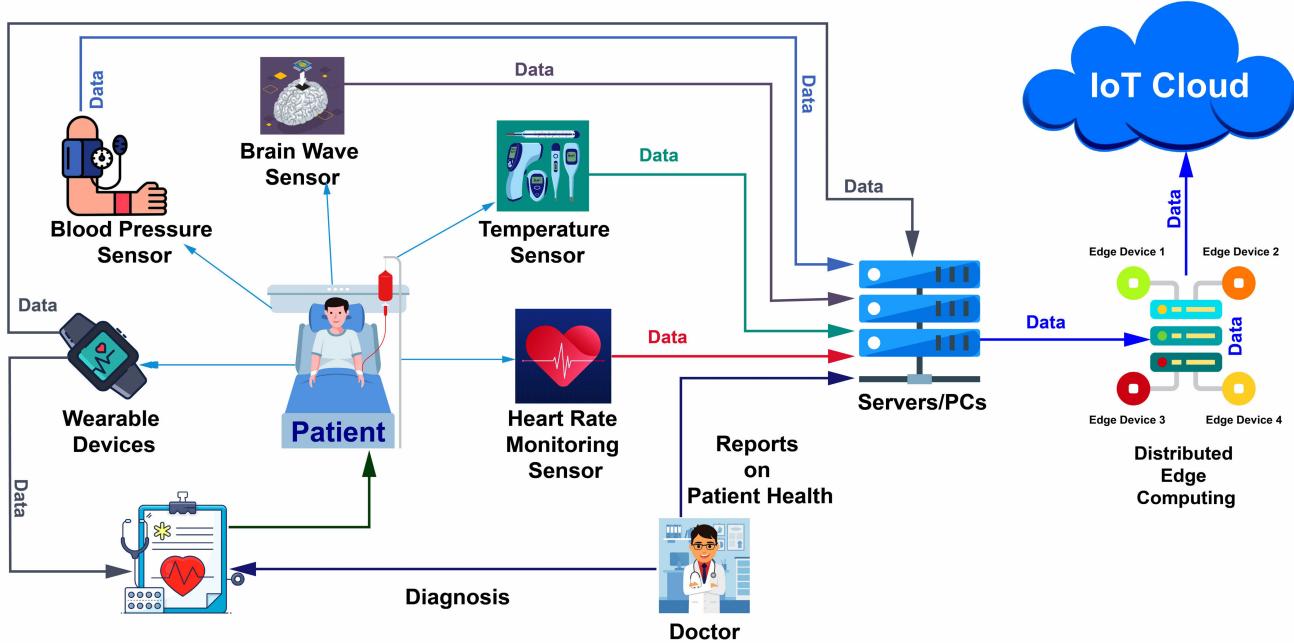
As per [11], the need and usage of IoT devices will increase significantly; by 2025, there will be more than 41 billion IoT devices used worldwide, with the capacity to produce 78 zettabytes of data. Because of its usability, efficiency, and applications, these devices have the potential to further advance healthcare by reducing costs, improving patient well-being, and facilitating the efficient delivery of faster diagnostics, thereby improving medical services [12]. Furthermore, IoT can provide the migration of patients from traditional healthcare management methods to new cloud-based systems, among other vital innovations [13]. Employing Healthcare-IoT (H-IoT), remote monitoring of patients can save millions of lives and money, while other functions still have a crucial role across healthcare environments [14]. This type of remote monitoring of patients can assist in identifying health issues early on and making treatment plans more personalized. Similarly, IoT can benefit medical management, including medication and instrumental errors, and medication administration-allowing patients to take their medications at the right time and with the correct dosage [15]. Medication error prevention programs can improve patient outcomes and reduce healthcare costs. For example, H-IoT could significantly improve health outcomes and healthcare costs for residents of care homes who frequently manage multiple medical conditions and take various medications [16].

IoT healthcare frameworks utilize a variety of sophisticated sensors, including diagnostic, sensitive, and preventive sensors, for the implementation of healthcare systems [17]. Over the past few years, healthcare researchers have primarily focused on finding ways to monitor patients remotely and transmit health reports in real-time to physicians. Researchers have identified several major challenges related to health surveillance systems. The challenges include data privacy, interoperability issues, data quality issues, and limitations associated with real-time analysis [18], [19]. Patient monitoring concerns can be classified into two categories: static and dynamic monitoring. Smart hospitals use static monitoring systems to record patients' health status periodically. Moreover, as a static monitoring system, medical staff, including doctors and nurses, manually collect patients' vital signs during specific periods. The frequency of manual data collection within hospitals varies based on factors such as physicians' workload, working hours, patients' health conditions, and hospital leadership guidance [20].

In contrast to static patient monitoring systems, dynamic patient monitoring systems can be used at home, work, or in the hospital. According to Figure 1, healthcare systems consist of identifying, locating, sensing, and connecting. H-IoT components include emergency medical services, information technology, sensors, lab-on-a-chip technologies, wearable devices, connectivity devices, big data, and cloud computing [21].

Nowadays, smartphones enable rapid task completion by monitoring and collecting regular updates on patients' healthcare data [22]. For instance, an individual can promptly receive notifications when their heart rhythm changes when they wear a wristband linked to their smartphone [23]. Furthermore, IoT allows the healthcare system to monitor and track community resources more efficiently and reliably [24]. However, H-IoT has several risks, including privacy leakage during medical data uploading [25]. The risk of patient data disclosure may considerably discourage patients from sharing their medical information because confidentiality is at risk [26]. Maintaining confidentiality and credibility in healthcare interactions are fundamental factors for addressing these risks. Moreover, resolving such security concerns will facilitate seamless deployment and adoption of H-IoT.

Over the years, several review papers have been published on the secure H-IoT [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38]. There is, however, a noticeable gap in the existing review regarding the security of H-IoT, often failing to address all necessary aspects holistically. Most of the discussions focus heavily on the technical aspects of H-IoT devices, diving deep into their specs and applications and skipping over the essential issue of data security. During the discussion of machine learning, the focus is on its potential application in healthcare instead of exploring how it can enhance security protocols, such as detecting unusual data patterns that may indicate a cybersecurity threat. Security issues related to remote patient monitoring in H-IoT have not been discussed in existing reviews either. In [39], the authors analyze the Internet of Medical Things (IoMT) security controls in a sustainable context but do not address specific issues like remote patient monitoring or the use of AI in IoMT security. In [40], IoT and AI are explored, and a smart pill bottle case study is presented; however, detailed comparisons of these technologies appear lacking, and alternative cybersecurity strategies may not be fully considered. In [41], the authors reviewed the wireless body area network-based IoT healthcare systems but did not provide a detailed exploration of real-world implementations and case studies. Furthermore, although the discussion acknowledges security and privacy concerns, it does not provide in-depth solutions or strategies to address identified challenges within IoT healthcare systems. In [42], a review of the Internet of Healthcare Things (IoHT), covers its technologies, applications, and inherent challenges, particularly security and privacy concerns. Though it explores many issues, notably privacy and security, it modestly



**FIGURE 1.** IoT based healthcare architecture.

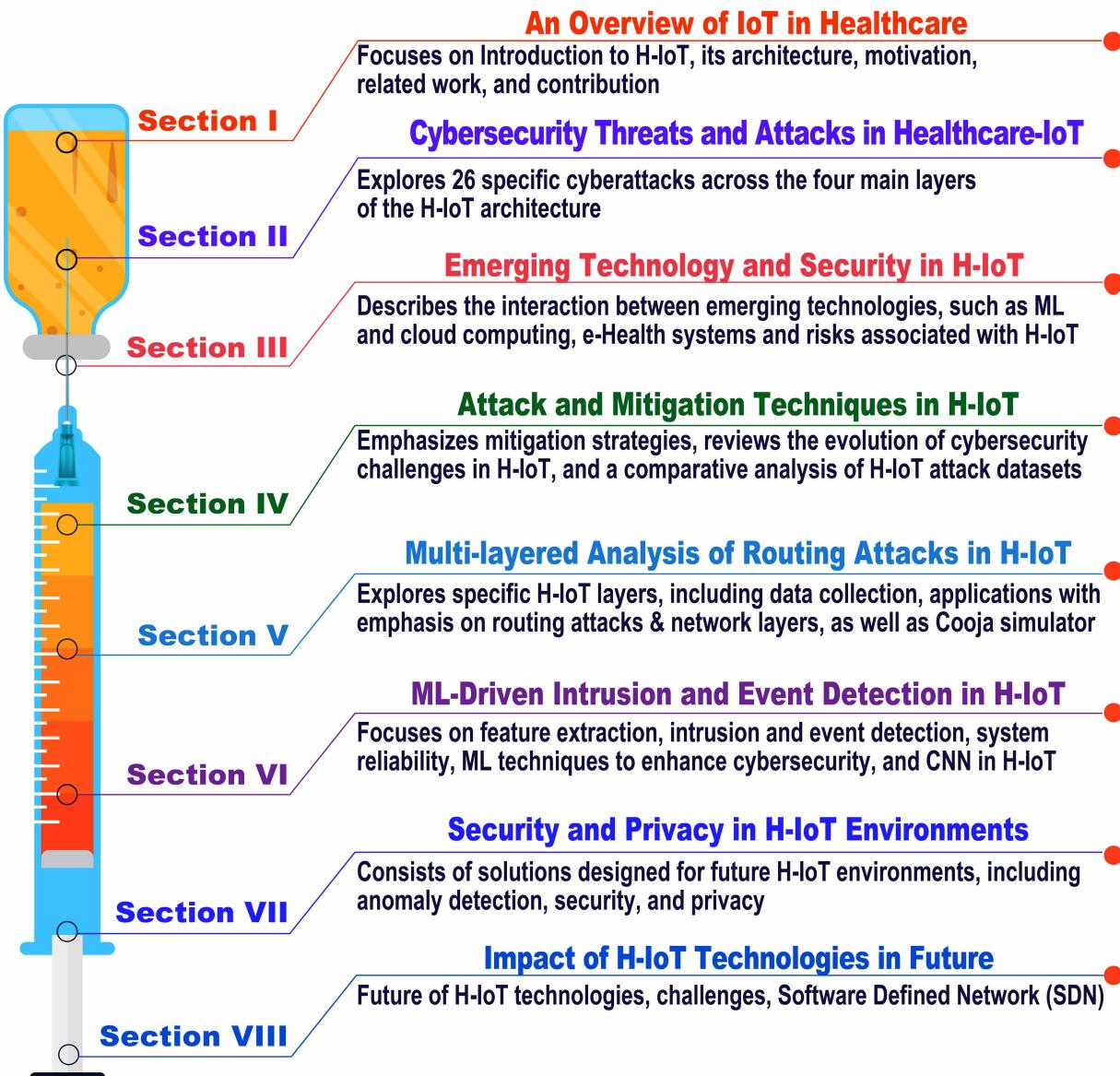
limits its explanations to practical solutions. In [43], the authors discuss the development of fifth-generation (5G) technology within the H-IoT space, including network slicing, security, and energy efficiency. Despite this, certain topics remain unresolved and require more exploration and innovation. These include data security, efficient resource management, and energy conservation. Healthcare services use large amounts of energy for heating, ventilation, and air conditioning (HVAC) [44]. HVAC systems can adjust their settings in real time using IoT sensors.

In H-IoT research, secure data access presents a pivotal challenge, particularly regarding healthcare data regulations and strict policies that protect patient identity/confidentiality. Looking at the various ransomware attacks and data breaches [45] that healthcare sectors have suffered in the past, affecting millions of patients globally, demonstrates the urgency and need to mitigate these growing cyber risks. The COOJA simulator has reshaped this complex research area, allowing researchers to emulate H-IoT device behaviors without interacting directly with sensitive data. Data collection from H-IoT devices was not discussed in previous surveys. In addition, there was a limitation on how malicious data could be collected for anomaly detection by ML. This paper reviews the security aspects of H-IoT applications, pinpoints vulnerabilities, and uses ML to suggest solutions, providing an enhanced understanding of the security issues associated with H-IoT that incorporates both practical and theoretical considerations. In addition to highlighting the mitigation of H-IoT security challenges, this review also illustrates the use of COOJA simulator tools, which allows a unique perspective to be gained that makes this survey distinctive from those previously conducted.

This paper aims to review current research on AI and ML techniques that can enhance H-IoT security, build cyber resilience within the healthcare infrastructure, and enable it to detect, protect, and respond to novel cyber threats. The paper also covers a broad spectrum of cybersecurity issues from the European Union Agency for Cybersecurity (ENISA) 2030 cyber threat landscape foresight [46] perspective, including complexities associated with IoT layers. Furthermore, this review outlines promising avenues for future research and highlights the advancements in the field. The paper highlights the following key contributions:

- Reviews key aspects of cybersecurity, big data, e-health, and cloud computing in H-IoT.
- Discusses machine learning techniques such as anomaly detection, device classification, and critical use cases for security enhancement such as intrusion detection, authentication, and access control.
- Highlights the challenges and potential solutions related to H-IoT security, along with future research directions.

Figure 2 presents the structure of this survey paper as follows: section II explains 26 different types of cyber attacks carried out across the four main layers of the H-IoT architecture, section III describes the interaction between emerging technologies, such as machine learning and cloud computing, e-Health system and also discusses the risks associated to Healthcare-IoT, section IV emphasizes risk mitigation strategies, reviews the evolution of cybersecurity challenges in healthcare over the last five years, and provides a comparative analysis of H-IoT attack datasets, section V explores specific H-IoT layers, including data collection, applications with an emphasis on routing attacks, and network layers, as well as COOJA simulator,



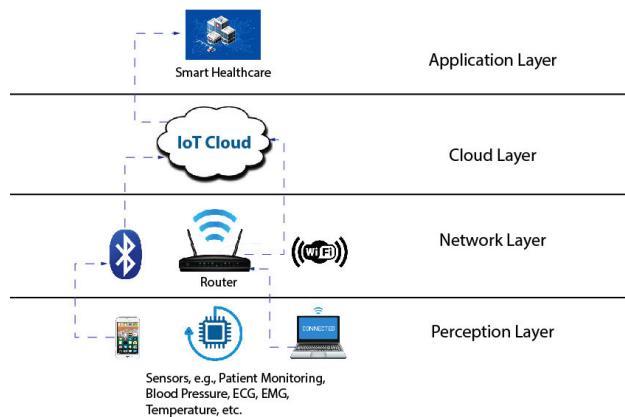
**FIGURE 2.** Structure and outline of the paper.

section VI focuses on feature extraction, intrusion and event detection, system reliability, and machine learning techniques to enhance cybersecurity, and convolutional neural network in the H-IoT, section VII consists of solutions designed for future H-IoT environments, including anomaly detection, security, and privacy, section VIII outlines the future of H-IoT technologies, software defined networks, challenges, and mitigation strategies and finally, section IX concludes the paper, exploring future directions in H-IoT security.

## II. CYBERSECURITY THREATS AND ATTACKS IN HEALTHCARE-IoT

Healthcare Internet of Things (H-IoT) requires a thorough understanding of the technical architecture, typically categorized into four layers. These layers include (I) the perception

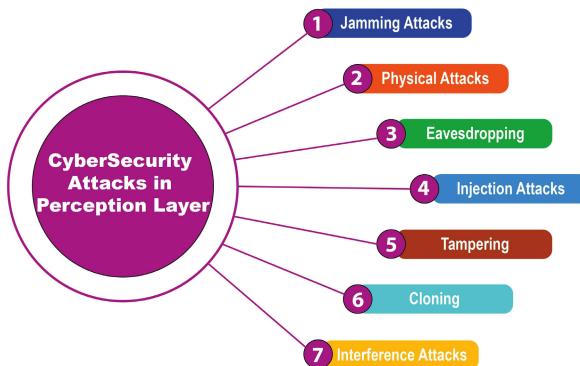
layer, (II) the network layer, (III) the cloud or processing layer, and (IV) the application layer [47]. Cybersecurity threats and attacks emerge at these layers, causing significant challenges (i.e., routing attacks, impersonating, tampering, or data transit attacks at the perception layer, denial of service and distributed denial of service (DoS/DDoS) or man-in-the-middle (MITM) attacks at the network layer, Cloud-malware injection or Brute-force attacks at the Cloud-IoT Layer and SQL injection or Cross-Site Scripting (XSS) attacks at the application layer) [48], [49], [50], [51], [52], [53], [54]. This section discusses 26 different cyberattacks and demonstrates their specific mechanisms and impact on the infrastructure. Figure 3 illustrates the details of healthcare IoT layers. It also provides a detailed explanation and insights into the most prevalent threats and attacks at different H-IoT layers.



**FIGURE 3.** The layers of H-IoT.

### 1) THE PERCEPTION LAYER

This layer can also be termed the “physical layer,” or the “sensor layer,” as it refers to the physical devices [55], [56] that serve the purpose of sensing and collecting essential information about patients, such as their medical history. IoT healthcare frameworks enable the interconnection of key stakeholders such as doctors, nurses, technicians, pharmacists, and medical devices as part of the perception layer. A specialist can monitor the data the perception layer collects in real time over the Internet. There are multiple communication protocols (i.e., Radio Frequency Identification (RFID), Bluetooth Low Energy (BLE), Wireless Sensor Networks (WSNs), Zigbee, and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)) used for collecting and transmitting data from IoT nodes [57], [58], [59], [60]. This layer is susceptible to multiple attacks affecting the infrastructure in various ways, as depicted in Figure 4.



**FIGURE 4.** Cybersecurity attacks in perception layer.

Here, we summarise each threat in this layer briefly:

- **Physical Attacks:** These attacks focus on the IoT architecture’s perception layer or physical layer consisting of hardware devices. To attack this layer, the malicious actor must remain closer to network infrastructure or gain unauthorized physical access to execute an attack [61]. These exploitations may facilitate the threat actor to tamper with implanted medical devices (i.e., Wi-Fi-enabled pacemakers and insulin pumps).

- **Eavesdropping:** IoT devices are vulnerable to eavesdropping if such attacks are executed successfully, which gives the malicious actor direct access to retrieve confidential information exchanged between the devices or radio frequency identification (RFID) tags and readers [62], [63], [64]. Eavesdropping attacks may have a variety of malicious intents, such as taking intellectual property, biometrics, and genome data for personal gain or using personally identifiable information/genetic data for espionage [65]. Such attacks have been carried out in the past [66].

- **Jamming:** The majority of wireless devices communicate with each other via radio frequency (RF) signals, which stronger signals can obstruct. In this scenario, a malicious actor may interrupt and block communications between sensors and receivers, leading to an absolute downtime and lack of availability [67], [68]. Jamming stands out as one of the most common attacks carried out at perception layer attack, alongside physical tampering, false data injection, and eavesdropping [69], [70], [71], [72], [73], [74], [75], [76]. The impact of jamming attacks in H-IoT can be catastrophic as it could disrupt on-going surgeries, medical diagnostics, access to online-systems. In short, it can lead the healthcare facility to an absolute downtime, affecting human lives. These types of cyber-attacks have an escalated impact on an infrastructure’s operational and financial aspects and the ethical/social dimensions.

- **RFID Cloning:** These attacks have emerged as a major security concern at the IoT’s perception layer as they camouflage themselves in different forms, such as RFID cloning and tag cloning. RFID cloning involves replicating and deceiving readers with duplicate tags that simulate the original to gain unauthorized access to information [77], [78]. The concept of tag cloning, however, encompasses duplicating various tag-based identification systems beyond RFID [79]. These two forms of hacking endanger the system’s integrity and increase risks related to bio-hacking [80].

- **Injection Attacks:** These attacks can occur on various IoT layers; however, at the perception layer, it is carried out by injecting malicious code and modifying the firmware of an IoT device. IoT infrastructures face the greatest challenge when a single compromised/malicious node can spread across and infect the entire network, causing complete operational disruptions [81]. As per the European Cyber Resilience Act, digital and critical infrastructures must have the ability to detect, protect, respond, mitigate cyber threats, and maintain operational resilience simultaneously [82], [83].

- **Interference:** An intruder can disrupt network communication by interrupting network traffic and constantly broadcasting radio waves [84], for spreading false information. As per the European Network and Information Security Directive (NIS2-D), the healthcare

infrastructures fall under the mandatory infrastructures to comply with the high common level of cyber security across the European jurisdiction [85]. These types of attacks can potentially spread misinformation and catalyze panic situations.

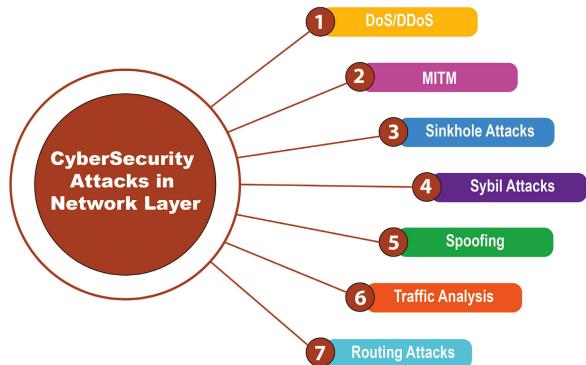
- **Tampering:** Attackers who manipulate nodes' memory to alter their functionality are called node tamperers. Furthermore, attackers may physically tamper with a device by turning it on and off, restarting it, stealing its key code, and manipulating the data [49], affecting the data integrity of the environment. Due to the misuse of generative AI, adversaries have been orchestrating and executing such attacks more frequently. As per the European General Data Protection Regulation (GDPR) [86], if any sensitive, personally identifiable information (PII) or healthcare data is breached in terms of integrity (data altered, amended, and tampered.), if so, it is considered as a data breach. An individual can suffer catastrophic consequences if their personal information is misused.

Defenses against perception-layer cyber-attacks in IoT are discussed in [87]. However, the approaches may not effectively mitigate the adversarial and escalating cyber threats due to generative AI.

## 2) THE NETWORK LAYER

Data packets are received and processed through this layer by the perception layer. Afterward, the layer transmits the made-trust data to the cloud layer immediately above it. The cloud layer's role is to store and share/build trust mechanisms between the smart devices [88], [89]. The network layer can be enabled with different wireless networks (Wi-Fi 6, 5G, Bluetooth, NB-IoT, and LTE) [90]. As part of the IEEE wireless communication standards, such as 802.11a, 802.11g, 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6), and 802.11p (for vehicular communications), orthogonal frequency division multiplexing (OFDM) is employed for the effective transmission of data across multiple frequency bands [91]. In the case of IoT devices, high-speed Wi-Fi has recently been recognized as an attractive option due to its compatibility with existing infrastructure [92]. The IEEE 802.11ax, a sixth-generation protocol popularly known as High Efficiency (HE), reports a 30% improvement in throughput over the older IEEE 802.11ac protocol known as very high throughput (VHT) [93]. A 5G-enabled energy-efficient routing protocol (EERP) that uses Wi-Fi 6 makes it easier for medical devices to communicate with one another, while multi-user, multiple input, multiple outputs (MU-MIMO) allows parallel communications [94]. A data-centric protocol prioritizes the transmission of critical health information, and content-centric networking (CCN) improves the efficiency of the distribution of healthcare information between IoT devices [95].

The vulnerability to DDoS attacks has increased dramatically with the advent of 5G. A distributed network



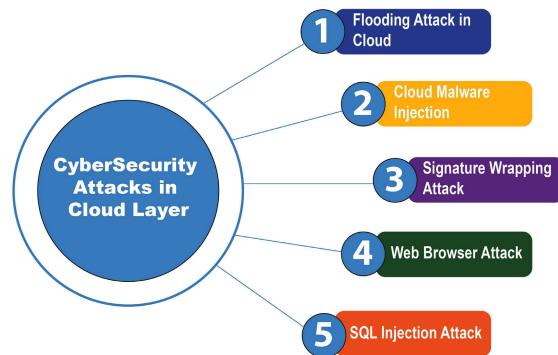
**FIGURE 5. Cybersecurity attacks in network layer.**

architecture with multiple remote edge computing sites is essential for achieving low latency, which is critical for vehicle-to-vehicle communication. Additionally, the dense network of connected devices, open-source applications, and additional access points contribute to increasing "attack surfaces". Furthermore, higher wireless speeds dramatically increase the impact of DDoS attacks on the network since each device can transmit an order of magnitude higher attack throughput to the network (at MECs and the core). As mentioned, this effect is amplified by the plurality of IoT devices, which is expected in 5G, due to the vulnerability of IoT devices to cyberattacks [96]. Figure 5 illustrates seven attacks that are most encountered at this layer. The following discussion highlights key attacks in the network layer of the IoT:

- **Dos/DDoS Attacks:** In smart ecosystems, denial of service and distributed denial of service attacks are prevalent [97]. A hacker attempts to consume legitimate network resources or bandwidth during a DoS attack. This attack is referred to as a DDoS when it originates from multiple compromised nodes [98] and falls into different categories such as traffic/fragmentation attack, bandwidth attack, and application attack) [99]. Wireless and wired networks are critical to DDoS attacks, which target the network layer [100]. Flooding the Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) with excessive data leading to delays, resource consumption, potential system crashes, and ultimately disrupting services are common methods for executing these attacks [101], [102]. These attacks would lead to absolute downtime and operational disruption.
- **Routing Attacks:** Throughout the Internet of Things, IPv6 is widely used, especially in wireless sensor networks. IPv6-centric WSNs are particularly vulnerable to routing attacks. Furthermore, WSN sensors are frequently constrained by memory limitations, narrow bandwidths, and energy consumption [48]. These attacks are generally carried out at the Internet Service Provider level, and Information and Communication

Technology (ICT) service providers must be NIS2-D compliant [103]. Detailed information about routing attacks can be found in section V-C.

- **Traffic Analysis:** Network traffic is analyzed for detecting and monitoring malicious behavior and anomalies. Depending on the network traffic, routers manage data packets. Each router is equipped with a certain amount of capacity. Clogging or unusually high traffic may indicate traffic analysis or even a denial-of-service attack [104]. Malicious actors sometimes observe the traffic for guessing passwords by analyzing the packets sent during each keystroke and assessing the duration between them. By using such a pattern, they can reconstruct the users' passwords.
- **Spoofing Attacks:** Several types of spoofing are possible, such as email, uniform resource locator (URL), and frame spoofing. However, MAC or IP address spoofing is most widespread [105]. IoT uses the MAC address to authenticate wireless networks at the data link layer. Spoofing attacks occur when malicious entities imitate legitimate users' MAC addresses to gain network access illegally, affecting the data confidentiality and integrity of the environment [106]. Lack of data confidentiality means unauthorized/malicious actors may know the contents of data, whereas lack of integrity means the data may have been amended, altered, tampered or discarded. As per GDPR, a lack of security (Confidentiality, Integrity, and availability) metrics and controls is considered a GDPR breach.
- **Sybil Attacks:** IoT devices are vulnerable to the Sybil attack [107], [108]. In this attack, legitimate nodes are impersonated by malware to redirect traffic towards malicious ones. An individual node can appear in multiple locations simultaneously or impersonate several others [109]. During this attack, a malicious node claims to have multiple identities. Due to their ability to control the flow of information within a network, these types of attacks affect data integrity and resource allocation.
- **Sinkhole Attacks:** In sinkhole attacks, the attacker redirected or discarded traffic, preventing the base station from receiving full data transmission. This attack spreads misleading routing details from one node to another, resulting in energy drain and reduced network durability. Energy depletion is particularly damaging to wireless sensor networks [110]. These types of attacks affect the integrity, availability, and reliability of data in a network.
- **Man-in-the-Middle (MITM) Attacks:** Man-in-the-middle attacks involve intercepting communications between two devices by an attacker [51]. The main target of MITM attacks is the confidential details of users [53]. Malicious actors exploit existing or new vulnerabilities in IoT systems to carry out this attack. An example would be a temperature reading of a sensor



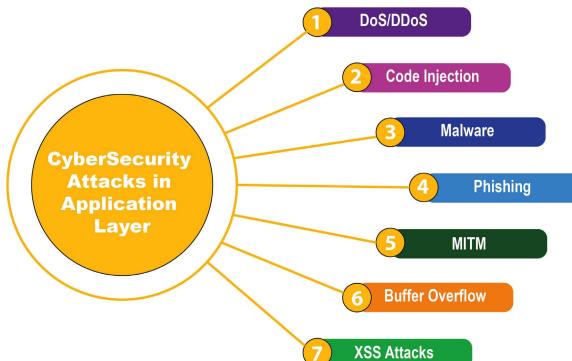
**FIGURE 6. Cybersecurity attacks in cloud layer.**

or malfunctioning of a device enabling hackers to steal sensitive information [111].

### 3) THE CLOUD LAYER

The cloud allows for convenient and secure backup and preservation of confidential health information, and sharing between authorized parties (such as doctors, insurance providers, medical staff, and pharmacies) is convenient. Similarly, independent and public healthcare providers can maintain confidential data online and share it with trusted colleagues to improve the quality of treatment. These protocols include transmission control protocol (TCP), user datagram protocol (UDP) [112], and protocols for data analysis, prediction, and machine learning [113]. Figure 6 depicts several attacks related to cloud layers. These specific vulnerabilities are explained in the following sections:

- **Flooding Attacks:** Flooding attacks are a type of DDoS attack that disrupt services by overloading the servers with enormous traffic from compromised computers. During these attacks, excessive messages are sent to servers, which causes legitimate users to be denied access to the Internet [114]. In the cloud environment, attackers often rely on sophisticated methods to exploit its inherent scalability and flexibility [115].
- **Web Browser Attacks:** Throughout the modern digital era, web browsers have become integral tools that allow users to access various online services and connect to the vast internet. Nowadays, browsers are a crucial component of almost every computer. Nevertheless, browsers are not immune from vulnerabilities [116], [117]. As a result of these vulnerabilities, attackers often gain access to a victim's computer, steal PII, corrupt files, or use the hacked machine to attack others, potentially becoming a part of a botnet [118].
- **Signature Wrapping Attacks:** Cloud infrastructure attacks may provide attackers with root-level access to systems without targeting the cloud environment directly [119]. The authentication systems of cloud interfaces are vulnerable to advanced cross-site scripting methods and signature wrapping [120]. In addition to



**FIGURE 7.** Cybersecurity attacks in application layer.

manipulating virtual machine operations and password resets, signature-wrapping attacks are also known as XML signature-wrapping attacks [121]. In contrast, attackers can steal login credentials by exploiting the XSS vulnerability [122].

- **Cloud Malware Injection Attacks:** Attackers perform malware injections by inserting malicious code or services into a network, appearing as if these components were legitimate components already present [54]. As a result of this attack, users are often deceived into downloading software or opening malicious emails. This type of attack is sometimes driven by downloading or meta-data spoofing. An attacker may trick users into downloading harmful software by creating a deceptive environment. In the aftermath of such an attack, users may have limited access to their systems, while attackers may be able to execute malicious activities in the cloud and gain unauthorized control [123].

- **Structured Query Language (SQL) Injection Attacks:** Cloud computing often exposes web services to various security threats due to their inherent Internet accessibility. SQL injection is one of the most widespread risks [52]. By manipulating SQL queries, SQL injection attacks can achieve malicious objectives. Consequently, sensitive data may be modified unauthorized, confidential details may be accessed, or the server may crash due to such manipulation [124].

#### 4) APPLICATION LAYER

Within the IoT architecture, the application layer resides at the top level. This layer provides the user interface, which includes services such as healthcare, smart homes, and connected cars [125], [126]. It recognizes spam and filters out the malicious content [127].

Figure 7 illustrates IoT applications' primary security attacks. The following sections delve into the application layer vulnerabilities:

- **DoS/DDoS Attacks:** DDoS attacks are carried out by a group of compromised computers operating from

multiple locations that flood a particular target with traffic. In this attack, the primary goal is to overwhelm and render unavailable a server, website, or online service [128], [129]. In a DDoS attack, IoT devices such as smart appliances, healthcare monitors, and industrial sensors can be rendered useless [130]. In addition to affecting their immediate functionality, disruptions can jeopardize critical operations they oversee, like monitoring patient health or maintaining optimal building conditions [131].

- **Phishing Attacks:** Phishers can use compromised devices such as smartphones, appliances, and smart cars to conduct phishing attacks at the application layer. Through this method, attackers impersonate legitimate devices and send messages that appear to be authentic. A malicious attacker can then manipulate or obtain credentials to authenticate or identify, which can be used for criminal purposes [132]. For example, the Irish HSE Conti Cyber attack [133], which was initially a phishing attack, soon escalated to a ransomware attack after an employee accidentally clicked on the malicious email, disrupting the healthcare facility operations and IT outages across the country for days. However, it took four months for the Irish HSE to recover from the aftermath completely. This is why it is mandatory to build cyber resilience within such infrastructures.

- **Buffer Overflow Attacks:** Buffers hold data while it is transferred from one location to another. In buffer overflows, data exceeds the buffer's storage capacity. As a result, the application may crash, memory access errors may occur, and results may be incorrect. Memory overwrite vulnerabilities can be exploited by attackers. It can affect execution paths, leak confidential information, and corrupt files [134]. Legacy systems are most vulnerable to these attacks as they have limited memory [1].

- **Malware:** A malware attack attempts to use a malicious program to commit an offense with IoT applications, and recently, many malicious programs have been released to attack IoT devices, including rootkits, spyware, and adware [135], [136]. In [1] and [137], the authors outline different types of malware and their impact on the national security (i.e., Red October), social (transportation, communications, energy, and water sectors), financial (BaFin) [138] and economic domains (manufacturing, fintech) affecting human lives [139].

- **Cross-site Scripting (XSS) Attacks:** In cross-site scripting attacks, harmful code is embedded into an authentic and trusted website [140]. An attacker can alter the content of an application through this potentially dangerous intrusion [141]. Due to the inability of the targeted browser to distinguish between genuine and malicious code, the infected code is executed. Consequently, this malicious code can access cookies,

session identifiers, or other confidential information. In addition, the attacker can control the device directly, sending users to malicious websites or causing direct damage to the device.

- **Unauthorised Scripts Attacks:** These attacks occur when unwanted or malicious scripts are executed without the user's consent. In contrast to XSS attacks, which target the user's browser, unauthorized scripts can run anywhere in the system or application. Data breaches, system malfunctions, or other vulnerabilities may result from this [142].
- **Code Injection Attacks:** Code injection attacks that use SQL injection break the data-code isolation rule by inserting malicious SQL codes into input fields [50]. Attackers can embed these malicious SQL commands in web forms, URLs, or page requests. Without proper filters, a web application may process these harmful commands incorrectly. As a result, unwanted access to the database can occur [143].

### III. EMERGING TECHNOLOGY AND SECURITY IN H-IoT

Technological advancements, including the IoT, machine learning, and cloud computing, are gradually reshaping healthcare. This development creates innovative healthcare solutions but also challenges, particularly when it comes to data security. AI and machine learning have made great progress in cyber security domains such as intrusion detection and malware mitigation [144]. This section explores the conjunction of machine learning and cloud technologies, investigating emerging trends and attendant security considerations within e-health applications to establish a secure and innovative framework for H-IoT implementations. This section further explores the connections between machine learning and cloud technologies within e-health, navigating through emerging trends and assessing related security concerns. Deep learning (DL) and machine learning are increasingly integral to mitigating cyber threats; however, how these technologies impact e-health is a crucial issue [145]. This section aims to provide a secure and innovative foundation for H-IoT implementations.

#### A. MACHINE LEARNING WITH CLOUD COMPUTING

Researchers all over the world have applied machine learning to a variety of applications and domains [146]. Recently, ML has drawn the attention of H-IoT researchers [147]. In the context of H-IoT, machine learning is beneficial for remote monitoring and real-time treatment of diseases [19], [148]. ML algorithms such as Support Vector Machines (SVMs), decision trees, random forests, and Artificial Neural Networks (ANNs) can analyze huge volumes of medical data collected by healthcare-related smart devices, including vital signs and medical histories [149]. In this process, ML techniques are applied to analyze massive datasets to find patterns and generate insights that may assist clinical decisions, improve patient outcomes, and reduce healthcare

expenditures. Cloud computing, however, provides computing power and storage resources for H-IoT to support machine learning based on big data collected from IoT devices [150]. ML algorithms utilize the cloud to process and analyze data and provide a secure and scalable computing environment [151].

Desai et al. [152] developed a Health-Cloud platform using machine learning and cloud computing to track patients suffering from heart-related diseases. Moreover, the researchers built a live data analysis iOS App using Google Cloud Firebase.

Abdelaziz et al. [153] investigate the use of IoT and cloud computing in healthcare to predict chronic kidney illness in a city of the future. IoT devices transmit chronic kidney disease (CKD) data to cloud storage, improving prediction accuracy. The hybrid model, which combines linear regression and neural networks, predicts CKD with 97.8% accuracy. Cloud IoT offers tremendous potential in healthcare services, benefiting patients and smart city stakeholders.

#### B. ELECTRONIC-HEALTH (E-HEALTH) SYSTEMS

The exchange of health records between doctors and patients is now conducted largely electronically, using technology to transfer patient data efficiently and facilitate communications between doctors and their patients. As illustrated in Figure 8, e-health application systems can solve several problems associated with traditional healthcare systems, including online appointments, medical evidence, information technology, communication, e-prescribing, medical history, reminders, payment management, and lab analysis. e-healthcare services can enhance patient data and health information management [154]. As a result, patients can access their medical records online, receive remote consultations, and use mobile health applications to manage their health, which increases accessibility and empowers patients.

Maksimović and Vujović [155] describe the gradual adoption of e-health platforms primarily due to infrastructure and political restrictions. Despite these challenges, e-health and IoT convergence is progressing. However, there are hurdles like consistency, security, and interoperability in IoT integration. Privacy concerns and regulations further complicate the adoption of large-scale technologies. The paper highlights the influence of IoT in e-health and outlines these crucial challenges, emphasizing the importance of overcoming barriers to implementation. Zhang et al. [156] explore how 5G technology can revolutionize e-health. While 5G promises reliable access to e-health, current efforts are insufficient. This paper also discusses technological aspects, practical use cases, research trends, and challenges in advancing 5G e-health.

#### C. BIG DATA IN HEALTHCARE-IoT

IoT networks generate enormous amounts of data at every moment. Therefore, manipulating so many datasets

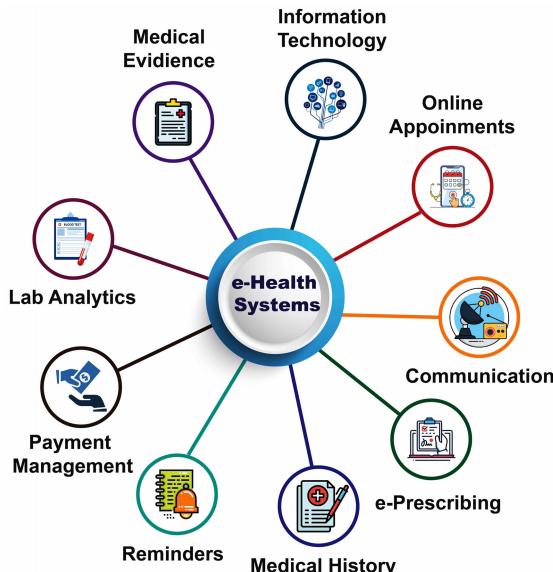


FIGURE 8. e-Health systems.

requires considerable technical expertise. IoT architecture and machine learning techniques boost big data capacity, and advanced deep learning models are essential [157]. Smart healthcare systems have dynamically transformed mathematical modeling with data collection using big data analytics. Besides collecting and storing data, big data is also about empowering machines to think and act like humans to simplify complex tasks [158], [159]. Wearable sensors continuously collect data, such as sleep patterns, exercise levels, walking distances, heart rates, etc. The latest IoT sensors can also monitor heart rate, blood sugar levels, and pulse. A major benefit of big data for the medical industry is that it could reduce the costs of accommodations, travel time, and transportation delays. In addition, big data analytics have improved healthcare facilities and enabled patients to recover at home [160]. H-IoT devices can also decrease medical expenses by reducing personnel and transport costs with big data [161], [162].

Asri and Jarir [163] developed a real-time disease prediction platform that enhances patient care and reduces healthcare costs with a Big Data platform. It helps users make better decisions in real-time, improving health and safety. Heart attacks, obesity, and miscarriages can be detected using this approach. Long-term treatment and hospitalization costs can be reduced by early detection and accurate prediction of health problems.

Sasubilli and Kumar [164] utilize machine learning and big data to analyze the use of electronic health record applications in neuro- and cardiac-related fields. Integrating machine learning approaches and big data frameworks in healthcare architecture enhances data management while improving patient care. Advanced technologies enable more precise diagnostics, personalized treatment plans, and better outcomes, elevating patient care standards.

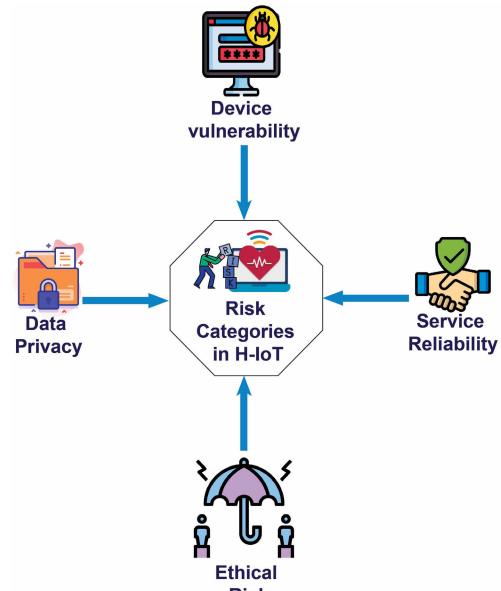


FIGURE 9. Risk categories in H-IoT.

#### D. RISK CATEGORIES IN HEALTHCARE-IoT

H-IoT brings multiple risks associated with medical devices integrated with advanced technologies. Data privacy, device vulnerability, service reliability, and ethical issues are all included in these risks. Both security and user trust depend on addressing these issues.

As depicted in Figure 9, these risk categories apply to the H-IoT industry. The following sections discuss each risk category and its impact within the context of H-IoT:

- Data Privacy Risk:** During the COVID-19 pandemic, several countries reduced their data privacy guidelines as part of their emergency response [165]. Per the EU General Data Protection Regulation, implementing data security, governance, risk, and control metrics has been mandatory since the regulation was enacted in 2018; the regulation also enabled and improved the cyber security posture of organizations working across Europe in comparison to other countries/jurisdictions, and this is why Europe suffered lesser data breaches in comparison to the rest of the world. In the context of digitally enabled precision healthcare 5.0, securing systems and enforcing strong data controls are essential to mitigate risks associated with emerging technologies [166]; this would mean enabling end-to-end data (data-in-use, data-in-transit, and data-in-store) security, encrypting, anonymizing and pseudonymizing it, to mitigate the risks of data breach. Whenever adversaries can steal data that has been encrypted, anonymized, and pseudonymized, the data will have no value to the hackers [137].

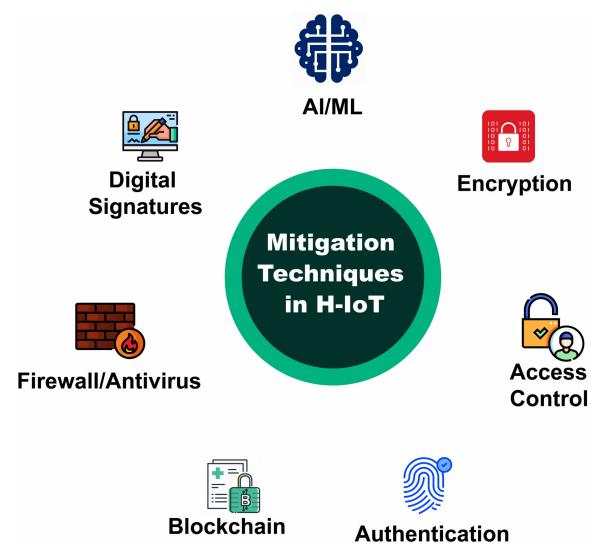
- Device Vulnerability Risk:** IoT has many security vulnerabilities, especially in the H-IoT space, because these devices would be manufactured by different suppliers who would not have considered security

by design and privacy-by-design metrics, leading to unencrypted network services, inadequate password protocols, and user interface credentials. These issues have been identified as serious security lapses in 70% of H-IoT devices [167]. In addition, 90% of these devices collect personal data [168], illustrating the complexity and diversity of this issue. Healthcare sectors worldwide are particularly vulnerable to cyber threats due to their diverse operating environments and intricate regulatory frameworks. However, ENISA has passed new cybersecurity standards and regulations to combat supply chain, digital services, digital market, and third-party risks [137].

- **Service Reliability Risk:** In H-IoT, service reliability risks refer to service interruptions or failures, which can cause critical delays or data loss. This is a major concern for emergency response and ongoing health monitoring. H-IoT services require effective interference mitigation and optimization of 5G networks. To fully benefit from 5G and IoT, these steps will enhance reliability and efficiency [169]. With 5G and Beyond 5G (B5G) deployment, service interruptions, data loss, and seamless communications between multiple devices will be prevented in H-IoT or the Internet of Medical Things [170]. The ability to transmit real-time, accurate patient data to medical personnel through 5G and B5G is especially crucial in medical emergencies [171].
- **Ethical Risk:** A potential ethical risk associated with IoT devices is that of unethical actions [172]. There is an example from the automotive industry that serves as a cautionary tale, even though it isn't directly related to H-IoT. In violation of the Clean Air Act, Volkswagen developed and installed software to manipulate diesel emissions tests [173]. Reputational and financial damages resulted from this breach of ethics. When it comes to H-IoT, where patients' health and well-being are at risk, cyber ethical breaches such as harm to privacy, harm to property, and misuse of technical resources [137] can be detrimental [174].

#### IV. ATTACK AND MITIGATION TECHNIQUES IN H-IoT

With cutting-edge technologies in the healthcare industry, the security and privacy risks have drastically increased [137]. As per [175], in 2022, more than 200 cyber attacks were carried out across healthcare organizations in the world daily by malicious actors, impacting millions of people worldwide. The number of cyber attacks on H-IoT increased by an alarming 74% in 2023 [176]. Demystifying cyber threats and attack scenarios is crucial to preventing these escalating risks. Therefore, this section explores the cybersecurity landscape of H-IoT. Table 1 surveys cybersecurity challenges within the healthcare sector over the last five years. Furthermore, this section discusses attack datasets for detecting and mitigating anomalies in H-IoT environments and threats, potential impacts, and mitigation strategies.



**FIGURE 10. Mitigation techniques in H-IoT.**

#### A. MITIGATION TECHNIQUES

This section presents findings on mitigation strategies employed in prior research to mitigate cyber security threats associated with IoT in healthcare. Figure 10 illustrates the mitigation techniques for access control, encryption, authentication, AI/ML, blockchain, digital signatures, and firewalls/antivirus. H-IoT solutions also integrate modern AI and deep learning technologies. For instance, Al-Garadi et al. [177] described that machine learning models have been incorporated into security solutions to identify vulnerabilities and attack surfaces. Qiu et al. [178] explore the integration of healthcare and smart cities, enhancing health practices in countries worldwide. Blockchain technology addresses this integration's security concerns, ensuring the confidentiality of patient data. The authors discussed the benefits and drawbacks of each model used in the research at different IoT layers.

#### B. COMPARATIVE REVIEW OF H-IoT ATTACK DATASETS

Datasets are crucial in identifying and mitigating anomalies in the ever-expanding world of the IoT in healthcare, industry, and general applications. H-IoT attack datasets are reviewed in this subsection, including simulations and real-world data from H-IoT sensors. In the constantly evolving area of H-IoT, these datasets serve as essential tools for research [179]. Similarly, machine learning applications require high-quality healthcare data, and exact labeling improves its accuracy [180], [181], [182]. Table 2 provides a detailed overview of datasets, attacks, mitigation techniques, benefits, and limitations.

#### V. MULTI-LAYERED ANALYSIS OF ROUTING ATTACKS IN H-IoT

This section focuses on routing attacks in the H-IoT domain, reviewing key components sequentially. The first step is to

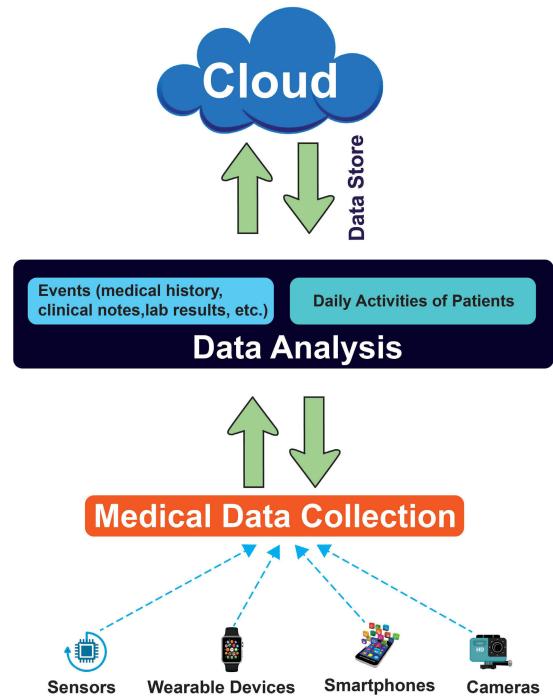
**TABLE 1.** Cybersecurity challenges in H-IoT.

Key Publications	Area	Security and Privacy Issues
Garcia-Perez et al. [183] (2023)	H-IoT	The paper highlights the lack of cyber risk awareness, management, and security risks related to emerging technologies.
Cartwright et al. [184] (2023)	IoMT, COVID-19	Security gaps in protected health information (PHI), IoMT challenges, COVID-19 amplification, and funding shortages.
Javaid et al. [185] (2023)	H-IoT	Data security risks identified in the paper include ransomware attacks, unauthorized access to patient information, device vulnerabilities, and healthcare data source complexity.
Kumar et al. [186] (2023)	H-IoT	H-IoT devices face various security threats and scalability and latency challenges.
Sharma et al. [187] (2023)	DL, Cyber-attacks, Intrusion Detection System (IDS), Healthcare	A Deep Learning-based IDS detecting cyberattacks achieves 84% accuracy, increasing to 91% with Generative Adversarial Networks(GANs) balanced data.
Khatkar et al. [188] (2023)	DL, Intrusion Detection, Healthcare	For intrusion detection in healthcare, evaluating a DL-based Long Short-Term Memory (LSTM) algorithm against a Decision Tree, SVM, K-nearest neighbors (KNN).
Ksibi et al. [189] (2023)	IoMT, Cybersecurity, ML, Risk Assessment	Analyzes the security risks in the Internet of Medical Things (IoMT) using ML algorithms for anomaly detection and introducing of a new model of risk assessment.
Bouabida et al. [190] (2022)	Pandemic-driven, patient data risks	A significant concern raised by the COVID-19 crisis is the security and confidentiality of patient data.
Wang et al. [191] (2019)	Big Data, H-IoT	An Analysis of Big Data Analytics in healthcare is presented, including its advantages and challenges.
Coventry et al. [192] (2018)	Cybersecurity in Healthcare	Due to cybercrime risks, healthcare technology needs a holistic security program.

discuss the vital process of collecting health-related data in the layer for medical data collection. After collecting raw medical data, the medical application layer transforms it into meaningful healthcare services. Next, this section discusses the role and vulnerabilities of the routing and network layers in the context of routing attacks. The next step is emphasizing that the medical application layer is crucial to translating data into actionable insights. In addition, this section discusses the role of the COOJA simulator in collecting data and generating datasets in the H-IoT environment.

#### A. MEDICAL DATA COLLECTION LAYER

Healthcare data is collected by smart healthcare sensors, such as devices for tracking brain activity and blood pressure.

**FIGURE 11.** Data collection layers in healthcare.

A doctor can track the progress of an elderly patient by using IoT devices that record every detail and activity. Staff members and nurses who care for elderly patients receive information. H-IoT integrates healthcare devices at home for disabilities. Therefore, the doctor may follow and monitor patients' cases at times. Despite this, the data generated and collected are susceptible to various threats. As a result of the attacks, hackers can gain complete command and control (C&C), disrupting the devices [1]. These attacks can drain sensors' power, causing them to fail or run afoul of the entire IoT network in the healthcare industry. Medical data collection includes collecting, analyzing, and monitoring data, as shown in Figure 11.

As a starting point, several types of devices are used for collecting data within the medical data collection layer. These devices include sensors, cell phones, wearable devices, and cameras, among other things. The second phase involves data analysis, which analyzes every event and activity of an elderly patient. A secure server then processes and stores the data. Monitoring healthcare data remotely and automatically recording it includes a patient's medical history and status [201].

#### B. MEDICAL APPLICATION LAYER

The traditional application layer in IoT environments handles data processing, storage, and user interfaces. On the other hand, the medical application layer is uniquely designed for handling healthcare-related applications, data, and services, ensuring it follows the highest regulations following the EU General Data Protection Regulation (GDPR) or Health

**TABLE 2.** Comparative analysis of techniques and targeted attacks in published research.

Reference	Techniques Used	Targeted Attacks	Key Benefits	Limitations	Dataset Employed
Wagan et al. [193] (2023)	Dynamic Fuzzy C-Means clustering, Customized Bi-LSTM technique.	Botnet-based DDoS, Zero-day network attacks.	- Separates attacks from regular IoMT data. - Securely handles medical data. - Analyzes attack patterns in IoMT.	- Inequity in the model. - Model decisions are not comprehensible. - Possibility of corruption of data.	WUSTL-EHMS-2020 is a heart disease dataset with 36 attributes and 18940 instances developed with the Enhanced Healthcare Monitoring System (EHMS).
Thulasi et al. [194] (2023)	Multi Step Convolutional neural network Stacked Long short term memory architecture (MSCSL), light spectrum optimizer (LSO) for optimizing MSCSL's hyperparameters.	Port scans, Brute force, DoS attacks.	- Data adaptability improved. - Reduced computational complexity. - High precision and accuracy.	- Privacy issues are not addressed. - Not optimized for multi-cloud/fog-based dynamic environments with multiple devices.	Supervisory Control and Data Acquisition International Electrotechnical Commission (SCADA IEC 60870-5-104) datasets.
Gupta et al. [195] (2022)	Tree classifier-based network intrusion detection model.	Man in the Middle Attack (Data Alteration and Data Spoofing).	- Reduced input data dimension effectively. - Accelerates anomaly detection.	- The dataset only consists of data alterations and data spoofing attacks. - Tested on a restricted network. - Difficulties in formulating IoMT security design.	A combined network flow and biometrics dataset by [196]
Saif et al. [197] (2022)	Hybrid Intelligent Intrusion Detection System (HIIDS), known-nearest Neighbor (kNN) and decision tree (DT), Hybrid approach for feature selection and classification.	Cyber-attacks such as Ipsweep, Portsweep, Smurf, and Brute Force target cloud servers containing Electronic Health Records (EHR).	- Malicious traffic detection and prevention in H-IoT applications. - Metaheuristic algorithms for feature selection reduced computation costs. - Hybrid approach improves intrusion detection accuracy.	- Uncertain performance under high-traffic or larger datasets. - The comparison is limited to Decision Tree and kNN models. There are several ML algorithms, and some are preferable for particular types of data or threats than others.	The NSL-kDD dataset contains 41 features with 125,973 samples.
Ray et al. [198] (2022)	A novel DDoS detection algorithm, DDoS preventive algorithms.	Distributed Denial of Services (DDoS) attack.	- Effectively detect DDoS attacks. - A system that restricts access to attackers.	- Other DDoS attacks may not be suitable for this approach. - The system may become complex if nodes do not filter false data.	Cloud-based simulated dataset.
Kumar et al. [199] (2022)	A fuzzy min-max neural network (FMMNN) based on fuzzy sets, Supervised algorithm for classification.	DoS, Remote to Local (R2L), User to Root (U2R).	- Nonlinear class boundaries can be learned in one pass. - Detects intrusions more effectively. - Reduced error rate.	- The training time of the FMMNN algorithm needs to be optimized.	NSL-KDD dataset.
RM et al. [200] (2020)	ML algorithms (Supervised & unsupervised), Deep Neural Network (DNN).	Replay, Man-in-the-middle, Impersonation, Privileged-insider, Remote hijacking, Password guessing, DoS attacks, Malware attacks.	- Classification & detection (network/host). - Detects anomalies reliably. - DNN compared to other ML algorithms.	- Unpredictable attacks. - Scalability issues. - Network behavior changes rapidly. - Evolving attacks quickly.	Kaggle benchmark dataset for intrusion detection.

Insurance Portability and Accountability Act (HIPAA) [86], [202] while processing United States healthcare data. This layer presents unique challenges and complexities. For

example, electronic health records (EHRs) for patient data, remote consultation platforms, real-time monitoring systems, medical resources, medical care, and diagnosis personnel.

Moreover, the medical application layer processes organizes, and maintains medical records. This layer ensures that patients' data is authentic, secure, private, and reliable when transmitted over the communication system [203]. Numerous application layer protocols exist, including Message Queuing Telemetry Transport (MQTT), Hypertext Transfer Protocol (HTPP), WebSockets, RESTful, Secure-MQTT, and Constrained Application Protocol (CoAP) [204]. Choosing the appropriate protocol for H-IoT depends on its application [205].

### C. ROUTING ATTACK AND NETWORK LAYER

The network layer defines paths for the routing of data over the network. It has been demonstrated that low-power wireless networks with multiple hops are susceptible to a wide range of attacks, with routing attacks emerging as one of the most significant threats in the H-IoT environment [206]. There are many routing attacks, including selective forwarding attacks and replay attacks [207]. In the selective forwarding attack, control packets are deliberately forwarded within the Routing Protocol for Low-Power and Lossy Networks (RPL) while data packets are dropped. In conjunction with sinkhole attacks, this strategy can disrupt established routing paths and lead to severe consequences for the network [208]. A replay attack entails capturing and re-transmitting packets captured from nearby nodes by an unauthorized node or attacker [209]. The purpose of these attacks is to manipulate or obstruct the transmission of data packets to impair the integrity of the network [210]. Furthermore, rank and wormhole attacks are susceptible to IoT routing protocols due to their lightweight nature and limited computational resources. Using these attacks, IoT infrastructures can be devastated by attacks targeting control messages and resources [211].

Routing and network layers receive data sent by medical data collection layers. These layers use protocols such as Wi-Fi 6, Narrowband Internet of Things (NB-IoT), Bluetooth, IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPAN), RPL, WiMAX, ZigBee, Sigfox, LoRa, and 5G NR (New Radio) to transmit data to the medical application layer [212], [213], [214]. This setup requires the analysis of routing attacks, potentially compromising confidentiality and accessibility of medical data. To ensure reliable and secure data transmission, protocol configurations designed for power-efficient and unstable networks should be carefully reviewed for vulnerability to various routing attacks [215]. Following the discussion of routing attacks and network layers, this section explores the use of machine learning to detect such cyber attacks in H-IoT environments.

As highlighted by [216], H-IoT networks are vulnerable to routing attacks, such as sinkholes and wormholes. The authors have introduced various ways to detect such attacks. As a result of the limited resources of devices used in H-IoT, intrusion detection systems cannot be used. The proposed method efficiently detected and handled network attacks

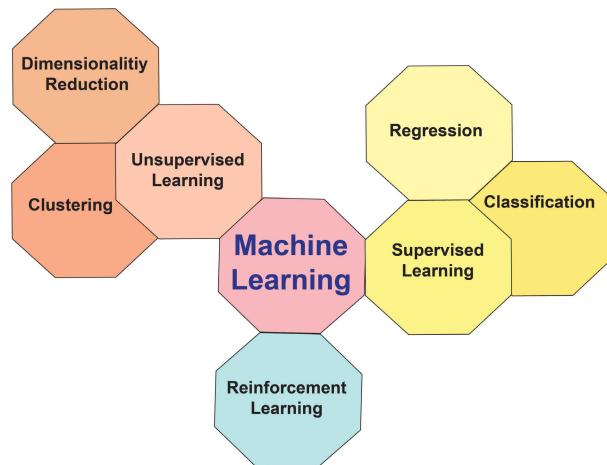
using machine learning and deep learning while considering device limitations.

According to [217], especially in e-health applications, protecting sensitive patient data from routing attacks and security threats is pivotal in 5G-IoT. Cloud-based e-health data is at risk of various cyber-threats (i.e., ransomware, loss of privacy, and digital identity fraud) and attacks mentioned in section II. CNN-DMA is a deep learning model that detects malware attacks using a Convolutions Neural Network (CNN). The e-health apps enabled with 5G-IoT and deep learning models such as CNN-DMA are useful for ensuring data safety and system security against cyber-attacks. The deep learning models can be trained directly from original data, such as images and text [218]. Therefore, raw data does not need to be preprocessed before being used for training. Moreover, deep learning algorithms enable the seamless execution of security protocols without consuming significant computing resources, which is one of the major benefits of 5G cybersecurity [219].

In light of the delicate nature of healthcare data, enhancing security within H-IoT's network layers is imperative. The examples show that leveraging machine learning and deep learning can neutralize and mitigate these risks. Following this sub-section, the discussion will focus on the COOJA simulator, a useful tool for studying and understanding these attacks in a simulated IoT environment to help develop secure network protocols.

### D. COOJA SIMULATOR

The COOJA simulator runs on Contiki OS, a portable operating system with limited resources designed specifically for devices such as sensor nodes [220]. It is built upon an event-driven kernel while also supporting multi-threading. It supports a complete TCP/IP stack through IP and programming protothreads. Simulating sensor nodes based on their real characteristics is the main advantage of the COOJA simulator. The process executes program code from ContikiOS and TinyOS using Java Native Interface (JNI). A Java Virtual Machine and C programming (a programming language commonly used in firmware sensor nodes) are interconnected by the JNI. As a result, COOJA can provide accurate simulations of sensor nodes or devices across multiple platforms, including H-IoT, closely replicating real-world functionality. Moreover, it is crucial to note that the primary objectives of COOJA are extensibility and plug-in support. In contrast to the interface, the plug-in allows users to interact with the simulator. Plug-ins, for example, enable users to control simulation speeds or observe network traffic between nodes [221]. COOJA also has several inherent tools, including the "radio logger," which records all packets dispatched by nodes in the simulation and associates them with a universal timestamp [30]. As a versatile simulation tool, COOJA allows for research across diverse environments by generating and collecting data to thoroughly assess wireless sensor networks and body area networks (WBANs)



**FIGURE 12.** Machine learning techniques for H-IoT cybersecurity.

in the H-IoT domain. Using emulated H-IoT devices, the COOJA simulation can even construct attack scenarios to uncover cybersecurity vulnerabilities within H-IoT networks.

Hence, machine learning and deep learning techniques have been explored to prevent routing attacks on H-IoT networks. By reviewing examples, it becomes apparent that artificial intelligence models significantly defend against routing attacks in 5G-IoT e-health. COOJA has also been demonstrated to collect data from H-IoT devices.

## VI. MACHINE LEARNING-DRIVEN INTRUSION AND EVENT DETECTION IN HEALTHCARE-IoT

To ensure data security within the healthcare Internet of Things, it is necessary to explore a variety of strategic mechanisms. The section endeavors to illustrate the pivotal role of machine learning in establishing and reinforcing robust security protocols in healthcare, generalized ML techniques, and exploring potential cybersecurity applications. Following this, the discussion discusses how feature extraction is essential to identifying threats accurately and mitigating risks. Afterward, intrusion and event detection systems designed for healthcare environments will be offered, emphasizing mechanisms for identifying potential breaches. A discourse on the reliability of H-IoT systems is required to achieve consistent and reliable risk mitigation. The last topic of this section is the potential and challenges associated with convolutional neural networks (CNNs) in the context of IoT security.

### A. MACHINE LEARNING TECHNIQUES IN H-IoT CYBERSECURITY

The machine learning method involves using data and algorithms to create models replicating human learning processes. ML algorithms can be refined and optimized by improving an algorithm's loss function [222]. As depicted in Figure 12, ML is traditionally classified into three categories: supervised, unsupervised, and reinforcement learning [223], [224].

Over the past several years, machine learning techniques have been successfully applied to a diverse spectrum of

cybersecurity challenges [225]. In the specialized domain of H-IoT cybersecurity, these techniques have emerged as key assets, significantly enhancing the security level of healthcare devices and systems [226]. As illustrated in Figure 13, several potential use cases are encompassed, including intrusion detection and prevention system, classification of H-IoT devices, anomaly detection and prevention, H-IoT attacks classification, zero-day attack detection, predictive analytics for threat anticipation, identity, and access management (IAM), data breach prediction, Cloud anomaly detection, as well as H-IoT devices behavior analysis. According to Table 2, defenders can identify, evaluate, and mitigate possible attacks more precisely with machine learning, as outlined in section IV. Due to this, machine learning algorithms can automate various tasks, including identifying vulnerabilities, deceiving, and disrupting attacks [227]. This section discusses several potential use cases for ML in H-IoT cybersecurity.

- **Classifying Anomalies in Cybersecurity:** In classifying threats, machine learning offers a swift and efficient method for processing huge amounts of data. Machine learning analyzes behavior and continuously changes parameters to find anomalies that could indicate attacks [228]. Machine learning allows for intelligent security services learning that detects or predicts cyber attacks and anomalies.

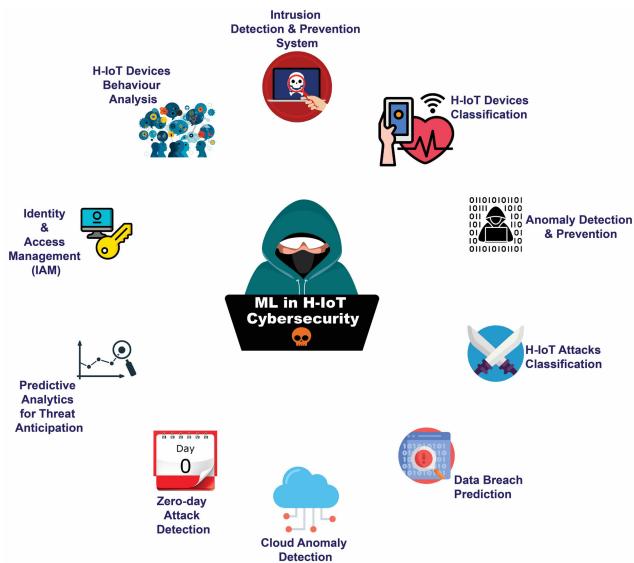
- **Predicting and Responding to Data Breaches and Cyber Attacks in Real-time:** With machine learning, large amounts of data can be analyzed from multiple sources to predict cyber threats [229]. A machine learning system can quickly build defensive patches in response to an attack after identifying a cyber threat without human intervention [230].

- **Automating processes:** In the H-IoT cybersecurity sector, machine learning is becoming increasingly crucial as time-consuming tasks such as vulnerability assessments, malware analysis, network log scrutiny, and intelligence assessments continue to multiply [231]. Automating security workflows enables organizations to respond quickly to threats and incidents, a feat that cannot be achieved through manual efforts alone [232]. Furthermore, automation offers sustainability by enhancing efficiency and scalability features and reducing unnecessary costs.

- **Authentication and Access Control:** Authentication technology is essential for medical devices since it validates a user's credentials with those stored in authorized user systems or authentication servers, enabling access to multiple systems simultaneously [233]. Machine learning determines when to request multi-factor authentication with intelligent authentication.

### B. FEATURE EXTRACTION

H-IoT feature extraction involves selecting and transforming relevant data attributes. Moreover, it is necessary to determine the most crucial features before embarking on any ML design



**FIGURE 13.** ML use cases for H-IoT cybersecurity.

process [234]. Specific attributes can reduce computing costs and improve storage efficiency [235]. For feature selection, we use the following methods:

- **Filter Methods:** This method calculates the correlation between attributes by comparing the results of their correlations. We select attributes based on statistical methods scores, based on the scores and the threshold values. There are a few popular methods for extracting features from data, such as correlation, information gain, and Chi-Square tests [236].
- **Wrapper Methods:** An ML model trains on selected features. The model's accuracy determines whether to include or exclude attributes depending on its reliability within the subset. Eliminating backward and selecting forwards are the most common methods [237].
- **Embedded Methods:** This method combines the benefits of both filters and wrappers (i.e., extracts the best features while maintaining the computational cost). These methods include Least Absolute Shrinkage and Selection Operator (LASSO) regularization, Random Forest [238].

In addition, this stage calculates parameter weights for unique features based on the training set using a deep learning algorithm. Each deep learning algorithm has several invisible layers embedded within the inputs and outputs, allowing for the extraction of detailed features [239].

### C. INTRUSION DETECTION SYSTEM IN HEALTHCARE-IoT

Intrusion detection systems for H-IoT are described in this section [240]. An intrusion typically targets a network or device's integrity, availability, or confidentiality by impairing its security. Due to the sensitive nature of healthcare data, H-IoT is a lucrative target for external or internal attackers. Monitoring and analyzing device and network activities is automated by IDS solutions, which are available

as hardware or software solutions. IDS consists of three components: information source, analysis, and response. Information sources feed data to the analysis component, which, upon identifying an attack, triggers a response - either passively, such as notifications, or actively, such as disabling communication.

In [241], the authors propose a 5G-driven healthcare landscape where the Internet of Medical Things enables remote patient monitoring. Nevertheless, ensuring the security of data remains a challenge. A new lightweight Intrusion Detection System for IoMT, utilizing kernel techniques for feature selection and a kernel extreme learning machine for decision-making, is introduced. This IDS detected anomalies with 99.9% accuracy on the dataset WUSTL-EHMS-2020.

In [242], the authors used mobile agents to detect intrusions in a medical environment. Furthermore, a simulation of hospital network topology was conducted to simulate IoMT experiments, which included the identification of network-level intrusions using machine learning and regression algorithms and the implementation of various digital imaging and communications in medicine (DICOM) protocols by connected devices such as ultrasound scanners and MRI machines, utilizing wireless body area networks. These networks are composed of wearable and implantable devices that transmit physiological data continuously, allowing patients to be monitored, diagnosed, and treated continuously. In total, 72 independent simulations were conducted across 216 network types, resulting in an overall best-and worst-case detection accuracy of 99.9% and 92.91%, respectively.

In [243], the proposed system integrates ensemble learning and cloud-based architecture to detect cyberattacks. In this ensemble setup, Decision Trees, Naive Bayes, and Random Forests are used as individual learners at the initial level. In the following level, XGBoost uses the classification results to differentiate between normal and attack cases. Using large-scale, diverse IoT networks, ToN-IoT provides an accurate dataset for the model. Experimental results indicate that the proposed framework can achieve a detection rate of 99.98%, a precision of 96.98%, and a reduction in false alarms.

By demonstrating significant accuracy and reduced false alarms in cybersecurity, these examples show that machine learning enhances intrusion detection systems in H-IoT.

### D. EVENT DETECTION SYSTEM

A H-IoT system uses event detection to identify and capture significant occurrences and incidents. An event detection algorithm analyzes sensor data, network traffic, and device interactions to detect patterns, anomalies, and predefined triggers that indicate critical events, such as emergencies, device malfunctions, and abnormal patient conditions. Several machine learning techniques investigate classification, including supervised, unsupervised, and reinforcement learning. A supervised learning algorithm employs a labeled dataset for training that is used to determine the relationship

between inputs and outputs. Based on the correlation between the input samples, unsupervised learning algorithms can classify the provided data into clusters. The third category of algorithms is reinforcement learning and online learning. These algorithms utilize current knowledge and explore the environment to classify the data [244], [245].

#### E. RELIABILITY IN HEALTHCARE-IoT SYSTEMS

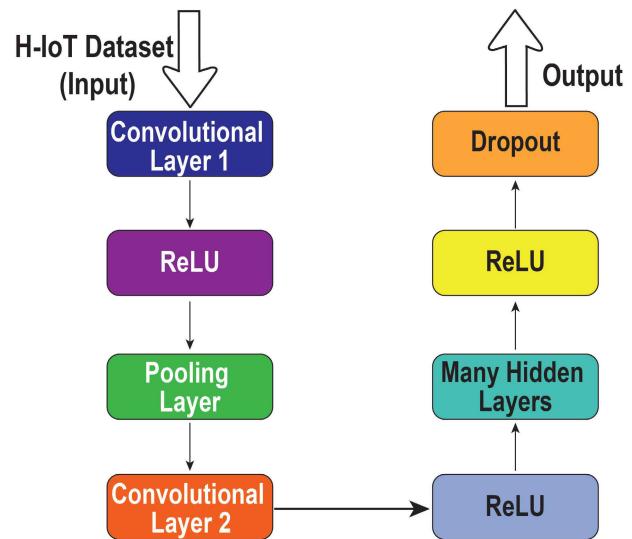
Data exchange between e-health systems must be reliable and efficient in H-IoT for enabling cyber resilience, security metrics (Confidentiality, Integrity, Availability (CIA) Triad), and controls within the ecosystem [1], [137], [246]:

- **Confidentiality:** It is illegal for unauthorized individuals to access medical information.
- **Integrity:** There is no possibility of adversaries altering data during transit or storage.
- **Non-repudiation:** Data transmission and reception are inevitable.
- **Data Freshness:** There is no way to re-generate old data.
- **Resilience to Attacks:** The system should adapt to failed nodes, and there should be no single point of failure.
- **Data Authentication:** It is necessary to authenticate the addresses and object information retrieved.
- **Access Control:** Providing access control to data is a requirement for information providers.
- **Client Privacy:** A lookup system should only be able to infer its purpose from the information provider.
- **Fault Tolerance and Self-healing:** An IoT device or battery energy failure should not disrupt health service continuity.

#### F. CONVOLUTIONAL NEURAL NETWORKS (CNNs) IN HEALTHCARE-IoT

Using Convolutional Neural Networks has been demonstrated to be significantly more effective than previous methods in identifying threats, surpassing techniques like Decision Trees, SVMs, and K-nearest neighbors (KNNs) [247]. In classification problems, CNNs are used as feed-forward networks [248]. Essentially, Convolutional Neural Networks are characterized by two processes. First, convolution involves transforming inputs into outputs using filters or kernels. In particular, CNNs have streamlined image recognition to self-contained, removing the need for external image processing software. Furthermore, it can recognize outcomes efficiently and adapt seamlessly to changing identification criteria. Moreover, their ability to leverage preexisting networks enhances system versatility and applicability [249]. Neurons are arranged in layers in a three-dimensional configuration, spanning width, height, and depth. As shown in Figure 14, which illustrates a CNN architecture for analyzing H-IoT data.

As part of the architecture of Convolutional Neural Networks, the initial layer, called Layer 1, is composed of a significant number of neurons to effectively process



**FIGURE 14.** The convolutional neural network architecture.

input data [250]. There are three fundamental parameters: dataset size, quality, and type. Multiple receptive layers can be used to process input layers effectively. This configuration creates overlapping input regions, allowing high-resolution outputs from the original input. For detecting features, CNNs employ operations such as pooling and convolution. Using the fully connected layer as a classifier follows extracting features. Typically, the architecture of CNN, convolutional, and pooling layers are merged, though it is not mandatory.

##### 1) RECTIFIED LINEAR UNIT (RELU)

In neural networks, ReLUs follow convolution modules. The primary function of ReLU is to activate specific neurons within the network. The Rectified Linear Unit (ReLU) keeps the values of active neurons while converting inactive neurons to 0 using a simple threshold [251], [252]. The activation information retained by this segment of the neural network remains significant for future inferences made by other network segments.

An activation function like the ReLU is essential for introducing nonlinear operations into inherently linear neural networks. Adding nonlinearity to the network increases its ability to fit data to capture intricate patterns and relationships accurately.

The ReLU activation function does not alter the dimensions of the input or output data. A mathematical expression for this function can be found in equation (1)

$$y = \max\{0, x\} \quad (1)$$

##### 2) POOLING LAYER

Pooling layers contribute significantly to CNN performance by strategically inserting them between CNN layers. By reducing the number of network parameters and down-sampling the data, this integration achieves two objectives:

increasing computational efficiency and reducing computation time. Furthermore, the downsampling process, which is more precise than average pooling, preserves texture information by minimizing the differences in evaluation values resulting from the convolutional layers [253], [254]. Max pooling is essential because it detects and retains the maximum value within each receptive field. Consequently, it preserves essential features while reducing data dimensions, and in each window, it displays the maximum value [255].

### 3) FULLY CONNECTED LAYER

The Fully Connected Layer follows the pooling and convolution layers. Based on the features extracted by the previous layers, this layer classifies the input data. The activation functions of the neurons in this layer perform a significant role in processing the information from the preceding layer. Fully connected neurons allow the network to recognize complex patterns and relations. According to [217], CNN deep learning classifiers can be used to identify malware instances in healthcare datasets. This research demonstrates the networks' capability to analyze intricate data and provide valuable insight into several domains vital to human health and security.

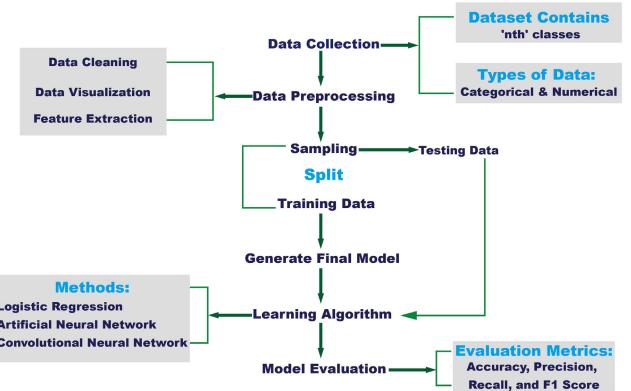
### 4) SOFTMAX

The Softmax activation functions are commonly assigned to the neural networks' final layer to perform multi-class classification. Data can be transformed using the Softmax function into a probability distribution from 0 to 1 with a sum of 1. As a result of the function, data classification is easier since it emphasizes differences between input values. According to Sharma et al., [256], a CNN-Bidirectional LSTM architecture is proposed for using deep learning in smart healthcare networks for intrusion detection. The model detects DDoS attacks using softmax activation functions by classifying traffic flows as benign or malicious. Faruqui et al. [257] propose SafetyMed, a specialized Intrusion Detection System for securing the Internet of Medical Things. IoMT-specific intrusions are identified with SafetyMed using CNN and LSTM. In the output layer, Softmax activation functions convert raw scores into probabilities ranging from 0 to 1. This enhances the accuracy of the decision-making process. IoMT vulnerabilities are effectively addressed by SafetyMed, which has an average detection accuracy of 97.63%.

The scope of this section encompassed a wide range of machine learning techniques, applications, and advanced CNN-based mechanisms illuminating multifaceted strategies for protecting H-IoT devices.

## VII. SECURITY AND PRIVACY IN H-IoT ENVIRONMENTS

This section emphasizes the importance of effective safeguards and rigorous protocols to protect sensitive data and preserve user confidentiality in H-IoT environments. In-depth analysis explores key challenges, effective strategies, and



**FIGURE 15.** ML-based anomaly detection architecture in H-IoT.

emerging trends. IoT is being transformed into a network of interconnected devices, where security and privacy are becoming crucial challenges. Therefore, the IoT network is built around anomaly detection techniques. Anomaly detection algorithms detect abnormal patterns immediately in the IoT, preventing serious problems. However, healthcare and the IoT combine to raise the stakes even higher. As a result, machine learning could potentially provide remedies for these challenges. Additionally, a machine learning-based architecture for anomaly detection is described in detail in the section.

### A. ANOMALY DETECTION

The term anomaly refers to data segments that do not follow the expected pattern or features of the rest of the data. Anomaly detection is crucial since anomalous activities contain critical information and relevance [258]. Anomaly detection involves several independent processes in H-IoT, as illustrated in Figure 15. Data collection is the first step in this architecture. Following the dataset's creation, it should be analyzed thoroughly to determine the data types.

It is also crucial to preprocess the data before analyzing it [135]. The preprocessing of data includes filtering, visualizing, and extracting features. These steps convert the data into feature vectors. It is then necessary to divide the feature vectors into training and testing sets to an 80:20 ratio. The learning algorithm develops an optimal final model by utilizing the training set. It is possible to use a variety of classifiers to experiment with the most accurate accuracy [259].

With 5G networks facilitating rapid, high-volume data exchanges, the IoMT has gained momentum in the healthcare sector. In [260], the emphasis is on detecting anomalies using deep learning for enhanced security within 5G contexts in IoM. By utilizing multi-model autoencoders for feature extraction, the complexity of traffic feature information has been significantly reduced. A new algorithm for detecting multi-featured sequence anomalies, optimized to cope with the high data volume of 5G networks, is also presented. It has

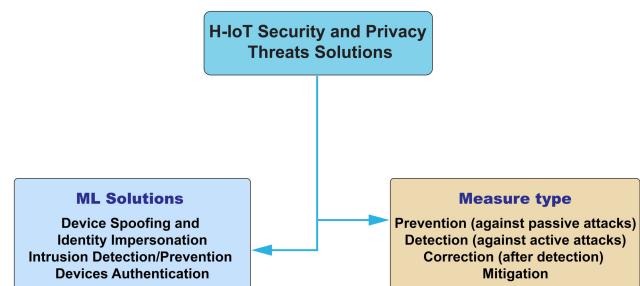
been demonstrated that deep learning combined with 5G technology can identify and mitigate anomalies efficiently, thereby increasing IoMT systems' resilience and reliability.

### B. BEST PRACTICES FOR ENABLING DATA PRIVACY, SECURITY, AND BUILDING RISK MITIGATION STRATEGIES IN SMART ENVIRONMENTS

Digital healthcare environments [261] are becoming more prevalent despite numerous security and privacy concerns, and they are susceptible to a unique set of challenges (i.e., securing the massive amount of healthcare data harvested every second from thousands of connected IoT devices). Healthcare procedures and decisions are made based on this data; in situations where this data is compromised or breached, this may result in a wrong diagnosis/treatment affecting human life. Securing smart environments requires implementing defense-in-depth strategies and multiple layers of security across the ecosystem such as: (i) Standards and data governance risk and control (DGRC) policies for access control, data protection, encryption, remote access (ii) Monitoring and response mechanisms for Security Information and Event Management (SIEM), identity and access management, log analysis, cyber forensics, (iii) Perimeter controls for intrusion detection, prevention and next generation firewalls, (iv) Securing the network using VPN services, web-filtering, securing remote services and site-to-site connections (v) Hardening end-point security by enabling Zero Trust mechanisms, patching the systems with latest updates to mitigate vulnerabilities, using an up-to-date antivirus tool to detect and protect the end-point for new vulnerabilities, (vi) the human element is the weakest link and its essential to build cyber awareness within the workplace environment and train them so that they are cyber prepared, (vii) enabling application security using vulnerability scanners and making sure that only inventoried tools are used, (viii) last but not the least, to ensure data security mechanisms are in place (i.e. end-to-end secured data, data classification and have a data loss prevention/backup strategy) [1]. However, the impact and frequency of cyber attacks have escalated due to generative AI. Since the attacks are constantly evolving and new threats are coming to the surface, there is a possibility that the novel threats would go undetected. This is why there is an essential need for a versatile machine-learning solution to neutralize and mitigate these threats.

### C. MITIGATING HEALTHCARE-IoT SECURITY AND PRIVACY THREATS USING MACHINE LEARNING

The security and privacy of sensitive health information has become a worldwide concern. In healthcare security and privacy, machine learning-based solutions are essential among cryptographic, password-based, and digital signature-based solutions. As shown in Figure 16, machine learning models can detect Device Spoofing and Identity Impersonation, Intrusion Detection and Prevention, and Device Authentication. A machine learning model can prevent anomalies after detection. As a result, ML models perform



**FIGURE 16. H-IoT security and privacy threat solution.**

a significant role in H-IoT [262]. In healthcare systems, Hau et al. applied machine learning techniques to increase security and privacy [263]. Begli et al. implemented SVM-based intrusion detection to monitor remote healthcare [264]. Sengan et al. developed an adaptive, ML-driven routing system for healthcare data security [265].

## VIII. IMPACT OF HEALTHCARE-IoT TECHNOLOGIES IN THE FUTURE

Healthcare and smart cities benefit greatly from the Internet of Things (IoT). This technology will significantly change everyday life and urban environments in the coming years. This section discusses the potential impact of H-IoT on smart cities, including relevant challenges and innovative solutions. Quality of service is integral to this discussion, which entails ensuring the reliability of services. Furthermore, H-IoT networks can be made more flexible, scalable, resource-efficient, and secure with the help of Software-Defined Networks (SDNs).

### A. FUTURE OF HEALTHCARE-IoT TECHNOLOGIES

Generally, people expect H-IoT systems to integrate with their living environments. The future of infrastructure lies in smart cities. As a result, affiliating the H-IoT system within modern city architecture facilitates widespread deployment of the H-IoT [266]. Software-defined networking plays a significant role in smart cities and H-IoT systems. Using SDN in H-IoT, cities can gain more efficient management, more secure provision of services, effective resource allocation, and overall better performance.

### B. CHALLENGES

Despite the growing popularity of IoT applications in healthcare, several challenges restrict their implementation. In the following section, we explore key challenges connected to H-IoT development [267].

#### 1) HETEROGENEOUS NETWORKS

Developing H-IoT requires devices to interact and interoperate across diverse networks and operating systems. Among the technologies used in communication are Bluetooth, IrDA, UWB, Zigbee, WLANs, Wi-Fi 6, and 5G. Batteries drain out faster when communicating over long

distances [268], [269]. It is essential that these devices, regardless of their heterogeneity in implementation and communication, can identify and communicate with each other.

## 2) QUALITY OF SERVICE (QOS)

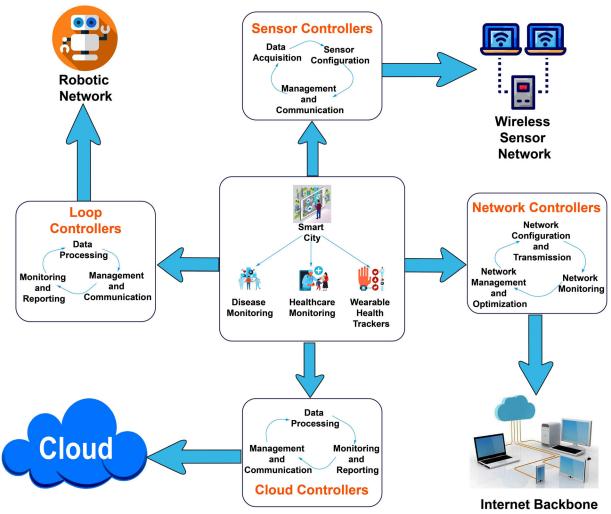
Healthcare IoT is characterized by low latency and low power consumption. There is a risk to a patient's health when dealing with issues related to the Internet of Things. Consequently, H-IoT signals should be transmitted and processed with the least possible delay. High-bandwidth networking resources can achieve this [270]. A 5G network, with its ability to ensure quality of service through rapid data transmission, minimal latency, and extensive connectivity, presents itself as an ideal solution for H-IoT applications [271]. Quality of service refers to the ability of a system to maintain a basic level of performance and reliability, ensuring that data is transmitted and received accurately and promptly.

## 3) PRIVACY AND SECURITY

In H-IoT, the privacy and security of patients and their data are paramount as any compromise could result in severe consequences (i.e., loss of command and control of a cobot arm used for precision surgeries may lead to its malfunctioning causing harms to person, property, loss of availability could lead to healthcare service disruption leaving critical patients who may need immediate attention vulnerable, loss of integrity would risk patients to wrong diagnosis or medication, loss of confidentiality would lead to loss of privacy, digital identity frauds, deep fakes, bio-hacking issues, etc.). In many cases, H-IoT uses heterogeneous networks to communicate and store data, exposing it to attack over long distances [272]. Thus, the security and privacy of data require anomaly detection, mitigation, robust encryption, and authentication techniques, as mentioned in section VII-B. However, in designing and implementing the defense-in-depth techniques, it is necessary to consider the resource constraints of the devices involved in H-IoT, and the developed solutions should be lightweight and energy-efficient.

## C. SOFTWARE-DEFINED NETWORK (SDN) IN HEALTHCARE-IOT

An emerging paradigm in computer networking is software-defined networking. Data planes, control planes, and application planes are the three tiers of SDN. Data and control planes are separated to improve network performance. In contrast, traditional architectures combine data and control planes onto one device, while SDN separates them to simplify network management [273], [274]. SDNs forward packets according to predefined policies [275]. SDN-based H-IoT consists of Sensor Controllers, Cloud Controllers, Network Controllers, and Closed-Loop Controllers, which provide four types of services: data acquisition, network



**FIGURE 17. Software defined network-based H-IoT.**

configuration and transmission, processing, and actionable feedback, as illustrated in Figure 17.

The software-defined network is used by Google, for example, to manage its wide-area network traffic [276]. The network infrastructure increasingly relies on SDNs, and protecting a network from attack is crucial to ensure its integrity and availability [277]. In [278], a novel software-defined network architecture is presented, incorporating a new controller and load-balancing algorithms based on machine learning for the healthcare IoT. A support vector machine algorithm, which achieved 95.1% accuracy through extensive simulations, validates the architecture's effectiveness. In preparation for broader 5G integration, this approach represents an important advance in H-IoT. Adding deep learning to SDNs makes H-IoT services, such as telemedicine, more reliable and secure [279]. A software-defined network system illustrates the communication process between medical services and nano-networks inside individuals' bodies [280]. A certain set of software rules controls this method, which makes healthcare more efficient.

## IX. CONCLUSION

This paper systematically dives into digital healthcare's fundamental elements and practical applications. It discusses the essential technologies and methodologies for optimizing these systems within Healthcare 5.0. The research focuses on various cyber threats, vulnerabilities, and cyber attacks carried out at the different IoT layers and explores the security and privacy of H-IoT through deep neural networks and AI. A demonstration of a cloud-based solution and big data analytics using IoT and software-defined networks is provided. This illustrates the advantages of a precise, efficient, and secure healthcare ecosystem. The authors also present insights on the security challenges related to wireless and communication technologies (i.e., 5G) in H-IoT and how

ML algorithms can enable the digital healthcare environment to bridge those security gaps.

## REFERENCES

- [1] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap," *Sensors*, vol. 21, no. 11, p. 3901, Jun. 2021.
- [2] S. Zardari, N. Nisar, Z. Fatima, and L. L. Dhirani, "IoT—Assets taxonomy, threats assessment and potential solutions," in *Proc. Global Conf. Wireless Opt. Technol. (GCWOT)*, Jan. 2023, pp. 1–8.
- [3] S. Latif, J. Qadir, S. Farooq, and M. Imran, "How 5G wireless (and concomitant technologies) will revolutionize healthcare?" *Future Internet*, vol. 9, no. 4, p. 93, Dec. 2017. [Online]. Available: <https://www.mdpi.com/1999-5903/9/4/93>
- [4] S. Majumder, T. Mondal, and M. Deen, "Wearable sensors for remote health monitoring," *Sensors*, vol. 17, no. 12, p. 130, Jan. 2017.
- [5] N. Wickramasinghe and F. Bodendorf, *Delivering Superior Health and Wellness Management With IoT and Analytics*. Cham, Switzerland: Springer, 2019.
- [6] O. Postolache, D. J. Hemanth, R. Alexandre, D. Gupta, O. Geman, and A. Khanna, "Remote monitoring of physical rehabilitation of stroke patients using IoT and virtual reality," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 562–573, Feb. 2021.
- [7] P. K. Gupta, M. H. Nawaz, S. S. Mishra, K. Parappa, A. Silla, and R. Hanumegowda, "New age approaches to predictive healthcare using in silico drug design and Internet of Things (IoT)," *Sustain. Energy Efficient Comput. Paradigms Soc.*, vol. 8, pp. 127–151, Sep. 2021.
- [8] M. Jayashankara, S. S. Udmale, A. K. Pandey, and R. S. Singh, "IoT healthcare architecture," in *IoT-Based Data Analytics for the Healthcare Industry*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 9–29.
- [9] C. A. Tavera, J. H. Ortiz, O. I. Khalaf, D. F. Saavedra, and T. H. Aldhyani, "Wearable wireless body area networks for medical applications," *Comput. Math. Methods Med.*, vol. 2021, Apr. 2021, Art. no. 5574376.
- [10] D. Gangwani, "AI- and IoT-based body sensor networks for healthcare system," *Artif. Intell. Cyber-Phys. Syst., Princ. Appl.*, vol. 2, p. 17, Mar. 2023.
- [11] Dell Inc. (2023). *Edge to Core and the Internet of Things and Data Placement*. Accessed: Dec. 15, 2023. [Online]. Available: <https://tinyurl.com/mwj4ywfb>
- [12] A. P. Plageras and K. E. Psannis, "Algorithms for big data delivery over the Internet of Things," in *Proc. IEEE 19th Conf. Bus. Informat. (CBI)*, vol. 1, Jul. 2017, pp. 202–206.
- [13] M. Usak, M. Kubiatko, M. S. Shabbir, O. V. Dudnik, K. Jermitsiparsert, and L. Rajabion, "Health care service delivery based on the Internet of Things: A systematic and comprehensive study," *Int. J. Commun. Syst.*, vol. 33, no. 2, p. e4179, Jan. 2020.
- [14] S. M. Karunaratne, N. Saxena, and M. K. Khan, "Security and privacy in IoT smart healthcare," *IEEE Internet Comput.*, vol. 25, no. 4, pp. 37–48, Jul. 2021.
- [15] A. Hanson and L. Haddad, *Nursing Rights of Medication Administration*. Treasure Island, FL, USA: StatPearls Publishing, 2022.
- [16] M. Ciampi, A. Coronato, M. Naeem, and S. Silvestri, "An intelligent environment for preventing medication errors in home treatment," *Expert Syst. Appl.*, vol. 193, May 2022, Art. no. 116434.
- [17] G. Muhammad, M. S. Hossain, and N. Kumar, "EEG-based pathology detection for home health monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 603–610, Feb. 2021.
- [18] L. Shrotriya, K. Sharma, D. Parashar, K. Mishra, S. S. Rawat, and H. Pagare, "Apache spark in healthcare: Advancing data-driven innovations and better patient care," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, pp. 1–9, 2023.
- [19] S. U. Amin and M. S. Hossain, "Edge intelligence and Internet of Things in healthcare: A survey," *IEEE Access*, vol. 9, pp. 45–59, 2021.
- [20] T. Shaik, X. Tao, N. Higgins, L. Li, R. Gururajan, X. Zhou, and U. R. Acharya, "Remote patient monitoring using artificial intelligence: Current state, applications, and challenges," *WIREs Data Mining Knowl. Discovery*, vol. 13, no. 2, p. e1485, Mar. 2023.
- [21] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar, and A. Khan, "An intelligent IoT based healthcare system using fuzzy neural networks," *Sci. Program.*, vol. 2020, pp. 1–15, Dec. 2020.
- [22] A. A. Al-Atawi, F. Khan, and C. G. Kim, "Application and challenges of IoT healthcare system in COVID-19," *Sensors*, vol. 22, no. 19, p. 7304, Sep. 2022.
- [23] J. Mao, P. Zhou, X. Wang, H. Yao, L. Liang, Y. Zhao, J. Zhang, D. Ban, and H. Zheng, "A health monitoring system based on flexible triboelectric sensors for intelligence medical Internet of Things and its applications in virtual reality," 2023, *arXiv:2309.07185*.
- [24] V. Subramaniyaswamy, G. Manogaran, R. Logesh, V. Vijayakumar, N. Chilamkurti, D. Malathi, and N. Senthilselvan, "Retracted article: An ontology-driven personalized food recommendation in IoT-based healthcare system," *J. Supercomput.*, vol. 75, no. 6, pp. 3184–3216, Jun. 2019.
- [25] P. He, C. Lan, Y. Cui, R. Wang, and D. Wu, "Accelerated federated learning with dynamic model partitioning for H-IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2023, pp. 1–6.
- [26] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2159–2187, Apr. 2019.
- [27] F. Subhan, A. Mirza, M. B. M. Su'ud, M. M. Alam, S. Nisar, U. Habib, and M. Z. Iqbal, "AI-enabled wearable medical Internet of Things in healthcare system: A survey," *Appl. Sci.*, vol. 13, no. 3, p. 1394, Jan. 2023.
- [28] S. Swain, B. Bhushan, G. Dhiman, and W. Viriyasitavat, "Appositeness of optimized and reliable machine learning for healthcare: A survey," *Arch. Comput. Methods Eng.*, vol. 29, no. 6, pp. 3981–4003, Oct. 2022.
- [29] S. S. Gopalan, A. Raza, and W. Almobaiden, "IoT security in healthcare using AI: A survey," in *Proc. Int. Conf. Commun., Signal Process., Their Appl. (ICCSPA)*, Mar. 2021, pp. 1–6.
- [30] N. Finne, J. Eriksson, T. Voigt, G. Suciu, M.-A. Sachian, J. Ko, and H. Keipour, "Multi-trace: Multi-level data trace generation with the cooja simulator," in *Proc. 17th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Jul. 2021, pp. 390–395.
- [31] H. K. Bharadwaj, A. Agarwal, V. Chamola, N. R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, "A review on the role of machine learning in enabling IoT based healthcare applications," *IEEE Access*, vol. 9, pp. 38859–38890, 2021.
- [32] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, Oct. 2021, Art. no. 103164.
- [33] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167, 2nd Quart., 2020.
- [34] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and robust machine learning for healthcare: A survey," *IEEE Rev. Biomed. Eng.*, vol. 14, pp. 156–180, 2021.
- [35] G. S. Karthick and P. B. Pankajavalli, "A review on human healthcare Internet of Things: A technical perspective," *Social Netw. Comput. Sci.*, vol. 1, no. 4, p. 198, Jul. 2020.
- [36] F. T. Al-Dhief, N. M. A. Latiff, N. N. N. A. Malik, N. S. Salim, M. M. Baki, M. A. A. Albadr, and M. A. Mohammed, "A survey of voice pathology surveillance systems based on Internet of Things and machine learning algorithms," *IEEE Access*, vol. 8, pp. 64514–64533, 2020.
- [37] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of Internet of Things in Healthcare: A systematic literature review and classification," *Universal Access Inf. Soc.*, vol. 18, no. 4, pp. 837–869, Nov. 2019.
- [38] K. Shailaja, B. Seetharamulu, and M. A. Jabbar, "Machine learning in healthcare: A review," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Mar. 2018, pp. 910–914.
- [39] G. Hatzivasilis, O. Soulatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 457–464.
- [40] S. K. Jagatheeperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107691.
- [41] M. M. Dhamvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

- [42] S. Ketu and P. K. Mishra, "Internet of Healthcare Things: A contemporary survey," *J. Netw. Comput. Appl.*, vol. 192, Oct. 2021, Art. no. 103179.
- [43] S. K and N. D. C, "Advancements and challenges in 5G networks," in *Proc. Int. Conf. Smart Syst. Appl. Electr. Sci. (ICSSES)*, Jul. 2023, pp. 1–6.
- [44] K. Bawaneh, F. G. Nezami, M. Rasheduzzaman, and B. Dekan, "Energy consumption analysis and characterization of healthcare facilities in the united states," *Energies*, vol. 12, no. 19, p. 3775, Oct. 2019.
- [45] E. Kost. (2023). *14 Biggest Healthcare Data Breaches [Updated 2023]*. Accessed: Dec. 16, 2023. [Online]. Available: <https://tinyurl.com/axrpc6x5>
- [46] R. Mattioli, A. Malatras, E. N. Hunter, M. G. B. Penso, D. Bertram, and I. Neubert, "ENISA foresight cybersecurity threats for 2030," Eur. Union Agency Cybersecurity (ENISA), Athens, Greece, Tech. Rep., 2023. Accessed: Dec. 15, 2023. [Online]. Available: <https://tinyurl.com/3ahnvd7>; doi: [10.1016/j.cswea.2021.116434](https://doi.org/10.1016/j.cswea.2021.116434).
- [47] N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in IoT," *e-Prime-Adv. Electr. Eng., Electron. Energy*, vol. 4, Jun. 2023, Art. no. 100158.
- [48] F. Y. Yavuz, D. Ünal, and E. Güll, "Deep learning for detection of routing attacks in the Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, pp. 39–58, 2018.
- [49] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May 2016.
- [50] H. R. Abdulqadir, S. R. M. Zeebaree, H. M. Shukur, M. M. Sadeeq, B. W. Salim, A. A. Salih, and S. F. Kak, "A study of moving from cloud computing to fog computing," *Qubahan Academic J.*, vol. 1, no. 2, pp. 60–70, Apr. 2021.
- [51] A. R. Chordiya, S. Majumder, and A. Y. Javaid, "Man-in-the-middle (MITM) attack based hijacking of HTTP traffic using open source tools," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 0438–0443.
- [52] J. M. Alkhathami and S. M. Alzahrani, "Detection of SQL injection attacks using machine learning in cloud computing platform," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 15, pp. 1–14, 2022.
- [53] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—A review," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA) (Fall)*, Sep. 2017, pp. 1–6.
- [54] A. Malik, B. Bhushan, S. B. Khan, R. Kashyap, R. Chaganti, and N. Rakesh, "Security attacks and vulnerability analysis in mobile wireless networking," in *5G Beyond*. Singapore: Springer, 2023, pp. 81–110.
- [55] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 296–312, Feb. 2023.
- [56] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.
- [57] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Y. Z. Yusupov, and D. Kodirov, "Architecture, protocols, and applications of the Internet of Medical Things (IoMT)," *J. Commun.*, vol. 17, no. 11, pp. 900–918, 2022.
- [58] A. M. Albalawi and M. A. Almaiah, "Assessing and reviewing of cybersecurity threats, attacks, mitigation techniques in IoT environment," *J. Theor. Appl. Inf. Technol.*, vol. 100, pp. 2988–3011, 2022.
- [59] A. Bekkali, M. Essaidi, M. Boulmalf, and D. Majdoubi, "Systematic literature review of Internet of Things (IoT) security," *Adv. Indynamical Syst. Appl.*, vol. 21, pp. 25–39, Jan. 2022.
- [60] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq, and K.-K. Wong, "Thinking out of the blocks: Holochain for distributed security in IoT healthcare," *IEEE Access*, vol. 10, pp. 37064–37081, 2022.
- [61] V. Mohindru and A. Garg, "Security attacks in Internet of Things: A review," in *Proc. ICRIC*, 2021, pp. 679–693.
- [62] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustain. Eng. Innov.*, vol. 3, no. 1, pp. 23–28, Jan. 2021.
- [63] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.
- [64] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016.
- [65] I. Cvitić and M. Vujić, "Classification of security risks in the IoT environment," *Ann. DAAAM*, vol. 26, no. 1, pp. 1–10, 2015.
- [66] J. DiMaggio, *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. San Francisco, CA, USA: No Starch Press, 2022.
- [67] A. Roohi, M. Adeel, and M. A. Shah, "DDoS in IoT: A roadmap towards security & countermeasures," in *Proc. 25th Int. Conf. Autom. Comput. (ICAC)*, Sep. 2019, pp. 1–6.
- [68] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 97–110, Jun. 2018.
- [69] M. Adil, R. Khan, J. Ali, B.-H. Roh, Q. T. H. Ta, and M. A. Almaiah, "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment," *IEEE Access*, vol. 8, pp. 163209–163224, 2020.
- [70] M. N. Khan, H. U. Rahman, M. A. Almaiah, M. Z. Khan, A. Khan, M. Raza, M. Al-Zahrani, O. Almomani, and R. Khan, "Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks," *IEEE Access*, vol. 8, pp. 176495–176520, 2020.
- [71] M. H. Qasem, N. Obeid, A. Hudaib, M. A. Almaiah, A. Al-Zahrani, and A. Al-Khasawneh, "Multi-agent system combined with distributed data mining for mutual collaboration classification," *IEEE Access*, vol. 9, pp. 70531–70547, 2021.
- [72] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6461–6471, 2020.
- [73] A. K. A. Hwaiyat, M. Amin, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 1–12, 2020.
- [74] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohal, "A lightweight hybrid deep learning privacy preserving model for FC-based industrial Internet of Medical Things," *Sensors*, vol. 22, no. 6, p. 2112, Mar. 2022.
- [75] M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, and O. Almomani, "A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS," *Sensors*, vol. 22, no. 4, p. 1448, Feb. 2022.
- [76] F. Almudaires and M. Almaiah, "Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 732–738.
- [77] Y. Alotaibi and M. Ilyas, "Security risks in Internet of Things (IoT): A brief survey," in *Proc. 26th World Multi-Conf. Systemics, Cybern. Inform. (WMSCI)*, 2022, pp. 1–5.
- [78] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of Things protocols comparison, architecture, vulnerabilities and security: State of the art," in *Proc. 2nd Int. Conf. Comput. Wireless Commun. Syst.*, Nov. 2017, pp. 1–6.
- [79] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A review of Internet of Things (IoT) security issues, challenges and techniques," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–6.
- [80] Help Net Security. (2023). *As Biohacking Evolves, How Vulnerable are we to Cyber Threats?* [Online]. Available: <https://tinyurl.com/yt6bmrm3>
- [81] V. Varadharajan, U. Tupakula, and K. Karmakar, "Study of security attacks against IoT infrastructures," ISIF ASIA Funded Project, Tech. Rep. TR1, 2018.
- [82] *Cyber Resilience Act, Shaping Europe's Digital Future, Legislative Proposal COM(2022) 713 Final*, European Commission, Brussels, Belgium, 2022, Accessed: Dec. 15, 2023. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>
- [83] H. Meagher and L. L. Dhirani, "Cyber-resilience, principles, and practices," in *Cybersecurity Vigilance and Security Engineering of Internet of Everything*. Springer, 2023, pp. 57–74.
- [84] S. Sinha and B. Sindhu, "Impact of DoS attack in IoT system and identifying the attacker location for interference attacks," in *Proc. 6th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jul. 2021, pp. 657–662.

- [85] European Commission. (2023). *Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)*. Accessed: Dec. 15, 2023. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- [86] “Complete guide to GDPR compliance,” Proton AG, Eur. Union, Planles-Ouates, Switzerland, Tech. Rep., 2023. Accessed: Dec. 15, 2023. [Online]. Available: <https://gdpr.eu/>
- [87] M. M. Nasralla, I. García-Magariño, and J. Lloret, “Defenses against perception-layer attacks on IoT smart furniture for impaired people,” *IEEE Access*, vol. 8, pp. 119795–119805, 2020.
- [88] M. Sugadev, S. J. Rayen, J. Harirajkumar, R. Rathi, G. Anitha, S. Ramesh, and K. Ramaswamy, “Implementation of combined machine learning with the big data model in IoMT systems for the prediction of network resource consumption and improving the data delivery,” *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–12, Jul. 2022.
- [89] I. Aliahmadi, A. A. Madi, and A. Addaim, “Proposed architecture of e-health IoT,” in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2019, pp. 1–7.
- [90] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, “A survey of IoT security threats and defenses,” *Int. J. Adv. Comput. Res.*, vol. 9, no. 45, pp. 325–350, Oct. 2019.
- [91] E. A. A. Hagras, S. Aldosary, H. Khaled, and T. M. Hassan, “Physical layer authenticated image encryption for IoT network based on biometric chaotic signature for MPFrFT OFDM system,” *Sensors*, vol. 23, no. 18, p. 7843, Sep. 2023.
- [92] Y. Zhu and M. Xu, “Enhancing network throughput via the equal interval frame aggregation scheme for IEEE 802.11ax WLANs,” *Chin. J. Electron.*, vol. 32, no. 4, pp. 747–759, Jul. 2023.
- [93] M. Chotalia and S. Gajjar, “Performance comparison of IEEE 802.11ax, 802.11ac and 802.11n using network simulator NS3,” in *Proc. Int. Conf. Comput. Sci., Commun. Secur.* Springer, 2023, pp. 191–203.
- [94] S. S. Sefati and S. Halunga, “Ultra-reliability and low-latency communications on the Internet of Things based on 5G network: Literature review, classification, and future research view,” *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 6, p. e4770, Jun. 2023.
- [95] A. Anjum, P. Agbaje, A. Mitra, E. Oseghale, E. Nwafor, and H. Olufowobi, “Towards named data networking technology: Emerging applications, use cases, and challenges for secure data communication,” *Future Gener. Comput. Syst.*, vol. 151, pp. 12–31, Feb. 2024.
- [96] D. C. Valadares, N. C. Will, Á. Á. C. Sobrinho, A. C. Lima, I. S. Morais, and D. F. Santos, “Security challenges and recommendations in 5G-IoT scenarios,” in *Proc. Int. Conf. Adv. Inf. Netw. Appl.* Cham, Switzerland: Springer, 2023, pp. 558–573.
- [97] A. Sinha, A. R. Thukkaraju, and O. Vyas, “A multi agent framework to detect in progress false data injection attacks for smart grid,” in *Proc. Int. Conf. Adv. Netw. Technol. Intell. Comput.* Cham, Switzerland: Springer, 2021, pp. 123–141.
- [98] K. Sonar and H. Upadhyay, “A survey: DDoS attack on Internet of Things,” *Int. J. Eng. Res. Develop.*, vol. 10, no. 11, pp. 58–63, 2014.
- [99] B. S. Rawal, S. Patel, and M. Sathyanarayanan, “Identifying DDoS attack using split-machine learning system in 5G and beyond networks,” in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2022, pp. 1–6.
- [100] A. Munshi, N. A. Alqarni, and N. A. Almalki, “DDoS attack on IoT devices,” in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–5.
- [101] E. Džaferović, A. Sokol, A. A. Almisreb, and S. M. Norzeli, “DoS and DDoS vulnerability of IoT: A review,” *Sustain. Eng. Innov.*, vol. 1, no. 1, pp. 43–48, Jun. 2019.
- [102] P. Porambage, C. Schmitt, P. Kumar, A. Gurkov, and M. Ylianttila, “PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications,” *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, Jul. 2014, Art. no. 357430.
- [103] Cyber Risk GmbH. (2022). *The NIS 2 Directive*. [Online]. Available: <https://www.nis-2-directive.com/>
- [104] K. G. Kumar and S. Sengan, “Improved network traffic by attacking denial of service to protect resource using Z-test based 4-tier geomark traceback (Z4TGT),” *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3541–3575, Oct. 2020.
- [105] S. Hijazi and M. S. Obaidat, “Address resolution protocol spoofing attacks and security approaches: A survey,” *Secur. Privacy*, vol. 2, no. 1, p. e49, Jan. 2019.
- [106] P. Madani, N. Vlajic, and S. Sadeghpour, “MAC-layer spoofing detection and prevention in IoT systems: Randomized moving target approach,” in *Proc. Joint Workshop CPS&IoT Secur. Privacy*, Nov. 2020, pp. 71–80.
- [107] S. Murali and A. Jamalipour, “A lightweight intrusion detection for sybil attack under mobile RPL in the Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 1, pp. 379–388, Jan. 2020.
- [108] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of threats to the Internet of Things,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.
- [109] K. Ávila, P. Sammartin, D. Jabba, and J. Gómez, “An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN,” *Wireless Pers. Commun.*, vol. 122, no. 4, pp. 3687–3718, Feb. 2022.
- [110] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, “Passive rule-based approach to detect sinkhole attack in RPL-based Internet of Things networks,” *IEEE Access*, vol. 11, pp. 94081–94093, 2023.
- [111] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, “A survey of security and privacy issues in the Internet of Things from the layered context,” *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e3935, Jun. 2022.
- [112] C. Hong and D. Shi, “A cloud-based control system architecture for multi-UAV,” in *Proc. 3rd Int. Conf. Robot., Control Autom.*, Aug. 2018, pp. 25–30.
- [113] M. K. Hooshmand and D. Hosahalli, “Network anomaly detection using deep learning techniques,” *CAAI Trans. Intell. Technol.*, vol. 7, no. 2, pp. 228–243, Jun. 2022.
- [114] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, “A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network,” *J. Parallel Distrib. Comput.*, vol. 164, pp. 55–68, Jun. 2022.
- [115] A. R. Wani, Q. Rana, U. Saxena, and N. Pandey, “Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques,” in *Proc. IEEE Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 870–875.
- [116] I. Baako and S. Umar, “An integrated vulnerability assessment of electronic commerce websites,” *Int. J. Inf. Eng. Electron. Bus.*, vol. 12, no. 5, pp. 24–32, Oct. 2020.
- [117] A. Singh, A. Sharma, N. Sharma, I. Kaushik, and B. Bhushan, “Taxonomy of attacks on web based applications,” in *Proc. 2nd Int. Conf. Intell. Comput., Instrum. Control Technol. (ICICICT)*, vol. 1, Jul. 2019, pp. 1231–1235.
- [118] H. Ibrahim, “A review on the mechanism mitigating and eliminating Internet crimes using modern technologies: Mitigating Internet crimes using modern technologies,” *Wasit J. Comput. Math. Sci.*, vol. 1, no. 3, pp. 76–108, 2022.
- [119] T. Hu, Z. Zhang, P. Yi, D. Liang, Z. Li, Q. Ren, Y. Hu, and J. Lan, “SEAPP: A secure application management framework based on REST API access control in SDN-enabled cloud environment,” *J. Parallel Distrib. Comput.*, vol. 147, pp. 108–123, Jan. 2021.
- [120] I. M. M. Kaur, M. Raj, S. R., and H.-N. Lee, “Cross channel scripting and code injection attacks on web and cloud-based applications: A comprehensive review,” *Sensors*, vol. 22, no. 5, p. 1959, Mar. 2022.
- [121] N. Krishnamoorthy and S. Umarani, “An experimental study on cloud computing security issues and a framework for xml DDoS attack prevention,” *J. Phys., Conf. Ser.*, vol. 2007, no. 1, Aug. 2021, Art. no. 012058.
- [122] U. K. Jannat and M. Mohankumar, “Proposed on attack analysis using risk assessment and security risk assessment using attacks for cloud cyber security,” *Comput. Sci.*, vol. 3, p. 1, Mar. 2023.
- [123] R. Geetha, A. K. Suntheya, and G. U. Srikanth, “Cloud integrated IoT enabled sensor network security: Research issues and solutions,” *Wireless Pers. Commun.*, vol. 113, no. 2, pp. 747–771, Jul. 2020.
- [124] R. Ponnumani and N. Partheepan, “Various threats and attack on cloud computing: A review,” in *Proc. 5th Int. Conf. Contemp. Comput. Informat. (ICI)*, Dec. 2022, pp. 1296–1300.
- [125] M. Abbasi, M. Plaza-Hernández, J. Prieto, and J. M. Corchado, “Security in the Internet of Things application layer: Requirements, threats, and solutions,” *IEEE Access*, vol. 10, pp. 97197–97216, 2022.
- [126] S. Padmanaban, M. A. Nasab, M. E. Shiri, H. H. S. Javadi, M. A. Nasab, M. Zand, and T. Samavat, “The role of Internet of Things in smart homes,” in *Artificial Intelligence-based Smart Power Systems*. Hoboken, NJ, USA: Wiley, 2023, pp. 259–271.

- [127] M. Kumar, C. Kondaiah, A. R. Pais, and R. S. Rao, "Machine learning models for phishing detection from TLS traffic," *Cluster Comput.*, vol. 26, no. 5, pp. 3263–3277, Oct. 2023.
- [128] A. Gaurav, B. B. Gupta, W. Alhalabi, A. Visvizi, and Y. Asiri, "A comprehensive survey on DDoS attacks on various intelligent systems and its defense techniques," *Int. J. Intell. Syst.*, vol. 37, no. 12, pp. 11407–11431, Dec. 2022.
- [129] R. Ahuja and M. Gupta, "Improved heuristic framework for cyber security system on DDoS attack," *J. Data Acquisition Process.*, vol. 38, no. 3, p. 3033, 2023.
- [130] F. Shaikh, E. Bou-Harb, N. Neshenko, A. P. Wright, and N. Ghani, "Internet of Malicious Things: Correlating active and passive measurements for inferring and characterizing Internet-scale unsolicited IoT devices," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 170–177, Sep. 2018.
- [131] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, "Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications," *Autom. Construct.*, vol. 101, pp. 111–126, May 2019.
- [132] A. Shifa, M. N. Asghar, and M. Fleury, "Multimedia security perspectives in IoT," in *Proc. 6th Int. Conf. Innov. Comput. Technol. (INTECH)*, Aug. 2016, pp. 550–555.
- [133] "Conti cyber attack on the HSE," Nat. Cyber Secur. Centre, Dublin, Ireland, Tech. Rep. 2105161000-NCSC, 2021, Accessed: Dec. 15, 2023. [Online]. Available: [https://www.ncsc.gov.ie/pdfs/HSE\\_Conti\\_140521\\_UPDATE.pdf](https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf)
- [134] M. S. Akhtar and T. Feng, "A systemic security and privacy review: Attacks and prevention mechanisms over IoT layers," *EAI Endorsed Trans. Secur. Saf.*, vol. 8, no. 30, pp. 1–12, 2022.
- [135] M. A. Khatun, N. Chowdhury, and M. N. Uddin, "Malicious nodes detection based on artificial neural network in IoT environments," in *Proc. IEEE 22nd Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2019, pp. 1–6.
- [136] M. Al-Amin, M. A. Khatun, and M. N. Uddin, "Development of cyber attack model for private network," in *Proc. 2nd Int. Conf. Interdiscipl. Cyber Phys. Syst. (ICPS)*, May 2022, pp. 216–221.
- [137] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical dilemmas and privacy issues in emerging technologies: A review," *Sensors*, vol. 23, no. 3, p. 1151, Jan. 2023.
- [138] N. Comfort, "German banking regulator BaFin's website hit by cyber attack," Bloomberg, New York, NY, USA, Tech. Rep., Sep. 2023. Accessed: Dec. 15, 2023. [Online]. Available: <https://tinyurl.com/tmjaj7yn>
- [139] A. Raj, "Critical infrastructure cyberattack on Japan's biggest port," Tech Wire Asia, Kuala Lumpur, Malaysia, Tech. Rep., 2023. Accessed: Dec. 15, 2023. [Online]. Available: <https://tinyurl.com/2kn4mdxn>
- [140] K. A. Nagaty, "IoT commercial and industrial applications and AI-powered IoT," in *Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security*. Cham, Switzerland: Springer, 2023, pp. 465–500.
- [141] S. Gupta and B. B. Gupta, "Cross-site scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art," *Int. J. Syst. Assurance Eng. Manage.*, vol. 8, no. S1, pp. 512–530, Jan. 2017.
- [142] M. T. Louw and V. N. Venkatakrishnan, "Blueprint: Robust prevention of cross-site scripting attacks for existing browsers," in *Proc. 30th IEEE Symp. Secur. Privacy*, May 2009, pp. 331–346.
- [143] D. Lu, J. Fei, and L. Liu, "A semantic learning-based SQL injection attack detection technology," *Electronics*, vol. 12, no. 6, p. 1344, Mar. 2023.
- [144] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022.
- [145] S. M. Mathews, "Explainable artificial intelligence applications in NLP, biomedical, and malware classification: A literature review," in *Proc. Comput. Conf. Intell. Comput.*, vol. 2. Cham, Switzerland: Springer, 2019, pp. 1269–1292.
- [146] M. R. Islam, M. U. Ahmed, S. Barua, and S. Begum, "A systematic review of explainable artificial intelligence in terms of different application domains and tasks," *Appl. Sci.*, vol. 12, no. 3, p. 1353, Jan. 2022.
- [147] H. H. Nguyen, F. Mirza, M. A. Naeem, and M. Nguyen, "A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback," in *Proc. IEEE 21st Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, Apr. 2017, pp. 257–262.
- [148] S. S. Ram, B. Apduhan, and N. Shiratori, "A machine learning framework for edge computing to improve prediction accuracy in mobile health monitoring," in *Proc. 19th Int. Conf. Comput. Sci. Appl. (ICCSA)*, Saint Petersburg, Russia. Cham, Switzerland: Springer, Jul. 2019, pp. 417–431.
- [149] P. Vanin, T. Newe, L. L. Dhirani, E. O'Connell, D. O'Shea, B. Lee, and M. Rao, "A study of network intrusion detection systems using artificial intelligence/machine learning," *Appl. Sci.*, vol. 12, no. 22, p. 11752, Nov. 2022.
- [150] L. L. Dhirani, T. Newe, and S. Nizamani, "Hybrid multi-cloud demystifying slas for smart city enterprises using IoT applications," in *IoT Architectures, Models, and Platforms for Smart City Applications*. Hershey, PA, USA: IGI Global, 2020, pp. 52–67.
- [151] A. Sharma and U. K. Singh, "Modelling of smart risk assessment approach for cloud computing environment using AI & supervised machine learning algorithms," *Global Transitions Proc.*, vol. 3, no. 1, pp. 243–250, Jun. 2022.
- [152] F. Desai, D. Chowdhury, R. Kaur, M. Peeters, R. C. Arya, G. S. Wander, S. S. Gill, and R. Buyya, "HealthCloud: A system for monitoring health status of heart patients using machine learning and cloud computing," *Internet Things*, vol. 17, Mar. 2022, Art. no. 100485.
- [153] A. Abdelaziz, A. S. Salama, A. Riad, and A. N. Mahmoud, "A machine learning model for predicting of chronic kidney disease based Internet of Things and cloud computing in smart cities," in *Security in Smart Cities: Models, Applications, and Challenges*. Cham, Switzerland: Springer, 2019, pp. 93–114.
- [154] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and privacy in IoT-cloud-based e-health systems—A comprehensive review," *Symmetry*, vol. 12, no. 7, p. 1191, Jul. 2020.
- [155] M. Maksimović and V. Vujović, "Internet of Things based e-health systems: Ideas, expectations and concerns," in *Handbook of Large-Scale Distributed Computing in Smart Healthcare*. Cham, Switzerland: Springer, 2017, pp. 241–280.
- [156] D. Zhang, J. J. P. C. Rodrigues, Y. Zhai, and T. Sato, "Design and implementation of 5G e-health systems: Technologies, use cases, and future challenges," *IEEE Commun. Mag.*, vol. 59, no. 9, pp. 80–85, Sep. 2021.
- [157] M. S. Hossain, S. U. Amin, M. Alsulaiman, and G. Muhammad, "Applying deep learning for epilepsy seizure detection and brain mapping visualization," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, no. 1s, pp. 1–17, Jan. 2019.
- [158] C. Hewson, C. Vogel, and D. Laurent, *Internet Research Methods*. Newbury Park, CA, USA: Sage, 2015.
- [159] H. Asri, "IoT and reality mining for real-time disease prediction," in *IoT and Smart Devices for Sustainable Environment*. Cham, Switzerland: Springer, 2022, pp. 85–102.
- [160] F. D. G. Solfa and F. R. Simonato, "Big data analytics in healthcare: Exploring the role of machine learning in predicting patient outcomes and improving healthcare delivery," *Int. J. Comput., Inf. Manuf.*, vol. 3, no. 1, pp. 1–9, 2023.
- [161] G. Arji, H. Ahmadi, P. Avazpoor, and M. Hemmat, "Identifying resilience strategies for disruption management in the healthcare supply chain during COVID-19 by digital innovations: A systematic literature review," *Inform. Med. Unlocked*, vol. 38, Feb. 2023, Art. no. 101199.
- [162] L. L. Dhirani, T. Newe, and S. Nizamani, "Can IoT escape cloud QoS and cost pitfalls," in *Proc. 12th Int. Conf. Sens. Technol. (ICST)*, Dec. 2018, pp. 65–70.
- [163] H. Asri and Z. Jarir, "Toward a smart health: Big data analytics and IoT for real-time miscarriage prediction," *J. Big Data*, vol. 10, no. 1, pp. 1–23, Mar. 2023.
- [164] G. Sasubilli and A. Kumar, "Machine learning and big data implementation on health care data," in *Proc. 4th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2020, pp. 859–864.
- [165] A. D. C. Barriga, A. F. Martins, M. J. Simões, and D. Faustino, "The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?" *Social Sci. Humanities Open*, vol. 2, no. 1, 2020, Art. no. 100096.
- [166] S. D. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in IoT-based healthcare environment," *J. Reliable Intell. Environ.*, vol. 6, no. 1, pp. 3–13, Mar. 2020.
- [167] E. Gelenbe and M. Nakip, "Real-time cyberattack detection with offline and online learning," in *Proc. IEEE 29th Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jul. 2023, pp. 1–6.

- [168] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 30–35.
- [169] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, and C. Del-Valle-Soto, "Utilization of 5G technologies in IoT applications: Current limitations by interference and network optimization difficulties—A review," *Sensors*, vol. 23, no. 8, p. 3876, Apr. 2023.
- [170] A. M. Seid, A. Erbad, H. N. Abishu, A. Albaseer, M. Abdallah, and M. Guizani, "Multi-agent federated reinforcement learning for resource allocation in UAV-enabled Internet of Medical Things networks," *IEEE Internet Things J.*, p. 1, 2023.
- [171] A. Rai, D. K. Singh, A. Sehgal, and K. Cengiz, *Paradigms of Smart and Intelligent Communication, 5G and Beyond*. Singapore: Springer, 2023.
- [172] M. Vermanen, M. M. Rantanen, and V. Harkke, "Ethical framework for IoT deployment in SMEs: Individual perspective," *Internet Res.*, vol. 32, no. 7, pp. 185–201, Dec. 2022.
- [173] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, pp. 1–18, Dec. 2020.
- [174] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet Things*, vol. 15, Sep. 2021, Art. no. 100420.
- [175] L. Phillips, "Healthcare cybersecurity in 2023: Hive's shutdown is good news but cyberattacks are only getting worse," *Insider Intell.*, Jan. 2023. [Online]. Available: <https://tinyurl.com/mryu9yc>
- [176] J. McKeon, "Biggest healthcare data breaches reported this year, so far," TechTarget, Newton, MA, USA, Tech. Rep., 2023. [Online]. Available: <https://tinyurl.com/2s3t6dmh>
- [177] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.
- [178] J. Qiu, X. Liang, S. Shetty, and D. Bowden, "Towards secure and smart healthcare in smart cities using blockchain," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2018, pp. 1–4.
- [179] I. R. Vanani and M. Amirhosseini, "IoT-based diseases prediction and diagnosis system for healthcare," in *Internet of Things for Healthcare Technologies*. Singapore: Springer, 2021, pp. 21–48.
- [180] A. W. Kempa-Liehr, C. Y.-C. Lin, R. Britten, D. Armstrong, J. Wallace, D. Mordaunt, and M. O'Sullivan, "Healthcare pathway discovery and probabilistic machine learning," *Int. J. Med. Informat.*, vol. 137, May 2020, Art. no. 104087.
- [181] A. U. Haq, J. P. Li, J. Khan, M. H. Memon, S. Nazir, S. Ahmad, G. A. Khan, and A. Ali, "Intelligent machine learning approach for effective recognition of diabetes in e-healthcare using clinical data," *Sensors*, vol. 20, no. 9, p. 2649, May 2020.
- [182] R. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, "Artificial intelligence (AI) applications for COVID-19 pandemic," *Diabetes Metabolic Syndrome, Clin. Res. Rev.*, vol. 14, no. 4, pp. 337–339, 2020.
- [183] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol. 121, Mar. 2023, Art. no. 102583.
- [184] A. J. Cartwright, "The elephant in the room: Cybersecurity in healthcare," *J. Clin. Monitor. Comput.*, vol. 37, no. 5, pp. 1123–1132, Oct. 2023.
- [185] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insightsing cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100016.
- [186] M. Kumar, A. Kumar, S. Verma, P. Bhattacharya, D. Ghimire, S.-H. Kim, and A. S. M. S. Hosen, "Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues," *Electronics*, vol. 12, no. 9, p. 2050, Apr. 2023.
- [187] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Comput. Electr. Eng.*, vol. 107, Apr. 2023, Art. no. 108626.
- [188] M. Khatkar, K. Kumar, B. Kumar, and P. Agarwal, "Parametric influence of intrusion detection system in healthcare sector using deep neural [LSTM] network," *J. Pharmaceutical Negative Results*, vol. 14, no. 1, pp. 685–692, 2023.
- [189] S. Ksibi, F. Jaidi, and A. Bouhoula, "IoMT security model based on machine learning and risk assessment techniques," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2023, pp. 614–619.
- [190] K. Bouabida, B. Lebouché, and M.-P. Pomey, "Telehealth and COVID-19 pandemic: An overview of the telehealth use, advantages, challenges, and opportunities during COVID-19 pandemic," *Healthcare*, vol. 10, no. 11, p. 2293, Nov. 2022.
- [191] L. Wang and R. Jones, "Big data, cybersecurity, and challenges in healthcare," in *Proc. SoutheastCon*, Apr. 2019, pp. 1–6.
- [192] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018.
- [193] S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 131–144, Jan. 2023.
- [194] T. Thulasi and K. Sivamohan, "LSO-CSL: Light spectrum optimizer-based convolutional stacked long short term memory for attack detection in IoT-based healthcare applications," *Expert Syst. Appl.*, vol. 232, Dec. 2023, Art. no. 120772.
- [195] K. Gupta, D. K. Sharma, K. D. Gupta, and A. Kumar, "A tree classifier based network intrusion detection model for Internet of Medical Things," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108158.
- [196] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," *IEEE Access*, vol. 8, pp. 106576–106584, 2020.
- [197] S. Saif, P. Das, S. Biswas, M. Khari, and V. Shanmuganathan, "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare," *Microprocessors Microsyst.*, Aug. 2022, Art. no. 104622.
- [198] S. Ray, K. N. Mishra, and S. Dutta, "Detection and prevention of DDoS attacks on M-healthcare sensitive data: A novel approach," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1333–1341, May 2022.
- [199] A. Kumar, R. S. Umurzoqovich, N. D. Duong, P. Kanani, A. Kuppusamy, M. Praneesh, and M. N. Hieu, "An intrusion identification and prevention for cloud computing: From the perspective of deep learning," *Optik*, vol. 270, Nov. 2022, Art. no. 170044.
- [200] R. M. S. Priya, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020.
- [201] S. O. M. Kamel and S. A. Elhamayed, "Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network," *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 4, pp. 11–29, Aug. 2020.
- [202] N. Terry, "Existential challenges for healthcare data protection in the united states," *Ethics, Med. Public Health*, vol. 3, no. 1, pp. 19–27, Jan. 2017.
- [203] M. Bansal and Priya, "Application layer protocols for Internet of Healthcare Things (IoHT)," in *Proc. 4th Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2020, pp. 369–376.
- [204] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.
- [205] B. Mittelstadt, "Designing the health-related Internet of Things: Ethical principles and guidelines," *Information*, vol. 8, no. 3, p. 77, Jul. 2017.
- [206] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6LoWPAN of Internet of Things," *Sensors*, vol. 22, no. 9, p. 3400, Apr. 2022.
- [207] R. Saminathan, S. Saravanan, and P. Anbalagan, "Blockchain in healthcare: A new dimension to healthcare data security," in *Hybridization of Blockchain and Cloud Computing: Overcoming Security Issues in IoT*. New York, NY, USA: Taylor & Francis Group, 2023, p. 45.
- [208] B. H. Patel and P. Shah, "RPL routing protocol performance under sinkhole and selective forwarding attack: Experimental and simulated evaluation," *TELKOMNIKA, Telecommun. Comput. Electron. Control*, vol. 18, no. 4, pp. 1849–1856, 2020.
- [209] I. Tomic and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.
- [210] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT smart health security threats," in *Proc. 19th Int. Conf. Comput. Sci. Its Appl. (ICCSA)*, Jul. 2019, pp. 26–31.

- [211] F. Zahra, N. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and wormhole attack detection model for RPL-based Internet of Things using machine learning," *Sensors*, vol. 22, no. 18, p. 6765, Sep. 2022.
- [212] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023.
- [213] A. Haghrah, M. P. Abdollahi, H. Azarhava, and J. M. Niya, "A survey on the handover management in 5G-NR cellular networks: Aspects, approaches and challenges," *EURASIP J. Wireless Commun. Netw.*, vol. 2023, no. 1, pp. 1–57, Jun. 2023.
- [214] T. M. Ghazal, "Retracted article: Positioning of UAV base stations using 5G and beyond networks for IoMT applications," *Arabian J. Sci. Eng.*, vol. 48, no. 4, p. 5687, Apr. 2023.
- [215] A. Peivandizadeh and B. Molavi, "Compatible authentication and key agreement protocol for low power and lossy network in IoT environment," *Social Sci. Res. Netw. (SSRN)*, Amsterdam, The Netherlands, Tech. Rep. 4454407, 2023.
- [216] Y. Rbah, M. Mahfoudi, Y. Balboul, M. Fattah, S. Mazer, M. Elbekkali, and B. Bernoussi, "Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey," in *Proc. 2nd Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, Mar. 2022, pp. 1–9.
- [217] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications," *Sensors*, vol. 21, no. 19, p. 6346, Sep. 2021.
- [218] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—A review," *J. Cybersecurity Privacy*, vol. 2, no. 3, pp. 527–555, Jul. 2022.
- [219] P. N. Mahalle, G. R. Shinde, Y. S. Ingle, and N. N. Wasatkar, "Data-centric AI in information, communication and technology," in *Data Centric Artificial Intelligence: A Beginner's Guide*. Singapore: Springer, 2023, pp. 109–124.
- [220] I. N. R. Hendrawan and I. G. N. W. Arsa, "Zolertia z1 energy usage simulation with cooja simulator," in *Proc. 1st Int. Conf. Informat. Comput. Sci. (ICICoS)*, Nov. 2017, pp. 147–152.
- [221] E. Q. Shahra, T. R. Sheltami, and E. M. Shakshuki, "A comparative study of range-free and range-based localization protocols for wireless sensor network: Using COOJA simulator," in *Sensor Technology: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2020, pp. 1522–1537.
- [222] Q. Wang, Y. Ma, K. Zhao, and Y. Tian, "A comprehensive survey of loss functions in machine learning," *Ann. Data Sci.*, vol. 9, no. 2, pp. 187–212, Apr. 2022.
- [223] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 160, May 2021.
- [224] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 524–552, 1st Quart., 2021.
- [225] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 112392–112415, 2022.
- [226] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of IoT security challenges and its solutions using artificial intelligence," *Brain Sci.*, vol. 13, no. 4, p. 683, Apr. 2023.
- [227] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects," *Ann. Data Sci.*, vol. 10, no. 6, pp. 1473–1498, Dec. 2023.
- [228] I. H. Sarker, "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100393.
- [229] D. Alahakoon, R. Nawaratne, Y. Xu, D. De Silva, U. Sivarajah, and B. Gupta, "Self-building artificial intelligence and machine learning to empower big data analytics in smart cities," *Inf. Syst. Frontiers*, vol. 25, no. 1, pp. 221–240, Feb. 2023.
- [230] K. Kumar and B. P. Pande, "Applications of machine learning techniques in the realm of cybersecurity," in *Cyber Security and Digital Forensics*. Hoboken, NJ, USA: Wiley, 2022, pp. 295–315.
- [231] V. Ravi, T. D. Pham, and M. Alazab, "Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1–10, Aug. 2022.
- [232] A. Singla and E. Bertino, "How deep learning is making information security more intelligent," *IEEE Secur. Privacy*, vol. 17, no. 3, pp. 56–65, May 2019.
- [233] S. Roobini, M. Kavitha, M. Sujaritha, and D. R. Kumar, "Cyber-security threats to IoMT-enabled healthcare systems," in *Cognitive Computing for Internet of Medical Things*. London, U.K.: Chapman & Hall, 2022, pp. 105–130.
- [234] Q. Qiao and A. Yunusa-Kaltungo, "A hybrid agent-based machine learning method for human-centred energy consumption prediction," *Energy Buildings*, vol. 283, Mar. 2023, Art. no. 112797.
- [235] B. Sharma, L. Sharma, and C. Lal, "Feature selection and deep learning technique for intrusion detection system in IoT," in *Proc. Int. Conf. Comput. Intell. (ICCI)*. Singapore: Springer, 2022, pp. 253–261.
- [236] P. R. S. Rohith and H. Rathore, "Sentiment analysis of IMDb movie reviews: A comparative analysis of feature selection and feature extraction techniques," in *Proc. 21st Int. Conf. Hybrid Intell. Syst. (HIS)*, vol. 420, Cham, Switzerland: Springer, 2022, p. 283.
- [237] A. Z. Ul-Saufie, N. H. Hamzan, Z. Zahari, W. N. Shazayani, N. M. Noor, M. R. R. M. A. Zainol, A. V. Sandu, G. Deak, and P. Vizureanu, "Improving air pollution prediction modelling using wrapper feature selection," *Sustainability*, vol. 14, no. 18, p. 11403, Sep. 2022.
- [238] Doreswamy, M. K. Hooshmand, and I. Gad, "Feature selection approach using ensemble learning for network anomaly detection," *CAAI Trans. Intell. Technol.*, vol. 5, no. 4, pp. 283–293, Dec. 2020.
- [239] D. He, Q. Qiao, Y. Gao, J. Zheng, S. Chan, J. Li, and N. Guizani, "Intrusion detection based on stacked autoencoder for connected healthcare systems," *IEEE Netw.*, vol. 33, no. 6, pp. 64–69, Nov. 2019.
- [240] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of machine learning based intrusion detection methods for Internet of Medical Things," *Appl. Soft Comput.*, vol. 140, Jun. 2023, Art. no. 110227.
- [241] O. Taouali, S. Bacha, K. B. Abdellaouf, A. Aljuhani, K. Zidi, R. Alanazi, and M. F. Harkat, "Intelligent intrusion detection system for the Internet of Medical Things based on data-driven techniques," *Comput. Syst. Sci. Eng.*, vol. 47, no. 2, pp. 1593–1609, 2023.
- [242] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020.
- [243] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021.
- [244] A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tili, and A. Erbad, "Edge computing for smart health: Context-aware approaches, opportunities, and challenges," *IEEE Netw.*, vol. 33, no. 3, pp. 196–203, May 2019.
- [245] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.
- [246] A. Ukil, S. Bandyopadhyay, C. Puri, and A. Pal, "IoT healthcare analytics: The importance of anomaly detection," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2016, pp. 994–997.
- [247] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 3648–3656.
- [248] A. Mehra, M. Mandal, P. Narang, and V. Chamola, "Correction to 'reviewnet: A fast and resource optimized network for enabling safe autonomous driving in hazy weather conditions,'" *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, p. 2888, Mar. 2022.
- [249] R. A. Mohammed and K. M. A. Alheeti, "Intrusion detection system for healthcare based on convolutional neural networks," in *Proc. Iraqi Int. Conf. Commun. Inf. Technol. (IICCIT)*, Sep. 2022, pp. 216–221.
- [250] D. Gil, M. Johnsson, H. Mora, and J. Szymanski, "Review of the complexity of managing big data of the Internet of Things," *Complexity*, vol. 2019, pp. 1–12, Feb. 2019.
- [251] L. Datta, "A survey on activation functions and their relation with xavier and he normal initialization," 2020, *arXiv:2004.06632*.

- [252] V. Andrcarczyk and P. F. Whelan, "Convolutional neural network on three orthogonal planes for dynamic texture classification," *Pattern Recognit.*, vol. 76, pp. 36–49, Apr. 2018.
- [253] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," *Proc. IEEE*, vol. 105, no. 12, pp. 2295–2329, Dec. 2017.
- [254] K. Khalil, O. Eldash, A. Kumar, and M. Bayoumi, "Designing novel AAD pooling in hardware for a convolutional neural network accelerator," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 3, pp. 303–314, Mar. 2022.
- [255] R. Nirthika, S. Manivannan, A. Ramanan, and R. Wang, "Pooling in convolutional neural networks for medical image analysis: A survey and an empirical study," *Neural Comput. Appl.*, vol. 34, no. 7, pp. 5321–5347, Apr. 2022.
- [256] A. Sharma, S. Rani, S. H. Shah, R. Sharma, F. Yu, and M. M. Hassan, "An efficient hybrid deep learning model for denial of service detection in cyber physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 1–10, Sep./Oct. 2023.
- [257] N. Faruqui, M. A. Yousuf, M. Whaiduzzaman, A. Azad, S. A. Alyami, P. Liò, M. A. Kabir, and M. A. Moni, "SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization," *Electronics*, vol. 12, no. 17, p. 3541, Aug. 2023.
- [258] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100059.
- [259] R. Patgiri, H. Katari, R. Kumar, and D. Sharma, "Empirical study on malicious URL detection using machine learning," in *Proc. 15th Int. Conf. Distrib. Comput. Internet Technol. (ICDCIT)*, Bhubaneswar, India, Cham, Switzerland: Springer, Jan. 2019, pp. 380–388.
- [260] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, "Anomaly detection in Internet of Medical Things with blockchain from the perspective of deep neural network," *Inf. Sci.*, vol. 617, pp. 133–149, Dec. 2022.
- [261] S. Chaudhary, R. Kakkar, N. K. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, M. D. Alshehri, R. Sharma, G. Sharma, and I. E. Davidson, "A taxonomy on smart healthcare technologies: Security framework, case study, and future directions," *J. Sensors*, vol. 2022, pp. 1–30, Jul. 2022.
- [262] S. Rajendran, R. K. Panneerselvam, P. J. Kumar, V. A. Rajasekaran, P. Suganya, S. K. Mathivanan, and P. Jayagopal, "Prescreening and triage of COVID-19 patients through chest X-ray images using deep learning model," *Big Data*, vol. 11, no. 6, pp. 408–419, Dec. 2023.
- [263] Z. Hau and E. C. Lupu, "Exploiting correlations to detect false data injections in low-density wireless sensor networks," in *Proc. 5th Cyber-Physical Syst. Secur. Workshop*, Jul. 2019, pp. 1–12.
- [264] M. Begli, F. Derakhshan, and H. Karimipour, "A layered intrusion detection system for critical infrastructure using machine learning," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2019, pp. 120–124.
- [265] S. Sengan, O. I. Khalaf, V. P. Sagar, D. K. Sharma, A. L. J. Prabhu, and A. A. Hamad, "Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach," *Int. J. Reliable Quality E-Healthcare*, vol. 11, no. 3, pp. 1–11, Oct. 2021.
- [266] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167, 2nd Quart., 2020.
- [267] R. Sharma, "Software-defined networking for healthcare Internet of Things," in *Applications of Machine Learning in Big-Data Analytics and Cloud Computing*. New York, NY, USA: River Publishers, 2022, pp. 231–247.
- [268] P. Ajmani and P. Saigal, "5G and IoT for smart farming," in *Applying Drone Technologies and Robotics for Agricultural Sustainability*. Hershey, PA, USA: IGI Global, 2023, pp. 124–139.
- [269] L. M. Broell, C. Hanshans, and D. Kimmerle, "IoT on an ESP32: Optimization methods regarding battery life and write speed to an SD-card," *InTechOpen*, Rijeka, Tech. Rep., 2023.
- [270] D. Gowda V, A. Sharma, B. K. Rao, R. Shankar, P. Sarma, A. Chaturvedi, and N. Hussain, "Industrial quality healthcare services using Internet of Things and fog computing approach," *Measurement, Sensors*, vol. 24, Dec. 2022, Art. no. 100517.
- [271] S. Sutradhar, S. Karforma, R. Bose, and S. Roy, "A dynamic step-wise tiny encryption algorithm with fruit fly optimization for quality of service improvement in healthcare," *Healthcare Anal.*, vol. 3, Nov. 2023, Art. no. 100177.
- [272] M. Adil, J. Ali, M. M. Jadoon, S. R. Alotaibi, N. Kumar, A. Farouk, and H. Song, "COVID-19: Secure healthcare Internet of Things networks, current trends and challenges with future research directions," *ACM Trans. Sensor Netw.*, vol. 19, no. 3, pp. 1–25, Aug. 2023.
- [273] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven healthcare 4.0 technologies: A survey, current challenges and future directions," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 1, pp. 361–407, Jan. 2023.
- [274] F. Sallabi, F. Naeem, M. Awad, and K. Shuaib, "Managing IoT-based smart healthcare systems traffic with software defined networks," in *Proc. Int. Symp. Netw. Comput. Commun. (ISNCC)*, Jun. 2018, pp. 1–6.
- [275] J. H. Abawajy and M. M. Hassan, "Federated Internet of Things and cloud computing pervasive patient health monitoring system," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 48–53, Jan. 2017.
- [276] R. Taheri, H. Ahmed, and E. Arslan, "Deep learning for the security of software-defined networks: A review," *Cluster Comput.*, vol. 26, no. 5, pp. 3089–3112, Oct. 2023.
- [277] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks," *Appl. Sci.*, vol. 13, no. 6, p. 3828, Mar. 2023.
- [278] M. Ciciglu and A. Çalhan, "A multiprotocol controller deployment in SDN-based IoMT architecture," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 20833–20840, Nov. 2022.
- [279] V. Lakshminarayanan, A. Ravikumar, H. Sriraman, S. Alla, and V. K. Chattu, "Health care equity through intelligent edge computing and augmented reality/virtual reality: A systematic review," *J. Multidisciplinary Healthcare*, vol. 16, pp. 2839–2859, Sep. 2023.
- [280] A. S. Ahmed and H. A. Salah, "Development a software defined network (SDN) with Internet of Things (IoT) security for medical issues," *J. Al-Qadisiyah Comput. Sci. Math.*, vol. 15, no. 3, p. 98, Sep. 2023.

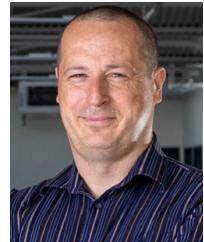


**MIRZA AKHI KHATUN** (Member, IEEE) received the B.Sc. degree in computer science and engineering and the M.Sc. degree in computer science and engineering from Jagannath University, Bangladesh, focusing on Internet of Things (IoT) security and machine learning, in 2019. She is currently pursuing the Ph.D. degree with the Department of Electronic and Computer Engineering, University of Limerick, Ireland. Her ongoing research delves into the healthcare-IoT security and utilizing AI/ML innovations. She has an exemplary academic background, underscored by a scholarship from the Science Foundation Ireland Centre for Research Training in Foundations of Data Science awarded, in 2022. During the master's program, she secured the first position in her class. She has also published research papers at renowned IEEE international conferences. Her research interests include the IoT, artificial intelligence, machine learning, data analysis, network security, and systems architecture. She is also reflecting her deep commitment to the professional community.



**SANOBER FARHEEN MEMON** (Member, IEEE) received the B.Eng. degree in electronic engineering and the M.Eng. degree in electronic systems engineering from the Mehran University of Engineering & Technology (MUET), Jamshoro, Pakistan, in 2010 and 2014, respectively, and the Ph.D. degree in electronic and computer engineering from the University of Limerick, Ireland, in 2023. She is currently a Researcher on the OXI-SMART Project with the Optical Fibre Sensors Research Centre, Department of Electronic and Computer Engineering (ECE), UL. During the Ph.D. research, she developed plastic optical fiber sensors for in-situ and real-time ultra-low-level ethanol concentration measurement in microalgal bioethanol production applications. She was with MUET, Pakistan, for more than three years as a Faculty Member (a Lecturer and a Visiting Lecturer) and taught a variety of modules to the B.Eng. students. Her current research interests include

optical fiber sensors, medical sensors, photonics engineering, instrumentation and measurement, and intelligent systems. She has received multiple funding grants, including the European Union EM INTACT Doctorate Scholarship, UL Postgraduate Residential Scholarship, UL Funding & ECE Departmental Funding, Merit Scholarship from MUET, and some international travel/conference participation grants. She is a member of IEEE WIE, IEEE Photonics Society, IEEE Instrumentation & Measurement Society, and SPIE.



**Ciarán Eisling** (Senior Member, IEEE) received the B.E. degree in electronic and computer engineering and the Ph.D. degree from NUI Galway, in 2003 and 2010, respectively. From 2009 to 2020, he was a Computer Vision Architect Senior Expert with Valeo. In 2020, he joined the University of Limerick as an Associate Professor in AI.



**LUBNA LUXMI DHIRANI** (Senior Member, IEEE) received the B.Eng. degree in computer systems, the M.Sc. degree in business information technology, and the Ph.D. degree in hybrid cloud computing QoS and SLA-based issues in heterogenous cloud environment. She is currently an Assistant Professor with Department of Electronic and Computer Engineering, University of Limerick. She is also the Course Director of the B.Sc. Cybersecurity Practitioner Apprenticeship Program. She is also the first WIE Ambassador from Ireland in the IEEE WIE (U.K.&I Section) and a member of the National Standards Authority of Ireland (NSAI). She has worked on interdisciplinary, industry-based projects securing machine-to-machine communications in industry 4.0, V2I safety and security, and digital healthcare. Her publications are listed at: [Google Scholar](#), she has delivered more than 35 technical workshops, tutorials, masterclasses, panel, and keynote speeches at international conferences and platforms. Her research interests include cybersecurity, privacy, data governance, risk, cyber law, regulations, the IIoT, IT/OT, and cloud and security standards.

• • •