Security and Privacy

WILEY

RESEARCH ARTICLE OPEN ACCESS

IoT and Man-in-the-Middle Attacks

Hamidreza Fereidouni[1] | Olga Fadeitcheva[2] | Mehdi Zalai[2]

[1]Department of Computer Science and Operations Research, University of Montreal, Montreal, Quebec, Canada | [2]Department of Computer Engineering and Software Engineering, Polytechnique Montreal, Montreal, Quebec, Canada

Correspondence: Hamidreza Fereidouni (hamidreza.fereidouni@umontreal.ca)

Received: 4 April 2024 | **Revised:** 29 November 2024 | **Accepted:** 17 February 2025

Funding: The authors received no specific funding for this work.

Keywords: Internet of Things | IoT | IoT security | Man-in-the-Middle | MitM | MitM detection | MitM prevention

ABSTRACT

This article provides an overview of the Internet of things (IoT) and its growing significance in today's interconnected world. It discusses the concept of man-in-the-middle (MitM) attacks in detail, including their various types, causes, and potential impacts on IoT networks. The article analyzes MitM attacks at different layers of the IoT architecture and explores current prevention techniques and mitigation strategies. It addresses the challenges in detecting and preventing such attacks, particularly in the context of the heterogeneous and resource-constrained nature of IoT devices. The article also examines emerging technologies, such as machine learning and blockchain, for enhancing IoT security. Furthermore, it discusses open issues, including the challenges of prevention, the potential impact of new technologies, and future trends in MitM attacks. By exploring these aspects, the article aims to provide insights into improving detection and prevention mechanisms against MitM attacks in IoT environments.

1 | Introduction

Today, the Internet plays a pivotal role in our lives. The Internet can be primitively considered a network of networks. Moreover, it is technically defined as a unified, interconnected system of computer networks, from educational computer networks to governmental ones, which operate on predefined, accepted networking protocols [1]. Conventionally, we use the Internet to do our daily routines, from official correspondence and private communications to buying goods and banking operations. The Internet of things (IoT) is defined as a network of physical objects comprising sensors and actuators, and connections, which allows these things to connect and trade data through the Internet [2]. This concept, independent of this name, has been around for more than two decades since the unveiling of the Internet publicly.

IoT has facilitated our modern life, from industries to our personal life. For instance, a smart home utilizes IoT to provide residents with a better experience of living. The fundamental goal of IoT innovations is to provide connectivity and improve the quality of life (QoL) for clients. On a hot summer day, a smart home can determine if its resident is returning home, check the temperature and lighting level, and then make the home ready for the resident by turning on the air conditioners and the necessary lamps. Therefore, it can help us save energy while maintaining suitable living conditions. Given this example, we readily find the term IoT as an augmented utility of the Internet, which is growing rapidly in numbers and applications. Given this context, the world has witnessed to a burgeoning ecosystem of IoT in terms of economics and the number of connected devices. Based on the IoT Analytics reports, the global market size is predicted to grow 15% annually and reach around $690 billion in spending on enterprise IoT technologies by 2030 [3]. Besides, IoT Analytics mentions that in 2023, 16.6 billion IoT devices were connected to the Internet, with forecasts predicting more than 40 billion IoT devices to be connected by 2030 [4]. This might be

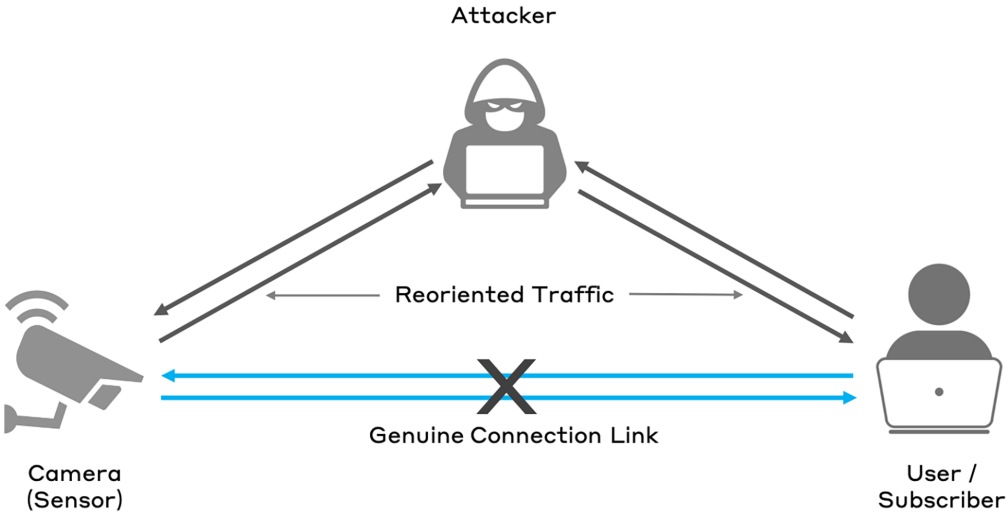

FIGURE 1 | A general schema of man-in-the-middle attack.

a conservative prediction, because other predictions show higher numbers of connected devices.

Internet users are witnessing a remarkable increase in the types and number of security and privacy issues when facing these emerging, fast-growing technologies. Due to the number of connected devices and volume of data exchanged among these devices, data leakage, authentication, and identification could be named as some of the major security vulnerabilities in the IoT. This matter becomes substantial when security analysts realize that 98% of all traffic among IoT devices is unencrypted [5]. Therefore, there are well-known threats and attacks, such as distributed denial of service (DDoS) and man-in-the-middle (MitM), which are commonly able to compromise IoT-based systems. DDoS is the most popular attack because of ease of launch and no need for complex, time-consuming exploitations [6]. DDoS is a security threat that can mainly disturb the availability of services. MitM can overshadow all security and privacy facets of a system. MitM attacks are usually more complex than other attacks and difficult to identify [7]. MitM, also known as on-path attack, refers to a category of attacks where a perpetrator positions themselves between two communicating parties to gain control of the communication channel. By reorienting the original connection link (as shown in Figure 1), they can intercept and/or alter the data being exchanged [8].

IoT and its innovative applications penetrate every facet of human life, from industrial automation to novel medical technologies. Although IoT is a widely discussed and disruptive concept in the current Internet landscape, there is currently no universally accepted security standard or framework among most businesses, despite conventional security standards that could be adapted for IoT-based environments [9]. However, there are some proposed best practices such as OWASP [10, 11], IoT Security Maturity Model (by Industry IoT Consortium) [12], and National Institute of Standards and Technology (NIST) Cybersecurity for IoT Program [13]. This situation poses a significant challenge for ensuring the security and privacy of IoT systems due to the heterogeneity of devices and protocols, as well as the wide variety of use cases that IoT-based systems can support. In these environments, there are various types of machines, sensors, and actuators with their authentic situation, protocol, and operation. These define a network with so many different nodes trading numerous transactions. This heterogeneous situation makes business bodies vulnerable to many various threats.

According to recent reputable reports, a significant percentage of secured hypertext transfer protocol (HTTPS) servers are vulnerable to MitM attacks due to misconfigurations, outdated protocols, and weak cipher suites [14]. These findings increase the significance of MitM attacks, mainly when they occur in IoT environments where a large amount of sensitive data may be exchanged among unsecured, heterogeneous devices. Furthermore, in many cases, MitM is intrinsically considered an advanced persistent threat (APT) because of the difficulty of detection. According to this, many regular and commonly used intrusion detection systems (IDS) even cannot differentiate and identify MitM properly [15]. Thus, MitM can be considered one of the most dangerous threats in telecommunication and computer networks, which influence both the security and privacy sides of a system.

This article explores proactive security measures and methods of identifying MitM attacks in IoT environments. It highlights important considerations to maximize the prevention of MitM in IoT systems. First, in the second section, the article provides a general overview of IoT and MitM attacks. Second, in the third section, it discusses the methodology we consider in this article. Third, in the fourth section, it delves into the vulnerabilities in IoT environments, analyzes MitM attacks in these settings, and examines current prevention techniques. Finally, in the fifth section, the article discusses future trends and challenges in the field.

2 | Background and Theory

2.1 | Description of IoT Devices and Architecture

The IoT is characterized by connected devices that can collect and transmit data. The subscriber–publisher model, implemented in

the message queuing telemetry transport (MQTT) protocol [16], is a common approach in IoT. Publishers, such as sensors, generate and send data to other devices, whereas subscribers receive data from publishers and can be devices such as actuators or users. This model enables efficient data exchange and communication between devices in IoT applications, resulting in the main four types of devices in IoT:

- Sensors: IoT devices rely heavily on sensors to collect and transmit data from the physical world, enabling monitoring, control, automation, services, and application. IoT sensors mostly transmit data wirelessly using protocols such as Wi-Fi, Bluetooth, and Zigbee.
- Actuators: IoT actuators convert digital commands into physical actions, enabling IoT devices to interact with the physical world.
- Broker: an IoT broker or gateway serves as a mediator between IoT devices and cloud-based services, performing tasks such as data filtering, translation, security, and storage. Brokers enable IoT devices to communicate with cloud-based platforms and facilitate local processing and analysis of IoT data.
- Users' devices: users are individuals who interact with an IoT system to access and control its services or applications through different interfaces. They play a crucial role in the successful adoption and operation of IoT systems by providing feedback and insights.

Figure 2 illustrates the devices commonly found in an IoT system, such as sensors (e.g., security cameras, smart home sensors), actuators (e.g., the speaker), and brokers that connect the elements. The figure also shows a router for Internet connectivity and a user interface for remote monitoring and control.

The IoT infrastructure is organized into interconnected layers (as shown in Figure 3), each serving distinct purposes. Cloud layer provides comprehensive services including analysis, batch processing, scheduling, monitoring, autoscaling, and storage capabilities for long-term data management and complex computations. Fog layer acts as an intermediary processing tier equipped with accelerators, network management, control systems, local storage, and computational resources to handle time-sensitive operations and reduce network congestion. Edge layer comprises multiple edge nodes that process data closer to its source, enabling quick decision-making and data filtering before transmission to higher layers. IoT devices-including industrial robots, energy systems, home appliances, connected vehicles, and surveillance systems-collect and transmit data while interacting with their environment. This layered architecture enables a streamlined flow of data and processing capabilities, with each layer performing specific functions to support the overall IoT ecosystem.

Another substantial subject in IoT is communication methods. IoT devices communicate using networking protocols across different layers. To comprehend the IoT domain, it is essential to define the constituent layers and elements of IoT and use them to delineate potential IoT architectures aligned with requisite services and fields. While IoT architecture is often divided into 3, 4, or 5 layers [17], from a computer networking perspective, the 3-layer model is more relevant, consisting of the application layer, network layer, and physical and link layer. Based on the inter-networking transmission control protocol (TCP)/IP protocol stack and OSI model, as shown in Figure 4, IoT protocols can be categorized into four logical layers [18]. The application layer includes protocols such as MQTT, advanced message queuing protocol [19], constrained application protocol (CoAP) [20, 21], and hypertext transfer protocol (HTTP) [19]. The transport and network layers utilize user datagram protocol [22], TCP [22], Internet Protocol version 4 and 6 (IPv4 and IPv6), and datagram transport layer security (DTLS) [21]. The physical and link layer uses technologies such as Wi-Fi, Bluetooth, and Zigbee. Finally, the perception layer consists of sensors and actuators that interact with the physical environment. As the perception layer is closely tied to the physical and link layer, and to provide a better networking overview, we consider it as part of the third layer, following [23].

Hitherto, the types of devices and layers of protocols in IoT have been briefly described. However, one crucial aspect remains undefined. It is essential for security specialists to understand the key differences between traditional networks and IoT when dealing with IoT systems [24]. This knowledge can help in designing secure IoT systems, as there are inherent attributes

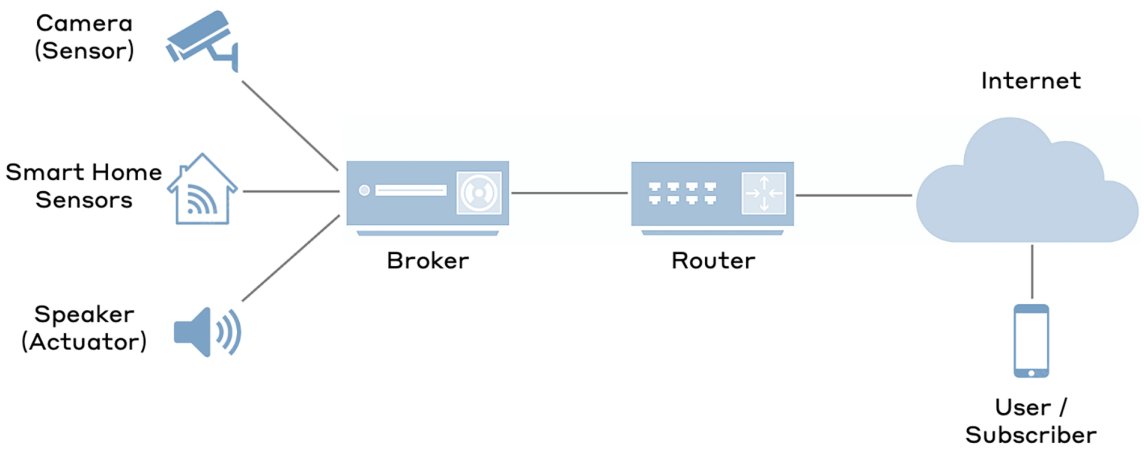

FIGURE 2 | A general view of IoT devices.

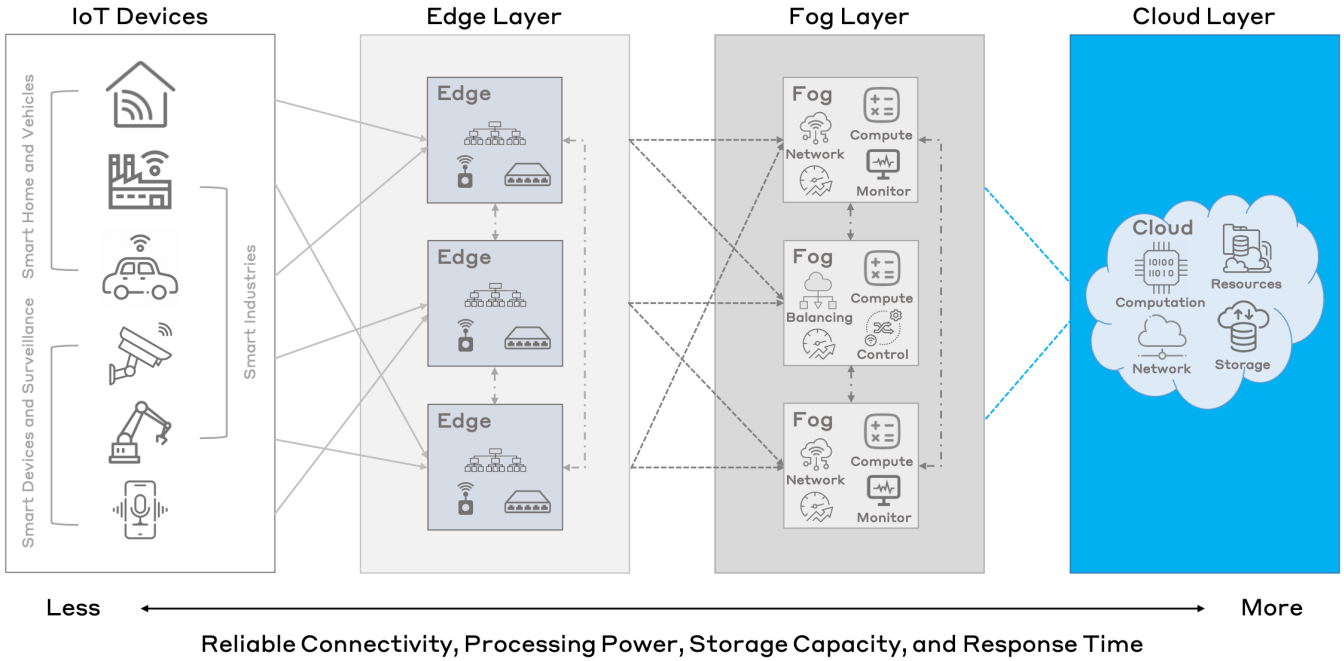

FIGURE 3 | A general view of IoT infrastructure.

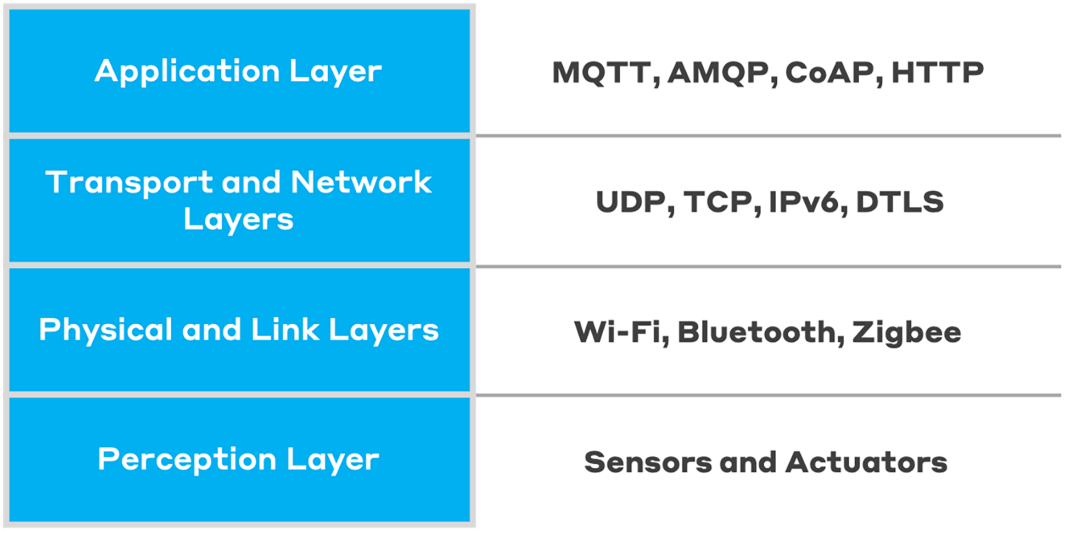

FIGURE 4 | IoT network architecture layers [18].

and constraints in IoT that set it apart from traditional networks. Figure 5 illustrates some of the significant differences between the two.

The first three rows of the table above are particularly crucial in an IoT system. This is due to the prevalence of large data transactions, resulting in difficulties in detecting anomalies amidst benign packets and connections. In addition, the heterogeneity of devices in IoT systems often utilize various protocols and exhibit unique behaviors, making it challenging to have a one-size-fits-all security standard. Furthermore, constrained hardware, such as limited memory, processor, and storage, along with limited power resources, make many IoT devices incapable of having robust detection and recovery functionalities.

2.2 | Explanation of MitM Attacks and Their Types

MitM is a significant threat from a cybersecurity perspective. Before delving into the details of MitM attacks, it is important to understand the aspects affected by this threat. A commonly used model to measure the facets of a threat is the confidentiality, integrity, availability (CIA) Triad [25]. According to this triad, the impacts of threats are categorized into three separate domains. As previously mentioned, DDoS attacks directly affect the availability of a system. However, MitM attacks directly affect all three sides of the triad, namely availability, integrity, and confidentiality. The triad implicitly involves privacy, which encompasses not only confidentiality but also authentication

Topic	Traditional Internet	Internet of Things
Data Volume	Low and Large	Large
Data and Device Formats	Basically Homogenous	Basically Heterogenous
HW Resource	Rich	Limited
Connection	Mostly Fast and Secured	Mostly Slow and Unsecured
Content Creator	Users (Human)	Machines (Publishers)
Content Exchange	Request-based	Pushing Data

FIGURE 5 | Traditional Internet vs. Internet of things [24].

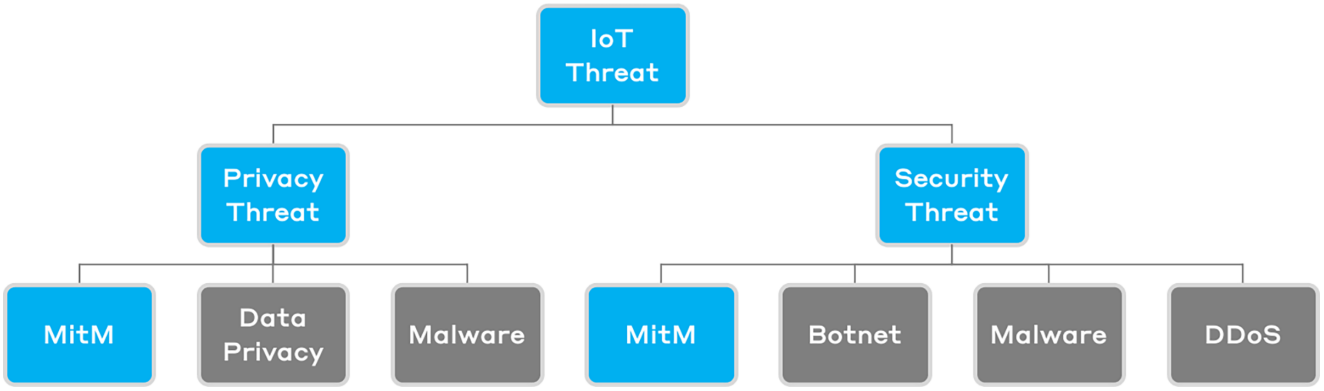

FIGURE 6 | Privacy and security threats in IoT.

and authorization. Therefore, as depicted in Figure 6, MitM is considered a direct privacy-security threat.

In terms of assets, it is possible to classify security issues into users, data, and infrastructure to examine the effects of attacks on each of them in a system. As for MitM, this attack has a direct influence on users, ranging from their privacy to their physical and mental health [26, 27]. Furthermore, this attack does not only impact data in motion directly but also impact data in rest and data in use. In addition, MitM can disturb and ruin network infrastructure, especially in IoT.

Overall, as shown in Figure 7, it is possible to divide MitM attacks into two distinct categories, which are passive and active attacks:

- A passive MitM attack occurs when an attacker does not change the communication actively. Instead, the attacker covertly listens to the communication to gain access to sensitive information. Even though the attacker is not manipulating the communication, they can still obtain sensitive information such as usernames, passwords, and other confidential data, as most traffic is not encrypted properly, according to the introduction section. Eavesdropping is a type of passive MitM.
- An active MitM attack occurs when an attacker intentionally intercepts and modifies the communication between two entities. Once the attacker is in the communication channel, they can manipulate the communication by intercepting, changing, or inserting new messages. Impersonation, spoofing attacks [28], and data tampering are the most common types of active MitM.

One of the essential points that should be mentioned here is that MitM is a multilayer threat [29], which means it overshadows all architecture layers of the IoT. A spoofing attack can prove this assertion. Domain name system (DNS) spoofing affects the application layer, IP spoofing influences the network layer, and address resolution protocol (ARP) spoofing acts on the link

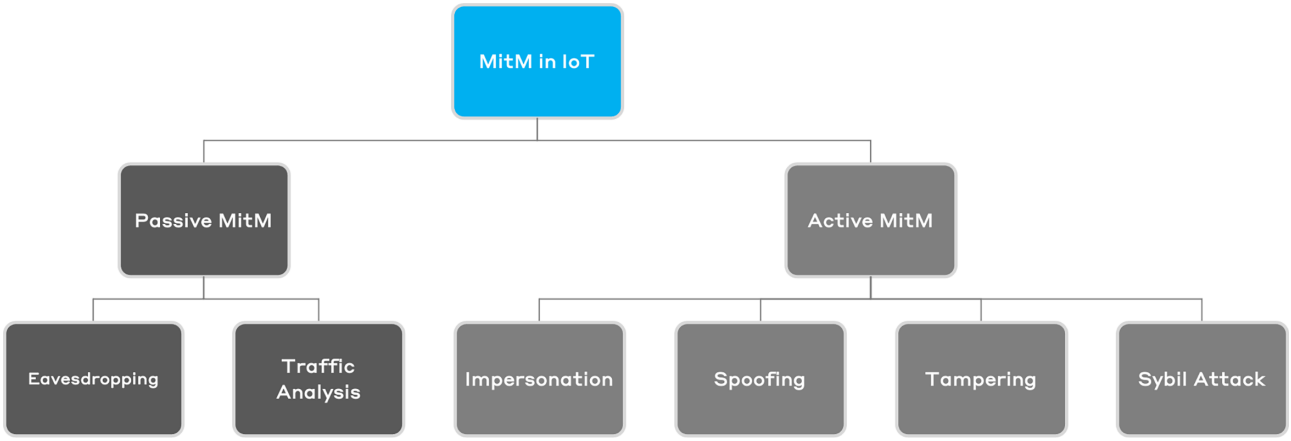

FIGURE 7 | Passive and active man-in-the-middle attacks.

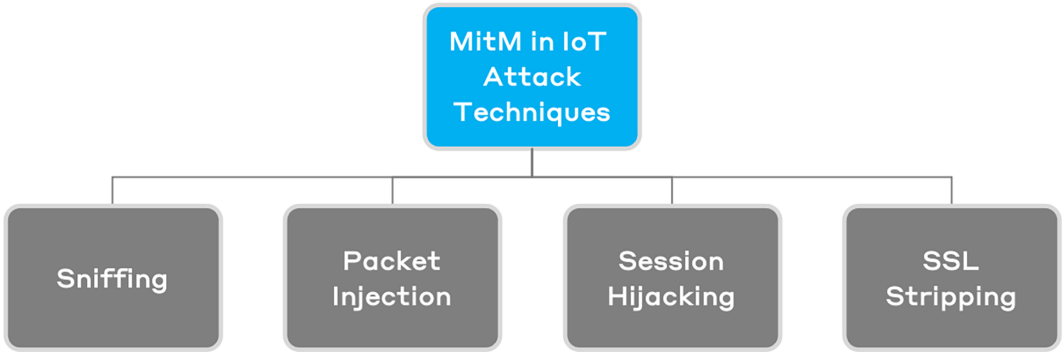

FIGURE 8 | Some techniques of man-in-the-middle.

layer. In addition, perpetrators can implement Rogue access point attacks to intercept a network on the physical layer.

Alongside the types of MitM attacks described above, several techniques can be used to implement these attacks. As shown in Figure 8, this part briefly explains the common techniques of MitM [30] to shed light on the subject.

- Sniffing refers to the interception and analysis of network traffic to obtain sensitive information between two devices. When it comes to IoT, attackers may utilize this method to gain access to unencrypted data transmitted among IoT devices and between IoT devices and cloud services. Wireshark [31] and Cain and Abel [32] are two valuable tools to execute this technique.
- Packet injection is a technique that permits attackers to manipulate network traffic by adding harmful packets to the network. In the realm of IoT, attackers may utilize this technique to interfere with the communication between IoT devices and cloud services or to inject commands that can modify the behavior of the devices. Scapy [33] and MITMf [34] are powerful tools for deploying this technique.
- Session hijacking is a method in which an attacker steals a user's session information, enabling them to impersonate the user and access their data. In the realm of IoT, an attacker may use session hijacking to gain access to the user's IoT devices and manipulate them remotely. Bettercap [35] is one of the most used, powerful tools to implement this technique.
- SSL stripping is a technique that involves converting an encrypted SSL connection to an unencrypted one. When it comes to IoT, attackers can utilize SSL stripping to intercept and alter data that is exchanged between IoT devices and cloud services in a stealthy manner. SSLStrip [36] is one of the well-known tools to perform this technique.

2.3 | How MitM Target IoT Devices and Their Impact

There are generally three major steps in executing a MitM attack in an IoT environment, simplified according to the attack models such as the cyber kill chain [37], ranging from simple eavesdropping to complex tampering attacks. The first step involves the adversary conducting reconnaissance of their target setting. The second step involves exploiting potential vulnerabilities to intercept targets, and the final step involves modifying communication data. These steps can be carried out using specific tools, defined as follows:

1. Network scanning and targeting: to execute a MitM attack on an IoT device, the attacker needs to first discover the IP address of the target device by scanning the network. This can be accomplished using tools such as Nmap [38]

or search engines such as Shodan [39], which can locate Internet-connected devices.

2. Interception and traffic analysis: once the target device is found, the hacker can utilize network traffic analyzers such as MITMf, and Bettercap tools to intercept the communication taking place between the devices. Following that, they can inspect the traffic using packet-capturing tools such as Wireshark and Tcpdump [40] to identify weaknesses in the communication protocol, such as unencrypted data, weak encryption, or other vulnerabilities that may be susceptible to exploitation. Moreover, in IoT settings, lightweight brokers such as Mosquitto Broker [41] are available as open-source MQTT brokers. These brokers can be utilized for MitM attacks, allowing the attacker to intercept and modify MQTT messages before sending them to their desired destination.
3. Data modification and vulnerability exploitation: upon identifying any vulnerabilities, the hacker can alter the transmitted data using tools such as Mallory [42], which could involve injecting malevolent code or stealing confidential data. In the event that the hacker has effectively tampered with the data, they can exploit the vulnerabilities to gain illicit access to the device or to steal data with the help of tools such as Metasploit [43]. This step describes active MitM attacks.

2.4 | Examples of Real-World MitM in IoT Networks

Reviewing recent real-world MitM attacks can enable security specialists to gain a comprehensive understanding of the drawbacks and potential methods to resolve the issues. Therefore, the following are some recent and relatively well-known MitM attacks that will be briefly discussed:

The Equifax data breach incident in 2017 is a perfect example of a MitM attack. The credit company neglected to renew a public key in their security systems, which was detected by hackers who exploited this vulnerability to create multiple web shells, ultimately luring many Equifax customers to fake websites [44].

In March 2021, a sophisticated MitM attack compromised Verkada's security camera systems. Hackers from the collective APT-69420 infiltrated the network by exploiting credentials stored on a Jenkins server. This breach granted them unauthorized access to thousands of customers' cameras, exposing sensitive video feeds and raising serious privacy concerns [45].

In late 2023, the "Terrapin Attack" exposed a severe vulnerability in SSH protocols, enabling attackers to manipulate sequence numbers during handshakes. This MitM exploit allowed malicious injection or deletion of messages within encrypted sessions, putting millions of servers at risk until patches were deployed to mitigate the issue [46].

3 | Methodology

In this section, the methodology that was utilized to locate articles for this article regarding MitM attacks in IoT networks, along with its challenges and solutions, will be presented. The research question posed was, "What are the challenges and potential solutions for preventing and mitigating MitM attacks in IoT networks?"

A combination of search terms and databases was utilized to retrieve articles relevant to the research question. This involved identifying key concepts and creating a list of search terms and synonyms for each concept, including "man-in-the-middle attacks," "IoT security and privacy," "IoT networks," "prevention," "security solutions," and others.

We compiled a list of potential articles and assessed their suitability for our article by examining factors such as author expertise, publication date, and source credibility. We evaluated each article's relevance to our research question on IoT security and MitM attacks by scrutinizing abstracts and introductions. Our methodology involved identifying key concepts, selecting search terms, and utilizing relevant databases. However, we encountered challenges during the article search, including a limited number of publications on the topic and non-standardized terminology for describing MitM attacks in IoT networks. Despite these limitations, we identified several high-quality articles that provided valuable insights into preventing and mitigating MitM attacks in IoT networks. The selected works, mentioned below, represent the most relevant and comprehensive sources aligned with our research aims.

In [47], the authors reviewed various algorithms and authentication methods for IoT security, considering system limitations. They noted that IoT devices' hardware constraints make traditional security methods challenging to implement, emphasizing the need for lightweight algorithms. While presenting several security solutions, they acknowledged that improvements are still needed to provide a trusted environment. They also highlighted ongoing challenges, such as unresolved side-channel attacks. In [48], the authors surveyed classifications of attacks against IoT and industrial IoT (IIoT) devices, along with mitigation methods. The authors presented security issues and challenges, aiming to provide a guide for securing networks. They emphasized the importance of understanding various cyber-attacks to develop effective protection mechanisms, acknowledging that fully securing such devices is a long-term process. In [49], the authors presented a comprehensive view of the IoT architecture, detailing each layer's characteristics and functions. They focused on identifying security requirements and vulnerabilities specific to each IoT layer, enhancing understanding of security challenges. Additionally, they discussed and classified various security attacks in IoT systems. This approach provides a thorough overview of both the IoT framework and its associated security landscape, offering valuable insights for researchers and practitioners in the field. In [50], the researchers surveyed existing countermeasures against MitM attacks, comparing them and proposing a categorization of prevention mechanisms. They analyzed MitM attacks, presenting a comprehensive classification based on impersonation techniques. The authors compiled a table of MitM prevention mechanisms, organized by approaches and context, summarizing the most effective methods discussed in their article. In [51], the researchers explored the most targeted IoT devices and common attack methods used by hackers, including DoS,

MitM, forgery, and replay attacks. Although numerous threats exist, many can be mitigated through network-wide end-to-end encryption. Additional preventive measures include regular network analysis, system security checks, and timely hardware and software updates with security patches. Their analysis provides insights into prioritizing device security and offers a comprehensive overview of hacking techniques. It presents both preventive solutions and countermeasures for ongoing attacks. In [52], the scholars explored the complex landscape of MitM attacks, examining various forms and methodologies, including IP spoofing and DNS manipulation. The authors explained challenges such as Wi-Fi eavesdropping and SSL stripping, while exploring proposed solutions. They discussed the Internet of medical things (IoMT) and its cybersecurity challenges, highlighting how machine learning (ML) and deep learning (DL) techniques are used to enhance MitM attack detection. The article emphasized that DL, behavioral analysis, and hybrid models demonstrate ongoing innovation in addressing MitM attacks in IoT contexts.

The reviewed literature offers valuable insights into IoT security, MitM attacks, and countermeasures. However, a more structured approach is needed to address MitM attacks in IoT networks specifically. To fill this gap, we have adopted a novel methodology based on computer networking layers. This layered approach enables a systematic analysis of security vulnerabilities and countermeasures at each network stack level, providing a comprehensive yet practical framework for understanding and mitigating MitM attacks in diverse IoT systems. Conceptually, this article is divided into three sections: statistical data (mostly in the first section: Introduction), definitions (mostly in the second section: Background and Theory), and challenges and solutions (especially in the fourth and fifth sections).

4 | A Comparative Analysis of the Current State of IoT and MitM Attacks

4.1 | Vulnerabilities of IoT Devices

IoT devices, being composed of mainly three layers of architecture as mentioned by [23], have different attack vectors at each layer (as shown in Figure 9).

The application layer is prone to data access and authentication security issues, the network layer is vulnerable to compatibility issues as well as privacy and cluster security problems, and the link, physical and perception layer is inclined to any node-related attack, such as war driving, node capture, fake node, and mass node authentication. Here is a list of some of these attacks, subdivided by each layer:

1. Application Layer:
   a. DNS spoofing attacks [53], as mentioned previously in Section 2, Section 2.2, is one of the most common types of active MitM attacks. They consist of intercepting the communication between a user and the server, changing the IP address linked to the domain name requested by the user, and providing a fraudulent website instead. This attack will be explained in detail in the following section.

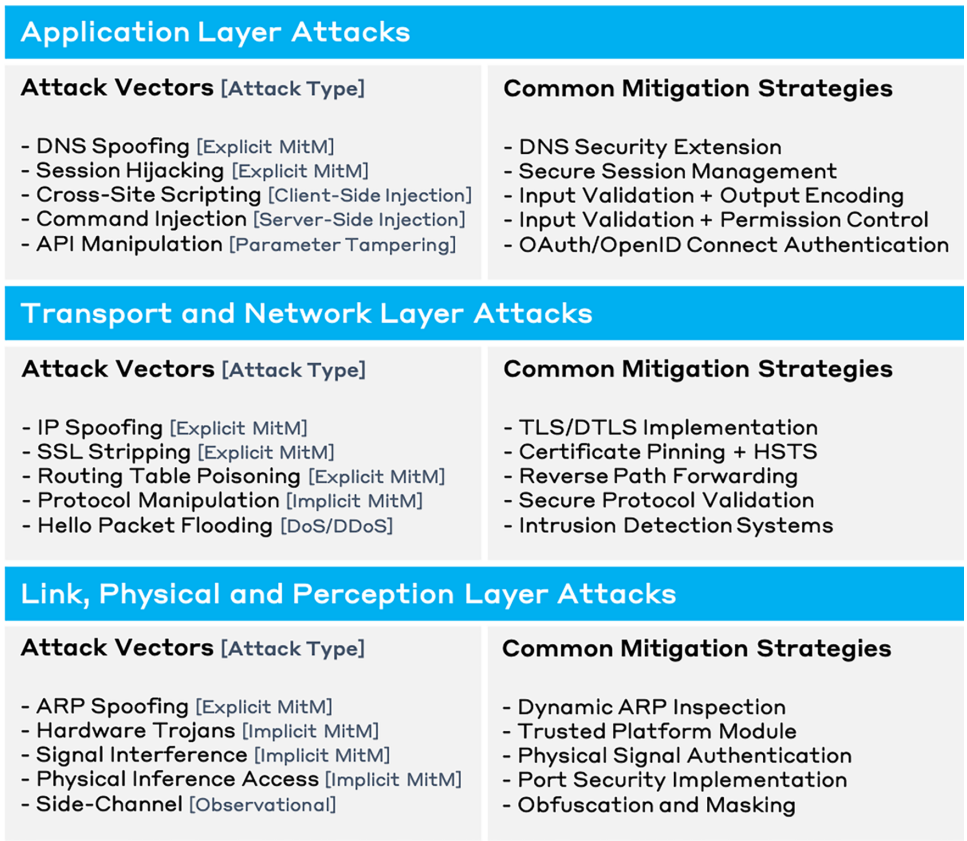

FIGURE 9 | MitM attack mitigation strategies across IoT architecture layers.

b. Session hijacking is a cyber-attack where the attacker takes control of a valid session between an IoT device and its connected application or server, allowing them to manipulate data or actions carried out by the IoT device [54]. It is considered a variant of a MitM Attack, but with a slightly bigger severity because the attacker takes over the application or the system instead of simply stealing or modifying some Internet packets.
c. Cross-site scripting attacks [55] can be a significant threat to IoT devices with web interfaces. Attackers inject malicious scripts into web pages viewed by users, potentially leading to unauthorized access or data theft. In IoT contexts, this could allow manipulation of device settings, theft of sensitive information, or control of physical actuators.
d. Command Injection attacks [56, 57] exploit vulnerabilities in IoT device interfaces that accept user input. Attackers can inject malicious system commands, potentially gaining control over the device. In IoT contexts, this could lead to manipulation of sensor readings, control of physical systems, or unauthorized access to the broader network.

2. Transport and Network Layer:
   a. IP spoofing [58] is an attack in which the source IP address of an IoT device is falsified, creating the illusion of a legitimate communication. It enables interception, manipulation, or injection of malicious data into the network. It can lead to the impersonation of a trusted entity in the communication between the IoT devices. This attack will be explained in the following section.
   b. Hello flooding is a type of DoS attack where the attacker exhausts node resources by sending multiple requests subsequently or at the same time [29]. This specific attack takes advantage of the routing protocols, which require nodes transmitting the HELLO packets to communicate with their neighboring nodes in the network. Therefore, when an intruder impersonates a node in the system, it can easily build communications with the rest of the nodes by convincing them that it's their neighbor and proceeding with the flooding.
   c. SSL stripping is a type of attack in which a perpetrator intercepts the communication between IoT devices that use SSL or TLS encryption and forcibly downgrades the connection to an unencrypted version [59].
   d. Routing table poisoning [60] is a form of attack in which an adversary manipulates network layer tables to redirect communication between IoT devices to a malicious destination, enabling interception, modification, or blocking of communication. It can result in unauthorized access, service disruption, or data leakage/disclosure.

3. Link, Physical, and Perception Layer:
   a. ARP poisoning [61] is a cyber-attack in which an attacker manipulates the ARP tables at the data link layer of an IoT system [28]. This manipulation involves associating the attackers' MAC address with the IP address of legitimate devices to deceive and obtain unauthorized access. This attack will be explained in the following section.
   b. An exhaustion attack is a type of DoS attack where by constantly attacking the network, the batteries of the IoT devices get exhausted and deactivated. As mentioned in [62], a collision between machines' communications through MAC protocols results in repeated attempts at re-transmission, which highly drains the battery resources. This will cause the devices' batteries to die, leading to exhaustion in the end nodes.
   c. Hardware implants, sometimes called hardware Trojans [63], are physical devices that attackers can secretly plant in IoT devices. Such implants enable the IoT devices to intercept, manipulate or inject malicious content into their communications. Implants can be concealed in different parts of a device, such as cables, connectors, or even circuit boards.
   d. Side-channel attacks [64] exploit physical characteristics of IoT devices, such as power consumption, electromagnetic emissions, or timing information, to indirectly extract sensitive data. Without accessing the device's internal data directly, attackers can analyze these external factors to deduce encryption keys, passwords, or other confidential information being processed by the device.

4.2 | Analysis of MitM Attacks on IoT Devices

As the MitM Attack is a multilayer threat [29], and spoofing is considered the most common of the MitM attacks [65], in this subsection, we will go over the various spoofing attacks that exist at each layer:

1. DNS spoofing is a MitM attack at the application layer. The DNS server is responsible for translating the commonly known domain name to the numerical IP address. This IP address creates a communication route between nodes to transfer the requested information [66]. If the domain name does not create a direct link to the IP address, it will query another server that might have that information, continuing this process until it can create a list of connected server names that will link the initial domain name to the numerical IP address. This list of translations is then cached on the user's computer in case the same address is requested in the near future.
   During a DNS MitM attack (as shown in Figure 10), a hacker alters the IP address associated with a domain name, thus providing false information to the user, who then proceeds to cache the fake DNS entry. The attack typically unfolds as follows: (1) an attacker manipulates the DNS server by associating a legitimate domain name (example.com) with a fake IP address (192.168.0.20); (2) when a user requests the domain name "example.com" from the DNS server, they receive the compromised IP address instead of the real one; (3) the user is then directed to a fake website (192.168.0.20) controlled by the attacker, rather than the real website (192.168.0.10); and (4) this deception allows the attacker to potentially steal sensitive information or perform other malicious actions without the user's knowledge.
   This attack exploits the trust users place in the DNS system, potentially leading to serious security breaches and compromise of sensitive data.

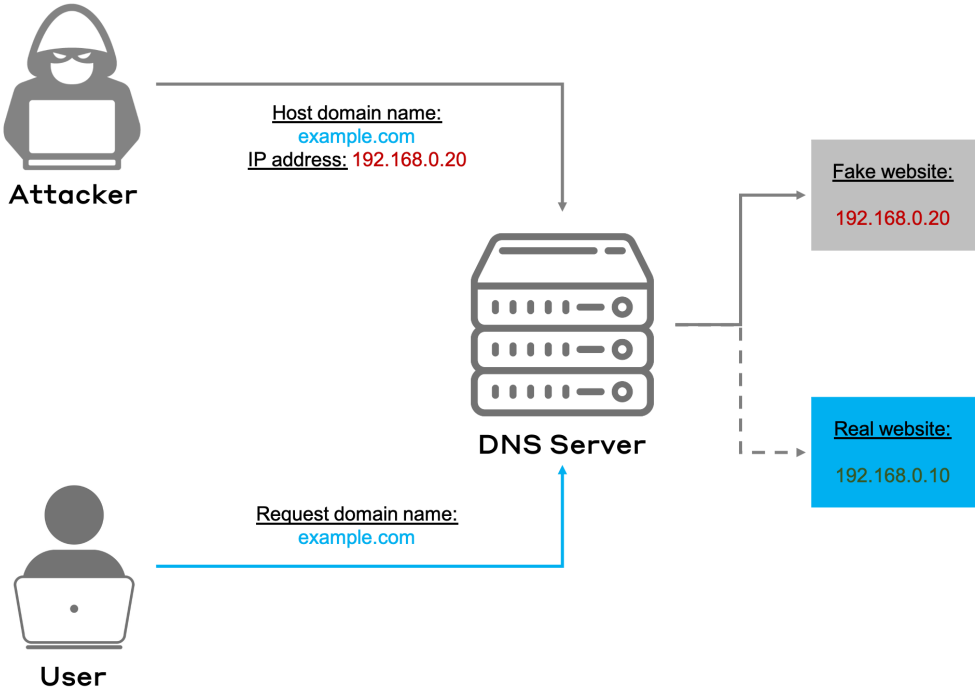

FIGURE 10 | Example of DNS spoofing.

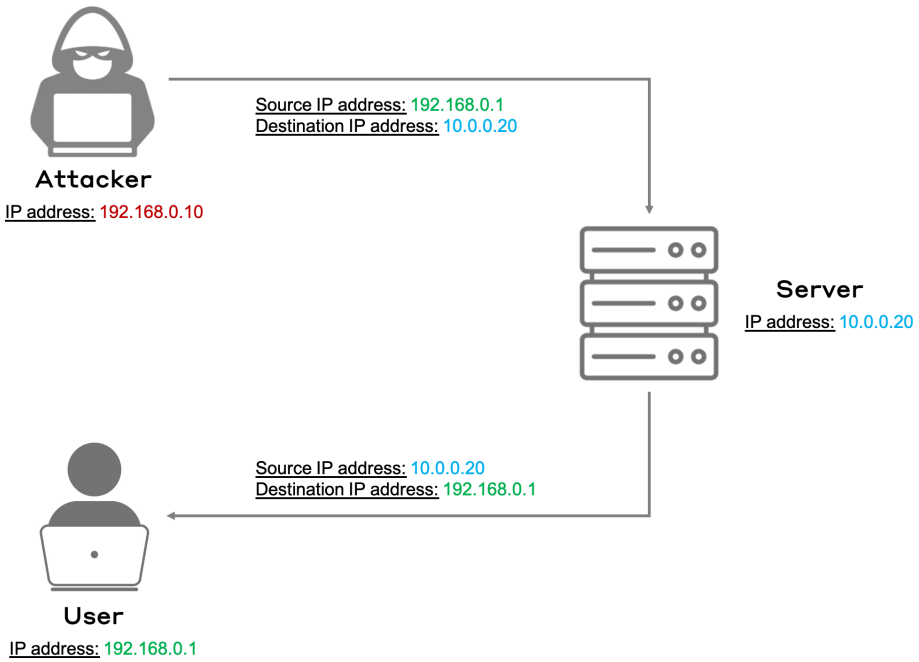

FIGURE 11 | Example of IP spoofing.

2. IP spoofing is a MitM attack that occurs at the network layer. In this type of attack, as illustrated in Figure 11: (1) the attacker intercepts the transmission of a packet and modifies the IP source address in the packet header. This modification is done to deceive the receiving party into believing that the packet originates from a legitimate source [67]; (2) the process begins with the attacker, who has the IP address 192.168.0.10, sending a packet to the server (IP: 10.0.0.20) while masquerading as the legitimate user (IP: 192.168.0.1); the packet's source IP address is falsified to appear as if it's coming from 192.168.0.1, tricking the server into thinking it's communicating with the genuine user; (3) once this deceptive connection is established between the attacker and the victim's IP address, it opens up communication channels that the attacker can exploit. This allows the attacker to potentially lure the victim to harmful and fake websites or intercept sensitive information; (4) the server, unaware of the deception, responds to what it believes is

the legitimate user's IP address (192.168.0.1). This response might be intercepted by the attacker, completing the cycle of the spoofing attack. Through this method, the attacker can effectively position themselves between the user and the server, potentially gaining unauthorized access or intercepting critical data, all while appearing as a trusted entity in the network.

3. ARP spoofing is a common MitM attack at the link layer. ARP is a stateless protocol that is used by a local machine to map the MAC address of the local area network to the IP address of that network. This is a weak protocol because it has no authentication method, making it a prone environment for a MitM attack. Such an attack is executed when the hacker sends an ARP reply with the legitimate IP address of the host the machine is trying to reach, but its own MAC address instead of the actual address of the host. To illustrate this process in more detail, as depicted in Figure 12: (1) the attacker, with IP address 192.168.0.2 and MAC address 00:BB:DD:11:CC:22, initiates the attack; (2) the attacker sends falsified ARP messages to both the user (192.168.0.1) and the router (192.168.1.1); (3) these ARP messages claim that the attacker's MAC address (00:BB:DD:11:CC:22) is associated with both the router's IP (192.168.1.1) and the user's IP (192.168.0.1); (4) the goal is to poison the ARP caches of both the router and the user; (5) if successful, the user will mistakenly believe that the attacker's MAC address belongs to the router, and vice versa; and (6) as a result, traffic intended for the router will be sent to the attacker instead, and similarly for traffic from the router to the user. Therefore, the victim will receive the ARP reply, which will contain the wrong information linking the right IP address to the wrong MAC address [68]. For example, in the case where the user of the local machine tries to reach a host database, if a MitM attack occurs at the ARP level, the user will end up sending its IP packets to the attacker instead of the database. This is called ARP poisoning [28].

4.3 | Current Prevention Techniques

From protocols to ML, there are multiple techniques being used to prevent attacks on IoT devices. First, there are multiple standardized protocols already in place that ensure basic security measures when implementing IoT devices. Based on this survey [29], here are the main protocols per each layer:

1. CoAP is an ultralight application level protocol. It is mainly used in machine-to-machine (M2M) applications on a low-power and low-bandwidth constrained network.
2. The DTLS protocol is used at the transport layer for situations requiring fast data transfer with short response times (such as video or game rendering). This protocol secures communication between clients and servers by using certification-based authentication methods [69].
3. IPv6 is the main Internet key protocol for IoT devices and has been considered the main Internet Standard since 2017 [70]. This protocol is behind any communication at the network layer between IoT devices.
4. IEEE 802.15.4 is the protocol used in Zigbee, which, along with Bluetooth and Wi-Fi, is a common wireless communication technology.

Nevertheless, these protocols are simply standard guides directing the way communication should function through networks. Such protocols should be followed to avoid being intercepted by intruders, yet it does not prevent all types of attacks from

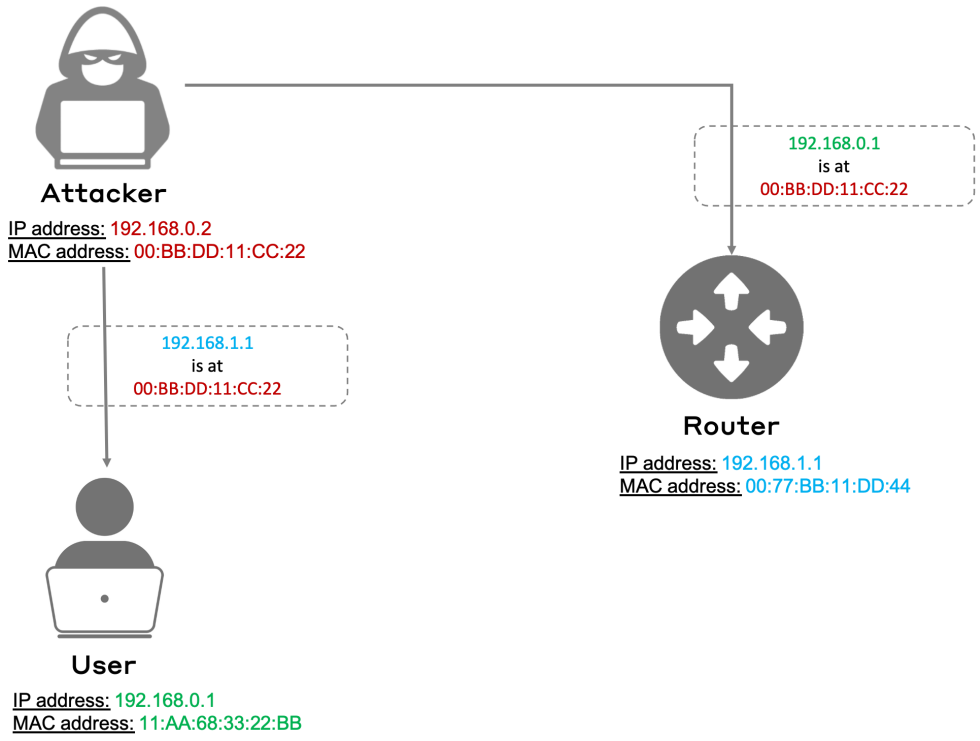

FIGURE 12 | Example of ARP spoofing.

happening. Therefore, here are different specialized prevention techniques that are used for the various attacks listed in Section 4, Section 4.1:

1. Application Layer:
   (a) Using domain name system security extension (DNSSEC) enhances DNS security with digital signatures, verifying data integrity and authenticity to prevent DNS spoofing attacks and malicious data injection into DNS caches [71]. However, improper key management or signature validation can lead to domain resolution failures, potentially causing widespread service outages. This method is highly scalable for large DNS infrastructures and practical for implementation, although it requires careful key management and regular updates.
   (b) Ensuring secure session management [72] with unique session IDs and regular password rotation can prevent session hijacking attacks. However, if session IDs are predictable or not properly encrypted during transmission, attackers might still be able to guess or intercept valid session tokens, compromising user accounts. This approach is scalable across various applications and practical to implement, but it requires consistent execution and ongoing user education.
   (c) Using application-layer encryption for IoT data, such as JSON web encryption or XML encryption, provides an additional security layer against MitM attacks [73]. This prevents attackers from reading intercepted communications. However, increased processing time and battery consumption may impact power-sensitive IoT applications. While practical for high-security IoT applications with sufficient power, this method has limited scalability for resource-constrained devices.
   (d) Implementing mutual authentication and certificate pinning in IoT devices mitigates MitM attacks [74]. Mutual authentication verifies both device and server identities, while certificate pinning restricts trusted certificates. Increased computational overhead and complex certificate management in large-scale deployments may strain resource-constrained IoT devices. This approach is challenging to scale in large IoT deployments but remains practical for critical systems with manageable device numbers.

2. Transport and Network Layer:
   (a) Using TLS and HTTP strict transport security (HSTS) [75], which is a security feature that allows a website to specify that it should only be accessed over HTTPS and not over HTTP. This can, however, create compatibility issues with older systems or browsers, potentially limiting access for some users. Despite these challenges, this method is highly scalable across web applications and is practical and widely adopted, though it may require updates to legacy systems.
   (b) Implementing role-based access control (RBAC) to restrict user permissions within a network based on roles (e.g., admin vs. regular user), utilizing encryption to safeguard stored data, and using data integrity checks (e.g., checksums, hash functions, digital signatures) to detect any data alterations [76]. However, misconfigured roles may lead to over-privileged users or unintended access restrictions. While scalable, this approach can become complex in large systems. It remains practical for organizations with clear role hierarchies and strong IT support.
   (c) Using specialized tools and techniques such as reverse path forwarding and unicast reverse path forwarding [77, 78], as well as network intrusion detection and prevention systems, to thwart IP spoofing attacks. These systems may generate false positives, particularly in networks with asymmetric routing, potentially blocking legitimate traffic and disrupting services. This method is scalable for large networks and practical to implement, but it requires significant infrastructure and ongoing management.
   (d) Using DL and optimization algorithms, for instance anomaly detection models such as autoencoders (AE) [79], can help mitigate Hello flooding attacks (a type of Denial of Service attack in IoT networks) [80], although the high computational resource requirements may impact overall system performance, especially in resource-constrained IoT environments. The scalability of this approach is limited by computational resources, but it remains practical for large IoT networks with sufficient processing power.
   (e) Hybrid routing can help detect MitM attacks in IoT networks. In [81], the authors propose a novel scheme using dedicated nodes with enhanced capabilities to manage routing between IoT devices and users. This approach offers secure path determination, stable travel times for improved accuracy, and packet inspection. While promising for enhancing security, the method's practicality and scalability in large-scale IoT deployments may be challenged due to potential bottlenecks and implementation complexities.

3. Link, Physical and Perception Layer:
   (a) An exhaustion attack can be avoided by using timers or a rate limitation on the number of requests sent to an IoT device [29]. However, if the rate limit is set too low, it may interfere with legitimate high-volume requests during peak usage periods, potentially affecting critical system functionality. This method is highly scalable across devices and practical to implement, but it requires careful tuning to balance security and functionality.
   (b) Enabling port security can limit MAC addresses, preventing unauthorized devices from connecting and protecting against ARP spoofing attacks. Deploying network monitoring and IDS helps detect ARP spoofing by reviewing logs and analyzing network traffic for signs of ARP spoofing attempts. In dynamic environments with frequent hardware changes or Bring-Your-Own-Device (BYOD) [82, 83] policies, this can lead to connectivity problems and increased administrative overhead to manage allowed devices. This approach has limited scalability in dynamic networks but remains practical for small to medium-sized static environments.
   (c) Network monitoring detects suspicious network traffic that may indicate hardware implants, such as unusual data flows, anomalies, or unauthorized access attempts.

Hardware integrity verification systems let us check components for unauthorized modifications using techniques such as hardware integrity checking, Trusted Platform Modules (TPM) [84, 85], or Hardware Security Modules (HSM) [86]. Despite these measures, sophisticated hardware implants that mimic normal behavior or exploit zero-day vulnerabilities may still evade detection. While scalable, this method is resource-intensive. It is practical for high-security environments.

(d) Monitoring for suspicious activity using Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS) [87, 88] involves reviewing logs and analyzing network traffic to detect and alert unauthorized devices or attempts to intercept wireless signals. Using strong encryption ensures that all wireless communications are protected using robust encryption algorithms. Media Access Control (MAC) address filtering allows specifying which devices can connect to a wireless network based on their MAC addresses. However, determined attackers may still bypass MAC filtering through MAC address spoofing, and managing a large list of allowed MAC addresses can become cumbersome in large or frequently changing networks. This approach is scalable for most wireless networks and practical to implement, but it can be management-intensive in large or dynamic environments.

Finally, ML and DL are being leveraged to counter some security threats as well, by building models that can predict which behaviors are threatening [89]. In classifications made by an ML algorithm, there is a chance of false positives and false negatives, making this technique not perfect. Nevertheless, DL can be used to determine the accuracy of every prediction, which makes DL great facility to use for detecting malicious attacks.

4.4 | Current Techniques to Mitigate and Manage MitM Attacks on IoT Devices

Multiple prevention techniques exist to avoid MitM attacks on IoT devices: multifactor authentication (MFA), setting up virtual private networks (VPNs), using secure communication tools, making sure SSL certificates are secure and systems are updated, etc. On top of that, ML can be leveraged to detect anomalies through unsupervised and supervised learning, as seen in the article [90]. ML and distributed ledger technologies (DLTs) can help improve IoT infrastructure and prevent cybersecurity attacks [91]. Here are some techniques used in the MitM attacks described previously in Section 4, Section 4.2:

1. DNS spoofing at the application layer: deep packet inspection (DPI) and deep flow inspection (DFI) are modules that analyze the traffic of a network and determine if it has anomalies [92]. A DPI performs an analysis of packets components, such as the header and the payload. A DFI analyzes packet features such as the total bytes flow, the packet count flow, the duration of flow, and the average packet bytes flow and flags whenever there is abnormal activity. In addition, DFI can support encrypted data, but DPI cannot.
2. IP spoofing at the network layer: It is difficult to determine when an attack has happened at the network level, but network monitoring tools can help determine when the information in the response has been modified. Ingress and egress filtering is one of the methods which can help prevent IP spoofing. Research in network security has proposed various classification schemes for prevention mechanisms. One approach categorizes methods into filtering-on-path techniques, which process packets en route, and end-to-end authentication methods that verify source addresses at the destination [93]. Another classification focuses on implementation location, dividing mechanisms into host-based, router-based, or hybrid approaches [94]. These schemes offer frameworks for understanding the diverse strategies in network security, highlighting the complexity of protecting digital communications and infrastructure.
3. ARP spoofing at the link layer: multiple existing techniques prevent ARP spoofing, ranging from static ARP tables that map the right MAC addresses to their corresponding IP addresses to switch security checks which consist of checking each ARP message and filter out messages that seem to be malicious [89]. There are ML algorithms being developed to mitigate this attack. In the article [95], the researchers use different classification algorithms to detect an ARP spoofing MitM attack. They used two different IoT devices, a voice recognition device SKT NUGU (NU 100) and a wireless EZVIZ WiFi camera, connected to a wireless network to which other devices were also connected. A variety of network packet files (pcap) with multiple packets in each were transmitted on this network, where 6 of the 42 raw pcap files contained MitM attacks. Each pcap file contained 7 features: packet sequence number, its transmission time, source IP address, destination address, the protocol used, length in bytes, and info containing additional details. These packets features were used to train the classification algorithms logistic regression (LR), random forest (RF), and decision tree (DT), which were then used on the test set, to determine which packets were compromised. The MitM dataset used in this experiment contained 194184 observations, where 52.74% were attack packets, and 47.53% were normal ones. The results for each classification algorithm were extremely good, giving 99% precision, recall, and f1-score for the LR, and a 100% score for the same metrics for the RF and DT algorithms. Such high scores certainly raise questions such as: what is the quality of the data and how can we assess that it's not biased? Nevertheless, this experiment demonstrates how ML algorithms can be leveraged to detect MitM ARP spoofing attacks.

5 | Open Issues

5.1 | Challenges of Prevention

The growth in the number of connected IoT devices discussed previously has led to the democratization of IoT devices. More devices are available to end-users with technological skills ranging from expert-level to tech beginners. For the latter, this means that end-users who may not have the technical knowledge or understanding of cybersecurity risks can become potential risks themselves. They may inadvertently introduce vulnerabilities into the network by failing to properly secure their devices or keep their software up to date.

For organizations, the deployment of a large number of IoT devices can make them vulnerable to MitM attacks, where attackers intercept and manipulate data sent between devices. Active monitoring becomes a significant challenge, as plain text communication, open ports, and weak credentials used on these devices can all be exploited by attackers to gain unauthorized access to the network and its large data volume. This is particularly problematic when patching security cameras and printers, where the sheer number of devices creates a window of vulnerability if a security patch is not applied promptly. Not only are these devices abundant but they are also the most vulnerable ones in an enterprise network [5]. To prevent MitM attacks, organizations must implement security policies that outline how IoT devices are deployed, managed, and monitored, and ensure that regular assessments are conducted to identify any vulnerabilities that may exist.

While active monitoring is improving with the use of ML in IT security (a subject which will be discussed in the next section), the recognition of malicious patterns is mainly based on previous experience or available datasets. However, generating such training data is challenging as the IoT device environment is itself constantly changing [96]. Additionally, finding high-quality publicly available datasets can be difficult [29]. For all these reasons, the prevention of attacks on these devices represents a major challenge that requires significant effort from organizations, manufacturers, and end-users to mitigate security risks.

5.2 | Emerging Technologies for IoT Security

The IoT security industry currently uses several commercial technologies to secure networks, including asset management and Computerized Maintenance Management Systems (CMMS), Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Next-Generation Firewalls (NGFW), Network Access Control (NAC), and wireless/network management solutions [5]. While these technologies are effective, they may not always detect sophisticated attacks. Emerging technologies in IoT security, such as intrusion detection using DL, show promise in addressing this limitation. DL algorithms can analyze large volumes of data and identify anomalous behavior patterns, which may indicate a potential security breach.

Figure 13 illustrates a comprehensive ML-based security architecture for MitM attack prevention across different layers of IoT infrastructure. The cloud layer [97] represents the centralized data centers that handle computationally intensive tasks such as federated learning [98] aggregation and global threat intelligence. The fog [99] acts as an intermediate computing layer, typically deployed at the network edge (such as gateways or local servers), managing tasks such as local model training and protocol validation. The edge layer [100] operates closer to data sources (e.g., routers, switches), performing lightweight inference and device authentication. Finally, the IoT device layer represents the

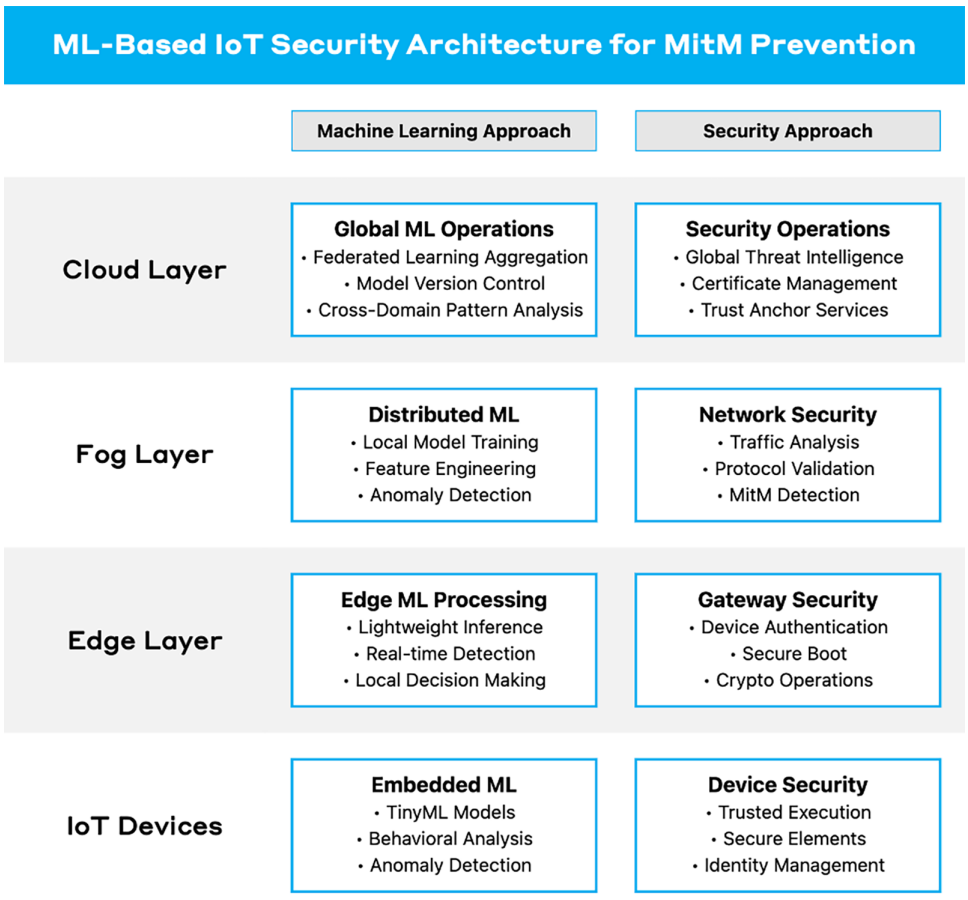

FIGURE 13 | ML-based IoT security architecture for MitM attack prevention.

end devices themselves, implementing embedded ML [96] for real-time anomaly detection alongside basic security measures. This hierarchical approach distributes security and ML capabilities based on each layer's computational resources and proximity to data sources.

Traditional ML methods such as logistic regression (LR), random forest (RF), or decision trees (DT) already show promising results, as some researchers can achieve around 99% accuracy on a publicly available dataset [95]. It is important to note that the said dataset is very simple and such precision is not to be expected in a real-world scenario, as it is mostly used to compare different approaches. In [101], the authors propose a Regression Modeling technique to detect and mitigate MitM attacks in IoT networks, providing an attack-free path from source to destination. Three ML algorithms are implemented and analyzed: linear regression, multivariate linear regression (MLR), and Gaussian process regression (GPR). The performance of each technique is evaluated using various metrics, including packet loss ratio and throughput. Results demonstrate that Gaussian Process Regression outperforms the other methods, achieving a higher detection rate for attacks and a lower misclassification rate. Overall, GPR proves to be the most efficient technique for detecting MitM attacks in IoT networks. However, DL is especially useful in detecting and responding to zero-day attacks, which exploit previously unknown vulnerabilities in IoT devices [102]. Current DL methods used and developed for intrusion detection include convolutional neural network (CNN), gated recurrent unit (GRU), and long short-term memory neural network (LSTM). Other classifiers being discussed in the research community include genetic algorithm (GA) and bidirectional long short-term memory (BiLSTM), with the hope that they will increase performance [102]. By leveraging emerging technologies such as DL, organizations can strengthen their IoT security posture and stay ahead of potential threats. In [103], the researchers applied four supervised classification methods combined with principal component analysis (PCA) for dimensionality reduction to detect MitM attacks in IoT environments. They achieved high performance, with all four methods exceeding 90% area under the curve (AUC). The models were evaluated using Tukey comparison and Kruskal–Wallis analysis of variance, which identified neural networks as the best model, achieving 99.2% AUC with 4 hidden layers and 10 neurons per layer. The study demonstrated that combining PCA with their methods provides a robust solution for MitM attack detection, improving upon their previous multiclassifier approach for various MQTT attacks. The researchers concluded that using a specific dataset for MitM attacks is the best approach for applying ML techniques. For future work, they proposed exploring other dimensionality reduction methods and unsupervised learning to facilitate the use of larger datasets.

Blockchain technology offers a promising solution for enhancing IoT network security [104], particularly against MitM attacks. A recent study proposes a blockchain-based IDS coalition for IoMT network [105]. This system utilizes a compact blockchain ledger to reduce processing and communication overhead, while using cryptographic hashes to ensure data integrity and secrecy. By incorporating peer-to-peer networks, the model achieves complete decentralization and effectively counters various attacks, including MitM, DoS, and impersonation attacks. The proposed method demonstrated exceptional performance, achieving a 100% F1-score and over 99% AUC value, highlighting blockchain's potential in creating robust security solutions for IoT networks.

5.3 | Future Trends of MitM Attacks and How to Start Preparing for Them

One of the prevention challenges previously discussed was linked to the growth in the number of connected devices. This has created a challenge due to the absence of a standard architecture for IoT. With an estimated billions of objects being connected to the Internet annually, it is essential to have an architecture that is adequate for easy connectivity, communication, and control. To ensure security in IoT, devices should contain an Identity Manager [24]. Without it, the heterogeneity of the environment gives MitM attackers a perfect ground to find vulnerabilities. It is also much more difficult for the security community as they would have to patch these on a device basis.

The heterogeneity of IoT devices and networks not only complicates security measures but also opens up new avenues for attacks. One particularly vulnerable area is the communication infrastructure used by IoT devices. For instance, MitM attacks on IoT devices that use long range wide area networks (LoRaWAN) [106] have significantly increased. Hackers can target these networks using ARP spoofing, which sends fake ARP messages over a LoRaWAN. During an ARP spoofing attack, an attacker sends forged ARP messages to the target's device or router, tricking it into associating the attacker's MAC address with the IP address of the intended destination. As a result, any traffic intended for the destination is sent to the attacker's device instead. This could allow the attacker to eavesdrop on the communication between the two devices without being detected and can be used to steal login credentials, redirect users to a fake website, or launch other types of attacks. One way to prevent these attacks is to use Static ARP Tables. By having static addresses stored, it ensures that any modification would need a manual update of the tables by the user on all the hosts [89]. Note that this method is not applicable to particularly large networks with many devices, as manual updates would require significant effort.

When faced with a MitM attack on a network, it can be observed that there is an unusual delay, caused by the attacker's information rerouting. This characteristic can be used as a prevention and detection method. A technique called Hybrid Routing [107] for MitM attack detection in IoT Networks was developed to appoint dedicated nodes to route IoT traffic. By selecting devices with enough computational capabilities as nodes, traffic can be routed through them to improve the stability of travel times. Coupled with an inference algorithm, this would make anomaly detection much easier as a MitM attack would result in an inconsistent transmission time [81]. By implementing these network-wide techniques, the challenge brought on by the heterogeneity of the IoT device landscape could be tackled and could prepare users against potential attacks.

5.4 | The Potential Impact of New Technologies in IoT and MitM Attacks

New technologies in IoT have the potential to significantly impact the security landscape. As more IoT devices are becoming interconnected, the risk of MitM attacks is increasing. To mitigate this risk, it is essential that new IoT technologies include robust security features that can not only detect but also prevent MitM attacks. It is also important to consider the impact of compatibility and scalability, as the lack of standardization in the IoT industry can create compatibility issues and security risks. The development of new standards that ensure interoperability, scalability, monitoring, and attack prevention is essential to ensure the widespread adoption of new IoT technologies [108].

Regulation is also a critical consideration for the IoT industry, as IoT devices collect and transmit sensitive data. There is a need for regulations to ensure the security of IoT devices and to protect users from potential harm caused by breaches and leaks. The main issue is that laws and public guidelines are created and updated at a much slower pace than the technologies they are governing. Reacting slowly to innovation could have negative impacts on every party, whether it is on a consumer, an industrial member, or even a whole state.

Overall, the development of new IoT technologies must consider the potential impact on security and privacy, compatibility, and regulation to ensure the safe and widespread adoption of IoT. By prioritizing these considerations, IoT can continue to grow and expand, offering increased connectivity, convenience, and efficiency in various applications.

6 | Conclusion

IoT devices are gaining popularity amongst technology professionals and regular individual end-users. Currently, while the security of such devices is crucial, it is often lacking. They are subject to many MitM attack vectors due to the heterogeneity of the IoT space. These attacks are considered direct privacy and security threats. Many current methods are used to prevent and combat such attacks but have some limitations. Some of these limitations are the complexity brought on by the increase in network size, the limited compute power and battery capacity of IoT devices, and the simplicity of the datasets used to train ML and DL models, as they do not accurately mimic real-world use cases. Now, techniques using DL are being explored and used to detect intrusions. As for the industry in general, it is important to prioritize security and privacy, but also compatibility, regulation, and the integration of emerging technologies to improve active monitoring and detection of potential security breaches. In terms of future research, network architecture optimization or standardization for hybrid routing can be interesting to investigate to try to adapt the technique to larger network sizes. Other broader avenues would be to help other researchers with dataset creation to mimic larger size networks. Finally, the use of blockchain or DLTs as immutable decentralized databases can be explored to enhance IoT security.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

References

1. NIST Internet Definition, https://csrc.nist.gov/glossary/term/internet, 2024.

2. M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of Internet of Things: Review and Open Research Issues Related to Detection and Prevention of Iot-Based Security Attacks," *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 8669348.

3. IoT Analytics, "Iot Market Size," https://iot-analytics.com/iot-market-size/.

4. Number of Connected Iot Devices, https://iot-analytics.com/wp/wp-content/uploads/2024/09/INSIGHTS-RELEASE-Number-of-connected-IoT-devices-vf.pdf, 2024.

5. Palo Alto Networks, "2020 Unit 42 Iot Threat Report," 2024, https://unit42.paloaltonetworks.com/iot-threat-report-2020.

6. K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A Survey of Distributed Denial of Service Attack," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)* (IEEE, 2016), 1–6.

7. M. Husamuddin and M. Qayyum, "Internet of Things: A Study on Security and Privacy Threats," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (IEEE, 2017), 93–97.

8. M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-Channel Man-In-The-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review," *Expert Systems with Applications* 210 (2022): 118401.

9. N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, *A Review of Security Standards and Frameworks for Iot-Based Smart Environments*, vol. 9 (IEEE Access, 2021), 121975–121995.

10. OWASP, "Owasp Internet of Things," 2024, https://owasp.org/www-project-internet-of-things/.

11. T. Micro, "The IOT Attack Surface: Threats and Security Solutions," https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions.

12. Industry IOT Consortium, "Iot Security Maturity Model," 2024, https://www.iiconsortium.org/smm/.

13. NIST, "Nist Cybersecurity for Iot Program," 2024, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

14. Qualys SSL Labs, "Ssl Pulse: Survey of the Ssl/Tls Configuration of the Most Popular Websites," 2024, https://www.ssllabs.com/ssl-pulse/.

15. A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security Considerations for Internet of Things: A Survey," *SN Computer Science* 1 (2020): 1–19.

16. M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and Open Issues of Mqtt Protocol," in *2017 International Conference on Engineering & MIS (ICEMIS)*, vol. 2017 (Ieee, 2017), 1–6.

17. H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A Survey on Internet of Things Security: Requirements, Challenges, and Solutions," *Internet of Things* 14 (2021): 100129.

18. A. Huč and D. Trček, "Anomaly Detection in Iot Networks: From Architectures to Machine Learning Transparency," *IEEE Access* 9 (2021): 60607–60616.

19. C. B. Gemirter, Ç. Şenturca, and Ş. Baydere, "A Comparative Evaluation of Amqp, Mqtt and Http Protocols Using Real-Time Public Smart City Data," in *2021 6th International Conference on Computer Science and Engineering (UBMK)* (IEEE, 2021), 542–547.

20. M. A. Tariq, M. Khan, M. T. Raza Khan, and D. Kim, "Enhancements and Challenges in Coap-A Survey," *Sensors* 20, no. 21 (2020): 6391.

21. A. Sara and J. Randa, "Data Protection in Iot Using Coap Based on Enhanced Dtls," in *AIP Conference Proceedings*, vol. 2729 (AIP Publishing, 2024).

22. S. Mahmoodi Khaniabadi, A. Javadpour, M. Gheisari, W. Zhang, Y. Liu, and A. K. Sangaiah, "An Intelligent Sustainable Efficient Transmission Internet Protocol to Switch Between User Datagram Protocol and Transmission Control Protocol in Iot Computing," *Expert Systems* 40, no. 5 (2023): e13129.

23. K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in *In 2013 Ninth International Conference on Computational Intelligence and Security* (IEEE, 2013), 663–667.

24. S. U. R. Aqeel-ur Rehman, I. U. Khan, M. Moiz, and S. Hasan, "Security and Privacy Issues in Iot," *International Journal of Communication Networks and Information Security* 8, no. 3 (2016): 147–157.

25. Fortinet, "Cia Triad," 2024, https://www.fortinet.com/resources/cyberglossary/cia-triad.

26. O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, "Man-In-The-Middle Attack Mitigation in Internet of Medical Things," *IEEE Transactions on Industrial Informatics* 18, no. 3 (2021): 2053–2062.

27. R. Shandler, M. L. Gross, and D. Canetti, "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis," *Journal of Global Security Studies* 8, no. 1 (2023): ogac042.

28. R. Petrović, D. Simić, S. Stanković, and M. Perić, "Man-In-The-Middle Attack Based on Arp Spoofing in Iot Educational Platform," in *2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)* (IEEE, 2021), 307–310.

29. S. Khanam, I. B. Ahmedy, M. Y. I. Idris, M. H. Jaward, and A. Q. B. M. Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," *IEEE Access* 8 (2020): 219709–219743.

30. Rapid7, "Man in the Middle (Mitm) Attacks: MITM Techniques, Detection, and Best Practices for Prevention," 2024, https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

31. Wireshark, "Wireshark," 2024, https://www.wireshark.org.

32. Cain and Abel, "Cain and Abel," 2024, https://sectools.org/tool/cain/.

33. Scapy, "Scapy," 2024, https://scapy.net.

34. MITMF, "Mitmf," 2024, https://github.com/byt3bl33d3r/MITMf.

35. Bettercap, "Bettercap," 2024, https://www.bettercap.org.

36. SSLSTRIP, "Sslstrip," 2024, https://www.kali.org/tools/sslstrip/.

37. N. Naik, P. Jenkins, P. Grace, and J. Song, "Comparing Attack Models for It Systems: Lockheed Martin's Cyber Kill Chain, Mitre Att&Ck Framework and Diamond Model," in *2022 IEEE International Symposium on Systems Engineering (ISSE)* (IEEE, 2022), 1–7.

38. NMAP, "Nmap," 2024, https://nmap.org.

39. Shodan, "Shodan," 2024, https://www.shodan.io.

40. Tcpdump, "Tcpdump," 2024, https://www.tcpdump.org.

41. Eclipse Mosquitto, "Eclipse Mosquitto," https://mosquitto.org.

42. Mallory, "Mallory," 2024, https://github.com/intrepidusgroup/mallory.

43. Rapid7, "Metasploit," 2024, https://www.metasploit.com.

44. J. Thomas, "A Case Study Analysis of the Equifax Data Breach 1 a Case Study Analysis of the Equifax Data Breach," 2019, https://www.researchgate.net/publication/337916068.

45. C. Rollet, "150,000 Verkada Security Cameras Hacked-to Make a Point," https://www.malwarebytes.com/blog/news/2021/03/150000-verkada-security-cameras-hacked-to-make-a-point.

46. F. Bäumer, M. Brinkmann, and J. Schwenk, "Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation," *arXiv* (2024): 2312.12422, https://arxiv.org/abs/2312.12422.

47. A. Hameed and A. Alomary, "Security Issues in Iot: A Survey," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (IEEE, 2019), 1–5.

48. Y. Shah and S. Sengupta, "A Survey on Classification of Cyber-Attacks on Iot and Iiot Devices," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, vol. 2020 (IEEE, 2020), 406–413.

49. M. Ahmid and O. Kazar, "A Comprehensive Review of the Internet of Things Security," *Journal of Applied Security Research* 18, no. 3 (2023): 289–305.

50. M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 2027–2051.

51. V. Tyagi, A. Saraswat, and S. Bansal, "An Analysis of Securing Internet of Things (Iot) Devices From Man-In-The-Middle (Mima) and Denial of Service (dos)," in *Smart Cities* (CRC Press, 2023), 337–357.

52. M. Narang, A. Jatain, and N. Punetha, "A Survey on Detection of Man-In-The-Middle Attack in Iomt Using Machine Learning Techniques," in *International Conference on Computational Intelligence* (Springer, 2023), 117–132.

53. F. Alharbi, Y. Zhou, F. Qian, Z. Qian, and N. Abu-Ghazaleh, "Dns Poisoning of Operating System Caches: Attacks and Mitigations," *IEEE Transactions on Dependable and Secure Computing* 19, no. 4 (2022): 2851–2863.

54. A. K. Baitha and S. Vinod, "Session Hijacking and Prevention Technique," *International Journal of Engineering &Technology* 7, no. 2.6 (2018): 193–198.

55. G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-Site Scripting (Xss) Attacks and Mitigation: A Survey," *Computer Networks* 166 (2020): 106960.

56. S. Liu, P. Feng, and K. Sun, "Honeybog: A Hybrid Webshell Honeypot Framework Against Command Injection," in *2021 IEEE Conference on Communications and Network Security (CNS)* (IEEE, 2021), 218–226.

57. M. Usama and M. N. Aman, "Command Injection Attacks in Smart Grids: A Survey," *IEEE Open Journal of Industry Applications* 5 (2024): 75–85.

58. V. Singh and S. Pandey, "Revisiting Cloud Security Threats: Ip Spoofing," in *Soft Computing: Theories and Applications: Proceedings of SoCTA 2018* (Springer, 2020), 225–236.

59. H. A. Adjei, M. T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah, and E. S. Gyarteng, "Ssl Stripping Technique (Dhcp Snooping and Arp Spoofing Inspection)," in *2021 23rd International Conference on Advanced Communication Technology (ICACT)* (IEEE, 2021), 187–193.

60. V. Kumar and N. Malik, "Machine Learning-Based Attacks Detection in Lot Networks Routing Protocols," in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (IEEE, 2024), 1–6.

61. A. Majumdar, S. Raj, and T. Subbulakshmi, "Arp Poisoning Detection and Prevention Using Scapy," *Journal of Physics: Conference Series* 1911, no. 1 (2021): 012022.

62. Q. M. Ashraf and M. H. Habaebi, "Autonomic Schemes for Threat Mitigation in Internet of Things," *Journal of Network and Computer Applications* 49 (2015): 112–127.

63. S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware Security in Iot Devices With Emphasis on Hardware Trojans," *Journal of Sensor and Actuator Networks* 8, no. 3 (2019): 42.

64. M. Devi and A. Majumder, "Side-Channel Attack in Internet of Things: A Survey," in *Applications of Internet of Things: Proceedings of ICCCIOT 2020* (Springer, 2021), 213–222.

65. A. Mallik, "Man-In-The-Middle-Attack: Understanding in Simple Words," *Cyberspace: Jurnal Pendidikan Teknologi Informasi* 2, no. 2 (2019): 109–134.

66. A. Dua, V. Tyagi, N. Patel, and B. Mehtre, "Iisr: A Secure Router for Iot Networks," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)* (IEEE, 2019), 636–643.

67. A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security Issues in Iiot: A Comprehensive Survey of Attacks on Iiot and Its Countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)* (IEEE, 2018), 124–130.

68. S. M. Morsy and D. Nashat, "D-Arp: An Efficient Scheme to Detect and Prevent Arp Spoofing," *IEEE Access* 10 (2022): 49142–49153.

69. S. Arvind and V. A. Narayanan, "An Overview of Security in Coap: Attack and Analysis," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)* (IEEE, 2019), 655–660.

70. Internet Society, "Internet Protocol Version 6 (ipv6)," https://www.internetsociety.org/deploy360/ipv6/.

71. "Domain Name System Security Extensions (DNSSEC)," https://www.internetsociety.org/deploy360/dnssec/basics/.

72. S. Calzavara, H. Jonker, B. Krumnow, and A. Rabitti, "Measuring Web Session Security at Scale," *Computers & Security* 111 (2021): 102472.

73. V. Kampourakis, G. Kambourakis, E. Chatzoglou, and C. Zaroliagis, "Revisiting Man-In-The-Middle Attacks Against Https," *Network Security* 3 (2022): 2022.

74. D. Diaz-Sanchez, A. Marín-Lopez, F. A. Mendoza, P. A. Cabarcos, and R. S. Sherratt, "Tls/Pki Challenges and Certificate Pinning Techniques for Iot and m2m Secure Communications," *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3502–3531.

75. The CIO Council, "Http Strict Transport Security," https://https.cio.gov/hsts/.

76. A. M. Abdul, A. A. K. Mohammad, P. Venkat Reddy, et al., "Enhancing Security of Mobile Cloud Computing by Trust-and Role-Based Access Control," *Scientific Programming* 2022, no. 1 (2022): 9995023.

77. Juniper Networks, "Understanding How Unicast Reverse Path Forwarding Prevents Spoofed ip Packet Forwarding, Reverse-Path Forwarding," https://juniper.net/documentation/en_US/junos/topics/concept/unicast-rpf-understanding.html.

78. K. Sriram, D. Montgomery, and J. Haas, *Rfc 8704: Enhanced Feasible-Path Unicast Reverse Path Forwarding* (RFC Editor, 2020).

79. I. Ko, D. Chambers, and E. Barrett, "Adaptable Feature-Selecting and Threshold-Moving Complete Autoencoder for Ddos Flood Attack Mitigation," *Journal of Information Security and Applications* 55 (2020): 102647.

80. T. A. S. Srinivas and S. Manivannan, "Prevention of Hello Flood Attack in Iot Using Combination of Deep Learning With Improved Rider Optimization Algorithm," *Computer Communications* 163 (2020): 162–175.

81. J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua, and P. Haskell-Dowland, "Hybrid Routing for Man-In-The-Middle (Mitm) Attack Detection in Iot Networks," in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)* (IEEE, 2019), 1–6.

82. M. Ratchford, O. El-Gayar, C. Noteboom, and Y. Wang, "Byod Security Issues: A Systematic Literature Review," *Information Security Journal: A Global Perspective* 31, no. 3 (2022): 253–273.

83. Y. Barlette, A. Jaouen, and P. Baillette, "Bring Your Own Device (Byod) as Reversed It Adoption: Insights Into Managers' Coping Strategies," *International Journal of Information Management* 56 (2021): 102212.

84. A. Muñoz and E. B. Fernandez, "Tpm, a Pattern for an Architecture for Trusted Computing," *Proceedings of the European Conference on Pattern Languages of Programs* 2020 (2020): 1–8.

85. P. G. Wagner, P. Birnstill, and J. Beyerer, "Establishing Secure Communication Channels Using Remote Attestation With Tpm 2.0," in *Security and Trust Management: 16th International Workshop* (Springer, 2020), 73–89.

86. G. Messina, "Tpms or Hsms and Their Role in Full-Disk Encryption (FDE)," https://resources.infosecinstitute.com/topic/tpms-or-hsms-and-their-role-in-full-disk-encryption-fde/.

87. M. Thankappan, H. Rifà-Pous, and C. Garrigues, *A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-In-The-Middle Attacks Against Protected Wi-Fi Networks* (IEEE Access, 2024).

88. S. M. Kasongo and Y. Sun, "A Deep Learning Method With Wrapper Based Feature Extraction for Wireless Intrusion Detection System," *Computers & Security* 92 (2020): 101752.

89. A. A. Olazabal, J. Kaur, and A. Yeboah-Ofori, "Deploying Man-In-The-Middle Attack on Iot Devices Connected to Long Range Wide Area Networks (Lorawan)," in *2022 IEEE International Smart Cities Conference (ISC2)*, vol. 2022 (IEEE, 2022), 1–7.

90. R. Zagrouba and R. Alhajri, "Machine Learning Based Attacks Detection and Countermeasures in Iot," *International Journal of Communication Networks and Information Security* 13, no. 2 (2021): 158–167.

91. N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and Privacy in Iot Using Machine Learning and Blockchain: Threats and Countermeasures," *ACM Computing Surveys* 53, no. 6 (2020): 1–37.

92. A. Ghosh and A. Senthilrajan, "An Approach for Detecting Man-In-The-Middle Attack Using Dpi and Dfi," in *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2019)* (Springer, 2020), 563–574.

93. O. Fonseca, Í. Cunha, E. Fazzion, et al., "Identifying Networks Vulnerable to Ip Spoofing," *IEEE Transactions on Network and Service Management* 18, no. 3 (2021): 3170–3183.

94. T. Ehrenkranz and J. Li, "On the State of Ip Spoofing Defense," *ACM Transactions on Internet Technology* 9, no. 2 (2009): 1–29.

95. O. Toutsop, P. Harvey, and K. Kornegay, "Monitoring and Detection Time Optimization of Man in the Middle Attacks Using Machine Learning," in *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)* (IEEE, 2020), 1–7.

96. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in Iot Security: Current Solutions and Future Challenges," *IEEE Communications Surveys & Tutorials* 22, no. 3 (2020): 1686–1721.

97. H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of Iot Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors* 20, no. 13 (2020): 3625.

98. M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-Iiotset: A New Comprehensive Realistic Cyber Security Dataset of Iot and Iiot Applications for Centralized and Federated Learning," *IEEE Access* 10 (2022): 40281–40306.

99. N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A Mechanism for Securing Iot-Enabled Applications at the Fog Layer," *Journal of Sensor and Actuator Networks* 8, no. 1 (2019): 16.

100. H. HaddadPajouh, R. Khayami, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "Ai4safe-Iot: An Ai-Powered Secure Architecture for Edge Layer of Internet of Things," *Neural Computing and Applications* 32, no. 20 (2020): 16119–16133.

101. N. Sivasankari and S. Kamalakkannan, "Detection and Prevention of Man-In-The-Middle Attack in Iot Network Using Regression Modeling," *Advances in Engineering Software* 169 (2022): 103126.

102. A. M. Banaamah and I. Ahmad, "Intrusion Detection in Iot Using Deep Learning," *Sensors* 22, no. 21 (2022): 8417.

103. Á. Michelena, J. Aveleira-Mata, E. Jove, et al., "A Novel Intelligent Approach for Man-In-The-Middle Attacks Detection Over Internet of Things Environments Based on Message Queuing Telemetry Transport," *Expert Systems* 41, no. 2 (2024): e13263.

104. G. Gkogkos, C. Patsonakis, A. Drosou, and D. Tzovaras, "A Dlt-Based Framework for Secure Iot Infrastructure in Smart Communities," *Technology in Society* 74 (2023): 102329.

105. K. Gupta, K. D. Gupta, D. Kumar, G. Srivastava, and D. K. Sharma, "Bids: Blockchain and Intrusion Detection System Coalition for Securing Internet of Medical Things Networks," *IEEE Journal of Biomedical and Health Informatics* (2023): 1–9.

106. M. Jouhari, N. Saeed, M.-S. Alouini, and E. M. Amhoud, "A Survey on Scalable Lorawan for Massive Iot: Recent Advances, Potentials, and Challenges," *IEEE Communications Surveys & Tutorials* 25, no. 3 (2023): 1841–1876.

107. B. D. Deebak and F. Al-Turjman, "A Hybrid Secure Routing and Monitoring Mechanism in Iot-Based Wireless Sensor Networks," *Ad Hoc Networks* 97 (2020): 102022.

108. P. Podder, M. Mondal, S. Bharati, and P. K. Paul, "Review on the Security Threats of Internet of Things," *International Journal of Computer Applications* 176, no. 41 (2020): 37–45.