IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 14 March 2025, accepted 3 May 2025, date of publication 4 June 2025, date of current version 12 June 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3576355

SURVEY

Navigating IoT Security: Architectures, Emerging Threats, and Adaptive Countermeasures

FARAH KANDAH, (Senior Member, IEEE), THILINA MENDIS, (Student Member, IEEE), LALITH MEDURY, (Student Member, IEEE), HEMANT SHERAWAT, AND HAOFAN WANG
Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA
Corresponding author: Farah Kandah (farah-kandah@auburn.edu)

ABSTRACT The Internet of Things (IoT) has revolutionized modern life, yet its interconnected nature poses significant security challenges. This survey investigates threats and countermeasures associated with IoT ecosystems, categorizes threats targeting network infrastructure, devices, and data security, and provides a taxonomy to understand vulnerabilities. By analyzing IoT architectures—including Cloud, Fog, and Edge—the study highlights how each architecture presents distinct vulnerabilities when integrated with IoT systems. It explores research on several countermeasures, including intrusion detection systems, secure authentication protocols, blockchain technology, and machine learning integration, evaluating both their advantages and limitations. Through a systematic review of recent literature, the survey identifies articles that contribute to IoT security understanding. The study advocates for lightweight, adaptable security measures that can be applied across diverse architectures and emphasizes the importance of standardized protocols through collaborative efforts among stakeholders. By mapping the current IoT security landscape, this survey guides future research and development toward a more secure and resilient IoT ecosystem, emphasizing the need for both innovation and standardization. Additionally, it critically evaluates the effectiveness of existing solutions and provides actionable insights into addressing the evolving security challenges within IoT environments.

INDEX TERMS IoT, security, architecture, countermeasures, cloud, edge, fog.

I. INTRODUCTION

The Internet of Things (IoT) has experienced exponential growth, connecting billions of devices and enabling transformative solutions for various domains [1]. It is estimated that billions of IoT devices are currently in use, with projections indicating a substantial increase over the coming years [1]. According to Forbes, by the end of 2024, approximately 207 billion IoT devices are expected to be connected to the Internet [2].

IoT architectures, serving as the backbone for a wide range of applications, from basic smart home devices to complex industrial automation systems, are susceptible to numerous cyber threats that exploit weaknesses in various architectural layers [3]. Over the years, many architectures and methodologies have been proposed and thoroughly investigated in IoT research offering comprehensive reviews of IoT technologies from diverse perspectives [4], [5]. These architectures and methodologies are essential as IoT systems operate across multiple layers, networks, and applications, each with its own vulnerabilities and requirements, necessitating secure and structured frameworks to ensure reliable operation.

This survey focuses on three core architectures—Edge Computing, Fog Computing, and Cloud Computing—each of which has distinct challenges and vulnerabilities when integrated with IoT devices [6], [7], [8]. For instance, Edge Computing processes data closer to the data source, which can potentially reduce latency and bandwidth usage but also introduces additional attack vectors due to limited processing power [6]. Similarly, Fog Computing, which provides a distributed approach to complement Edge and Cloud computing, faces its own security challenges, particularly in terms of data privacy and integrity [7]. On the other hand, cloud-based IoT architectures benefit from substantial

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

computational resources but are still vulnerable to attacks targeting data in transit or at rest, and there is added latency when communicating with the cloud server [7].

Countermeasures against these threats are multifaceted, ranging from advanced encryption methods to secure authentication protocols. However, the efficacy of these measures often comes with compromises in terms of computational overhead, complexity, or usability, presenting a significant challenge in their widespread adoption [6], [7], [9].

This survey provides an in-depth analysis of Cloud, Fog, and Edge architectures, with a particular focus on the myriad threats they encounter when interfacing with IoT devices. Furthermore, it explores the countermeasures that can help mitigate these risks.

This survey systematically categorizes threats, explores countermeasures, and critically evaluates their strengths and limitations. This analysis is structured around the following key aspects:

- **Identify threats associated with various IoT architectures:** Investigate the different threats associated with IoT devices and identify which architectures are most vulnerable to these threats.
- **Explore available countermeasures against these threats:** Categorize and review the threats associated with IoT devices, along with the countermeasures proposed and implemented by the research community.
- **Evaluate the pros and cons of these countermeasures:** Assess various existing security measures, from advanced encryption techniques to secure authentication protocols, and critically analyze their strengths and weaknesses, highlighting the advantages and limitations of the proposed solutions.

This survey aims to contribute to the field of IoT security by critically analyzing threats and countermeasures, providing readers with a thorough understanding of current challenges. It not only outlines the various security threats and their countermeasures but also provides a critical assessment of the effectiveness of current solutions.

The survey is structured as follows: Section II provides the background information to give readers foundational insights into the topics discussed in later sections. Section III covers related surveys, followed by our motivations. In Section IV, we detail the design and process of our survey. Section V presents an analysis of IoT architectures and the associated threats, along with a review of countermeasures used to address these risks and a critical evaluation of their limitations. Finally, the conclusion is presented in Section VI.

II. BACKGROUND

The Internet of Things is a network of physical objects [10]. It can be defined as a system of interconnected machines, encompassing billions of physical devices collecting or sharing data around the globe that are connected via the internet. IoT devices utilize universal computing methods, spanning from basic environmental sensors to advanced industrial machinery, often referred to as part of the Industrial

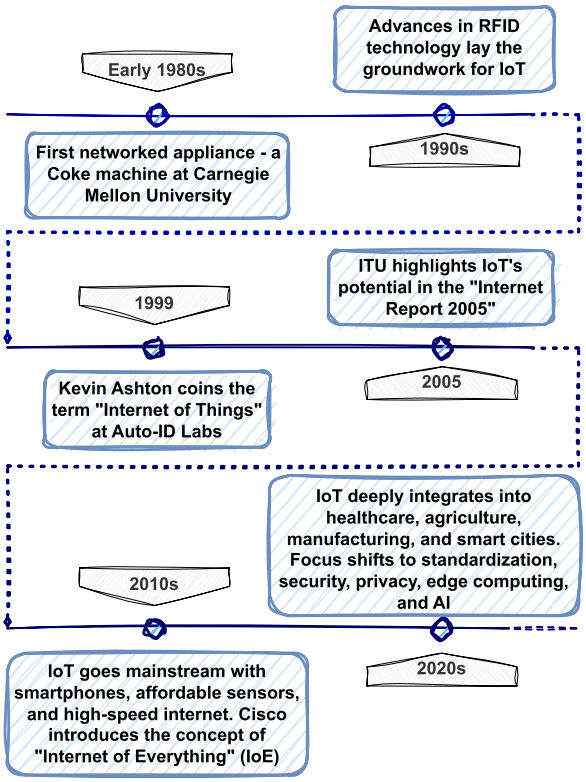


FIGURE 1. Overview of the IoT timeline.

Internet of Things (IIoT) [11]. These devices utilize advanced data analytics and machine learning algorithms to enable intelligent decision-making, driving automation, and efficiency in various domains, such as smart homes, agriculture, healthcare, and industrial automation systems [12].

A. HISTORY OF IoT

The history of IoT traces its evolution from basic networked appliances to a globally transformative technology, as depicted in Figure 1. The concept originated in the early 1980s with the first IoT device, a modified Coke machine at Carnegie Mellon University [13]. Significant advancements in Radio Frequency Identification (RFID) technology during the 1990s laid the groundwork for IoT applications. In 1999, Kevin Ashton coined the term 'Internet of Things' at MIT's Auto-ID Labs to describe a system where physical objects are connected to the internet via sensors [14], [15].

The 2000s marked the integration of RFID, wireless technologies, and Micro Electromechanical Systems (MEMS), enabling remote sensing and control of objects [16]. By the 2010s, IoT became mainstream, driven by the proliferation of smartphones, cost-efficient sensors, and high-speed internet, with concepts like Cisco's 'Internet of Everything' expanding IoT's scope to include people [17].

Today, IoT is deeply embedded across sectors such as healthcare, agriculture, manufacturing, and smart cities, driving innovation and efficiency. Emerging trends emphasize edge and fog computing, AI for localized decision making,

and addressing challenges in standardization, security, and privacy [6], [7], [18], [19].

B. CORE COMPONENTS IN THE INTERNET OF THINGS

Every IoT system requires certain fundamental components for efficient operations. Key elements like sensors, actuators, and controllers are essential for the smooth functioning of any IoT setup [20]. Sensors collect environmental data and send it to controllers, which then process the information and determine the best course of action to take based on preset rules and algorithms. Actuators then carry out these actions by altering the physical state of the system. This loop of sensing, decision-making, and acting allows IoT devices to operate intelligently and autonomously [7]. Figure 2 depicts an example of the communication between the components.

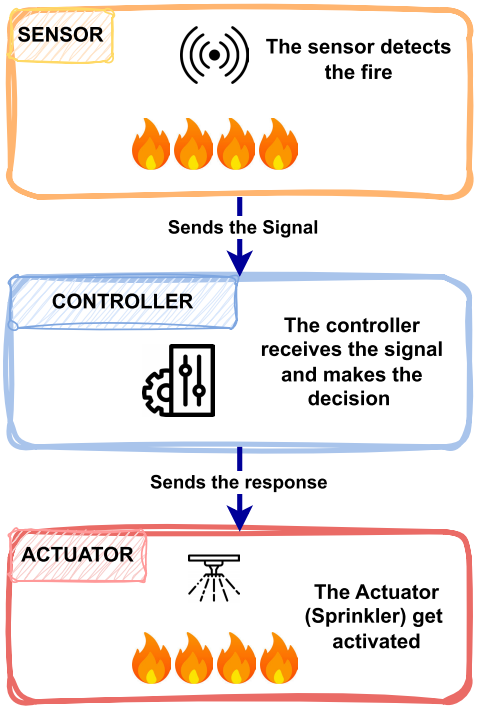


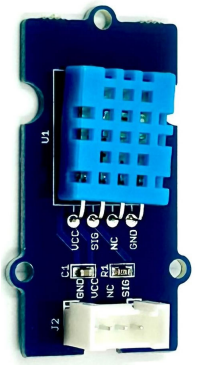
FIGURE 2. The sensor to actuator flow.

1) SENSORS

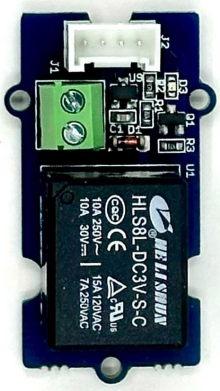
Sensors detect and measure changes in an environmental or physical conditions such as temperature, motion, and pressure. These devices are the foundation of IoT systems, providing data for decision-making and automation [20]. For example, the Grove Humidity Sensor (Figure 3a) measures humidity levels and transmits the data to the controllers, enabling efficient environmental monitoring [7].

2) ACTUATORS

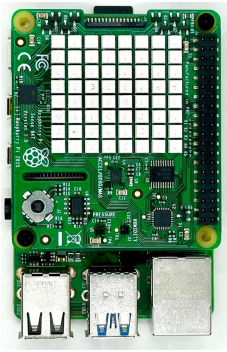
Actuators translate digital commands into physical actions, enabling IoT devices to interact with their surroundings. For instance, the Grove Relay (Figure 3b) acts as a switch for controlling high-power electrical circuits, making it



(a) Grove Humidity Sensor



(b) Grove Relay



(c) Raspberry Pi with Sense HAT

FIGURE 3. Sample of internet of things components (Seed studio grove).

ideal for applications such as motor control [20]. These components are critical for automating physical processes in IoT systems [7].

3) CONTROLLERS

Controllers act as the central processing units in IoT systems, managing input from sensors and directing actuators to perform specific tasks. Devices like the Raspberry Pi (Figure 3c) serve as versatile controllers capable of integrating and optimizing IoT components for efficient operation [7]. By bridging sensors and actuators, controllers ensure seamless data processing and system automation [20].

C. IoT-BASED ARCHITECTURE

In the domain of IoT, the term 'architecture' encompasses the dynamic and structured configuration of various components that enable the efficient management, processing, and transmission of data among a vast network of IoT devices and computing systems [21]. An IoT-based architecture is generally composed of three primary layers, though in certain instances, more complex multilayered architectures have also been implemented to cater to specific needs [22]. These foundational layers are comprised of several critical elements including sensors, actuators, connectivity protocols, data processing units, and application interfaces, each playing a

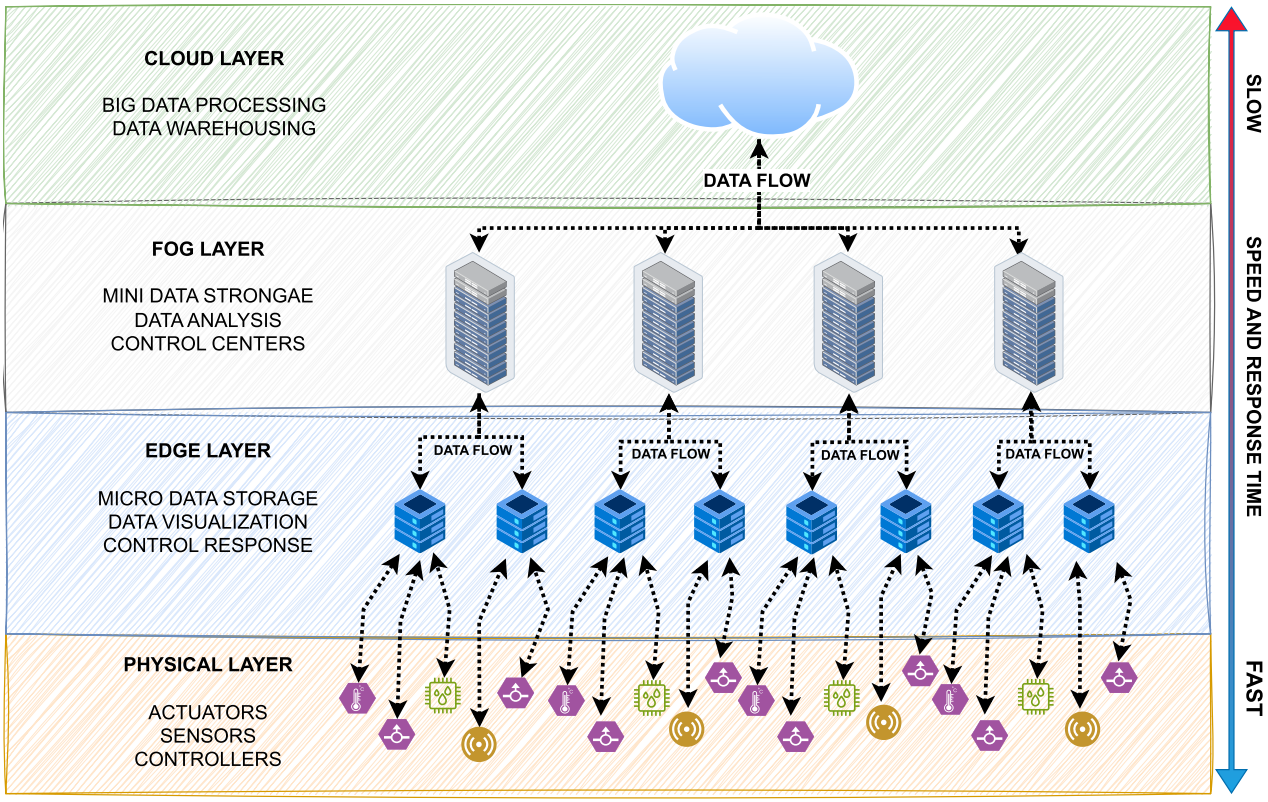


FIGURE 4. IoT architecture consisting of cloud, edge, fog, and physical layers.

pivotal role in ensuring the seamless operation of the IoT ecosystem.

Establishing a well-defined and task-focused IoT architecture brings a myriad of advantages, significantly enhancing system efficiency, scalability, security, and interoperability. These advantages are crucial as they enhance how data is processed, ensure the network can scale to include more devices, protect against cyber threats, and allow different technologies to work together seamlessly. To achieve these benefits, integrating cloud, edge, and fog computing into the IoT architecture is essential [21]. This integration not only extends the IoT infrastructure but also enables better management of data flow from the devices at the network's edge to the topmost layers. An overview of the IoT architecture is illustrated in Figure 4.

The three primary architectures (cloud, fog, and edge computing) play distinct yet complementary roles in IoT ecosystems. Table 1 summarizes a comparative analysis of these architectures.

1) CLOUD-BASED ARCHITECTURE

Cloud computing facilitates centralized data processing and storage over the Internet, offering scalable and on-demand resources for IoT systems [23]. Its key advantages include scalability, availability, and cost efficiency, making it well-suited for managing large volumes of IoT-generated data [24]. However, cloud-based architectures pose challenges, particularly for applications requiring real-time responsiveness. Issues such as high latency, increased bandwidth usage, and dependence on stable internet connectivity can hinder performance in latency-sensitive IoT deployments [25]. Moreover, transmitting sensitive data to centralized cloud providers raises security and privacy concerns, including the risk of potential data breaches [26]. While cloud computing excels in centralized analytics and scalability, alternative approaches like fog and edge computing are often more effective for real-time, low-latency IoT applications.

2) FOG-BASED IoT ARCHITECTURE

Fog computing extends cloud capabilities by processing data closer to its source, typically at intermediary nodes known as fog nodes. This approach reduces latency and bandwidth consumption, making it ideal for IoT applications that require near real-time processing and decision-making [25]. By keeping data processing and storage closer to end devices, fog computing enhances security and privacy by minimizing the transmission of sensitive data over public networks [27]. It also mitigates bandwidth constraints by performing preliminary data filtering and analysis locally. However, fog architectures introduce additional complexity and infrastructure costs compared to centralized cloud systems. Managing distributed fog nodes requires robust

TABLE 1. Comparison of cloud computing, fog computing, and edge computing.

Feature	Cloud Computing	Fog Computing	Edge Computing
Location of Processing	Centralized, distant from data source	Intermediate, near data source	At the data source or device
Latency	High	Moderate	Low
Bandwidth Usage	High	Moderate	Low
Security	Lower	Moderate	Higher
Scalability	High	Moderate	Low
Cost	Low	Moderate	Higher
Best Use Case	Big data analytics, global services	Smart cities, connected vehicles	Real-time applications, IIoT

security controls and increases the challenge in ensuring system-wide scalability and reliability [28], [29]. Despite these challenges, Fog computing is particularly well-suited for IoT scenarios such as smart cities and industrial automation, where localized processing can improve responsiveness and reduce dependence on centralized resources [6], [7]. While fog computing offers a middle ground between cloud and edge architectures, edge computing pushes processing even closer to the data source, enabling ultra-low-latency IoT applications.

3) EDGE-BASED IoT ARCHITECTURE

Edge computing brings data processing and storage directly to the source of data generation, enabling real-time decision-making with ultra-low latency and reduced bandwidth requirements [7]. By minimizing the need to transmit large volumes of data to centralized cloud or fog nodes, edge architectures enhance responsiveness and alleviate network congestion [30]. This localized processing also improves data security and privacy, as sensitive information can be processed and retained closer to the device, reducing exposure to potential threats during transmission [27]. Edge computing is particularly beneficial in Industrial IoT (IIoT) environments, where large volumes of sensor data require immediate analysis to support automation and critical operations [31], [32]. However, the distributed nature of edge architectures increase system complexity and maintenance overhead. Scalability can also be limited, as deploying and managing a large number of edge nodes requires significant resources and robust security measures [30]. Despite these challenges, edge computing complements cloud and fog architectures in hybrid IoT systems, delivering an optimal balance of latency, scalability, and cost for diverse application scenarios.

III. EXISTING SURVEYS

In this section, we review the latest research on security solutions for the Internet of Things (IoT) ecosystem and categorize existing surveys based on their specific areas of interest. This section aims to offer a clear overview of the current survey landscape and underscores the unique characteristics of our survey.

A. ARCHITECTURE-FOCUSED SURVEYS

A survey on IoT architectures (Cloud, Fog, and Edge) and their security implications was presented in [6], where the authors provided a foundational understanding of IoT security and privacy including the discussion of unique security vulnerabilities and threats associated with each architectural layer, considering critical factors such as scalability, efficiency, latency, and security. Additionally, the survey addresses the integration of Cyber-Physical systems (CPS) with IoT, focusing on issues of confidentiality, integrity, and availability.

The integration of 5G wireless systems with IoT was covered in another survey, focusing on research initiatives and industry visions for 5G-enabled IoT architectures [33]. The survey highlights several key technologies that enable 5G IoT, and other application areas where 5G architectures can be implemented including smart cities, healthcare, agriculture, and transportation. While it primarily addresses the potential benefits and improvements offered by 5G networks, it provides a less detailed analysis of specific security challenges and countermeasures.

Swessi et. al provided a taxonomy of IoT security issues based on IoT architecture, categorizing threats and countermeasures across different layers (perception, network, support, and application) [34]. The authors emphasized the architectural aspects of IoT security and discussed how emerging technologies like Blockchain and AI can address these challenges. However, the survey lacks a critical evaluation of countermeasures in terms of metrics such as resource limitations, cost, and scalability, which are essential for assessing the proposed countermeasures' practicality in real-world IoT deployments.

In contrast, our survey extends beyond these studies by offering a more in-depth exploration of security threats and vulnerabilities inherited in various IoT architectures, regardless of the underlying network technology. While previous surveys provide a solid foundation for understanding the architectural and technological aspects of IoT, we aim

to deliver a more thorough examination of the specific security challenges faced by IoT systems and the current architectural-specific countermeasures aiming to enhance IoT security.

B. APPLICATION-FOCUSED SURVEYS

Other surveys focused on examining security threats across key application areas of IoT, such as smart cities, healthcare, and industrial automation. The authors in [7] provided a detailed review of security-related challenges and threats in the IoT ecosystem. The survey highlighted various emerging technologies focused on achieving high trust among IoT devices, through the integration of blockchain, fog computing, edge computing, and machine learning to enhance IoT device security. While highlighting the potential of machine learning (ML) and blockchain for enhancing security, it lacks a detailed analysis of the limitations and challenges associated with these technologies. For example, it doesn't consider the resource constraints and scalability issues that can hinder the widespread adoption of these solutions in real-world IoT deployments.

Vulnerabilities and risks related to smart home security were surveyed and analyzed through the framework of the CIA triad (Confidentiality, Integrity, Availability) in [35]. While offering valuable insights into this specific application domain, its scope is limited to smart home security, neglecting the broader security landscape of IoT. This limits its relevance to understanding the overall security challenges faced by IoT devices and systems. Finally, the work presented by Ahmed et. al focused on the application of IoT forensics in areas such as criminal investigations, incident response, and legal processes [36]. The authors discussed challenges in extracting and analyzing evidence from IoT devices and networks, as well as the procedural and ethical issues in IoT forensics. However, the authors do not critically analyze the scalability of forensic solutions in large-scale IoT networks.

In contrast, our work broadens the scope by examining a wide range of IoT applications and architectures, offering a comprehensive view of the overall security landscape. This enables us to present a holistic perspective on IoT security, addressing threats, and vulnerabilities across different domains. Additionally, our survey critically evaluates the effectiveness and applicability of various countermeasures, taking into account factors such as resource constraints and scalability.

C. TECHNOLOGY-FOCUSED SURVEYS

Three surveys were identified with a focus on the technology behind IoT security, such as forensics, machine learning, and blockchain. One survey examined the emerging field of IoT forensics, exploring challenges, approaches, and open issues. While it highlights the potential of blockchain for establishing a secure chain of custody for digital evidence, it does not extensively cover other forensic techniques or the integration of forensics with broader security strategies [37].

Another survey explored the use of Machine Learning (ML) and Deep Learning (DL) techniques for enhancing IoT security, detailing the technical challenges involved in implementing these models [38]. However, the focus remained on the technical aspects of ML/DL algorithms, without fully addressing the practical challenges and limitations of real-world deployments, such as scalability and resource constraints.

Williams et. al [39] explored the integration of emerging technologies such as machine learning, blockchain, and quantum computing into IoT security. The authors identified and discussed the challenges and solutions associated with these technologies, including lightweight cryptographic solutions and hardware-based security measures. However, the authors do not critically evaluate the practical challenges, such as scalability, resource constraints, and real-world implementation issues. Further, this work does not adequately address application-specific security challenges or provide a critical evaluation of lightweight security solutions tailored for resource-constrained IoT devices.

In contrast, our survey broadens the scope by considering the interaction between various security technologies and assessing their effectiveness within a larger IoT ecosystem.

D. OUR SURVEY

Our Survey aims to provide a thorough evaluation of the security landscape for the Internet of Things (IoT), focusing on the challenges and countermeasures within the context of Cloud, Fog, and Edge computing architectures. Table 2 provides an overview of the comparison between our survey and the current surveys considering the focus areas and the security aspects that are covered in each survey. In our survey and to address the research gaps, we categorize the security threats faced by IoT devices into three categories: Network-Related, Device-Related, and Data-Related threats. The taxonomy used to define these threats is further explained in Section V. This classification helps identify the most critical threats and tailor our analysis accordingly.

For each of the identified threat categories, we conducted an in-depth analysis of the countermeasures proposed in existing research. This involves examining a range of techniques, including traditional security measures like firewalls and intrusion detection systems (IDS), emerging technologies such as blockchain and fog computing, and approaches like behavioral analysis. We analyzed the advantages, disadvantages, and limitations of each countermeasure, considering the following questions:

- Can the countermeasure be effectively applied in real-world IoT environments that have limited resources?
- Is the countermeasure capable of managing the growing number of IoT devices and the increasing volume of data they generate?
- Does the countermeasure demand significant computational power or storage capacity to function effectively?

TABLE 2. Comprehensive Comparison of IoT security aspects and threats in different technology contexts.

Authors	Focus Area	IoT Security Aspects Covered	Identified Research Gaps	Network-Related Threat	Data-Related Threat	Device-Related Threat	Technology Contexts
Lin et al. [6]	Architectural	General overview of IoT security and privacy	Lacks focus on specific threats and countermeasures for different architectural layers	✓	✓	✓	Cloud, Edge, Fog
Hassija et al. [7]	Application-Specific	Security threats and solutions in various IoT applications	Limited analysis of limitations and challenges of proposed countermeasures	✓	✓	✓	Cloud only
Chettri & Bera [33]	Architectural	5G and IoT: architectural overview, security challenges, potential improvements	Limited focus on specific security countermeasures and their effectiveness	✓	✓	✓	5G only
Stoyanova et al. [37]	Technology-Specific	IoT forensics: challenges, approaches, open issues	Limited coverage of forensic techniques and integration with broader security strategies	✓	×	✓	None
Al-Garadi et al. [38]	Technology-Specific	ML/DL for IoT security	Lack of focus on practical challenges and limitations of ML/DL in real-world IoT deployments	✓	×	✓	Edge only
Hammi et al. [35]	Application-Specific	Smart home security: vulnerabilities, risks, countermeasures	Limited scope to a specific application domain	✓	×	✓	None
Ahmed et al. [36]	Application-Specific	IoT forensics: challenges, approaches, and open issues	Lack of standardization, limited focus on scalability, and insufficient exploration of emerging technologies	✓	✓	✓	Cloud, Edge, Fog
Swessi et al. [34]	Architectural	IoT security threats and countermeasures categorized by IoT architecture layers and emerging technologies	Limited analysis of practical challenges, scalability issues, and resource constraints in real-world deployments	✓	✓	✓	5G
Williams et al. [39]	Technology-Specific	IoT security threats and solutions with a focus on emerging technologies like ML, blockchain, and quantum computing	Limited analysis of practical challenges, scalability, and application-specific security issues	✓	✓	✓	Cloud, Edge
Our Survey	Comprehensive	Threat taxonomy, countermeasure analysis, comparative analysis, emerging trends, future research directions	Need for lightweight security solutions, standardization and interoperability challenges, AI/ML integration for threat detection, privacy-preserving analytics	✓	✓	✓	Cloud, Edge, Fog, 5G

- How well does the countermeasure mitigate the specific threat it was designed to address?
- Does the implementation of the countermeasure introduce any significant limitations?
- Whether the architecture contributes to specific threats within the IoT network?

To address these questions, we selected several research articles that provided relevant insights into the identified threats and countermeasures. This selection was based on a thorough analysis according to our methodology presented in Section IV. Following this rigorous and detailed methodology, our survey offers a comprehensive and critical analysis of IoT security, addressing the limitations of prior research and contributing to a better understanding of the threats that IoT devices face in each architecture.

IV. METHODOLOGY

Through our data collection, we considered proceedings and journal publications from three digital libraries: IEEE Xplore [40], ACM Digital Library [41], and Science Direct [42] between 2020 - 2024. The article selection process is illustrated in Figure 5.

A. ARTIFACTS COLLECTION

To collect research articles, we applied the following search strings on digital libraries' search engine: "IoT", "Architecture", "Security", "Threats", and "Countermeasures". Additionally, different combinations and synonyms of these search terms were also applied to retrieve relevant articles. The precise search queries include:

- "IoT" AND "Architecture" AND "Threats"
- "IoT" AND ("Security" OR "Threats")
- "IoT" AND "Security" AND ("Threats" OR "Countermeasures")
- "IoT" AND ("Threats" OR "Countermeasures")
- "IoT" AND "Threats" AND "Framework"
- "IoT" AND "Threats" AND "Design"
- "IoT" AND ("Vulnerabilities" OR "Countermeasures")
- "IoT" AND ("Vulnerabilities" OR "Mitigations")
- "IoT" AND "Framework" AND ("Vulnerabilities" OR "Mitigations")
- "IoT" AND "Framework" AND ("Threats" OR "Countermeasures")

The search was applied to all metadata in the digital library's search feature. This study focuses on the latest research, therefore we applied a date filter to retrieve artifacts between 2020 - 2024. Our initial search yielded 347 results across all three digital libraries.

B. INCLUSION AND EXCLUSION CRITERIA

To ensure the selection of relevant research articles for our study, we applied a rigorous inclusion and exclusion process. The research articles' abstracts were reviewed manually and

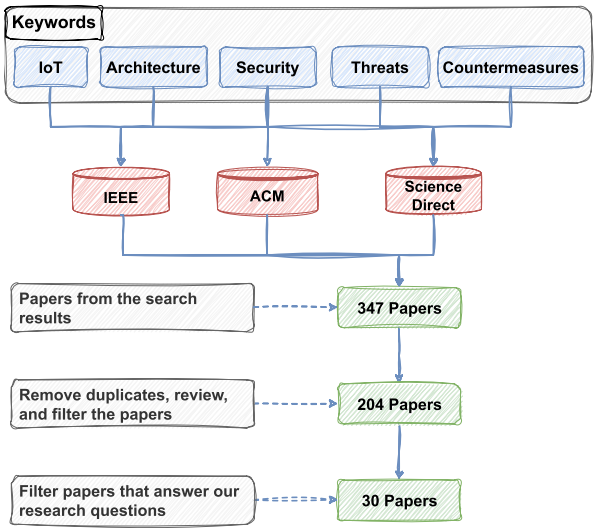


FIGURE 5. Artifacts selection process.

articles matching any of the criteria below were selected in our studies:

- Relevance to IoT Threat Models and Architectures: Articles were included if they explicitly addressed IoT-related threat models, security challenges, or architectural frameworks. This ensured that the selected studies were directly aligned with the research objectives.
- Focus on Original Research: Only original research articles were considered. These articles presented novel findings, methodologies, or frameworks rather than summarizing or reviewing existing literature. This was essential to ensure that the studies provided novel and meaningful contributions to the field.
- Application to IoT Infrastructures: Articles were included if they examined architectures specifically developed for or applied to IoT infrastructures. This ensured that the research was directly applicable to IoT systems.

The exclusion criteria was applied to identify and remove articles that were not relevant to our study's objectives according to the following criteria:

- Duplicate articles retrieved from multiple digital libraries were removed by filtering for unique titles. This step ensured that each article in the dataset was distinct and not repeated.
- Articles categorized as surveys, systematic reviews, or general reviews were excluded. This was determined by identifying keywords such as "Survey," "Systematic Review," or "Review" in the titles. The rationale was to focus on original research rather than secondary analyses or summaries of existing work.

We consider these set of key aspects throughout our research:

- What specific security challenge does the article address?
- What countermeasure does the article propose to mitigate the identified threat?
- How does the article evaluate the effectiveness of the proposed countermeasure? What benefits and drawbacks of the countermeasure are discussed by the authors?

C. ARTICLE CATEGORIZATION

From the remaining articles, the research team conducted an in-depth analysis of each article to evaluate their relevance to IoT architectures, security, threats, and data privacy. After a comprehensive review, we identified and selected 30 articles that specifically focused on threats and corresponding countermeasures within the context of IoT infrastructure.

V. THREATS AND COUNTERMEASURES ANALYSIS

We present the threat taxonomy illustrated in Figure 6, which is utilized to classify the various threats encountered by IoT systems into three primary categories: Network-related, Device-related, and Data-related threats. Additionally, we outline the proposed countermeasures designed to address these challenges and summarized the related articles in Tables 3, 4, 5, and 6 for Fog, Edge, Cloud, and Hybrid architectures respectively. We provide a summary of the pros and cons of each of the proposed countermeasures in Table 7, and a clear mapping of the threats identified in existing literature and their corresponding countermeasures in Table 8.

A. NETWORK-RELATED THREATS

The chosen architectures including Cloud, Fog, and Edge significantly influence the emergence of network-related threats in IoT systems. Malicious Traffic Injection, associated with Cloud architecture, showcases vulnerabilities in centralized systems that attackers can exploit to disrupt data transmission. Denial of Service (DoS) attacks categorized as Fog and Edge threats reveal how networks can be overwhelmed due to their reliance on resource-constrained devices. Additionally, Traffic Policy Exploitation and Network Congestion highlight weaknesses in security policies within the Edge architecture, which can be manipulated by attackers.

IoT devices are often connected to wireless networks for functionality, making network-related vulnerabilities a significant concern. Threats that aim to disrupt or disable the IoT network, affecting its availability and overall performance, fall under this category. Common examples include Denial of Service (DoS) attacks and side-channel attacks, which are designed to overwhelm or exploit network vulnerabilities, leading to service outages or reduced functionality [63].

1) **Denial of Service Attack:** One of the most common network-related threats are the Denial-of-Service (DoS) or the Distributed DoS (DDoS) attacks launched on IoT devices [6]. IoT devices often have limited processing power and are resource-constrained, making them vulnerable to DoS attacks. These limitations mean that IoT devices can be easily overwhelmed by a flood of malicious traffic, causing them to become unresponsive or fail to function correctly.
2) **SYN Flood Attacks:** A SYN flood attack is a type of Denial-of-Service (DoS) attack that specifically targets the TCP handshake process used to establish connections between devices in a network [72]. In this attack, the attacker exploits the way a legitimate device responds to a SYN (synchronize) packet, which is part of the three-step TCP handshake (SYN, SYN-ACK, ACK) that initiates a connection between two devices [72].
3) **Traffic Policy Exploitation Attacks:** Traffic policy exploitation attacks involve manipulating or bypassing the security policies designed to manage network traffic [3]. These attacks exploit weaknesses in the predefined rules and policies that describe how traffic is routed within the network.
4) **Network Overwhelming Attacks:** Network overwhelming attacks are designed to flood a network or its components with excessive traffic [6]. This malicious traffic overwhelms network resources, causing legitimate requests to be delayed or denied, leading to disruptions in service.

1) PROPOSED COUNTERMEASURES

One approach to monitoring DoS attacks is behavioral analysis. SXC4IoT attempted to prevent DoS attacks by detecting the device's behavior and communication patterns, and whether it is deviating from the defined actions for that specific device [63]. These patterns are stored in a security contract, and a centralized fog node is responsible for monitoring network traffic in real-time to differentiate malicious and normal traffic. Aegis+ took a similar approach by collecting data on user activities and developed a user-specific context model [73]. Aegis+ continuously updates and trains this model using real-time data and user feedback to enhance its accuracy and effectiveness in identifying potential threats. This model, when provided with user activity data can predict whether the traffic is malicious or benign.

DoS attacks can also be achieved through SYN flood attacks, as demonstrated in the FUPE framework [60]. The FUPE model worked towards mitigating SYN flood attacks by combining attack detection and secure task scheduling. Attack detection is achieved through a credit-based connection rate-limiting to detect suspicious connection patterns from user's devices. Additionally, the secure task scheduling module assigns tasks from validated users' devices to trustworthy fog devices. The combination of the two modules effectively blocked malicious requests by identifying requests originating from malicious nodes.

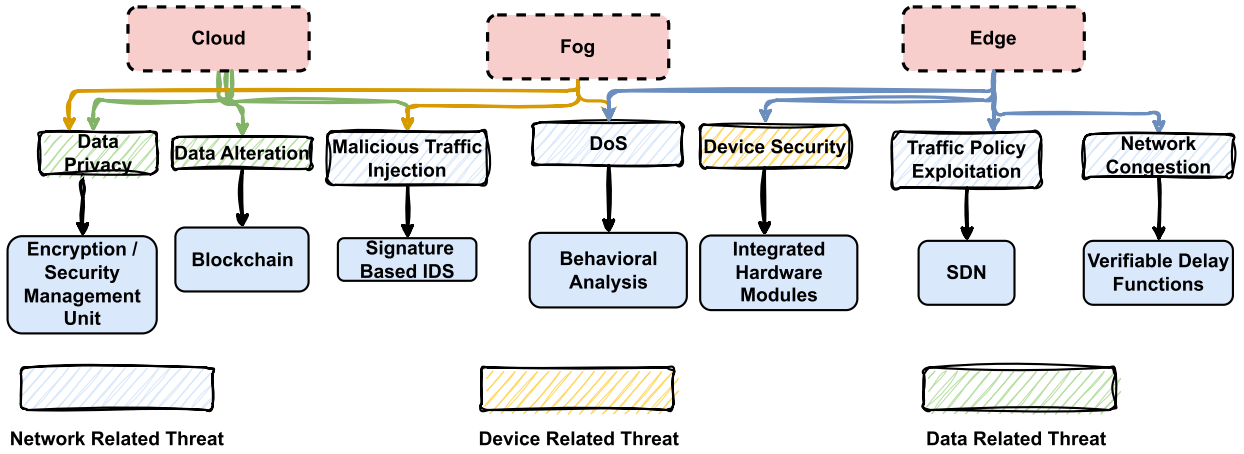


FIGURE 6. IoT threat taxonomy and countermeasures.

TABLE 3. IoT security threats and countermeasures - fog-based architecture.

Authors	Threats/Impact	Countermeasures
Attias et al. [43]	DoS attacks preventing data processing	Verifiable Delay Function for consensus instead of blockchain to avoid transaction fees and improve efficiency
Hroub et al. [44]	Data privacy/security risks due to limited device resources	Security Management Unit for managing sensitive data (keys, encryption, secure transfer)
Bouzzati et al. [45]	Memory corruption attacks on IoT gateways	Hardware-based IDS below LoRaWAN physical layer for detecting memory corruption attacks
Ebrahimi et al. [46]	Network compromise from colluding IoT devices	Context-aware trust evaluation scheme resistant to bad-mouthing, good-mouthing, and on-off attacks
Malche et al. [47]	Vulnerabilities in IoT devices due to weak firmware and lack of secure boot mechanisms	Proposes a lightweight firmware validation mechanism to prevent unauthorized firmware updates and ensure device integrity
Tamri et al. [48]	Compromised patient privacy, potential tampering with medical data, delays in healthcare service delivery, and resource exhaustion in IoT devices	Integrate a secure software-defined fog gateway that reduces latency by processing data near the source, secures data exchanges using blockchain for privacy and integrity, and uses an SDN controller to manage and monitor IoT devices efficiently

TABLE 4. IoT security threats and countermeasures - edge-based architecture.

Authors	Threats/Impact	Countermeasures
Rui et al. [49]	Firmware, resource, and DDoS attacks; inaudible voice commands affecting device security	Traffic/system monitoring modules for anomaly detection, vulnerability management, and user alerts
Karmakar et al. [50]	Device/data compromise due to lack of authentication and policy enforcement	SDN-enabled architecture for device authentication and enforcement of rule-based policies
Barbareschi et al. [51]	Traditional authentication methods are hard to deploy on resource-constrained medical IoT devices, risking security and privacy breaches	After extracting the Physical Unclonable Functions (PUF) response, it is processed using a fuzzy extractor to generate a stable 32-byte private key, which is then used to generate a key pair

Another approach towards preventing DoS attacks is a signature-based system that detects and prevents security threats by applying predefined rules [3]. Hemalatha et. al proposed a real-time ML-based intrusion detection framework by integrating feature extraction and classification directly into the IoT architecture, leveraging behavior-based anomaly detection to handle diverse threats [59]. Similarly, Srivastava and Jain proposed a multi-layered security framework combining real-time response, secure boot, blockchain, and machine-learning based intrusion detection for enhanced IoT network protection [66]. Tukur et. al have proposed a hybrid architecture of fog computing and Tangle technology (a decentralized communication framework for rule sharing and updates similar to blockchain but using a directed acyclic graph) to overcome DoS attacks [3]. This architecture combined with the use of Apache Kafka for data exchange

TABLE 5. IoT security threats and countermeasures - cloud-based architecture.

Authors	Threats/Impact	Countermeasures
Sikder et al. [52]	Impersonation, data injection, DoS, malicious apps affecting operations	Context-aware framework analyzing user/device behavior to detect and mitigate threats based on learned patterns
Tarawneh et al. [53]	Data leakage of sensitive patient information	Secure medical framework with patient data encryption before transmission and cloud storage
Tukur et al. [54]	Data compromise from manipulated IoT nodes providing incorrect data	Smart contract on Ethereum blockchain to validate data and ensure integrity within acceptable thresholds
Giannoutakis et al. [55]	Device/network compromise through vulnerable devices with outdated firmware	Private blockchain for managing IP blocklists and device firmware/hardware registry
Lodha et al. [56]	Sensitive data (e.g., medical records) compromise due to lack of security protocols	Hybrid fog-cloud architecture with blockchain and IPFS for secure storage and access control
Sarac et al. [57]	Device/network compromise through code injection in API responses	Blockchain-based solution for reviewing and filtering IoT device requests to remove sensitive/malicious information
Amraoui et al. [58]	Device compromise due to malicious commands issued remotely	Framework authenticating user commands and machine learning-based legitimacy detection
Hemalatha et al. [59]	DDoS attacks due to insufficient security measures, low computational resources of IoT devices	Real-time ML-based intrusion detection framework with behavior-based anomaly detection

between devices provided a fast communication channel for distributing security rules across the network.

The research community has also suggested the use of blockchain technology to prevent DoS attacks as the network imposes transaction fees to prevent spamming [6]. Attias. et. al explored the use of Verifiable Delay Functions (VDFs) within fog nodes as an alternative to blockchain to avoid transaction fees, but retain other advantages that a blockchain can offer [43]. The authors designed a VDF that forces a mandatory delay for every transaction, and ensures only one transaction can be approved at once to prevent DoS attacks.

2) CHALLENGES AND FUTURE DIRECTIONS

Although behavioral analysis frameworks work with certain IoT hubs (Samsung SmartThings and Amazon Alexa), achieving compatibility with all devices remains a challenging task. Additionally, such frameworks may also require a separate component for data monitoring and analysis as this is a computationally intensive task [73]. The introduction of a cloud-based component increases the data access latency and might prove inefficient for IoT devices that require real-time processing [73].

Implementing solutions on fog or edge architectures can prove expensive in terms of storage costs and these devices are often limited in computational resources [60], [73]. Additionally, a hybrid architecture may introduce compatibility challenges as seen in the work proposed by Tukur. et. al [3]. While the Tangle technology emphasizes decentralization, the introduction of a cloud-based component (a centralized component) can complicate data access and availability.

B. DEVICE-RELATED THREATS

The growing number of IoT devices leads to the generation and transmission of large amounts of sensitive data. Specifically, edge-based architecture for IoT deployments can significantly increase the risk of device-related threats. The vulnerabilities that expose individual IoT devices, such as unauthorized network access, malicious commands, and buffer overflow attacks, carry a higher impact in Edge environments due to their limited processing power and security measures. These threats can arise from weak authentication protocols, allowing malicious devices to infiltrate the network, or from command injection attacks that exploit the remote control capabilities of IoT devices. This category focuses on threats compromising individual IoT devices by exploiting their vulnerabilities. Such threats could result from collusion between malicious IoT devices, insufficient data provenance information, or attacks like buffer overflow, which can be used to gain unauthorized control or disrupt device functionality.

1) **Unauthorized Network Access:** Unauthorized network access occurs when malicious devices gain access to an IoT network without proper authentication or permission [37]. In IoT environments, this can happen due to weak authentication protocols as devices are often equipped with minimal security measures, or through device impersonation as attackers may spoof a legitimate device, tricking the network into allowing unauthorized access [37].
2) **Malicious Commands:** In an IoT network, devices are often remotely controlled by users, which makes them susceptible to command-based attacks, including command injection [58]. If an attacker gains control of a legitimate device (through weak authentication, for example), they can issue malicious commands to other connected IoT devices [58].
3) **Buffer Overflow Attacks:** A buffer overflow occurs when an attacker deliberately sends more data to a

TABLE 6. IoT security threats and countermeasures - hybrid architecture.

Authors	Threats/Impact	Countermeasures
Javanmardi et al. [60]	TCP SYN flood attacks disrupting service and resource utilization	Security-aware task scheduler (FUPE) with DDoS detection and resource allocation based on device trustworthiness
Gunduz et al. [61]	CIA triad, data injection, DoS attacks impacting grid operations and infrastructure	Encryption, authentication, access control, IDS/IPS, adherence to security standards and best practices
Gulatas et al. [62]	Diverse IoT malware (e.g., botnets) targeting network devices	Defense-in-depth approach: changing defaults, blocking malicious IPs, deploying anti-malware tools
Giaretta et al. [63]	DoS attacks disrupting service availability	Security contracts ensuring normal device behavior and automatic detection/isolation of malicious devices
Tukur et al. [3]	DoS, data compromise, resource depletion impacting service reliability and data integrity	Multi-layered approach with TLS, blockchain, access control, and resource management algorithms
Mata et al. [4]	DDoS, botnets, and weak configurations affecting service availability and network integrity	Host-based intrusion detection/prevention, decentralized processing, secure communication using Tangle
Daraghmi et al. [64]	High transmission delays, unauthorized access, and UDP vulnerabilities	Layered architecture with authentication protocols and machine learning for secure data management
Singh et al. [65]	Default IDs, malware attacks, and DDoS impacting service reliability	Multi-level authentication, AI-based intrusion detection, and optimization algorithms for anomaly detection
Srivastava et al. [66]	DDoS attacks, data compromise, and unauthorized access leading to service disruptions	Multi-layered security framework combining real-time response, blockchain, zero trust architecture, and machine learning-based intrusion detection
Zuo et al. [67]	Vulnerable IoT communication layers face attacks like privacy leaks, spoofing, and eavesdropping due to wireless transmission and lack of coordinated security	Introduces SDN-based layered security with virtualized firewalls, intrusion detection, and centralized policy enforcement to enhance real-time threat detection and control
Gamundani et al. [68]	Resource-constrained IoT devices in smart homes are prone to impersonation, replay, and MITM attacks during autonomous device interactions	Deploys a trusted Smart Home Agent (SHA) using the DIKW model to offload authentication, enabling secure, low-computation identity management
Yalda et al. [69]	Resource-constrained IoT devices are vulnerable to DoS attacks, malware, brute-force attempts, and port scans, posing serious risks to privacy, availability, and network integrity	Deploys a cost-effective Raspberry Pi-based host IDS/IPS using Suricata with custom rule sets, capable of detecting and preventing threats like ICMP floods, SYN floods, Telnet/SSH attacks, and malware in real-time
Li et al. [70]	Centralized access control models suffer from single-point failures and lack of scalability across distributed IoT devices	Proposes a blockchain and smart contract-based decentralized access control system with mutual identity verification using ECC and role/attribute-based access policies
Yoon et al. [71]	Compromised IoT device authentication, data breaches, loss of privacy, and reduced system reliability	Leverage PUF-based authentication to eliminate the need for storing private keys in non-volatile memory, instead generating keys dynamically in real time. It employs TLS-encrypted communication, fuzzy extractors for error correction, and mutual authentication protocols to mitigate threats like MITM, side-channel attacks, and cloning

device's memory buffer than it is designed to hold [45]. Since many IoT devices have limited memory, they are particularly vulnerable to this type of attack [45].

1) PROPOSED COUNTERMEASURES

Software-Defined Networking (SDN) has emerged as a promising solution to centralize and enforce traffic policies, helping mitigate unauthorized access to IoT networks [50]. Karmakar et al. proposed a security architecture that restricts network access to authenticated IoT devices, through their lightweight authentication protocol [50]. Additionally, their design suggests the use of fine-grained policies to secure flows to manage the IoT infrastructure for proactive handling of security attacks. This architecture includes components such as a policy manager to design traffic policies, and an evaluation engine to evaluate the validity of the network traffic based on the existing policies. Zuo et. al proposed leveraging SDN to deploy cloud-based virtual firewalls and enforce security policies with dynamic responses through OpenFlow-enabled devices [67].

Similarly, blockchain has been leveraged by researchers for authentication, data provenance, and integrity [6]. A secure blockchain interface was proposed by Sarac et. al to provide accountability and non-repudiation of events in the IoT network [57]. In this interface, instead of network requests being passed on directly by the router, the blockchain is responsible for intercepting these requests and removing all information that is not required to be processed by the server. Additionally, the blockchain is also responsible for ensuring the receiver's identity. Therefore, stripping potentially sensitive information by the blockchain and verifying the receiver, enhances the overall security of

TABLE 7. Countermeasure analysis: Discussing the pros and cons of each countermeasure for network, device, and data-related threats.

Targeted Threat	Countermeasure with References	Advantages	Disadvantages
DoS Attacks	Behavioral Analysis [63], [65], [52], [58], [66], [59]	Data collection to profile user activity enables identifying anomalies in real-time, and preventive measures can be taken to stop a malicious attack.	Compatibility issues may arise when IoT devices are connected to different IoT hubs. Separate components may be needed for analyzing and monitoring data. Additionally, there is a likelihood of false positives and false negatives.
Data Alteration	Decentralized Ledger Technology (DLT) for data integrity [56], [57], [61], [70], [48]	Data integrity can be ensured when leveraging a tamper-resistant DLT such as blockchain, thus holding IoT devices accountable for their actions.	Data stored in DLTs such as blockchains are often public by default, thus there is limited data privacy.
Data Privacy	Encryption [64], [53], [54], [69], [68]	Data encryption using a public-private key pair can ensure only the intended receiver can view data, including IoT sensor values, thus ensuring data confidentiality.	Public key discovery and private key management can become challenging as these may involve the use of an additional component (for ex: blockchain can be used for public key discovery, and a secure management unit can be used for private key management) which must also be secured to prevent unauthorized access.
Malicious Traffic Injection	Signature-based IDS [60], [3], [62]	A signature-based IDS can load and apply a pre-determined set of rules for accepting traffic into the network, and alert network administrators when there is any traffic that does not conform with the pre-determined set of rules. Therefore, network administrators can view and stop malicious traffic from entering into the network.	Signature-based IDS are usually incapable of detecting unknown or zero-day attacks. Additionally, the IDSs require frequent signature updates, thus requiring continuous monitoring for new threats. Continuous monitoring can lead to potential maintenance overhead.
Network Congestion	Verifiable Delay Functions (VDFs) [43], [4]	Introducing an approach to delay traffic coming into the network limits the attacker's ability to spam transactions.	VDFs must be designed to ensure there is no performance bottleneck in the network. Forcing a mandatory delay for each transaction can severely impact the performance of devices, especially the devices that continuously transmit traffic.
Traffic Policy Exploitation	SDN to centralize traffic policies [50], [46], [67]	In an SDN approach, a centralized controller has an entire view of the network, thus it can be applied to introduce traffic policies, route traffic, and secure traffic flows into the network.	While a centralized controller improves performance, it becomes a single point of failure. Thus, attackers that can take down the SDN controller can effectively stop any network traffic movement in the network.
Device Security	Integrated hardware modules [45], [44], [49], [55], [71], [47]	A hardware module responsible for cryptographic keys and certificates enables resource-constraint IoT devices to encrypt and decrypt information to enhance data confidentiality. Additionally, such modules can also be programmed to detect memory corruption attacks.	Such hardware modules present compatibility challenges as they must be applicable to different kinds of IoT devices, and must be retroactively fitted to existing IoT devices.

the device as the server (even if it is malicious) finds it challenging to attack the IoT device without such sensitive information. Similarly, Yalda et. al proposed the use of blockchain for decentralized, tamper-proof data management and smart contracts for secure and automated enforcement of access control policies [69].

Behavioral analysis has also been applied to trust management in IoT networks. Amraoui et. al developed a behavioral-analysis-based trust management framework to ensure only legitimate users can control IoT devices in the network [58]. The authors presented a behavioral model that computes behavioral scores and evaluates trust based on user commands. The command evaluation can be done either on the hub or the cloud, depending on how the users issue commands to their IoT devices. The behavioral model presented was claimed to be effective in classifying whether the command was legitimate or malicious in real-time. If the command was predicted to be malicious, the device would be de-authenticated by the network. The results show low false-positive and false-negative rates. Therefore the system does not allow adversaries and does not force users to re-authenticate themselves often.

In the context of buffer overflow attacks, Bouazzati et. al developed a proof-of-concept to demonstrate the buffer overflow attack on IoT devices [45]. To overcome this attack on a Reduced Instruction Set Computer-V (RISC-V) processor, the authors designed a hardware-based module capable of detecting buffer-overflow attacks based on the

number of branch and load stall instructions encountered by the module. Two thresholds were considered, wherein the first threshold determines whether the traffic was legitimate or malicious based on load stall instructions, and the second threshold determines whether the traffic depicted a stack overflow or a heap overflow attack based on the number of branches taken. Their proposed design involved the use of a decision tree classifier model with a detection rate of 99.98%. Yoon et. al propose leveraging Physical Unclonable Function (PUF)-based authentication to eliminate the need for storing private keys in non-volatile memory, instead generating keys dynamically in real time [71]. Their approach employs TLS-encrypted communication, fuzzy extractors for error correction, and authentication protocols to mitigate threats including Man-in-the-middle (MITM), side-channel attacks, and cloning [71]. Finally, Malche et. al proposed a lightweight firmware validation mechanism to prevent unauthorized firmware updates and ensure device integrity [47].

2) CHALLENGES AND FUTURE DIRECTIONS

Taking into account the research in this area, some challenges persist that need to be explored further to overcome device-related threats. Leveraging the use of a decentralized ledger (blockchain or other similar solutions) to intercept traffic and verify receivers' identity requires the setup phase to include device manufacturers to share information on every device it communicates with. This is often not feasible as several manufacturers create IoT devices, and sometimes they may not even wish to share that information [6]. The introduction of hardware-based modules on the fog layer can aid IoT devices in preventing buffer overflow attacks. However, such hardware-based modules must be adaptable to different processors and instruction set architectures [45]. Additionally, such modules must be physically installed with the IoT devices, therefore, they may encounter logistical challenges such as finding the right size and location to install the module [6].

C. DATA-RELATED THREATS

This category includes threats that impact the confidentiality, integrity, or availability of data generated, transmitted, or stored within the IoT ecosystem. Such threats may arise from the use of weak encryption algorithms, inadequate data processing safeguards, or insufficient access management policies, all of which can expose sensitive information to unauthorized access, tampering, or loss [6]. Opting for a Cloud architecture in IoT deployments can increase the risk of data-related threats, particularly concerning Data Privacy and Data Alteration [6]. The reliance on centralized cloud systems for data storage and processing exposes sensitive information to potential breaches, especially when weak encryption algorithms and inadequate access management policies are in place. This can lead to Sensitive Data Exposure, where malicious users gain unauthorized access to critical data, such as patient information in healthcare settings. Additionally, the risk of Data Alteration arises as attackers may exploit vulnerabilities during data transmission between devices and cloud servers, leading to unauthorized modifications.

1) **Sensitive Data Exposure:** Medical centers, such as hospitals often use IoT devices to collect patient physiological data through sensor networks. This data can include temperature, pulse rate, respiration rate, oxygen level, and blood pressure. This presents malicious users an opportunity to attack the infrastructure to get access to such sensitive information.
2) **Data Alteration:** Data alteration refers to the unauthorized modification or tampering of data being transmitted or stored in an IoT system [54]. In IoT environments, data is frequently transmitted between devices, gateways, and centralized servers, where it is often processed and analyzed. Attackers may exploit vulnerabilities to alter this data, leading to significant consequences, especially in critical sectors such as healthcare, industrial control systems, and smart cities [54].
3) **Cryptographic Key Management:** Cryptographic key management is the process of securely generating, storing, distributing, and revoking encryption keys used to protect the confidentiality, integrity, and authenticity of data in IoT systems [7]. Since IoT devices handle sensitive information, strong encryption is necessary. However, IoT devices usually do not have the capability to securely manage cryptographic keys due to their limited computational power, storage, and lack of advanced security features such as hardware security modules (HSMs) or trusted platform modules (TPMs) [44]. This makes managing cryptographic keys securely a significant challenge in IoT environments.

1) PROPOSED COUNTERMEASURES

Encryption techniques, as proposed by Tarawneh et al., aim to protect the privacy of sensitive data in IoT environments by ensuring that only authorized individuals can access the information using cryptographic keys [53]. The public key for encryption can be discovered through a public directory on the cloud, and the data can be decrypted using their private key. Lodha et. al worked in a similar domain but focused on the integrity and availability of medical information [56]. Their design leveraged the Inter-Planetary File System (IPFS) as a decentralized data store, and a blockchain to record the IPFS' Content Identifiers (CIDs) for file discovery. Additionally, the authors developed a blockchain-based smart contract to enable access to the anonymized, and encrypted medical information stored on IPFS in a secure manner. Similarly, Li et. al proposed leveraging lightweight blockchain mechanisms equipped with identity authentication, transaction validation, and access control to secure cryptographic key management [70]. Finally, the work proposed by Gamundani et. al discusses a hybrid cryptographic approach combining symmetric and

asymmetric encryption to balance security and performance in resource-constrained IoT environments [68].

In addition to privacy concerns, data integrity at the perception layer of IoT architectures remains a significant challenge, as highlighted by Tukur et al. [54]. A targeted attack on an IoT-based sensor can cause incorrect data values to be transmitted to the server. When processing such incorrect or invalid values, the server may produce undesirable alerts to the administrators. The example presented in their research was an insider threat tampering with IoT sensors to produce maximally or minimally extreme sensor values. The authors leveraged a blockchain to overcome such challenges, which contained logic to ensure the sensor values were within a pre-determined range, and if not, the authors fit into this pre-determined range to avoid outlier data being processed by the server.

Given the resource limitations of IoT devices, Hroub and Elrabaa proposed the integration of a Security Management Unit (SMU) for managing cryptographic keys, hashes, and security certificates [44]. The integration of SMU can power the IoT devices to handle cryptographic operations at the edge node itself, therefore avoiding an external cloud or a fog node component to manage these operations. Additionally, the security management unit, if properly implemented can enable Transport Layer Security (TLS) based communication, thus protecting privacy and confidentiality of communication between the IoT devices [44]. Additionally, the work proposed by Tamri et. al integrates a secure software-defined fog gateway that reduces latency by processing data near the source, secures data exchanges using blockchain for privacy and integrity, and uses an SDN controller to manage and monitor IoT devices [48].

2) CHALLENGES AND FUTURE DIRECTIONS

Despite recent advancements in countermeasures addressing data-related threats in IoT networks, there are still significant challenges that remain unsolved at its implementation level. One primary challenge is managing cryptographic keys, especially in resource-constrained environments. While encryption techniques such as those proposed by Tarawneh et al. are effective at protecting sensitive information, the authors introduce complexities in key sharing and management [53]. Public keys must be securely stored and made discoverable through public directories, and secure mechanisms must be in place to prevent unauthorized access to private decryption keys.

Moreover, the deployment of blockchain-based smart contracts, as suggested by Lodha et al. and Tukur et al., presents its own challenges [54], [56]. While smart contracts can effectively validate and authenticate data, their logic must be exhaustive to ensure they can accurately differentiate between legitimate and tampered data. Therefore, future research must focus on creating additional test cases for validating smart contract logic, capable of adapting to new types of data tampering attacks.

Another significant challenge lies in the integration of advanced security management units (SMUs), as proposed by Hroub et al [44]. While SMUs enable cryptographic operations at the edge, they still rely on the IoT device's limited computational resources. Implementing these units requires careful design to balance resource consumption and security performance.

D. COUNTERMEASURE ANALYSIS

To provide a comparative countermeasure analysis, we analyze and compare the countermeasures discussed in Table 7 in terms of scalability, cost, and ease of implementation. We first define our evaluation criteria for these three metrics.

1) SCALABILITY

Scalability refers to the ability of a countermeasure to efficiently handle an increasing number of IoT devices and data traffic without significant performance degradation.

- Low: The countermeasure struggles to handle large-scale IoT networks. It may degrade in performance or require significant resources to scale.
- Moderate: The countermeasure can handle medium-sized IoT networks but may face challenges in large or distributed systems.
- High: The countermeasure is designed to scale efficiently across large, distributed IoT networks without significant performance degradation.

2) COST

Cost pertains to the financial investment required to implement and maintain a countermeasure within an IoT environment. This includes initial setup costs, ongoing operational expenses, and any necessary upgrades or maintenance.

- Low: The countermeasure is cost-effective, requiring minimal investment in hardware, software, or maintenance.
- Moderate: The countermeasure involves a reasonable cost, such as software licenses, moderate hardware upgrades, or periodic maintenance.
- High: The countermeasure is expensive to implement and maintain, requiring significant investment in infrastructure, expertise, or ongoing operational costs.

3) EASE OF IMPLEMENTATION

Ease of Implementation describes how straightforward it is to deploy a countermeasure within existing IoT systems. This encompasses the complexity of the installation process, the need for specialized expertise, and the extent of changes required to the current infrastructure.

- Low: The countermeasure is complex to implement, requiring specialized expertise, significant infrastructure changes, or retrofitting existing systems.
- Moderate: The countermeasure requires effort to implement, such as integrating with existing systems or training personnel.

TABLE 8. IoT security threats and countermeasures.

Threats	Proposed Countermeasures
Denial of Service (DoS) Attack	• Behavioral analysis: Monitor device behavior and communication patterns to identify deviations and detect malicious activity in real-time [63], [59]. • Context-aware models: Use machine learning models to analyze user activity and traffic patterns, continuously updating them to differentiate between legitimate and malicious traffic [52], [46]. • Signature-based systems: Apply predefined rules to detect and prevent known attack patterns [3]. • Decentralized rule-sharing systems: Use distributed frameworks to update and share security rules across the network [4]. • Blockchain-based techniques: Impose transaction fees to prevent spamming and mitigate excessive traffic [54], [43]. • Rate-limiting techniques: Detect suspicious connection patterns and limit excessive connection attempts [65], [49]. • Multi-layered security framework: Combine secure boot and zero-trust principles to harden endpoints against DoS infiltration attempts [66].
SYN Flood Attack	• Rate-limiting mechanisms: Implement connection rate-limiting to detect and block malicious patterns during the TCP handshake process [43]. • Secure task allocation: Ensure tasks from devices are assigned to trusted resources to mitigate malicious requests [60].
Traffic Policy Exploitation	• Dynamic policy management: Leverage programmable network technologies, such as Software-Defined Networking (SDN), to dynamically monitor, enforce, and update traffic policies [3], [50].
Network Overwhelming Attack	• Traffic analysis: Monitor and analyze network traffic to distinguish between legitimate and malicious activity [62]. • Traffic filtering: Apply filters or rules to block excessive traffic from malicious sources [4].
Unauthorized Network Access	• Centralized traffic policy enforcement: Use Software-Defined Networking (SDN) to implement and manage fine-grained access policies and evaluate traffic against these rules [50]. • Lightweight authentication protocols: Restrict access to authenticated devices using efficient authentication mechanisms [64]. • Blockchain-based security: Leverage blockchain for secure authentication, data integrity, and non-repudiation, while removing sensitive information from network requests to enhance device privacy [55]. • Integration Checks: Firmware-integrity checks to confirm cryptographically signed firmware images before execution [47].
Malicious Commands	• Behavioral analysis frameworks: Evaluate user commands in real-time using trust scores and behavioral models to identify and block malicious commands [49], [46]. • Trust management systems: De-authenticate devices issuing suspicious commands and ensure only legitimate users control IoT devices [65].
Buffer Overflow Attacks	• Threshold-based traffic analysis: Use metrics such as load stalls and branching instructions to classify traffic as legitimate or indicative of stack/heap overflow attacks [45]. • Decision tree models: Deploy machine learning models for high-accuracy classification of overflow attacks in real-time [65].
Sensitive Data Exposure	• Encryption techniques: Use public-private key cryptography to ensure that sensitive data is only accessible to authorized users [53]. • Decentralized storage: Leverage the Inter-Planetary File System (IPFS) for secure storage and blockchain to manage file discovery through Content Identifiers (CIDs) [56]. • Blockchain-based smart contracts: Enable secure access to anonymized and encrypted medical information [44]. • SDN: Enforce cloud-based virtual firewalls controlled via SDN policies to isolate traffic flows that contain private data [67], [70].
Data Alteration	• Blockchain-based validation: Ensure data integrity using blockchain logic to verify sensor data ranges and avoid outlier values being processed by servers [54], [57], [70], [69]. • Real-time data integrity checks: Implement automated mechanisms to validate data consistency at the perception layer of IoT architectures [4]. • Hybrid cryptographic scheme: using symmetric and asymmetric algorithms for authenticity (no tampering) and confidentiality (no unauthorized viewing) [68].
Cryptographic Key Management	• Security Management Unit (SMU): Integrate SMUs in IoT devices to handle cryptographic operations such as key management, hashing, and security certificates [44]. • Edge-based TLS: Enable Transport Layer Security (TLS) communication directly at the edge node to ensure privacy and confidentiality without relying on external cloud or fog components [3], [65]. • Physically Unclonable Function (PUF): PUF-based key generation that avoids storing private keys in nonvolatile memory [48].

TABLE 9. Countermeasure comparison in terms of scalability, cost, and ease of implementation.

Countermeasure	Scalability	Cost	Ease of Implementation
Behavioral Analysis	Moderate	High	Moderate
Decentralized Ledger (DLT)	High	High	Low
Encryption	High	Moderate	Moderate
Signature-Based IDS	Low	Moderate	Moderate
Verifiable Delay Functions (VDFs)	Moderate	Low	Moderate
SDN for Traffic Policies	High	High	Low
Integrated Hardware Modules	Moderate	High	Low

- High: The countermeasure is straightforward to implement, with minimal changes to existing infrastructure or processes.

Table 9 shows the performance of the proposed countermeasures identified in existing literature in terms of the above metrics. Behavioral analysis is moderately scalable as it requires real-time monitoring and data collection, which can become resource-intensive in large-scale IoT networks [74]. Its cost is high due to the need for advanced analytics tools and continuous monitoring, while its ease of implementation is moderate as it requires integration with IoT hubs and components [74]. Decentralized Ledger Technology (DLT), such as blockchain, offers high scalability due to its distributed nature, but its cost is high because of the transaction costs and the volume of data to be stored on the ledger [75]. Its ease of implementation is low, as it demands expertise, infrastructure setup, and security audits [75]. Encryption is scalable and moderately costly, as it can be applied across devices and networks without significant performance degradation, but key management can be complex [76]. Its ease of implementation is moderate as encryption algorithms are widely available, though managing keys securely adds complexity [76]. Signature-based Intrusion Detection Systems (IDS) have low scalability because they require frequent updates [77]. Their cost and ease of implementation are moderate, as they rely on predefined rules and require ongoing maintenance [77]. Verifiable Delay Functions (VDFs) are moderately scalable and cost-effective, as they are computationally lightweight [78]. However, their ease of implementation is moderate, as they must be carefully designed to avoid performance bottlenecks [78]. Software-Defined Networking (SDN) provides high scalability by centralizing traffic policies, but its cost is high due to the infrastructure required, and its ease of implementation is low because it requires significant expertise and updates to existing systems [79]. Finally, Integrated Hardware Modules are scalable but expensive, as they require retrofitting into existing IoT devices [80]. Their ease of implementation is low due to compatibility challenges with diverse IoT devices [80].

E. STANDARDIZED REFERENCE ARCHITECTURES

To ensure a comprehensive understanding of IoT architectures, we acknowledge the existing reference architectures proposed by various standardization bodies such as the International Organization for Standardization (ISO), International Telecommunication Union (ITU), Alliance for Internet of Things Innovation (AIOTI), and Institute of Electrical and Electronics Engineers (IEEE) [81], [82], [83], [84]. These frameworks have significantly influenced the development of secure and scalable IoT solutions and have been widely utilized in multiple European Union (EU) projects, including Internet of Things Architecture (IoT-A) [85], Secure Connected Trustable Things (SCOTT) [86], and Intelligent Secure Trustable Things (InSecTT) [87].

1) IoT-A

The IoT-A project aims to establish a standardized architectural reference model for the Internet of Things [85]. Its primary objectives include scalability, security, and interoperability, which are essential for developing robust IoT ecosystems [85]. IoT-A combines top-down reasoning with simulation and prototyping to explore the technical implications of various design choices. The project defines key building blocks for future IoT architectures, providing guidelines that can enhance the alignment of security frameworks with industry standards [85].

2) SCOTT

SCOTT is a European initiative that emphasizes trust in IoT environments by integrating technology, social sciences, and human-centric approaches [86]. Specifically, it addresses privacy and security concerns associated with wireless IoT solutions, which are often perceived as unreliable in critical applications. SCOTT aims to create novel business models for IoT adoption by fostering secure and trustworthy interconnected devices [86].

3) InSecTT

InSecTT is a European-funded initiative aimed at integrating Artificial Intelligence (AI) and IoT (AIoT) to enhance security, trust, and intelligence in industrial applications [87]. The project addresses the challenges of secure and reliable data processing by moving AI processing closer to edge devices, allowing real-time decision-making in critical applications such as autonomous systems, transportation, healthcare and industrial automation [87].

4) SECURITY IMPLICATIONS OF STANDARDIZED IoT ARCHITECTURES

InSecTT ensures that AI and IoT evolve together, mutually benefiting each other by transforming raw data into actionable knowledge while maintaining security, trust, and user

acceptance [87]. The project methodology aligns with the European Union standards for trustworthy AI, making it a key reference model for future AIoT implementations [87].

The architectural principles outlined in IoT-A, SCOTT, and InSecTT provide a structured approach to addressing security challenges in IoT ecosystems. These frameworks align with the security concerns identified in our threat taxonomy, particularly in the areas of network, device, and data security.

Future research could investigate how these reference architectures enhance the alignment of security frameworks, offering a structured approach to mitigate IoT threats. By integrating standardized principles with emerging security techniques, researchers can support the development of more resilient and interoperable IoT ecosystems.

F. THE ROAD AHEAD: BUILDING A SECURE IoT ECOSYSTEM

The current countermeasures for IoT security, while effective in addressing specific threats, face several limitations that impact their scalability, cost-efficiency, and ease of implementation. These limitations highlight the need for lightweight and standardized solutions to secure IoT systems.

1) BEHAVIORAL ANALYSIS

Behavioral analysis systems require significant computational resources for real-time monitoring and data collection, making them unsuitable for large-scale IoT networks [74]. Additionally, they often produce false positives and negatives, which can reduce their reliability. Lightweight behavioral analysis systems can be developed by leveraging AI and machine learning models optimized for IoT devices. Further, federated learning can be employed to distribute the computational load across devices while preserving data privacy. Such systems should focus on reducing resource consumption and improving detection accuracy.

2) DECENTRALIZED LEDGER TECHNOLOGY

DLTs, such as blockchain, can become expensive due to transaction costs [75]. Additionally, their public nature often compromises data privacy [75]. Future research could focus on leveraging blockchains that support instant finality and low transaction costs. Privacy-preserving techniques, such as zero-knowledge proofs, can be integrated to ensure data confidentiality while maintaining the integrity of the ledger [88].

3) ENCRYPTION

While encryption is scalable, managing cryptographic keys securely remains a challenge, especially in resource-constrained IoT environments [76]. Key management systems often require additional infrastructure, increasing complexity. Lightweight cryptographic algorithms, including SIT, E3LCM, and SPECK, can be adopted to reduce computational overhead without compromising security [89], [90], [91]. Decentralized key management systems, potentially leveraging blockchain, can simplify key distribution and enhance security. One example could involve the design of an OAuth system with Decentralized Identity (DID) management, as designed by Boi and Esposito [92].

4) SIGNATURE-BASED IDS

Signature-based IDS struggle with detecting zero-day attacks and require frequent updates to remain effective [77]. This leads to maintenance overhead and limits scalability [77]. Lightweight anomaly-based IDS should be developed to dynamically detect threats using AI and deep learning. Additionally, exploring Hybrid IDS that combines signature-based and anomaly-based approaches can improve detection accuracy while reducing the need for frequent updates.

5) VERIFIABLE DELAY FUNCTIONS (VDFs)

VDFs can introduce performance bottlenecks in IoT networks, especially for devices that require real-time data transmission [78]. Mandatory delays can negatively impact system performance. Adaptive VDFs should be designed to dynamically adjust delay parameters based on network conditions. Such lightweight VDFs should ensure minimal impact on real-time applications while maintaining security against spam and denial-of-service attacks.

6) SOFTWARE-DEFINED NETWORKING (SDN)

The centralized nature of SDN controllers creates a single point of failure, making them vulnerable to attacks that can disrupt the entire network [79]. Lightweight, distributed SDN architectures should be explored to eliminate single point of failure. Blockchain-based SDN controllers can enhance fault tolerance and security while maintaining centralized control over traffic policies [93].

7) INTEGRATED HARDWARE MODULES

Hardware modules face compatibility challenges with diverse IoT devices, and are expensive to retrofit into existing systems [80]. Their implementation often requires a significant redesign of devices. Standardized, modular hardware security solutions should be developed to ensure compatibility across different IoT devices. These modules should be lightweight and designed for easy integration into existing systems without significant redesign. Additionally, hardware modules should incorporate energy-efficient designs to minimize power consumption.

VI. CONCLUSION

IoT promises a future of interconnected devices and intelligent automation, but its widespread adoption relies on addressing the critical security challenges in various architectures. This survey has explored the diverse threat landscape targeting Cloud, Fog, and Edge-based IoT systems, encompassing network, device, and data-related vulnerabilities.

This survey demonstrated that each architectural layer presents unique vulnerabilities, necessitating a multi-faceted

approach to security. While Cloud computing offers scalability and cost-efficiency, its centralized nature introduces latency concerns and potential single points of failure. Fog computing mitigates these issues by bringing processing closer to the data source, but introduces complexities in managing distributed resources and ensuring consistent security policies. Edge computing further reduces latency and enhances real-time responsiveness, but resource limitations on edge devices necessitate efficient security solutions.

Our analysis of existing countermeasures reveals a range of promising approaches, including advanced encryption techniques, secure authentication protocols, intrusion detection systems, and blockchain-based solutions. However, the effectiveness of these countermeasures often comes at the cost of computational overhead, complexity, and scalability challenges. Future research should prioritize the development of lightweight, efficient, and adaptable security solutions that can be seamlessly integrated into diverse IoT architectures.

Furthermore, fostering collaboration among stakeholders, including device manufacturers, service providers, and policymakers is crucial for establishing standardized security protocols and best practices. By adopting a holistic approach that addresses the multifaceted challenges of IoT security, we can ensure that the IoT devices are not only innovative technology but also secure devices that we can use in our day-to-day lives without risking our privacy.

REFERENCES

[1] (2023). *World Economic Forum 2023*. [Online]. Available: https://www.weforum.org/publications/state-of-the-connected-world-2023-edition

[2] B. Marr, "2024 IoT and smart device trends: What you need to know for the future," Feb. 2024. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2023/10/19/2024-iot-and-smart-device-trends-what-you-need-to-know-for-the-future/?sh=5358c0747f34

[3] Y. M. Tukur, D. Thakker, and I.-U. Awan, "Multi-layer approach to Internet of Things (IoT) security," in *Proc. 7th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2019, pp. 109–116.

[4] R. Z. A. da Mata, F. L. de Caldas Filho, F. L. L. Mendonca, A. A. Y. R. Fares, and R. T. de Sousa, "Hybrid architecture for intrusion prevention and detection in IoT networks," in *Proc. Workshop Commun. Netw. Power Syst. (WCNPS)*, Nov. 2021, pp. 1–7.

[5] H. S. K. Sheth, A. K. Ilavarasi, and A. K. Tyagi, "Deep learning, blockchain based multi-layered authentication and security architectures," in *Proc. Int. Conf. Appl. Artif. Intell. Comput. (ICAAIC)*, May 2022, pp. 476–485.

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[8] M. R. Bouakouk, A. Abdelli, and L. Mokdad, "Survey on the cloud-IoT paradigms: Taxonomy and architectures," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.

[9] I. Mohiuddin and A. Almogren, "Security challenges and strategies for the IoT in cloud computing," in *Proc. 11th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2020, pp. 367–372.

[10] K. K. Patel and S. M. Patel, "Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 6122–6127, May 2016.

[11] A. Hameed and A. Alomary, "Security issues in IoT: A survey," in *Proc. Int. Conf. Innov. Intell. Informat., Comput., Technol. (3ICT)*, Sep. 2019, pp. 1–5.

[12] S. A. Goswami, B. P. Padhya, and K. D. Patel, "Internet of Things: Applications, challenges and research issues," in *Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Dec. 2019, pp. 47–50.

[13] (Apr. 2023). *Decoding the Internet of Things | Carnegie Mellon University Computer Science Department 2023*. [Online]. Available: https://csd.cmu.edu/news/decoding-the-internet-of-things

[14] MIT Auto-ID Lab. *Mit Auto-id Laboratory*. Accessed: Sep. 18, 2024. [Online]. Available: https://autoid.mit.edu/

[15] K. J. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, Jan. 1999.

[16] (2005). *ITU Internet Reports 2005: The Internet of Things*. [Online]. Available: http://handle.itu.int/11.1002/pub/800eae6f-en

[17] J. Bradley, J. Barbier, and D. Handler, "Embracing the Internet of Everything to capture your share of $14.4 trillion," *White Paper, Cisco*, vol. 318, pp. 1–12, 2013.

[18] M. Surya and S. Manohar, "An interpretation of the challenges and solutions for agriculture-based supply chain management using blockchain and IoT," in *Proc. 7th Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Feb. 2023, pp. 1199–1205.

[19] R. Kenaza, A. Khemane, H. Bendjenna, A. Meraoumia, and L. Laimeche, "Internet of Things (IoT): Architecture, applications, and security challenges," in *Proc. 4th Int. Conf. Pattern Anal. Intell. Syst. (PAIS)*, Oct. 2022, pp. 1–5.

[20] R. K. Kodali, S. Soratkal, and L. Boppana, "IoT based control of appliances," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Apr. 2016, pp. 1293–1297.

[21] L. Pacheco, E. Alchieri, and P. Solis, "Architecture for privacy in cloud of things," in *Proc. 19th Int. Conf. Enterprise Inf. Syst.*, 2017, pp. 487–494.

[22] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, Feb. 2019.

[23] H. Cloud, "The NIST definition of cloud computing," *Nat. Inst. Sci. Technol.*, vol. 800, p. 145, Jan. 2011.

[24] L. Hou, S. Zhao, X. Xiong, K. Zheng, P. Chatzimisios, M. S. Hossain, and W. Xiang, "Internet of Things cloud: Architecture and implementation," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 32–39, Dec. 2016.

[25] B. Charyyev, E. Arslan, and M. H. Gunes, "Latency comparison of cloud datacenters and edge servers," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[26] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[27] B. Tank and V. Gandhi, "A comparative study on cloud computing, edge computing and fog computing," *Recent Develop. Electron. Commun. Syst.*, vol. 32, pp. 665–670, Jan. 2023.

[28] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Goren, and C. Mahmoudi, "Fog computing conceptual model," *NIST Special Publication*, vol. 500, no. 325, pp. 1–15, Mar. 2018.

[29] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure Fog-to-Things environment," *IEEE Access*, vol. 8, pp. 66878–66887, 2020.

[30] S. Khanagha, S. Ansari, S. Paroutis, and L. Oviedo, "Mutualism and the dynamics of new platform creation: A study of cisco and fog computing," *Strategic Manage. J.*, vol. 43, no. 3, pp. 476–506, Mar. 2022.

[31] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[32] G. S. S. Chalapathi, V. Chamola, A. Vaish, and R. Buyya, "Industrial Internet of Things (IIoT) applications of edge and fog computing: A review and future directions," *Fog/edge Comput. for Secur.*, vol. 83, pp. 293–325, Jan. 2021.

[33] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[34] D. Swessi and H. Idoudi, "A survey on Internet-of-Things security: Threats and emerging countermeasures," *Wireless Pers. Commun.*, vol. 124, no. 2, pp. 1557–1592, May 2022.

[35] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures," *Comput. Secur.*, vol. 117, Jun. 2022, Art. no. 102677. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740482200075X

[36] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani, and A. G. Abdulrahman, "IoT forensics: Current perspectives and future directions," *Sensors*, vol. 24, no. 16, p. 5210, Aug. 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/16/5210

[37] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[38] 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.

[39] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in Internet of Things with a focus on the impact of emerging technologies," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100564. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660522000592

[40] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, Apr. 2015. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[41] (Oct. 1997). *ACM Digital Library*. Accessed: Dec. 23, 2024. [Online]. Available: https://dl.acm.org/

[42] *ScienceDirect.com | Science, Health and Medical Journals, Full Text Articles and Books.—Sciencedirect.com*. Accessed: Dec. 23, 2024. [Online]. Available: https://www.sciencedirect.com

[43] V. Attias, L. Vigneri, and V. Dimitrov, "Preventing denial of service attacks in IoT networks through verifiable delay functions," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[44] A. Hroub and M. E. S. Elrabaa, "SecSoC: A secure system on chip architecture for IoT devices," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Jun. 2022, pp. 41–44.

[45] M. E. Bouazzati, R. Tessier, P. Tanguy, and G. Gogniat, "A lightweight intrusion detection system against IoT memory corruption attacks," in *Proc. 26th Int. Symp. Design Diag. Electron. Circuits Syst. (DDECS)*, May 2023, pp. 118–123.

[46] M. Ebrahimi, M. S. Haghighi, A. Jolfaei, N. Shamaeian, and M. H. Tadayon, "A secure and decentralized trust management scheme for smart health systems," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1961–1968, May 2022.

[47] T. Malche, P. Maheshwary, and R. Kumar, "Secret key based sensor node security in the Internet of Things (IoT)," in *Proc. 5th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jun. 2020, pp. 464–469.

[48] R. Tamri, J. Antari, and R. Iqdour, "An enhanced IoT architecture for healthcare using secure software-defined fog gateway," in *Proc. 10th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, vol. 2, Oct. 2023, pp. 1–4.

[49] R. Yu, X. Zhang, and M. Zhang, "Smart home security analysis system based on the Internet of Things," in *Proc. IEEE 2nd Int. Conf. Big Data, Artif. Intell. Internet Things Eng. (ICBAIE)*, Mar. 2021, pp. 596–599.

[50] K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, "SDN enabled secure IoT architecture," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, Apr. 2019, pp. 581–585.

[51] S. A. El-Moneim Kabel, G. M. El-Banby, L. A. Abou Elazm, W. El-Shafai, N. A. El-Bahnasawy, F. E. A. El-Samie, A. A. Elazm, A. I. Siam, and M. A. Abdelhamed, "Securing Internet-of-Medical-Things networks using cancellable ECG recognition," *Sci. Rep.*, vol. 14, no. 1, p. 10871, May 2024.

[52] A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, "Aegis: A context-aware security framework for smart home systems," in *Proc. 35th Annu. Comput. Secur. Appl. Conf.*, Dec. 2019, pp. 28–41.

[53] M. Tarawneh, F. AlZyoud, Y. Sharrab, and H. Kanaker, "Secure E-health framework in cloud-based environment," in *Proc. Int. Arab Conf. Inf. Technol. (ACIT)*, Nov. 2022, pp. 1–5.

[54] Y. M. Tukur, D. Thakker, and I.-U. Awan, "Ethereum blockchain-based solution to insider threats on perception layer of IoT systems," in *Proc. IEEE Global Conf. Internet Things (GCIoT)*, Dec. 2019, pp. 1–6.

[55] K. M. Giannoutakis, G. Spathoulas, C. K. Filelis-Papadopoulos, A. Collen, M. Anagnostopoulos, K. Votis, and N. A. Nijdam, "A blockchain solution for enhancing cybersecurity defence of IoT," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 490–495.

[56] L. Lodha, V. S. Baghela, J. Bhuvana, and R. Bhatt, "A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring," *Measurement: Sensors*, vol. 30, Dec. 2023, Art. no. 100904. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2665917423002404

[57] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture," *Energy Rep.*, vol. 7, pp. 8075–8082, Nov. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484721005448

[58] N. Amraoui, A. Besrour, R. Ksantini, and B. Zouari, "Securing smart homes using a behavior analysis based authentication approach," in *Proc. IEEE 8th Int. Conf. Commun. Netw. (ComNet)*, Oct. 2020, pp. 1–5.

[59] T. Hemalatha, S. Venkatakiran, M. Kaur, S. B. Manojkumar, V. V. Prasad, and B. Ashreetha, "Real-time threat detection and countermeasures in IoT environments," in *Proc. 7th Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Nov. 2023, pp. 1349–1357.

[60] S. Javanmardi, M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, and A. Pescapè, "FUPE: A security driven task scheduling approach for SDN-based IoT–Fog networks," *J. Inf. Secur. Appl.*, vol. 60, Aug. 2021, Art. no. 102853.

[61] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.

[62] I. Gulatas, H. H. Kilinc, A. H. Zaim, and M. A. Aydin, "Malware threat on Edge/Fog computing environments from Internet of Things devices perspective," *IEEE Access*, vol. 11, pp. 33584–33606, 2023.

[63] A. Giaretta, N. Dragoni, and F. Massacci, "S×C4IoT: A Security-by-contract framework for dynamic evolving IoT devices," *ACM Trans. Sensor Netw.*, vol. 18, no. 1, pp. 1–51, Oct. 2021, doi: 10.1145/3480462.

[64] Y.-A. Daraghmi, E. Y. Daraghmi, R. Daraghma, H. Fouchal, and M. Ayaida, "Edge–Fog–cloud computing hierarchy for improving performance and security of NB-IoT-based health monitoring systems," *Sensors*, vol. 22, no. 22, p. 8646, Nov. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/22/8646

[65] K. Singh and N. Singh, "Analysis of IoT attack detection and mitigation," in *Proc. Int. Conf. Artif. Intell. Smart Commun. (AISC)*, Jan. 2023, pp. 1229–1232.

[66] A. Srivastava and U. Jain, "Securing the future of IoT: A comprehensive framework for real-time attack detection and mitigation in IoT networks," in *Proc. 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2023, pp. 1–6.

[67] X. Zuo, X. Pang, P. Zhang, J. Zhang, T. Dong, and P. Zhang, "A security-aware software-defined IoT network architecture," in *Proc. IEEE Comput., Commun. IoT Appl. (ComComAp)*, Dec. 2020, pp. 1–5.

[68] A. M. Gamundani, A. Phillips, and H. N. Muyingi, "A scalable and lightweight authentication architecture for the Internet of Things (IoT) in smart home applications," in *Proc. 2nd Zimbabwe Conf. Inf. Commun. Technol. (ZCICT)*, Zimbabwe, Nov. 2023, pp. 1–5.

[69] R. Yalda, N. Nepal, and T. El Hawari, "Enhancing IoT security affordably with raspberry pi and open-source IDS/IPS," in *Proc. IEEE Int. Conf. Adv. Syst. Emergent Technol. (IC_ASET)*, Nepal, Apr. 2024, pp. 1–6.

[70] H. Li, S. Xu, S. Li, G. Sun, X. Zhang, and L. Yan, "Trust-driven distributed self-collaborative security architecture of IoT based on blockchain and smart contracts," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, Nov. 2020, pp. 1–5.

[71] S. Yoon, B. Kim, K. Kim, and Y. Kang, "Enhancing IoT security with PUF-based authentication scheme," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 2319–2321.

[72] M. Bogdanoski, T. Suminoski, and A. Risteski, "Analysis of the SYN flood DoS attack," *Int. J. Comput. Netw. Inf. Secur. (IJCNIS)*, vol. 5, no. 8, pp. 1–11, Jun. 2013.

[73] A. K. Sikder, L. Babun, and A. S. Uluagac, "Aegis+ a context-aware platform-independent security framework for smart home systems," *Digital Threats, Res. Pract.*, vol. 2, no. 1, pp. 1–33, 2021.

[74] J. Pacheco and S. Hariri, "Anomaly behavior analysis for IoT sensors," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 4, p. 3188, Apr. 2018.

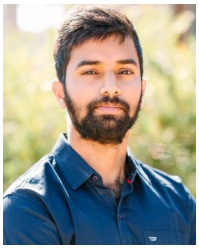
[75] A. Sunyaev, "Distributed ledger technology," *Internet Computing, Princ. Distrib. Syst. Emerg. Internet-Based Technol.*, vol. 29, no. 4, pp. 265–299, Jan. 2020.

[76] I. Kuzminykh, M. Yevdokymenko, and D. Ageyev, "Analysis of encryption key management systems: Strengths, weaknesses, opportunities, threats," in *Proc. IEEE Int. Conf. Problems Infocommunications. Sci. Technol. (PIC S&T)*, Oct. 2020, pp. 515–520.
[77] Y. Otoum and A. Nayak, "AS-IDS: Anomaly and signature based IDS for the Internet of Things," *J. Netw. Syst. Manage.*, vol. 29, no. 3, p. 23, Jul. 2021.
[78] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Proc. Annu. Int. Cryptol. Conf.*, Jan. 2018, pp. 757–788.
[79] A. Gelberger, N. Yemini, and R. Giladi, "Performance analysis of software-defined networking (SDN)," in *Proc. IEEE 21st Int. Symp. Model., Anal. Simul. Comput. Telecommun. Syst.*, Aug. 2013, pp. 389–393.
[80] N. Aaraj, A. Raghunathan, and N. K. Jha, "Analysis and design of a hardware/software trusted platform module for embedded systems," *ACM Trans. Embedded Comput. Syst.*, vol. 8, no. 1, pp. 1–31, Dec. 2008.
[81] *ISO: International Organization for Standardization*. Accessed: Oct. 3, 2024. [Online]. Available: https://www.iso.org
[82] *ITU: Committed To Connecting the World*. Accessed: Dec. 3, 2024. [Online]. Available: https://www.itu.int
[83] *AIOTI: Alliance for Internet of Things Innovation*. Accessed: Dec. 3, 2024. [Online]. Available: https://aioti.eu
[84] *IEEE: Advancing Technology for Humanity*. Accessed: Dec. 3, 2024. [Online]. Available: https://www.ieee.org
[85] (2013). *IoT–A–Internet of Things architecture*. [Online]. Available: http://www.iot-a.eu
[86] V. V. R. GmbH. (2025). *Scott-Secure Connected Trustable Things*. Accessed: Aug. 3, 2025. [Online]. Available: https://www.virtual-vehicle.at/projects/scottproject-eu/
[87] I. Consortium. (2025). *Insectt-Intelligent Secure Trustable Things*. Accessed: Aug. 8, 2025. [Online]. Available: https://www.insectt.eu/
[88] U. Fiege, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," in *Proc. 19th Annu. ACM Conf. Theory Comput. - STOC*, 1987, pp. 210–217.
[89] M. Usman, I. Ahmed, M. Imran Aslam, S. Khan, and U. Ali Shah, "SIT: A lightweight encryption algorithm for secure Internet of Things," 2017, *arXiv:1704.08688*.
[90] P. P., M. M., S. K. P., and M. S. Sayeed, "An enhanced energy efficient lightweight cryptography method for various IoT devices," *ICT Exp.*, vol. 7, no. 4, pp. 487–492, Dec. 2021.
[91] L. Sleem and R. Couturier, "Speck-R: An ultra light-weight cryptographic scheme for Internet of Things," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17067–17102, May 2021.
[92] B. Boi and C. Esposito, "Decentralized authentication for Web of things: A self-sovereign identity (SSI)-based solution," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2024, pp. 684–688.
[93] L. Medury and F. Kandah, "B2-c2: Blockchain-based flow control consistency for multi-controller SDN architecture," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2024, pp. 1–6.

FARAH KANDAH (Senior Member, IEEE) was a Faculty Member with the Computer Science and Engineering Department, The University of Tennessee at Chattanooga, from 2012 to 2022. He is currently an Associate Professor with the Computer Science and Software Engineering (CSSE) Department, Auburn University (AU). He is also leading the Center of Academic Excellence in Cybersecurity, AU. He led the Cybersecurity and Cyber-Physical Systems Thrust with the SimCenter (UTC). He Founded and is also leading the Network Communication Laboratory (NCL), which leverages expertise in smart communications, threat hunting, blockchain, digital forensics, and trust management, with research focuses on the Internet of Things, smart networking design, smart autonomous/connected vehicle networks, cybersecurity, and software-defined networks. He is the Program Coordinator and chairing the Cybersecurity Engineering Program with AU. His research interests and expertise span a wide range of topics in cybersecurity and cyber-physical systems.

THILINA MENDIS (Student Member, IEEE) received the B.Eng. degree (Hons.) in software engineering from the University of Westminster (UoW), U.K., in 2015, completed his CIM qualification (ACMA), in 2022, and the M.Sc. degree in software engineering from Auburn University, in 2024, where he is currently pursuing the Ph.D. degree with the Computer Science and Software Engineering Department. He was a Quality Assurance Engineer, with a focus on automation and security and a Technical Business Analyst, from 2015 to 2017. While engaging as a Freelance Contributor, later from 2018 to 2022, he was the IT Leader with Decathlon, Sri Lanka. He is a Graduate Assistant Software Engineer with the Biggio Center, Auburn University. Throughout his studies and experience, he gained a strong foundation in computer science, mathematics, electronics, and business. His research interests include quantum computing, machine learning, computer vision, and cybersecurity.

LALITH MEDURY (Student Member, IEEE) received the B.S. degree in computer science and engineering from the Vidya Jyoti Institute of Technology, India, in 2022. He is currently pursuing the M.S. and Ph.D. degrees in computer science and software engineering with Auburn University, Auburn, AL, USA. Since 2023, he has been a Graduate Research Assistant with the Department of Computer Science and Software Engineering. His research interests include machine learning techniques to enhance the privacy and security of the IoT devices, particularly within smart home environments. In 2023, he was honored with the prestigious Charles Gavin Fellowship to support his doctoral studies at Auburn University.



HEMANT SHERAWAT received the B.S. degree in computer science and engineering from Auburn University, Auburn, AL, USA, in 2023, where he is currently pursuing the double M.S. degree in management information systems and cybersecurity engineering. He is a Graduate Teaching Assistant with the Department of Computer Science and Software Engineering. His research interest focuses on enhancing the security of NFC and RFID technologies and how potential hackers could exploit vulnerabilities to extract sensitive information. His awards and honors include receiving the Academic Excellence from the Computer Science and Software Engineering Department, Auburn University, and graduating as an University Honors Scholar with Honors.

HAOFAN WANG received the M.S. degree in information science from the University of Pittsburgh, Pittsburgh, PA, USA. He is currently pursuing the Ph.D. degree in computer science and software engineering with Auburn University, Auburn, AL, USA. Since 2023, he has been a Teaching Assistant with the Department of Computer Science and Software, Auburn University. His research interests include network intrusion detection, ransomware detection, and the application of deep learning in cybersecurity.