Manchester Metropolitan University

e-space

Manchester Metropolitan University's Research Repository

Please cite the Published Version

Adam, Mumin, Hammoudeh, Mohammad, Alrawashdeh, Rana and Alsulaimy, Basil (2024) A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access, 12. pp. 57128-57149.

DOI: https://doi.org/10.1109/ACCESS.2024.3382709

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Version: Published Version

Downloaded from: https://e-space.mmu.ac.uk/635042/

Usage rights: CC BY Creative Commons: Attribution 4.0

Additional Information: This is an open access article which first appeared in IEEE Access

Enquiries:
If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines)

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 February 2024, accepted 21 March 2024, date of publication 28 March 2024, date of current version 26 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3382709

SURVEY

A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems

MUMIN ADAM[1], MOHAMMAD HAMMOUDEH[2], (Senior Member, IEEE), RANA ALRAWASHDEH[2], AND BASIL ALSULAIMY[2,3]

[1]Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[2]Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[3]Information Protection Department, Saudi Arabian Oil Company (Saudi Aramco), Dhahran 31311, Saudi Arabia

Corresponding author: Mumin Adam (g201708690@kfupm.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR) at the King Fahd University of Petroleum and Minerals.

ABSTRACT The Internet of Things (IoT) emerged as a pervasive technology, facilitating the seamless interaction of devices, individuals, and services, enabling data exchange and task execution across various domains. While the impact of IoT is undeniably transformative, its extensive proliferation raised significant concerns surrounding security, privacy, and trust, which stand as critical barriers to the widespread adoption and advancement of IoT technology. This review article explores IoT security, privacy, and trust research using a 3-layer IoT architecture. After introducing the fundamental tenets of IoT security, privacy, and trust, it proceeds to examine the prevalent security requirements within IoT architectures and their associated challenges. Then, the survey investigates the recent trends in research dedicated to addressing security, privacy, and trust issues within IoT systems. Furthermore, this article reviews the latest advancements and methodologies designed to secure IoT systems against security breaches and protect the privacy of sensitive data. Finally, the survey outlines unresolved challenges within the IoT security landscape and potential solutions. By offering this consolidated insight, this article offers a bridge between foundational and advanced IoT security topics, providing researchers with an in-depth understanding of current IoT security, privacy, and trust challenges, as well as cutting-edge solutions tailored to address the security and trust-related obstacles faced by IoT applications. In addition, it provides the IoT community with the knowledge necessary to navigate the complex terrain of security, privacy, and trust in IoT systems.

INDEX TERMS Countermeasures, IDS, IoT architecture, IoT attacks, mitigation, privacy, security, security requirements, trust.

I. INTRODUCTION

The Internet of Things (IoT) consists of a network of interconnected devices, or nodes, that exchange data among themselves to perform common tasks and achieve specified goals. The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) describes IoT as ''Global infrastructure for society, enabling improved services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies'' [11]. IoT is becoming an integral part of our lives linking everyday devices to one another so that data can be stored, organized, and processed. It has numerous uses in the delivery of energy, healthcare, transportation, and many other critical national infrastructure systems [12], [13], [14].

Due to its reliance on the Internet infrastructure, this rapid growth of IoT is associated with a rise in security, privacy, and trust concerns [15]. Also, the diverse nature of the extensive network of IoT introduces new security risks and challenges that broaden the threat landscape and make it possible for attackers to extract more sensitive IoT network data to aid in their attack. Therefore, strong security, privacy, and trust are essential to the operation and success of IoT at all IoT layers, namely physical devices, network, and service-application layers. In addition, nowadays, many intelligent systems and applications for logistics, manufacturing, healthcare, industrial surveillance, and other fields are built on top

The associate editor coordinating the review of this manuscript and approving it for publication was P. K. Gupta.

© 2024 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

of different communication infrastructures. Despite these differences, one of the objectives of IoT is to support these systems irrespective of their underlying infrastructure. To realize this goal, IoT implements many techniques such as intelligent sensors, wireless communication, networks, data analysis technologies, and cloud computing [16], [17], [18]. Many of these technologies are in the early stages of development, and addressing the technical challenges they present, particularly those related to security and privacy across different domains, is crucial [19]. Some examples of IoT issues are incorrect device configuration, a lack of effective and reliable security procedures, and user ignorance.

IoT systems are being deliberately targeted at the physical, network, and application layers. Each IoT layer poses its own unique set of requirements, and it is essential that these standards be satisfied whenever potential threats are eliminated. In IoT layers, the real world is brought into computer-based systems through sensors that generate, collect data, and share it with users via the network layer, which forwards this data to the IoT application layer, where users can use the data. As a result, the privacy and trust of IoT services, including sensitive data about users, enterprises, and governments, become increasingly important.

A. PRIOR STUDIES

Various studies and surveys about IoT security, privacy and trust exist. Table 1 summarizes the important contributions of prior reviews on IoT security and compares them to our study, as well as exclusion and/or inclusion criteria.

Khanam et al. [1] provided an overview of IoT attacks and a taxonomy of relevant security solutions. In [2], the authors studied IoT security issues at various IoT architecture layers and presented Machine Learning (ML)/DL-based intrusion detection techniques. They also listed available IoT public datasets. The studies in [3], [7], and [8] surveyed IoT attacks and countermeasures using Machine Learning (ML) and blockchain methods. In another blockchain-focused study [9], the authors provided a detailed examination of Internet of Medical Things (IoMT) cybersecurity threats and countermeasure techniques utilizing enabling technologies such as AI and blockchains as means for security and authentication.

In [5], the authors examine security attacks from two perspectives, attack taxonomy and layer-wise attacks. They then provide some classical security solutions to counter IoT threats. Another survey that focuses on IoT architectures, various risks at various IoT layers, and IoT security solutions such as Software Defined Networking (SDN) was presented in [4]. A comprehensive survey of the trustworthiness, privacy, and security of Mobile-IoT is presented in [10].

B. MOTIVATION AND CONTRIBUTION

IoT networks and systems are inherently vulnerable, and the proliferation of IoT devices and their ubiquitous availability pose a threat to users' security and privacy. Many critical infrastructures use IoT devices that are susceptible to cyber-attacks. This drives the need for a thorough examination of IoT threats, security requirements, architectural difficulties, and remedies to IoT cyber attacks. Extensive research was conducted to secure IoT systems and enhance privacy and trust, utilizing various methods. The purpose of this work is to examine the security, privacy, and trust concerns related to the IoT ecosystem by surveying and critically analyzing recent research efforts on the topic of IoT security, privacy, and trust.

The main contribution of this article can be summarized as follows:

1) A thorough analysis of the state-of-the-art IoT security privacy and trust challenges at different layers of the IoT.
2) A review of security requirements and architectural design issues that enhance IoT systems' security, privacy, and trust are investigated.
3) A wide range of classical IoT countermeasures as well as emerging and promising security solutions are investigated along with their advantages and drawbacks.
4) Open research challenges and potential research directions are identified.

The remainder of this article is organized as follows: Section II briefly introduces IoT and its architecture and provides a background of security challenges and concerns. Related work on IoT security and privacy is presented in Section III, and Section IV discusses and analyzes the effectiveness of architectural, privacy, trust, and security methods in protecting IoT systems from cyberattacks. Section V presents challenges and open issues that are not answered in the IoT field. Finally, Section VI presents a conclusion for the survey and identifies future research avenues. The organization of this review is visualized in Fig. 1.

II. SECURITY AND PRIVACY CHALLENGES IN IoT SYSTEMS

The rising popularity of IoT devices introduces various security challenges and vulnerabilities. These IoT security challenges are different from Conventional IT system challenges as summarised in Table 2. Below are common vulnerabilities that attackers frequently exploit:

1) Design Flaw-Induced IoT Exploits: An attack vector that arises from design flaws, allowing unauthorized device control, data breaches, and disruptions in the expanding IoT ecosystem.
2) Default Credentials: The use of default usernames and passwords is a significant vulnerability because it provides an easy entry point for attackers. Many IoT devices are left with their default settings, making them easy targets.
3) Insecure Network Services: Inadequately configured network services can expose devices to remote attacks, potentially giving attackers control over the device or access to the network it is connected to.
4) Lack of Encryption: Without encryption, data in transit can be intercepted, read, and modified by malicious

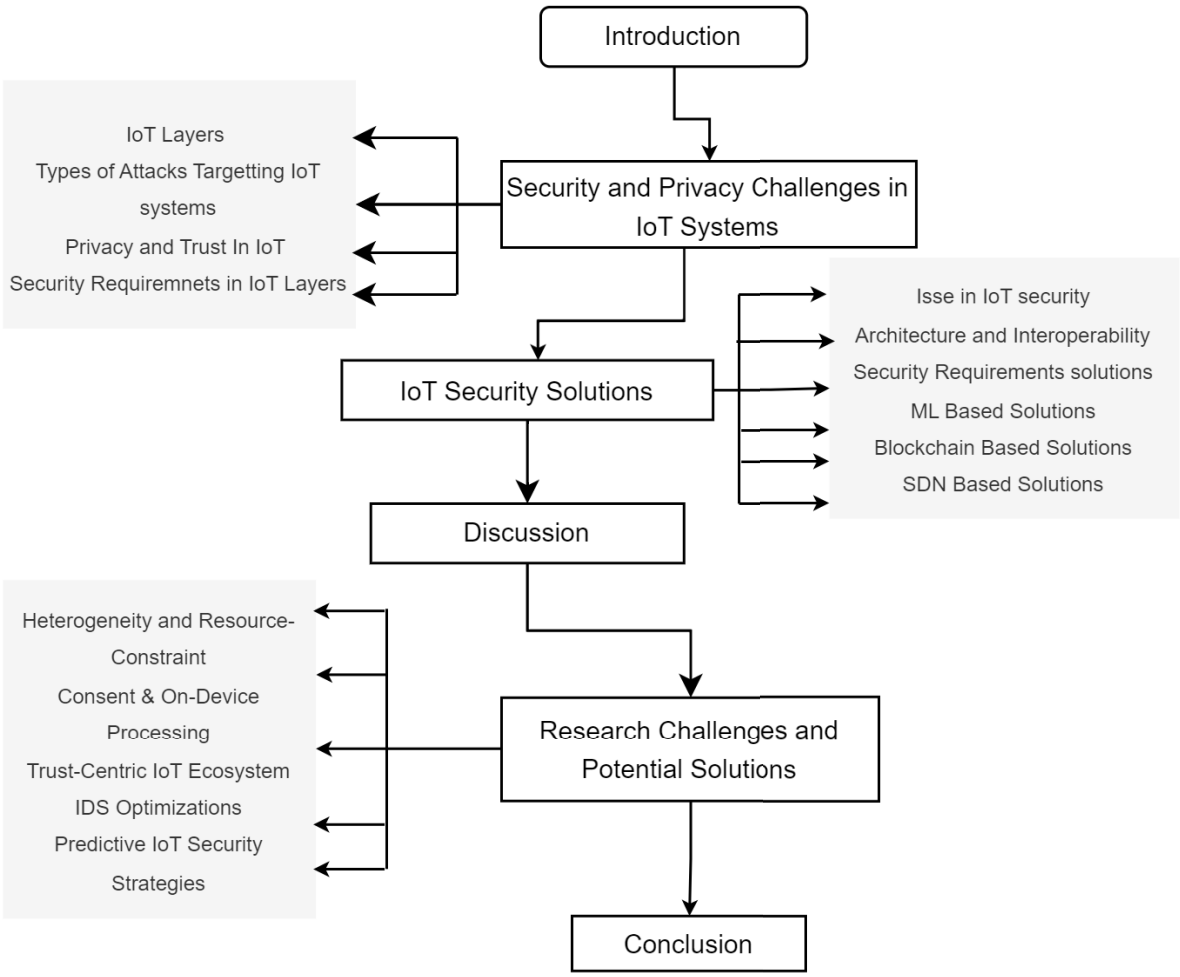


FIGURE 1. Article structure and organization.

actors. This can lead to data breaches and unauthorized control of devices.

5) Insecure Software or Firmware Updates: An insecure update mechanism resulting from outdated firmware can allow attackers to push malicious updates, effectively taking over the device or using it as a launchpad for further attacks.
6) Insecure Web Interface: Vulnerabilities in web interfaces, such as XSS or SQL injection, can provide attackers with control over the device, access to data, or a foothold in the network.
7) Insecure APIs: Given that many IoT devices communicate with external services, insecure APIs can lead to unauthorized access, data leakage, or manipulation of device functionality.
8) Lack of Network Segmentation: Without proper network segmentation, a compromised IoT device can be used as an entry point to access or attack other devices and systems on the same network.
9) Cross-Layer IoT Vulnerabilities: Refers to security weaknesses that exist throughout multiple layers of the IoT architecture, from physical devices to the application layer. These vulnerabilities also highlight the interconnected nature of IoT systems, where a flaw in one layer can potentially impact the security and functionality of other layers.

A. LAYERS OF IoT ARCHITECTURE

IoT is characterized by several functional architectural levels. Although there is no standard IoT architecture design, the fundamental IoT architecture often has three tiers, namely application, network, and perception layers. Fig. 2 shows how the layers of IoT architecture are based on their operation. Generally, the top layers send commands and actuate smart objects at the bottom layer to perform a specific task. The bottom layer generates data and sends it to the top layers for processing and use. Communication between the top and bottom layers occurs via the middle layer.

Each IoT layer differs from the others in terms of the functions and technologies it integrates with; hence, each layer presents its own security concerns. At the perception layer, also called the sensors layer, the data generated from IoT devices are located, collected, and prepared to be sent to the network layer. The network layer, on the other hand,

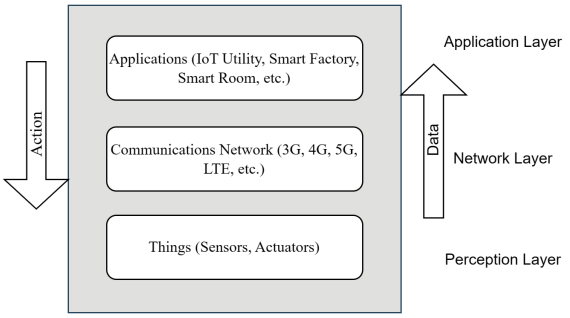


FIGURE 2. Layers of the assumed IoT architecture.

handles forwarding the IoT data generated at the lower layer to various hubs. It is comprised of critical components such as routers, switches, cloud computing platforms, and Internet gateways. The network layer employs various radio technologies, including 2G, 3G, LTE, WIFI, Bluetooth, and ZigBee. In addition, by gathering, filtering, and transferring data between sensors, gateways at this layer serve as an interface between nodes. Lastly, at the application layer, IoT serves its intended function by offering a variety of applications. Common IoT applications include smart cities, smart homes, smart offices, and smart transportation. IoT also has both personal uses, like those for mobile apps or smart wearable gadgets, and commercial ones, like those for autonomous vehicles.

B. TYPES OF ATTACKS TARGETING IoT SYSTEMS

IoT systems are susceptible to a variety of cyber threats. These attacks are examined in this subsection. A visual classification is provided in Fig. 3.

1) PHYSICAL ATTACKS

These attacks directly interact with the hardware components of IoT devices. Typically, such attacks are localized and require physical access to the device. Physical attacks can be devastating as they can bypass software-based security measures. In the following, we review some of the most common physical attack types on IoT devices.

Tampering is one form of physical attack where intruders alter the hardware components of IoT devices to change their behavior or access data. Another physical attack is radio frequency jamming, which involves the intentional transmission of radio signals to interfere with and disrupt the communication of these devices. Node Capturing sees attackers physically seizing an IoT device to exfiltrate data or modify its configuration or functionalities. An example of a node-capturing attack is Tag Cloning, where adversaries duplicate Radio Frequency Identification (RFID) or Near Field Communication (NFC) tags to impersonate genuine devices or surreptitiously access information. Sleep Deprivation strategically targets battery-powered devices, forcing them into repeated activations, which drains their energy and reduces their operational lifespan. Another concerning form of intrusion is through Hardware Trojans, where malicious modifications are embedded into a device's components, either during its manufacturing or afterward, which can later be triggered for harmful actions. Finally, there are Side-Channel Attacks that leverage inadvertent data leaks from a device's physical characteristics, such as its power consumption or electromagnetic emanations, to extract sensitive data.

2) NETWORK ATTACKS

Network attacks target the communication protocols and pathways that devices use to interact. By compromising these channels, adversaries can disrupt, manipulate, or eavesdrop on the data flow, leading to a range of malicious outcomes. For instance, Routing Attack manipulates the data transmission paths in IoT networks, potentially redirecting, delaying, or dropping the communicated packets. Moreover, using their IoT devices, network attackers can learn more about the users and utilize that information for illegal purposes. Such an example of an attack is sniffing. Sniffing allows attackers to eavesdrop on network traffic, enabling them to capture and analyze transmitted data.

Transitioning to more direct interventions, the Man-In-The-Middle (MITM) attack places the attacker covertly between two communicating parties, allowing them to intercept, modify, or reroute the exchanged data. The well-known Denial of Service/Distributed Denial of Service (DoS/DDoS) attack overwhelms an IoT device or network with an excessive volume of data requests, rendering it inoperable. Lastly, the Sybil attack involves a malicious device assuming multiple identities in a network to undermine systems that rely on redundancy and trust.

3) SOFTWARE ATTACKS

IoT software attacks focus on the vulnerabilities inherent within device firmware or embedded software. As IoT devices increasingly integrate into various sectors, the very core of a device's operational logic becomes an enticing target.

Through tactics such as manipulating functionalities, gaining unauthorized access, or even assuming control, the overarching security and integrity of the broader IoT ecosystem can be compromised. Malware is malicious software meticulously designed to infect and impede the standard operations of an IoT device. In some cases, it might even repurpose the device as a node within a more extensive malicious network termed a botnet. Following this, Code Injection comes into play where malicious actors seamlessly weave in or execute rogue code segments, subtly skewing a device's behavior or potentially pilfering its data.

Rootkits offer a covert approach, often going undetected at the kernel level, and provide intruders with a persistent, concealed foothold. Moreover, to further amplify their dominion, attackers resort to Privilege Escalation. By pinpointing and exploiting system vulnerabilities, they secure elevated access, thus widening the scope of potential disruptions. Lastly, the domain of software attacks also observes the

TABLE 1. Comparison with similar review articles.

Work	Contribution	Multilayered attacks	Encryption methods	Learning methods	Blockchain methods	SDN methods	Trust methods
[1]	An overview of IoT attacks and a taxonomy of security-based solutions	✓	✓	✓	✗	✗	✗
[2]	Addresses IoT security challenges at several tiers, with a special emphasis on ML/DL security approaches.	✓	✗	✓	✗	✗	✗
[3]	An overview of IoT threats and security challenges, as well as existing countermeasure techniques	✓	✗	✓	✓	✗	✗
[4]	Focuses on IoT architecture advancement, various risks on different IoT layers, and IoT security solutions such as SDN.	✓	✗	✗	✗	✓	✗
[5]	Examines security attacks from two perspectives: attack taxonomy and layer-wise attacks then provides some classical Security solutions.	✓	✓	✗	✗	✗	✗
[6]	Investigates security challenges associated with the IoT and how technologies like ML, and Blockchain can be used to address these challenges.	✓	✗	✓	✓	✗	✗
[7]	Studies security issue in IoT through layered architecture	✓	✗	✓	✓	✗	✗
[8]	Presents IoT security solutions using ML and Blockchain approaches	✓	✗	✓	✓	✗	✗
[9]	Provides a detailed examination of IoMT cybersecurity threats and countermeasure techniques utilizing Enabling Technologies such as AI and Blockchains as ways of security protection and authentication	✗	✓	✓	✓	✗	✗
[10]	A comprehensive analysis of the trustworthiness, privacy, and security of Mobile-IoT is provided in this survey.	✓	✓	✗	✗	✓	✓
This survey	Presents a comprehensive study of IoT threats, and various attacks, as well as all security methods listed here.	✓	✓	✓	✓	✓	✓

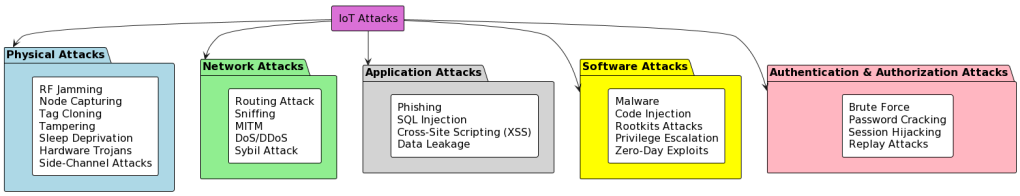


FIGURE 3. IoT attacks classifications.

unpredictable effectiveness of Zero-Day exploits. These occurrences emerge when undetected vulnerabilities are promptly and effectively exploited by attackers, frequently causing engineers to hastily seek countermeasures and rendering such attacks notably difficult to predict or prevent.

4) APPLICATION ATTACKS

IoT application attacks primarily target the user-facing interfaces and services of IoT systems. These interfaces, often designed for configuration, interaction, or data retrieval, can become focal points for attackers seeking unauthorized access or malicious manipulation.

One of the classical application attacks is Phishing. The Phishing attack uses deceptive techniques to lure users into revealing sensitive data, often by mimicking legitimate IoT application interfaces. SQL Injection targets the underlying databases of applications, where attackers embed malicious SQL commands to gain unauthorized access or manipulate data. In web-connected IoT platforms, Cross-Site Scripting (XSS) permits attackers to insert malicious scripts into web pages, which unsuspecting users' browsers then execute, potentially leading to data theft or session compromises. Data leakage, on the other hand, often results from vulnerabilities or misconfigurations in the application, inadvertently exposing sensitive information.

TABLE 2. Differences between IoT and traditional IT security challenges.

Aspect	IoT	Traditional IT
Scale and diversity	Large number of diverse devices and endpoints connected, ranging from sensors to appliances.	Primarily focused on computers, servers, and a smaller variety of devices.
Physical constraints	Typically have limited computational power, memory, and storage.	Often have more resources available for security measures.
Network environment	Often operates in resource-constrained and less secure network environments.	Operates in well-defined, controlled network environments, e.g., data centres.
Device distribution	Widely distributed across various locations, including remote and hostile environments.	Mostly centralized within controlled physical locations.
Communication protocols	Use a wide range of communication protocols, often with lower security.	Commonly use standard network protocols and can implement stronger security measures.
Patch and update challenges	Difficulty in updating devices due to varying hardware and software configurations.	Easier to update software and apply patches across standardized systems.
Legacy and lifecycles	Often have long lifecycles and may not receive regular updates.	May have shorter lifecycles and receive more frequent updates.
Resource efficiency	Security measures must be efficient to avoid straining limited device resources.	More resource-intensive security measures can be employed on traditional systems.
Physical tampering	Physical access and tampering risks are higher due to device distribution.	Physical access and tampering risks are relatively lower in controlled environments.
Authentication and identity	Identity management and authentication can be complex due to diverse device types.	Strong identity management and authentication systems can be more readily implemented.
Privacy concerns	Often collect personal data, raising significant privacy concerns.	Privacy concerns primarily revolve around data stored on traditional systems.
Manufacturer diversity	Multiple manufacturers and vendors create challenges for uniform security practices.	Hardware and software sources are usually limited to a few well-known vendors.
Regulatory compliance	May be subject to specific industry regulations and standards.	Often follows more established regulatory frameworks.
Security controls and measures	Must consider power consumption, encryption, device integrity, and secure boot.	Focuses on firewalls, intrusion detection systems, antivirus software, etc.
Human interaction	Limited interaction with users, which makes security configuration a challenge.	More user interaction, allowing for easier security configuration and monitoring.
Visibility and monitoring	May lack built-in monitoring capabilities, requiring external monitoring solutions.	Easier to implement network and system monitoring tools.

5) AUTHENTICATION AND AUTHORIZATION ATTACKS

Authentication and authorization form the cornerstone of IoT device security, verifying both the identity of users and granting appropriate access. Yet, as IoT ecosystems become more intricate, these processes are increasingly targeted.

Attackers, recognizing the potential to breach or assume control, exploit weaknesses in these security checkpoints, leading to unauthorized access and potential data compromise. For example, brute force attacks represent a straightforward yet relentless approach, where attackers attempt to gain access by trying all possible combinations of credentials until a successful match is found. Password cracking involves leveraging known information or using algorithms to predict or deduce the correct password, often exploiting weak or commonly used passwords. Transitioning from the entry point to ongoing sessions, session hijacking emerges as a formidable threat. Here, attackers intercept and take over an active session between the user and the IoT device, bypassing the need for direct login credentials. Lastly, replay attacks see malicious entities capturing and retransmitting data, especially authentication requests, to fool IoT devices into granting access or taking unintended actions. Each of these attacks underscores the vital need for robust and evolving security measures in the ever-expanding realm of IoT.

C. PRIVACY AND TRUST IN IoT SYSTEMS

The increasing number of IoT devices generates vast amounts of data that may include an individual's private information and daily activities. Therefore, protecting user privacy and instilling their trust is crucial when developing and deploying IoT solutions. However, as the ecosystem relies on sensors everywhere and data commonly transmitted in real-time, ensuring user privacy is one of the most challenging aspects of IoT [20]. Any breach of privacy can lead to a range of difficulties, including unauthorized access to data and modification or loss of sensitive information. Such breaches can also include leaking, impersonation, forgeries, and social engineering, thereby compromising users' privacy and sensitive data [21]. To maintain the confidentiality of user data, strong security measures such as encryption and authentication protocols must be implemented. By employing these measures, unauthorized access to sensitive data can be effectively prevented.

Additionally, clear and transparent communication with users about how their data is collected, stored, and used can help build trust and foster a positive relationship between users and IoT systems. Not only are encryption and authentications recommended approaches for safeguarding data privacy for IoT applications, but developing a secure architecture for IoT can also make

TABLE 3. Examples of the security requirements, concerns, challenges, threats, and solutions in IoT.

Security Requirements	Security Concerns	Concerned Layers	Security Difficulty	Security Threats	Security Solutions
Confidentiality	Insecure web service	Interface, service, network layers	Date Volume	Cloning	ICMetric with CRRP in combination
Authorization	Insufficient authentication or authorization	Interface, service, network, sensing layers	Resource limitations	Obfuscation implies the use of deceptive security measures	Dynamic IoT security based on immune system concepts
Authentication	Insecure network and services	Service, network layers	Protection	The revocation of security mechanisms by counterfeit makers even while the equivalent genuine items are protected, depends on low inspection rates across a variety of product categories	Key management with watermarks
Integrity	Lack of transport encryption	Service, network layers	Scalability	Attacks known as "removal reapplication" involve applying real security measures from (often abandoned) real items to fake goods	ECC cryptography
Availability	Privacy concerns	Services, network layers	Autonomous control	DoS Attack	Non-electronic security primitive

a significant contribution in this area, which is discussed in Section III-B.

IoMT is an example of a trendy research field for IoT systems, as IoMT devices generate and collect critical private data. In this direction, an integrated method of Federated Learning (FL) and blockchain was proposed by Singh et al. [22] to preserve users' private data. Each user model is trained locally and then the updated parameters are sent to the distributed servers in the cloud. The service is available in the cloud and secured by using blockchain technology, hence the proposed model provides both scalability and privacy.

Maintaining trust in IoT devices requires ensuring that data is safe and that only authorized people can access it. It also involves demonstrating qualities such as goodness, strength, reliability, and availability, which can be challenging to maintain over time. Trust in IoT systems can be fostered through transparency and accountability in the design and operation of these systems, as well as by providing users with control over their data [23]. Therefore, if IoT applications lack a solid security base, it is extremely hard for them to attain broad acceptance. Such a basis should prevent the creation of harmful models or, at the very minimum, lessen the impact their existence has. Hence, methods of authentication and encryption are used to keep IoT applications secure [24]. Also, Blockchain has been extensively used to achieve both privacy and trust in IoT applications [25].

Trust management can be looked at from an architecture perspective, e.g., centralized [26], decentralized [27] or hierarchical [28], [29]. Another approach of trust management is based on certain predefined rules and policies, e.g., [30] and [31]. Also, trust can be achieved through third-party-based based such as certificate-based approaches [32]. Another approach for trust management is based on the reputation and behaviour of IoT nodes [33], [34].

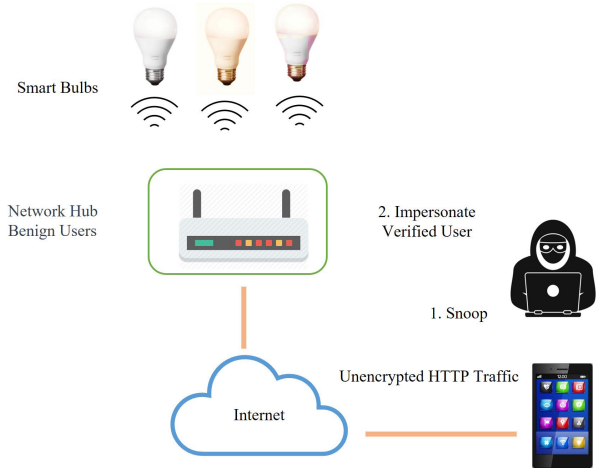


FIGURE 4. Attack on smart light.

1) SECURITY AND PRIVACY BREACHES SCENARIO

Smart spaces have become the essence of modern convenience and efficiency, outfitted with an array of interconnected IoT devices such as smart bulbs, thermostats, cameras, and locks. Nevertheless, these benefits are accompanied by substantial privacy and security challenges. A prime example is the vulnerabilities found in the Philips Hue Smart Bulb, which have shed light on broader issues that are common throughout smart home ecosystems as shown in Fig. 4.

These smart devices typically rely on communication protocols like Wi-Fi and Bluetooth to operate within a network. The Philips Hue Smart Bulb, for instance, was discovered to communicate via HTTP in plain text, a method that is susceptible to privacy and security breaches. This incident highlighted a specific vulnerability in its communication protocol, one that allowed attackers to easily intercept data. By doing so, they could gain intimate knowledge of user

habits and patterns of home occupancy. This problem is not limited to a single type of device but is indicative of a larger potential for security weaknesses that span across the diverse array of smart space components, leaving users vulnerable to risks such as eavesdropping and unauthorized system access. The ramifications of this privacy breach went well beyond the compromised bulb; without rigorous security measures in place for each device, the security of an entire smart home network could be at stake.

Attackers leveraged insecure communication protocol vulnerabilities across a spectrum of smart home devices, creating widespread privacy and security concerns. The implications of these vulnerabilities are extensive, especially considering user privacy. Attackers can construct a comprehensive profile of a user's private life by intercepting data from various smart home devices. This profile could include sensitive details like daily routines, behaviors, and personal preferences. Equipped with such information, attackers could engage in malicious activities ranging from planned data leakage to cyberstalking. Moreover, due to the interconnected nature of smart home ecosystems, a security breach in one component can initiate a domino effect, leading to a succession of privacy violations that ripple through the entire network of devices. To address these types of attacks that threaten the privacy and security of smart home devices, research in [35] introduced an independent module that leverages SDN to provide network-centric security measures. This approach diverges from conventional methods that typically reinforce individual devices' built-in security. The proposed approach is capable of identifying and isolating threats specific to devices within the network scope. It essentially provides security on a service basis to devices within a smart home environment. Additionally, this work details various smart home security vulnerabilities and privacy breach scenarios, along with proposing effective strategies to counter these attacks.

D. IoT SECURITY REQUIREMENTS AND CHALLENGES

In the realm of IoT security, five principal requirements outline the essentials for safeguarding IoT systems: confidentiality, integrity, authentication, authorization, and availability. In confidentiality, the information exchanged between parties must be secured against unauthorized reading. This can be achieved through the implementation of lightweight cryptographic algorithms suitable for the constrained nature of IoT devices. Elliptic Curve Cryptography (ECC), for instance, allows for secure encryption with minimal computational overhead, safeguarding data privacy even in resource-limited environments such as wearable health monitors. Integrity, however, protects the information against unauthorized alteration. While in authentication, only authorized users are permitted access to the system and sensitive data. In authorization, object rights ought to be limited so that users can only access the resources they require for particular tasks. Finally, availability ensures the continuity of service and the prevention of any potential operational malfunctions. State-of-the-art techniques to address security requirements are presented in Section III-C.

There are additional difficulties with meeting IoT security requirements when compared to classical IT systems. These are outlined as follows:

1) Date volume: Even though the majority of IoT applications use limited communication channels, IoT devices often generate large volumes of data to be transferred to the central network point [36].
2) Resource limitations: Since the majority of IoT nodes have low processing and storage capabilities, they typically have low bandwidth communication channels, which restricts the usage of various security solutions like the public key encryption algorithm.
3) Protection: It is simple to monitor objects such as tags and identify nodes because the majority of IoT systems employ weak authentication mechanisms. The intruder usually possesses the capacity to read, edit, and even delete data.
4) Scalability: IoT consists of a large number of nodes and grows over time. Consequently, its security system should be scalable.
5) Autonomous control: IoT nodes should be able to connect and set themselves up to change according to the platform. Therefore, it must incorporate certain procedures and approaches like self-configuration, self-management, and self-healing to meet the additional security required by automation and control.

For further understanding of the security requirements in IoT and the associated challenges, we refer interested readers to these works [37], [38], [39]. Table 3 lists some examples of the security requirements, concerns, challenges, solutions, and threats in IoT.

III. IoT SECURITY SOLUTIONS

This section reviews recent developments in IoT security. The security issues and requirements for IoT are reviewed first. Then, different proposed architectural designs of IoT that attempt to address some of the issues are evaluated. Afterward, multiple notable pieces of literature on the integration of ML, blockchain, and other trends in IoT security are discussed. Each subsection includes a table summarizing IoT security solutions, highlighting the strengths and weaknesses of the existing works.

A. ISSUES IN IoT SECURITY

Many recent works in the literature reviewed IoT security and privacy, providing a general sense of IoT, its layers, security and privacy concerns, and traditional solutions to address these concerns. One such study is [40], where several security threats, their solutions, and the future paths for IoT security were examined. In addition, this study examines crucial security technologies like encryption in the context of IoT. It also evaluates security risks to

the IoT network and discusses mitigation strategies. The implications of these IoT network attacks are also discussed in this study, along with several countermeasures to mitigate such vulnerabilities. The authors also provide a high-level overview of IoT by discussing the operation of its tiers before talking about several security flaws in its various IoT architectural IoT layers. Additionally, it offers defenses against security risks and safeguards against IoT network damage.

The authors of [41] introduced a three-layer design of IoT, discussed its primary security needs, and showcased potential solutions, with an emphasis on privacy challenges. Security and privacy concerns can hinder IoT adoption. It is crucial to develop robust frameworks that account for the complexities and variables of the IoT ecosystem. The ever-increasing number of diverse interconnected nodes, combined with the sensitive nature of most IoT data, exacerbates the challenges of implementing security measures. The potential vulnerabilities across every layer of IoT underscore the need for rigorous research in this domain. Outstanding issues include ensuring service quality, confidentiality, data management, addressing software and hardware vulnerabilities, and formulating relevant standards. A focal point in IoT security is data privacy, reliant on authentication and identification. Despite its importance, it often remains overlooked. Comprehensive security frameworks are essential to address all layers of IoT security. Abomhara Køien [42] provided in their study an explicit overview of the most significant IoT components, with a focus on the vision and security issues IoT presents.

To create and implement appropriate security solutions for IoT that take into account the limitations of its equipment, more research is required. Additionally, there is a need to create comprehensive security and privacy frameworks that address the problems at each tier and take influencing factors into account.

The study [5] introduces IoT security and privacy concerns that have a detrimental effect on IoT systems. This study compiles the data required to provide a comprehensive picture of IoT security issues and problems. Additionally, it helps with understanding what has to be done to safeguard IoT systems and how to stop attacks against them. IoT security and privacy issues can arise for a variety of causes. Different attack types are handled differently at multiple tiers and various methods are available to defend IoT systems from these threats. IoT systems are susceptible to numerous threats that put user privacy at risk. The degree of risk which is posed by different security and privacy threats varies based on their origin (internal or external).

Frustaci et al. [44] argue that the perception layer of the IoT system model is the most exposed level due to the physical exposure of IoT devices, their limited resource availability, and their technological variety. Therefore, it is necessary to begin tackling the level-one problems by designing lightweight security solutions that can adapt to heterogeneous environments with resource-constrained devices.

B. ARCHITECTURE AND INTEROPERABILITY BASED SOLUTIONS

To address IoT security, trust, and privacy issues, many works suggest a different layered architecture than the traditional three-layer architecture mentioned previously. For example, the authors of [43] analyze the security needs and potential risks in a four-layer architecture, in terms of communication security, network security, application security, and general device security. They also examined the security issues with IoT-enabling technologies. This study explores the trade-offs among security, privacy, and utility, aiming to enhance security within the complex, multi-layered IoT architecture. The approach of this study was based on a four-layer IoT framework that includes the sensor layer, network layer, service layer, and application layer. Moreover, IoT security needs and solutions were examined besides the security of enabling technologies, such as identifying and tracking technologies; Wireless Sensor Networks (WSN) and RFID, communication, networks, and service management, which were then discussed after the analysis of cross-layer threats. Also, this study covered the potential attacks in several layers such as Path-based DoS attacks and overwhelmed attacks conveyance layer attacks by flooding Malicious node attacks, Sybil attacks, wormhole attacks, spoofing attacks, routing attacks, etc. are examples of network layer attacks.

Conversely, Mrabet et al. [7] presented a novel, five-layer IoT architecture. Based on the new IoT framework, a new classification of security threats and attacks was proposed. The assumed IoT architecture is composed of the physical perception layer, a network and protocol layer, a transport layer, an application layer, and a data and cloud services layer. The IoT's foundational hardware is first included in the physical sensor layer. Then, they cover the security risks and solutions while highlighting the various network and protocol technologies used by IoT. The security threats against transport protocols were examined while common remedies were presented. Then, application protocols and thin IoT encryption methods were used at the application layer. Finally, the key security characteristics of IoT cloud platforms are enclosed in the data and cloud services layer [49]. confidentiality, integrity, authorization, authentication, and encryption techniques were discussed. This study concludes by outlining unresolved issues and potential future directions for securing IoT, such as the absence of standardized lightweight encryption algorithms, the use of ML algorithms to improve security and the associated difficulties, the application of blockchain to address security issues in IoT, and the implications of IoT deployment in 5G and beyond.

In [41], the authors proposed a novel IoT layered model that has layers of identification privacy, and security components, to support the implementation and evaluation of the proposed IoT system. The IoT nodes created by Amazon Web Service (AWS) as virtual machines are the bottom layer. The middle layer's (edge) implementation utilized the Greengrass Edge Environment on AWS along

TABLE 4. Recent works on IoT security issues and architectural design.

Work	Scope	Methodology	Strength	Limitations
[43]	Provides a comprehensive review of the security requirements and difficulties for the IoT.	Analyzes security requirements and solutions based on the four-layer IoT framework.	Summarizes the top ten vulnerabilities and examines security solutions for different enabling technologies and their consequences for different applications.	There are still unresolved issues in several domains, limited to specific areas and applications, and may give unreadable results in other areas.
[41]	Develops novel IoT layered model with layers of identification, privacy, and security components.	The IoT nodes created by AWS as VMs are the bottom layer. The middle layer's (edge) implementation utilized the Greengrass Edge Environment on AWS along with a Raspberry Pi.	Summarizes the existing security and privacy concerns and security solutions models required and suitable for various layers of IoT-driven applications.	Lack of the necessary awareness of the security consequences until after a breach has happened, leading to significant losses including the loss of vital data.
[40]	Examines several security concerns, their solutions, and the future paths for IoT security.	Not reported.	Summarizes and examines crucial security technologies like encryption in the context of IoT to prevent hazardous risks in light of the most recent research.	Limited description of security risks to the IoT network and not enough discussion of mitigation strategies.
[44]	Demonstrates that the IoT system paradigm includes several security vulnerabilities.	Surveys recent research in the IoT security domain.	Summarizes security vulnerabilities, including dangers that may take advantage of potential flaws.	This study suffers from resource restrictions for IoT devices.
[42]	Provides an overview of the most significant IoT components and the unique security issues IoT presents.	Not reported.	Summarizes and discusses the security issues surrounding security services, including authentication, privacy, trustworthiness, and end-to-end security.	Limited number of solutions that can be taken to solve these obstacles.
[45]	Presents a trusted architecture for IoT while different nodes are clustered under one coordinator for each cluster.	The study uses the Contiki Cooja simulator to build node clusters and to evaluate the proposed architecture.	Clustering nodes into specific clusters makes it easier to just accept the trusted node and isolate the bad nodes.	Lack of a trust rating of the nodes.
[46]	Securing MQTT IoT application protocol architecture.	The proposed MQTT was evaluated in Contiki cooja simulator.	It offers end-to-end encryption, also WSNs are used as a case study to evaluate the proposed MQTT secure architecture.	It is an application protocol-based solution.
[47]	Address security implications of interoperability in IoT devices and platforms.	Not reported	The proposed solution focuses on interoperability	Lack of specificity in addressing diverse IoT security threats.
[48]	Facilitate enhanced service/device discovery and management through IoT framework integration with edge computing.	Utilized SOA-based middleware	Integrated edge computing for better service/device discovery and management	Monolithic architectures limit scalability in large-scale IoT systems

with a Raspberry Pi 4 hardware kit. To implement the top layer, they utilized the cloud-enabled IoT ecosystem in AWS (the cloud). Moreover, between each of these layers, there were security protocols and crucial management sessions to guarantee the confidentiality of the users' information. To enable data flow between the levels of the cloud/edge-enabled IoT model, they implemented security certificates. They presented the advantages and risks of IoT systems. Despite the many advantages, risks to end users exist due to permitting unwanted access to sensitive private data and facilitating attacks.

A trust-based IoT architecture is crucial to utilizing IoT services and thereby contributing to their success. A study that follows this pattern was proposed in [45]. The proposed architecture is scalable and could work under an uncertainty network. The nodes were clustered according to their location and region by assigning a coordinator for each cluster. Each cluster is a fog computing domain. Coordinators can communicate with each other and communicate with the cloud as well. the proposed architecture was analyzed using the Contiki cooja simulator with different performance metrics to assess its efficiency and scalability. However, this

TABLE 5. Recent work on security requirement research.

Security Requirement	Proposed Solution	IoT Layer(s)	References
Confidentiality	Lightweight cryptographic algorithms and ECC for secure encryption, including countermeasures against side-channel attacks.	Application, Network, Perception	[2], [50], [51]
Integrity	Cryptographic methods (HMAC, digital signatures) and SDN-based architecture for data and software integrity.	Application and perception	[52] [53] [54].
Authentication	Challenge-response protocols and physical unclonable functions (PUF) for secure user and device authentication.	Application, Network, Perception	[55], [56], [57], [57]
Authorization	Capability-based security models and game theory models for access control and conflict resolution	Application	[58], [59]
Availability	Identifying vulnerabilities and employing recovery strategies like Moving Target Defense (MTD) and blockchain-based solutions.	Application, Network, Perception	[60], [61]

study has some limitations including the lack of a trust rating of the nodes. Furthermore, the target computing is the fog layer, whereas analyzing the IoT layer would be far superior. A similar study that focused on securing MQTT IoT application protocol architecture was presented in [46] to secure the communication between the publisher and subscriber. The proposed security architecture is based on end-to-end encryption. Moreover, WSNs are used as a case study to evaluate the proposed MQTT secure architecture. The proposed MQTT was evaluated its performance through the Contiki cooja simulator.

The authors of [62] discussed the security challenges and flaws in IoT and proposed a secure architectural solution for addressing these issues. The authors identified 12 weaknesses, attack vectors, and design flows in each layer of security, including physical, network, and application. To address these challenges and vulnerabilities, they proposed a shift-left approach to securely design and architect resource-intensive IoT use cases earlier in the life cycle. The article also suggests future research directions for improving the security of IoT systems, including the development of secure communication protocols and the use of cryptography algorithms. Overall, the research provides a comprehensive overview of the security challenges in IoT and proposes a solution for addressing these challenges, although it does not address the IoT devices' resource limitation in the proposed solution.

Interoperability in IoT networks is vital for device communication, but it poses substantial security challenges, heightened by the initiatives of major technology corporations such as Google and Microsoft to enhance device connectivity. These leading industry players are actively developing solutions to improve interoperability; for example, Google has introduced the Android Things toolbox, aimed at streamlining the connectivity of IoT devices in a manner as user-friendly as using Android applications [63]. Standards play a pivotal role in this landscape encompassing a broad spectrum of details, ranging from specific elements to broader, abstract concepts, based on their intended use. For instance, certain standards offer precise guidelines to ensure consistent and accurate functionality across various systems, preventing any loss of information. Popular network protocols like IEEE 802.11 [64], CoAP [65], and WebSocket [66] are few examples. These standards and frameworks set detailed guidelines ensuring effective communication between a sender and receiver. Similarly, Web standards such as HTML, CSS, and XML outline how to structure documents on Web pages. When these standards are properly implemented, they ensure seamless operations and enhanced security [67]. Beyond the technical specifics, Some standards focus on conceptual knowledge, including software architecture, frameworks, and reference models. They aim to provide key principles for the development of software, systems, and environments. These standards are crafted by specialists with deep expertise in particular areas, making these conceptual standards a reliable benchmark for software and system development. By applying these conceptual standards, developers can boost efficiency, save time, and mitigate risks during the development and management processes [68]. However, this integration of devices across diverse platforms and standards complicates the security landscape [69]. While such advancements by key industry figures promote easier communication among various IoT devices, they also underscore the urgency for uniform security standards to mitigate potential vulnerabilities. With the network's growth, the importance of robust, flexible security measures escalates, becoming crucial in safeguarding against the continuously evolving cyber threats in these interconnected environments.

In this inherently diverse IoT environment, where entities like sensors, platforms, and users are interconnected, interoperability and security need to be developed simultaneously. This requires secure identification methods, like authentication and authorization, ensuring that no information about these entities is lost in the process [70]. Additionally, when data are exchanged between different IoT entities, this transfer must happen without information loss, necessitating interoperable data exchange protocols and secure transport methods [71]. These considerations are vital across various IoT aspects, including architecture and framework design, platform development, and scenario building. Several solutions were proposed to address the security implications of interoperability in IoT devices and platforms [47], [72]. Both [48] and [73] utilized SOA-based middleware for IoT, facilitating device search and complex service interactions. A study by [72] furthered this approach by integrating edge computing into an IoT framework for enhanced service/device discovery and management. These methods typically adopt monolithic architectures [74], [75], but their limitations in large-scale IoT systems have shifted the focus towards SOA for better interoperability [47]. Currently, many IoT services are transitioning to microservices [76], [77] for scalability, agility in deployment, and fault tolerance, meeting evolving IoT middleware needs [78]. A summary of related works on IoT security issues and Architectural design is listed in Table 4.

C. SECURITY REQUIREMENTS RESEARCH

Five essential security requirements for IoT systems are identified in Section II-D. These include confidentiality, integrity, authentication, authorization, and availability. In Confidentiality, the information exchanged between parties must be secured against unauthorized reading [2]. This can be achieved through the implementation of lightweight cryptographic algorithms suitable for the constrained nature of IoT devices [50], [79]. ECC, for instance, allows for secure encryption with minimal computational overhead, safeguarding data privacy even in resource-limited environments such as wearable health monitors [51]. Moreover, research in the field explored the hardware aspects of standard block ciphers, highlighting the balance needed among cost, performance, and security in various IoT systems [80]. For instance, in scenarios like electronic ticket RFID tags, there is a high demand for reduced power usage and low latency, often at the expense of security [81].

The authors of [82] analyzed more than 40 block ciphers, categorizing them for use in different embedded devices, and noted their vulnerability to side-channel analysis attacks due to their simplicity. Similarly, [83] investigated fault and time-based side-channel attacks on common IoT cryptographic methods like RSA, AES, and ECC, offering counteractive strategies. Moreover [84] developed a comprehensive framework for examining algebraic fault attacks on these lightweight ciphers. It is crucial to emphasize that maintaining confidentiality is important across all layers of IoT networks. This includes safeguarding data at rest in both the perception and application layers, as well as ensuring the security of data in transit within the network layer.

Integrity, however, protects the information against unauthorized alteration. This encompasses both code integrity and data integrity, each vital for the consistent and secure functioning of IoT systems. Ensuring these aspects of integrity is crucial to maintaining the overall reliability and trustworthiness of these systems. Various approaches were proposed to preserve the integrity of data and codes in IoT networks including cryptographic approaches such as HMACHash-Based Message Authentication Code [52] and digital signatures [53]. A remote software attestation scheme that enhances integrity in IoT environments through SDN was introduced in [54]. It is a lightweight architecture designed to preserve the integrity of software on IoT devices, ensuring it serves its intended purpose effectively. Digital signatures are used in smart grids to ensure the data from smart meters is not altered, maintaining accurate energy distribution and billing.

In authentication, only authorized users are permitted access to the system and sensitive data. Through challenge-response protocols, IoT devices validate the identity of users, establishing a secure communication channel with the central system [55]. Also, the authentication is applied at the application layer where users interact with IoT applications to use the services provided by these IoT applications [56]. This mechanism is widely employed in smart home ecosystems, where devices must authenticate themselves to interact with the home automation system [57]. Building on the work of [57] and [85] presented a user authentication scheme for smart homes, using Physical Unclonable Functions (PUF) and validating it with Real-or-Random (RoR) model and Burrows-Abadi-Needham (BAN) logic. The scheme's robustness against attacks was tested with the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, and its efficiency was compared with previous methods in terms of communication and computational costs.

Authorization is applied only after devices are successfully authenticated [86]. In authorization, object rights ought to be limited so that users can only access the resources they require for particular tasks [87]. In IoT, capability-based security models are employed to grant specific rights, effectively limiting interactions to what is necessary for the task at hand [88]. For instance, within a smart building, IoT sensors may receive tokens that authorize them to execute actions aligned with their designated functions, such as environmental monitoring or security surveillance. Moreover, researchers are developing partially automated authorization systems using ML techniques. For example, the authors of [58] presented a game theory model for mutual intrusion detection in IoT, aiding nodes in decision-making. Similarly, [59] introduced a conflict resolution scheme for IoT services, using a semantic policy structure and soft constraints to address multi-service disputes.

Finally, availability ensures the continuity of service and the prevention of any potential operational malfunctions [87]. For instance, the critical role of IoT devices in remote patient monitoring systems makes their uninterrupted operation essential. Disruptions in service, whether from intermittent wireless connections, DoS attacks, or even routine maintenance such as replacing a depleted battery, can significantly decrease availability. If the IoT system becomes non-operational during such events, it not only interrupts data flow to healthcare providers but also poses a potential threat to patients' lives. Several studies [89], [90] identified key vulnerabilities in IoT devices, networks, and services, such as software, hardware, cloud services, and communication device failures, that could impede the resilience and availability of IoT systems. To address these challenges, different recovery strategies were proposed, including post-event automatic recovery mechanisms like MTD [60] and blockchain-based solutions [61], which are geared towards reinforcing the resilience of these crucial IoT components. A summary of recent works related to security requirements solutions are provided in Table 5.

D. MACHINE LEARNING-BASED SOLUTIONS

ML offers a dynamic approach to enhancing IoT security by enabling systems to learn from data patterns and detect anomalies, thereby fortifying defenses against evolving IoT threats. In this direction, the work [6] examined 145 recent articles in IoT security to discuss the security challenges associated with the IoT and how technologies like ML, Artificial Intelligence (AI), and blockchain can be used to address these challenges. Conventional ML methods were adopted for enhanced IoT attack mitigation as they detect threats accurately and process data rapidly. Since IoT traffic and patterns are not specified in ML techniques, they learn without explicit programming. The study in [2] reviews intrusion detection techniques with a focus on ML/DL and lists IoT public datasets available in the literature.

Yavuz et al. [101] presented an IoT intrusion detection system using two widely used ensemble multiclassification techniques; bagging and boosting for the prediction of normal and abnormal classes in IoT networks. TON-IoT datasets were used to evaluate the ensemble models. To get the best detection accuracy, hyper-parameter tunings were performed. Comparison analysis between bagging and boosting models was conducted in terms of performance matrices such as accuracy, precision, F1 score recall, and speed. While slightly less accurate, the LGB boosting technique performs better in terms of speed and ROC-AUC score. Better accuracy is achieved by random forest RF at the cost of longer execution times, more computing power, and complexity. This study recommends adopting LGB while developing intelligent and efficient IDS for IoT networks since IoT requires a lightweight intrusion detection system.

The authors of [102] extensively investigate cyberattacks on smart cities and how attacks on ML and Deep Learning (DL) models can impact them. Ensemble models like bagging, boosting, and stacking are used to enhance the detection system's performance and to mitigate and detect IoT-based ML and DL attacks. The proposed method was tested on the DS2Os dataset in the presence of sample attacks. Similarly, an effective and adaptable DNN was presented by [98] to protect smart grids, particularly for demand-side management, from cyberattacks. The proposed hybrid model combines DNN and a search technique called the Squirrel Search Algorithm (SSA). The latter technique optimizes the weight parameters, which considerably enhances model performance. While the DDN technique identifies, detects, and classifies anomalies. The presented approach identifies smart grid cyber threats while simultaneously conserving energy. In addition, ML-based solutions are more effective in detecting threats than other standard anomaly IDS strategies, as was demonstrated in earlier publications.

For ML models, an unsuitable dataset, however, might result in false positives and a decline in detection accuracy [101], [103]. Therefore, research efforts are shifting towards deep learning (DL) to predict IoT cyber-attacks [104] with faster and more real-time data streams. DL is a specific type of ML technique that automates the feature extraction process by using multiple layers of interconnected perceptrons or neuron processing units. Each layer uses the input from the layer before it to focus on a certain task. Due to their feature engineering capabilities, Multi-Layer Perceptron (MLP), Convolutional Neural Networks (CNN), and Generative Adversarial Networks (GAN) are now popular DL techniques used for IoT cyber-attack mitigation [105], [106]. Research findings in this domain, e.g., [107], [108], and [109], show that these mitigations are evolving into a feasible IoT cybersecurity solution.

A novel technique integrating CNN methods and GWO metaheuristics for cloud data network focus was presented by Garg et al. [91]. Metaheuristic optimization approaches were used to determine the best feature selection. The next step is to identify and categorize network anomalies using a CNN model. The proposed model offers a high level of detection accuracy, claim the authors. This cloud-based method is not suited for processing data while it is in use or in real-time IoT networks. Others have used the same CNN strategy in conjunction with transfer learning models to identify and categorize attacks [92]. Binary and multiple classifications are both used in the proposed model. This model was applied to several existing datasets and achieved a high degree of detection accuracy. The authors claim that their model takes less time to train. However, until experimental evidence backs it up, such a claim is unacceptable.

A CNN centralized network-based IDS technique was also developed in [93] to monitor data traffic and spot anomalies in IoT networks. The level of accuracy attained is high. As an alternative, a Recurrent Neural Network (RNN) is practical for managing time series data as well as sequential data. To identify and detect malicious activity in IoT devices,

TABLE 6. Summary of existing ML-based IoT security techniques.

Reference	Model	Dataset	Accuracy
[91]	CNN, GWO	DARPA'98 and KDD'99	95.68%
[92]	CNN, transfer learning	BoT-IoT, IoT-ID, MQTT-IoT-IDS2020, IoT-23, and IoT-DS2	99.03%
[93]	CNN	NID Dataset and BoT-IoT datasets	99.51%, 92.85%
[94]	LSTM,GRU, BiLSTM	NSLKDD, BoT-IoT, IoT-NI, IoT-23, MQTT, MQTTset, and IoT-DS2 datasets.	99.91%, 99.92%, 99.94%
[95]	ANN	BoT-IoT, TON-IOT, and IoTID20	99.9%
[96]	GAIL	Custom Dataset through simulation	Not reported
[97]	DNNMLP	DS2OS	99%
[98]	Adaptive DNN	Custom Dataset	98%
[99]	GRU	Custom Dataset	99.96%
[100]	GAN	Custom Dataset	90.5%

Ullah and Mahmoud [94] use three different RNN models, i.e., LSTM, BiLSTM, and GRU approaches. They start by applying CNN for feature learning. Several datasets, up to seven in total, are utilized for the model evaluation to evaluate and assess the proposed model. Performance for binary and multiclass classification is evaluated. For large datasets, the proposed solution achieved high accuracy.

While others focus on securing IoT networks with CNN and GAN, Huang et al. [96] presented an IoT data privacy preserving method termed generative adversarial imitation learning (GAIL) that uses an Inverse Reinforcement Learning (IRL) approach. The GAIL technique incorporates the ideas of the GAN to build complex behavior imitations. Protecting sensitive medical data was used as a case study for this work. The proposed method initially tries to learn data from experts (humans) as a reward and policy function such that it learns to have similar behaviors to the given experts. This work has certain limitations; the proposed GAIL does converge slowly, resulting in a longer training time. In addition, it requires professionals to learn from them, which is inefficient. Also, the author of [95] presents a novel solution for provisioning each IoT device with a lightweight Artificial Neural Network (ANN) model that can evolve and adapt to detect any anomaly events in the device. The model is kept in its basic setup to cut down on the time and resources needed to operate it and speed up the process of approaching the optimal operation zone. The model is evaluated using three distinct datasets, and the results show that the model is performing well in detecting the anomalies in each IoT device with minimal degradation of the network. The proposed solution by the author suits IoT devices that have greater capability in terms of resources, including computing, storage, and power.

Regarding IoT network layer security, a little effort has been made to tackle routing attacks on IoT networks using Anomaly IDS-based DL techniques. A possible explanation for this might be the scarcity of network layer datasets. This can be observed from the research works in this layer, where most studies use custom datasets. This is exemplified in work undertaken by [99], where they applied the Gated Recurrent Unit network model to detect and prevent RPL flooding attacks such as the hello flood attack. A custom dataset was generated through Contiki cooja simulation. The model accurately detects the hello flooding attack when there are few nodes. However, this model lacks scalability, and as the number of nodes grows, it will be unable to detect the targeted attack. Another drawback of the approach is that it can only detect one type of rooting assault on RPL networks. Likewise, authors in [100] developed a DL technique to detect routing attacks on RPL distributed environments using a combination of GAN and SVM models. The GAN model is used to identify traffic events considered to be routing attacks, while SVM classifies the routing attack class using multiclassification. The proposed hybrid technique is compared to the SVM standalone and proved to perform better in terms of accuracy and execution time. This work is better than the work done by [99] in terms of scalability and the number of detected attacks. However, the model cannot still detect other routing attacks on the RPL network.

Another notable research evaluated here is [116], where the authors look at the limitations of IoT devices used in real-world applications in terms of security. Most notably, they explain how the nature of these devices being in an unguarded area and with fairly underpowered processing capabilities makes them a prime target for exploitation. They describe how the IoT devices themselves often cannot apply active security measures that more established technology can and would therefore require some higher-level security consideration. Then, some related works are explored that tried to apply ML in IoT Security applications. Finally, the authors move on to explore specifically the use of DL through the application of an NN to aggregate a large amount of data collected by IoT devices and extrapolate odd behavior that could be indicative of security breaches. The study, however, lacks the specifics of the model and test performed. For example, the exact structure of the developed NN is not shared, nor are the IoT devices and data collected from them. Table 6 lists relevant studies on ML/DL-based IoT security solutions that have recently been presented.

E. BLOCKCHAIN-BASED SOLUTIONS

Blockchain technology has been proposed as a potential solution to the security and privacy challenges faced by IoT. Blockchain acts as a decentralized, distributed, and

TABLE 7. Summary of the recent works on IoT security using blockchain and SDN methods.

Work	Scope	Methodology	Strength	Limitations
[110]	Discusses the potential opportunities and challenges of using blockchain technology in IoT.	Follows a systematic way for the integration of blockchain and IoT. It also presents challenges, such as scalability and energy consumption.	Proves that the use of blockchain in IoT can improve communication security and provide a way for IoT nodes to securely communicate in heterogeneous environments.	Some of the opportunities listed, such as time reduction and risk management, are not explained sufficiently.
[111]	Proposes a method that uses a blockchain-based IoT network to defend against potential cyberattacks.	The proposed solution is validated through a series of experiments that show its ability to withstand various types of cyberattacks.	The findings show that this approach has the potential to enhance the cybersecurity of WBMSs, enabling their broader adoption in cyber-physical environments.	It is limited to only IBM's Hyperledger Fabric Blockchain platform.
[112]	Aims to solve access control challenges in IoT.	The Hyperledger Fabric platform is used to build and evaluate the proposed blockchain-based access control system.	Scalable and effective.	It still needs a reduction in storage overhead.
[113]	Focuses on both authentication and authorization to secure IoT communication using blockchain.	Simulated annealing and genetics to identify unknown clusters it builds using the same open-source platform as previous ones.	It prevents single-point failure as it is a distributed and scalable approach.	Suffers from overhead and energy consumption.
[114]	Study SDN-based security architecture for IoT.	The performance of the architectural design decisions made for SDN utilizing OpenFlow is investigated.	Networks with or without infrastructure can exist in each domain, and each controller is only in charge of that domain.	overhead and complexity.
[115]	Securing IoT communication using SDN.	The validation and implementation of the proposed architecture are done on ONOS SDN controller and Raspbian VMs.	It offers both authentications of network access as well as authorization of the traffic in the IoT network to prevent malicious devices and mitigate cyber-attacks.	To prevent unknown attacks requires a costly reconfiguration of the SDN controller.

public ledger for storing transactions among IoT nodes. Every block in a blockchain has a cryptographic hash code, a previous block hash, and its own data, and the transactions in a blockchain are the basic units used to transfer data between IoT nodes. There are many surveys available that discuss IoT security threats using enabled blockchain techniques [117], [118], [119], [120]. According to [110], the use of blockchain in IoT can improve communication security and provide a way for IoT nodes to securely communicate in a heterogeneous environment. However, the integration of blockchain and IoT also presents challenges, such as scalability and energy consumption. In this work, the author discusses the potential opportunities and challenges of using blockchain technology in the IoT. However, some of the opportunities listed in this article, such as time reduction and risk management, are not explained sufficiently.

This study investigates the vulnerability of the IoT to insider threats, focusing on the impact of environmental tampering on data integrity within the perception layer. The research aims to understand how altering the state of the environment affects sensor data accuracy and to develop mechanisms to safeguard this data, ensuring reliable analytics and processing. The approach centers on scenarios where insiders manipulate physical conditions to skew sensor readings. As a preliminary solution, a framework combining Ethereum blockchain and edge computing is proposed to validate and maintain the integrity of sensor data before it is analyzed, processed, and stored.

An example of using Blockchain to address IoT security and privacy issues is presented by the authors in [111], where they introduce a next-generation Wireless Battery Management System (WBMS) architecture and propose using a blockchain-based IoT network to defend against potential cyberattacks. The proposed solution is validated through a series of experiments that show its ability to withstand various types of cyberattacks. The results of their experiments suggest that this approach has the potential to enhance the cybersecurity of WBMSs, enabling their broader adoption in cyber-physical environments. Nevertheless, the study does not provide experimental evaluations or statistical analysis of the conducted experiments and it was limited to only IBM's Hyperledger Fabric Blockchain platform.

One of the primary security concerns in the IoT domain is presenting an effective access control for IoT devices. Ding et al. [112]. offered a study that solves access control challenges in IoT. The proposed access control system is a

distributed access system that ensures integrity and eliminates single-point failure. The Hyperledger Fabric platform is used to build and evaluate the proposed blockchain-based access control system. The obtained findings demonstrate that the proposed approach is scalable and effective. however, it still needs a reduction in storage overhead. Furthermore, Complexity and scalability are among the obstacles that blockchains must overcome. To address this problem, Abdi et al. [121] proposed a hierarchical blockchain solution. The proposed method is based on three levels of clustering. An edge BC manager enables local authentication for IoT devices at the edge level. While the second level functions as middleware to cluster the edge devices of the first level. The final level is the cloud layer, which grants authorized users access to IoT devices. The proposed method is assessed using the Hyperledger Fabric platform. Additionally, Tukur et al. [122] investigates the susceptibility of IoT devices to insider attacks, particularly how environmental manipulation impacts data integrity at the perception layer. They aim to protect sensor data from such tampering to guarantee accurate analysis and processing. Their solution involves a framework that uses blockchain and edge computing for data validation and integrity preservation before further processing. The related work of securing IoT networks using blockchain is listed in Table 7.

F. SDN-BASED SOLUTIONS

Other solutions in IoT security literature, such as SDN-based approaches, exist that neither necessitate architectural modifications nor rely on ML and Blockchain. One notable example is presented in [114], which describes the concept of SDN-based security architecture for IoT. The SDN-based architecture in this situation functions with or without the SDN-domain infrastructure. This study outlines the opportunity to provide network security more effectively and flexibly with SDN and shows how the proposed architecture operates. A new IoT system's design was presented along with a discussion of the existing SDN security applications and how to address their problems. In this study, they discussed world-wide traffic monitoring and network access management for ad-hoc networks. Finally, they explore the performance consequences of the architectural design decisions made for SDN utilizing OpenFlow. In this study, they have presented an outline of a new distributed controller SDN-based network architecture. Additionally, our technology applies to ad hoc networks and IoT. First, they introduced a novel architecture with numerous SDN controllers interacting equally. Second, they presented a scalable architecture with numerous SDN domains. Networks with or without infrastructure can exist in each domain, and each controller is only in charge of that domain. Border Controllers are specialized controllers used for cross-domain communication. To ensure each domain's independence in the event of failure, these edge Controllers must engage in a novel type of distributed interaction. With the idea of a grid of security built into each controller to thwart attacks, they adopt an architecture to ensure the security of the entire network.

Moreover, Karmakar et al. [115] present A novel SDN-based approach to secure IoT communication. The proposed method offers both authentications of network access as well as authorization of the traffic in the IoT network to mitigate and prevent malicious devices and cyber attacks. The validation and implementation of the proposed architecture are done on the Open Network Operating System (ONOS) SDN controller and a virtual machine called Raspbian VMs. To demonstrate the performance of the SDN Secure-based architecture various attacks are used. However, this study has drawbacks including unknown attacks that require a costly reconfiguration of the SDN controller.

In the past, perception layer security relied on spread spectrum techniques like frequency hopping to prevent unauthorized interception, but these methods lost effectiveness if compromised. Conversely, quantum cryptography offers theoretically perfect secrecy but faces practical challenges like reduced signal transmission efficiency and the need for weak signals. Additionally, implementing MIMO (Multiple Input Multiple Output) for secure communication, as recent studies suggest, is complex due to the need for numerous antennas on both sides of the connection. These evolving methods highlight the ongoing challenge of balancing security effectiveness and practical implementation in communication technologies. Hence, SDN emerges as a promising method to address this layer of security and privacy concerns. In this direction, Gheisari et al. [123] has introduced a new framework designed to enhance privacy within smart cities. This framework employs clustering methods to segregate smart devices into two categories. Devices marked with a high privacy requirement receive instructions from the network controller to encrypt communications using a predetermined encryption protocol. Conversely, devices not designated for privacy do not activate any encryption features. The authors, however, have not conducted any practical real-world application or simulation studies for this mechanism. In a related effort, authors of [124] have presented another method for improving privacy in urban smart environments. This strategy involves the SDN controller, which bases its operations on the level of data sensitivity and the characteristics of network paths, to determine whether IoT devices should be classified for standard operation or enhanced privacy measures. Devices that require privacy treatment are programmed to divide their sensitive data and transmit it via a Virtual Private Network (VPN) to ensure greater privacy protection. The related works of securing IoT networks using blockchain and SDN are listed in Table 7.

IV. DISCUSSION

The architectural design of IoT systems, which is fundamental to their functionality, is predicated on seamless interoperability and dynamic scalability. Although these systems exhibit robustness in terms of connectivity and

performance, they inadvertently create a convoluted mesh of data pathways, thereby potentially compromising user privacy. As the IoT landscape continues to densify, the architecture must evolve, not only to support the burgeoning network load but also to embed privacy by design, ensuring that user data remains secure through the labyrinth of interconnected devices. In addition, architectural design should be flexible so that it can be used across platforms. Another concern is the challenge of integrating heterogeneous technologies within this architecture, which can be addressed through a standardized, modular strategy, allowing for the streamlined adoption of new devices and services, thereby safeguarding the system's continuity and extensibility. Equally crucial is the management layer, which optimizes the efficiency and efficacy of the IoT system by providing comprehensive monitoring and control capabilities essential for the maintenance and troubleshooting of the network. An additional consideration that is absent from the current scope is the ethical and privacy dimensions associated with IoT deployment. The sensitive nature of data within IoT networks necessitates the integration of stringent security and privacy protocols to preempt breaches and maintain user confidentiality.

Privacy, which is also a crucial aspect of IoT architectural design, emerged as a top priority in IoT systems because the proliferation of IoT devices results in the accumulation of vast amounts of personal data. While convenient and efficient, the transparent nature of IoT networks poses significant risks to personal privacy. The challenge lies in instituting strong data protection protocols that are intrinsic to IoT networks, deterring unauthorized access, and providing users with control over their data. Privacy cannot be an afterthought; rather, it must be an integral part of the IoT architectural framework, imbued at every level to ensure data protection by default and design. IoT devices, owing to their limited resources, require a secure network architecture capable of integrating diverse technologies. The central challenge is maintaining data security and user privacy, given the device constraints and expansive IoT networks. Privacy is particularly vulnerable in applications prone to cyber-attacks, and current security measures are often insufficient. While recent advancements show promise in addressing threats, securing the layered IoT infrastructure, from devices to core networks, against a wide range of attacks remains a critical and ongoing concern. Closely allied with privacy is the issue of trust, an essential element in the acceptance and widespread adoption of IoT technologies. Trust in IoT systems is multifaceted, encompassing not only the trust between devices but also between devices and users. Our study underscores the need for transparent, verifiable mechanisms that can assure users of the security of their data and the reliability of their IoT devices. Building this trust requires a concerted effort to demonstrate consistent and dependable privacy-preserving practices across the IoT spectrum, bolstering user confidence and fostering a secure IoT ecosystem.

Several approaches were discussed in this survey to address both internal and external IoT threats. These include ML-based, blockchain, and SDN-based approaches. ML techniques are often praised for their proficiency in tackling cybersecurity threats in IoT; however, they face challenges such as scalability and the ability to process real-time data effectively. These obstacles are compounded by the extensive and constantly changing nature of IoT systems. The effectiveness of various models, including shallow and deep models, has been tested in real-world situations, revealing their potential for practical applications. Despite their progress, the performance of these models is limited by the challenges posed by IoT contexts and the distinctive attack patterns that target IoT infrastructure.

Blockchain technology presents a promising solution for decentralization, providing innovative ways to ensure privacy and trust without depending on central authorities. Its immutable ledger offers a compelling case for security, which enhances IoT security through encryption, guaranteeing that data on IoT devices remains inaccessible to unauthorized users. It also provides robust authentication and access control along with vulnerability management to prevent attacks. However, various threats to IoT systems using blockchain approaches remain unaddressed. These include direct interference with IoT hardware, the introduction of malware, DDoS attacks, and depletion of device batteries. The efficacy of the interactions between IoT devices and the blockchain network is contingent on the computational capacity and network bandwidth. Data accessibility in IoT could be compromised by exclusive reliance on certain providers, leading to subpar IoT products and restrictions on data exportation. The blockchain landscape lacks a platform that is robust, scalable, and cost-effective for IoT needs, requiring improvements in stability and governance, particularly in major blockchain frameworks such as Bitcoin and Ethereum.

Finally, SDN has been presented as a transformative approach for securing IoT networks, providing comprehensive visibility, and a centralized scheme for detailed operational oversight. However, this centralization inherently introduces a classic vulnerability, that is, a single point of failure, which can be exploited by malicious entities through a spectrum of cyberattacks. The potential for this vulnerability requires a critical review of the robustness of SDNs as a security measure within the IoT infrastructure. Merging the centralized control of SDN with the distributed nature of blockchain provides an integrated solution for securing IoT networks, enhancing operational control, and mitigating the risk of single points of failure. However, integrating SDN and BC is challenging. The harmonization of the centralized architecture of SDN with blockchain-distributed ledgers introduces complexities in achieving seamless, functional convergence. Such integration must address the trade-offs between centralization for efficiency and distribution for security while maintaining the performance and scalability essential for the burgeoning IoT domain.

V. RESEARCH CHALLENGES AND POTENTIAL SOLUTIONS

Because of the nature of IoT applications, developing a secure solution for limited resource-constrained devices is essential and rather difficult. As a result, numerous problems need to be solved. IoT security solutions should concentrate on IoT device requirements and resource shortages. Considering the resource constraints, heterogeneity, and real-time nature of IoT applications, securing these devices is a big challenge. This section highlights several unresolved research questions to help with future work on a countermeasure for cyberattacks in IoT networks. A concise summary of research challenges and potential solutions is listed in Table 8

A. HETEROGENEITY AND RESOURCE-CONSTRAINT

The current IoT security solutions face significant challenges in supporting the billions of distinct interconnected IoT applications, necessitating further research and development about integrating security features in diverse and resource-constrained systems. Moreover, due to the Heterogeneity of IoT devices, trust among nodes is a big issue, especially in the presence of a mobility environment where nodes can connect disjoint or sleep dynamically. One potential solution may be to apply RL which can adapt to the changes in the environment.

B. CONSENT AND ON-DEVICE PROCESSING

In order to effectively tackle the obstacles encountered in the IoT industry, it is imperative to prioritize the establishment of enhanced privacy protocols. A future direction involves the incorporation of dynamic user consent mechanisms, potentially allowing IoT devices to enable users to specify data collection permissions, tailored to particular contexts or uses. This mechanism is poised to offer unparalleled control over data privacy to users, allowing them to determine the circumstances under which their data is accessed. Providing such refined consent mechanisms is anticipated to enhance user trust and confidence in IoT devices, ensuring that data is accessed strictly when it is genuinely needed, thereby aligning with users' privacy expectations and improving overall user experience.

In parallel, enhancing privacy could also involve a paradigm shift toward processing more data directly on the device, utilizing edge computing, rather than relaying it to centralized servers. This method of on-device data processing is instrumental in mitigating data exposure risks, keeping sensitive information localized, and reducing susceptibility to security breaches. By localizing data processing, not only is user information more secure, but data management becomes more efficient, further solidifying user trust and integrity within IoT ecosystems, and maintaining a balance between innovation and user privacy in the academic discourse surrounding IoT development. For instance, FL emerges as a promising technique for on-device learning, aligning with privacy-enhancing strategies by processing data locally while still benefiting from collective insights.

TABLE 8. Challenges and potential solutions.

Challenge	Potential Solution
Heterogeneity and resource constraint	More research on integrating security in diverse systems. RL for Adaptive Security.
Elevating Privacy Standards	Dynamic user consent mechanisms; On-device processing with edge computing (FL).
Trust-Centric IoT Ecosystem	Transparency through operational logs; Global certification programs for devices.
IDS Optimizations and Enhancements	Trials for IDS adaptability; ML and DL optimization for IoT.
Predictive IoT Security Strategies	Proactive security with predictive models based on analytics, ML, and AI.

C. TRUST-CENTRIC IoT ECOSYSTEM: TRANSPARENCY AND CERTIFICATION

Addressing challenges within the IoT ecosystem necessitates future directions that prioritize transparency and trust. One such direction is for manufacturers to provide users with detailed operational logs, ensuring a comprehensive understanding of device functionality and data usage. This foresight in creating a transparent operational environment is pivotal for user confidence, fostering enhanced trust, and promoting more informed and responsible utilization of IoT devices. As users gain clarity on the workings of their devices and data handling, the reliability of IoT technology is likely to be strengthened. In parallel, the evolution of the IoT landscape may witness the inception of rigorous global certification programs. These programs are anticipated to subject IoT devices to stringent security and privacy evaluations. Devices that surpass these meticulous standards could be awarded trust badges, serving as beacons of security and reliability for consumers. The implementation of such certification and recognition systems is expected to guide consumers toward safer and more trustworthy device choices, thereby playing a critical role in shaping a more secure and dependable IoT ecosystem.

D. IDS OPTIMIZATIONS AND ENHANCEMENTS

IDS/IPS techniques are recognized as vital components for enhancing security in the IoT ecosystem, given their adaptability and proven effectiveness in various contexts. Many studies have discussed different IDS techniques, each giving specific security answers to the unique needs of IoT systems. These techniques have a good ability to adapt and spot new kinds of attacks. However, there's a need to show more clearly how well these adaptive features work in real-world situations. There's not enough evidence on how adaptability is applied and evaluated. Thus, more studies and trials are needed to understand these features better and to ensure they work effectively against ever-changing threats.

Moreover, the integration of ML and DL techniques within IDS presents a promising avenue for enhancing IoT security. They can learn and adapt, making them suitable for identifying different types of threats. However, these advanced

methods must be made to suit IoT systems, which usually work on devices with limited resources. These techniques must be not only refined but also optimized for efficiency and scalability to suit the unique needs and resource limitations of IoT systems. Advanced IDS methods, like those based on ML and DL, must be fine-tuned to work well within such constraints. This means developing security solutions that are both effective and efficient, ensuring the safe operation of IoT devices without using too many resources.

Adaptive learning models in IDS can greatly help in dealing with the dynamic nature of threats in IoT environments. These models can learn and adjust to new threats, allowing for early detection and handling of security risks. Integrating such models in IDS can help in creating more robust and flexible security solutions, capable of dealing with new and changing threats effectively. To optimize these IDS methods, there needs to be a balance between accuracy and efficiency. This requires exploring different optimization strategies to improve IDS methods based on ML and DL. The goal is to have these methods work seamlessly within the limitations of IoT environments, ensuring the security of diverse IoT networks without compromising on performance.

E. PREDICTIVE IoT SECURITY STRATEGIES

More broadly, the evolving domain of IoT security is increasingly recognizing the importance of shifting from traditional, reactive security measures to proactive strategies. This transition, essential for predicting and preventing potential threats before they occur, underscores the need for more extensive academic research in the field. The complexity and interconnectedness of IoT devices demand a sophisticated understanding of potential security breaches, which can be significantly addressed through predictive security models. These models, built on the pillars of advanced analytics, ML, and AI, require deep academic investigation to effectively analyze the immense data produced by IoT devices. Academic studies focusing on identifying patterns and anomalies in this data can lead to the development of robust predictive models, enabling pre-emptive identification of vulnerabilities and attack vectors. This proactive approach is crucial not only for enhancing the security of individual devices but also for strengthening the resilience of the broader IoT infrastructure.

Overall, an efficient and Secure IoT solution should guarantee confidentiality, access control, software integrity, and information availability while focusing on the scarcity of IoT resources

VI. CONCLUSION

The importance of IoT has been increasing rapidly in recent years as its impact become more apparent. From small smart home devices to advanced military-grade drones, IoT has become an integral part of our lives. Nevertheless, due to this enormity and heterogeneous nature, many security and privacy challenges were introduced. This survey presented a brief introduction to IoT and its three-layer design that includes physical, network, and application layers. It, then, provided a solid background on cyberattacks that target IoT layers. Then, IoT security requirements such as confidentiality, integrity, authentication, authorization, and availability were evaluated. The state-of-the-art IoT security solutions were investigated, including different architectural designs, ML and DL techniques, Blockchain, and SDN. Finally, some of the main IoT security and privacy challenges and open issues such as the heterogeneity of IoT devices, their constraints, real-time support, and IDS enhancements were highlighted as potential future research directions.

REFERENCES

[1] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020.

[2] N. Mishra and S. Pandya, "Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021.

[3] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-Art review on IoT threats and attacks: Taxonomy, challenges and solutions," *Sustainability*, vol. 13, no. 16, p. 9463, Aug. 2021.

[4] S. Bhardwaj and S. Harit, "SDN-enabled secure IoT architecture development: A review," in *Proc. Inventive Commun. Comput. Technologies ICICCT*, 2021, pp. 599–619.

[5] D. K. Alferidah and N. Z. Jhanjhi, "A review on security and privacy issues and challenges in Internet of Things," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 4, pp. 263–286, 2020.

[6] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.

[7] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020.

[8] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," *ACM Comput. Surveys*, vol. 53, no. 6, pp. 1–37, Nov. 2021.

[9] A. Saxena and S. Mittal, "Internet of Medical Things (IoMT) security and privacy: A survey of recent advances and enabling technologies," in *Proc. 14th Int. Conf. Contemp. Comput.*, Aug. 2022, pp. 550–559.

[10] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020.

[11] J. Zmud, M. Miller, M. Moran, M. Tooley, J. Borowiec, B. Brydia, R. Sen, J. Mariani, E. Krimmel, and A. Gunnels, "A primer to prepare for the connected airport and the Internet of Things," Number Project, Transp. Res. Board (TRB), Washington, DC, USA, Tech. Rep. 01-33, 2018.

[12] D.-L. Yang, F. Liu, and Y.-D. Liang, "A survey of the Internet of Things," in *Proc. 1st Int. Conf. E-Business Intell. (ICEBI)*, Amsterdam, The Netherlands. Atlantis Press, Dec. 2010, pp. 524–532.

[13] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wireless Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, Nov. 2020.

[14] E. Shakshuki, A. A. Elkhail, I. Nemer, M. Adam, and T. Sheltami, "Comparative study on range free localization algorithms," *Proc. Comput. Sci.*, vol. 151, pp. 501–510, 2019.

[15] M. Hammoudeh, G. Epiphaniou, S. Belguith, D. Unal, B. Adebisi, T. Baker, A. S. M. Kayes, and P. Watters, "A service-oriented approach for sensing in the Internet of Things: Intelligent transportation systems and privacy use cases," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15753–15761, Jul. 2021.

[16] I. Nemer, T. Sheltami, E. Shakshuki, A. A. Elkhail, and M. Adam, "Performance evaluation of range-free localization algorithms for wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 25, no. 1, pp. 177–203, Feb. 2021.

[17] S. Nižetić, P. Šolić, D. Lopez-de-Ipiña Gonzalez-De, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *J. Cleaner Prod.*, vol. 274, Nov. 2020, Art. no. 122877.

[18] M. H. Asghar, A. Negi, and N. Mohammadzadeh, "Principle application and vision in Internet of Things (IoT)," in *Proc. Int. Conf. Comput., Commun. Autom.*, May 2015, pp. 427–431.

[19] S. Medileh, A. Laouid, E. M. B. Nagoudi, R. Euler, A. Bounceur, M. Hammoudeh, M. AlShaikh, A. Eleyan, and O. A. Khashan, "A flexible encryption technique for the Internet of Things environment," *Ad Hoc Netw.*, vol. 106, Sep. 2020, Art. no. 102240.

[20] J. Cook, S. U. Rehman, and M. A. Khan, "Security and privacy for low power IoT devices on 5G and beyond networks: Challenges and future directions," *IEEE Access*, vol. 11, pp. 39295–39317, 2023.

[21] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie, and A. Jabban, "Disguised executable files in spear-phishing emails: Detecting the point of entry in advanced persistent threat," in *Proc. 2nd Int. Conf. Future Netw. Distrib. Syst.*, 2018, pp. 1–5.

[22] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology," *Future Gener. Comput. Syst.*, vol. 129, pp. 380–388, Apr. 2022.

[23] I. A. Elgendy, A. Muthanna, M. Hammoudeh, H. Shaiba, D. Unal, and M. Khayyat, "Advanced deep learning for resource allocation and security aware data offloading in industrial mobile edge computing," *Big Data*, vol. 9, no. 4, pp. 265–278, Aug. 2021.

[24] S. Belguith, N. Kaaniche, and M. Hammoudeh, "Analysis of attribute-based cryptographic techniques and their application to protect cloud services," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, pp. e366–7, Mar. 2022.

[25] G. Epiphaniou, P. Pillai, M. Bottarelli, H. Al-Khateeb, M. Hammoudesh, and C. Maple, "Electronic regulation of data sharing and processing using smart ledger technologies for supply-chain security," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1059–1073, Nov. 2020.

[26] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the Internet of Things (CTM-IoT)," in *Proc. 12th Int. Conf. Broad. Wireless Comput. Commun. Appl. (BWCCA)*. Barcelona, Spain: Springer, 2018, pp. 533–543.

[27] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May 2016.

[28] X. Wu and F. Li, "A multi-domain trust management model for supporting RFID applications of IoT," *PLoS ONE*, vol. 12, no. 7, Jul. 2017, Art. no. e0181124.

[29] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A mobile cloud hierarchical trust management protocol for IoT systems," in *Proc. 5th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Apr. 2017, pp. 125–130.

[30] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, and S. Bianchi, "ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.

[31] R. K. Chahal and S. Singh, "Fuzzy rule-based expert system for determining trustworthiness of cloud service providers," *Int. J. Fuzzy Syst.*, vol. 19, no. 2, pp. 338–354, Apr. 2017.

[32] M. F. Hinarejos, F. Almenárez, P. Arias Cabarcos, J. L. Ferrer-Gomila, and A. M. López, "RiskLaine: A probabilistic approach for assessing risk in certificate-based security," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1975–1988, Aug. 2018.

[33] V. Sharma, I. You, R. Kumar, and P. Kim, "Computational offloading for efficient trust management in pervasive online social networks using osmotic computing," *IEEE Access*, vol. 5, pp. 5084–5103, 2017.

[34] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the Internet of Things," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, Aug. 2017, pp. 1–6.

[35] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 163–167.

[36] M. Hammoudeh, R. Newman, C. Dennett, S. Mount, and O. Aldabbas, "Map as a service: A framework for visualising and maximising information return from multi-ModalWireless sensor networks," *Sensors*, vol. 15, no. 9, pp. 22970–23003, Sep. 2015.

[37] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on Internet of Things security: Requirements, challenges, and solutions," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100129.

[38] M. S. A. Muthanna, A. Muthanna, A. Rafiq, M. Hammoudeh, R. Alkanhel, S. Lynch, and A. A. Abd El-Latif, "Deep reinforcement learning based transmission policy enforcement and multi-hop routing in QoS aware LoRA IoT networks," *Comput. Commun.*, vol. 183, pp. 33–50, Feb. 2022.

[39] N. Alhirabi, O. Rana, and C. Perera, "Security and privacy requirements for the Internet of Things: A survey," *ACM Trans. Internet Things*, vol. 2, no. 1, pp. 1–37, Feb. 2021.

[40] A. Assiri and H. Almagwashi, "IoT security and privacy issues," in *Proc. 1st Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Apr. 2018, pp. 1–5.

[41] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020.

[42] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *Proc. Int. Conf. Privacy Secur. Mobile Syst. (PRISMS)*, May 2014, pp. 1–8.

[43] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: A security point of view," *Internet Res.*, vol. 26, no. 2, pp. 337–359, Apr. 2016.

[44] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[45] M. Ghaleb and F. Azzedin, "Towards scalable and efficient architecture for modeling trust in IoT environments," *Sensors*, vol. 21, no. 9, p. 2986, Apr. 2021.

[46] C.-S. Park and H.-M. Nam, "Security architecture and protocols for secure MQTT-SN," *IEEE Access*, vol. 8, pp. 226422–226436, 2020.

[47] L. Alonso, J. Barbarán, J. Chen, M. Díaz, L. Llopis, and B. Rubio, "Middleware and communication technologies for structural health monitoring of critical infrastructures: A survey," *Comput. Standards Interfaces*, vol. 56, pp. 83–100, Feb. 2018.

[48] S. Pulparambil and Y. Baghdadi, "Service oriented architecture maturity models: A systematic literature review," *Comput. Standards Interfaces*, vol. 61, pp. 65–76, Jan. 2019.

[49] A. Carlin, M. Hammoudeh, and O. Aldabbas, "Intrusion detection and countermeasure of virtual cloud systems–state of the art and current challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 6, 2015.

[50] I. T. Abdel-Halim and H. M. Zayan, "Evaluating the performance of lightweight block ciphers for resource-constrained IoT devices," in *Proc. 4th Novel Intell. Lead. Emerg. Sci. Conf. (NILES)*, Oct. 2022, pp. 39–44.

[51] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 129–146, Feb. 2020.

[52] K. Karthikeyan and P. Madhavan, "Building a trust model for secure data sharing (TM-SDS) in edge computing using HMAC techniques," *Comput., Mater. Continua*, vol. 71, no. 3, pp. 4183–4197, 2022.

[53] N. Kammoun, A. B. C. Douss, R. Abassi, and S. G. E. Fatmi, "Ensuring data integrity using digital signature in an IoT environment," in *Proc. 36th Int. Conf. Adv. Inf. Netw. Appl.* Cham, Switzerland: Springer, 2022, pp. 482–491.

[54] M. Conti, P. Kaliyar, and C. Lal, "CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 8, p. e497, Apr. 2019.

[55] T. Ahsan, F. Zeeshan Khan, Z. Iqbal, M. Ahmed, R. Alroobaea, A. M. Baqasah, I. Ali, and M. A. Raza, "IoT devices, user authentication, and data management in a secure, validated manner through the blockchain system," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–13, Feb. 2022.

[56] V. Kumar, N. Malik, J. Singla, N. Z. Jhanjhi, F. Amsaad, and A. Razaque, "Light weight authentication scheme for smart home IoT devices," *Cryptography*, vol. 6, no. 3, p. 37, Jul. 2022.

[57] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A secure and anonymous user authentication scheme for IoT-enabled smart home environments using PUF," *IEEE Access*, vol. 10, pp. 101330–101346, 2022.

[58] G. Yunchuan, H. Zhang, L. Zhang, L. Fang, and F. Li, "Incentive mechanism for cooperative intrusion detection: An evolutionary game approach," in *Proc. Int. Conf. Comput. Sci.*, Wuxi, China. Cham, Switzerland: Springer, 2018, pp. 83–97.

[59] E. Göynügür, S. Bernardini, G. de Mel, K. Talamadupula, and M. Şensoy, "Policy conflict resolution in IoT via planning," in *Proc. Adv. Artif. Intell., 30th Can. Conf. Artif. Intell.*, Edmonton, AB, Canada. Cham, Switzerland: Springer, May 2017, pp. 169–175.

[60] S. Safavi, A. M. Meer, E. Keneth Joel Melanie, and Z. Shukur, "Cyber vulnerabilities on smart healthcare, review and solutions," in *Proc. Cyber Resilience Conf. (CRC)*, Nov. 2018, pp. 1–5.

[61] A. Sood and K. Moidu, "Protection of healthcare information: Adding cyber resilience and recovery," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2018, pp. 132–134.

[62] S. N. G. Aryavalli and H. Kumar, "Top 12 layer-wise security challenges and a secure architectural solution for Internet of Things," *Comput. Electr. Eng.*, vol. 105, Jan. 2023, Art. no. 108487.

[63] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the Internet of Things using RFID: The RFID ecosystem experience," *IEEE Internet Comput.*, vol. 13, no. 3, pp. 48–55, May 2009.

[64] *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11-2012, 2012.

[65] Z Shelby, K Hartke, and C Bormann, *The Constrained Application Protocol (coap)*, document RFC 7252, IETF, 2014.

[66] I. Fette and A. Melnikov, "The websocket protocol," Internet Eng. Task Force (IETF), Reston, VA, USA, Tech. Rep. RFC 6455, 2011.

[67] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A survey on standards for interoperability and security in the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1020–1047, 2nd Quart., 2021.

[68] F. Thiesse, C. Floerkemeier, M. Harrison, F. Michahelles, and C. Roduner, "Technology, standards, and real-world deployments of the EPC network," *IEEE Internet Comput.*, vol. 13, no. 2, pp. 36–43, Mar. 2009.

[69] V. R. Konduru and M. R. Bharamagoudra, "Challenges and solutions of interoperability on IoT: How far have we come in resolving the IoT interoperability issues," in *Proc. Int. Conf. Smart Technol. For Smart Nation (SmartTechCon)*, Aug. 2017, pp. 572–576.

[70] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: New interoperability, management and security challenges," 2016, *arXiv:1604.04824*.

[71] A. Karpenko, T. Kinnunen, M. Madhikermi, J. Robert, K. Främling, B. Dave, and A. Nurminen, "Data exchange interoperability in IoT ecosystem for smart parking and EV charging," *Sensors*, vol. 18, no. 12, p. 4404, Dec. 2018.

[72] A. Javed, A. Malhi, T. Kinnunen, and K. Främling, "Scalable IoT platform for heterogeneous devices in smart environments," *IEEE Access*, vol. 8, pp. 211973–211985, 2020.

[73] Y. Mesmoudi, M. Lamnaour, Y. El Khamlichi, A. Tahiri, A. Touhafi, and A. Braeken, "A middleware based on service oriented architecture for heterogeneity issues within the Internet of Things (MSOAH-IoT)," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 32, no. 10, pp. 1108–1116, Dec. 2020.

[74] L. Sun, Y. Li, and R. A. Memon, "An open IoT framework based on microservices architecture," *China Commun.*, vol. 14, no. 2, pp. 154–162, Feb. 2017.

[75] M. Hammoudeh and R. Newman, "Information extraction from sensor networks using the watershed transform algorithm," *Inf. Fusion*, vol. 22, pp. 39–49, Mar. 2015.

[76] C. Lai, F. Boi, A. Buschettu, and R. Caboni, "IoT and microservice architecture for multimobility in a smart city," in *Proc. 7th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2019, pp. 238–242.

[77] A. de M. Del Esposte, E. F. Z. Santana, L. Kanashiro, F. M. Costa, K. R. Braghetto, N. Lago, and F. Kon, "Design and evaluation of a scalable smart city software platform with large-scale simulations," *Future Gener. Comput. Syst.*, vol. 93, pp. 427–441, Apr. 2019.

[78] T. Cerny, "Aspect-oriented challenges in system integration with microservices, SOA and IoT," *Enterprise Inf. Syst.*, vol. 13, no. 4, pp. 467–489, Apr. 2019.

[79] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[80] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Tallinn, Estonia: Springer, 2011, pp. 69–88.

[81] M. A. Orumiehchiha, J. Pieprzyk, and R. Steinfeld, "Cryptanalysis of WG-7: A lightweight stream cipher," *Cryptography Commun.*, vol. 4, nos. 3–4, pp. 277–285, Dec. 2012.

[82] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *J. Cryptograph. Eng.*, vol. 8, no. 2, pp. 141–184, Jun. 2018.

[83] L. A. Tawalbeh and T. F. Somani, "More secure Internet of Things using robust encryption algorithms against side channel attacks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.

[84] F. Zhang, S. Guo, X. Zhao, T. Wang, J. Yang, F.-X. Standaert, and D. Gu, "A framework for the analysis and evaluation of algebraic fault attacks on lightweight block ciphers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1039–1054, May 2016.

[85] S. Zou, Q. Cao, C. Wang, Z. Huang, and G. Xu, "A robust two-factor user authentication scheme-based ECC for smart home in IoT," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4938–4949, Sep. 2022.

[86] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33, 2017.

[87] D. Rani, N. S. Gill, P. Gulia, and J. M. Chatterjee, "An ensemble-based multiclass classifier for intrusion detection using Internet of Things," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–16, May 2022.

[88] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A BLockchain-enabled decentralized capability-based access control for IoTs," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1027–1034.

[89] J. Zhang, L. Li, G. Lin, D. Fang, Y. Tai, and J. Huang, "Cyber resilience in healthcare digital twin on lung cancer," *IEEE Access*, vol. 8, pp. 201900–201913, 2020.

[90] J. Rajamäki, J. Nevmerzhitskaya, and C. Virág, "Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2018, pp. 2042–2046.

[91] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Trans. Netw. Service Manage.*, vol. 16, no. 3, pp. 924–935, Sep. 2019.

[92] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021.

[93] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107810.

[94] I. Ullah and Q. H. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," *IEEE Access*, vol. 10, pp. 62722–62750, 2022.

[95] M. Baz, "SEHIDS: Self evolving host-based intrusion detection system for IoT networks," *Sensors*, vol. 22, no. 17, p. 6505, Aug. 2022.

[96] C. Huang, S. Chen, Y. Zhang, W. Zhou, J. J. P. C. Rodrigues, and V. H. C. de Albuquerque, "A robust approach for privacy data protection: IoT security assurance using generative adversarial imitation learning," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17089–17097, Sep. 2022.

[97] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, S. Wibowo, S. Gordon, and G. Fortino, "Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications," *Comput. Secur.*, vol. 120, Sep. 2022, Art. no. 102783.

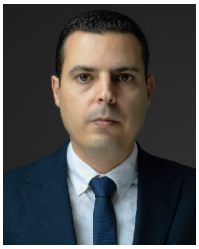
[98] S. Sivarajan and S. D. Sundarsingh Jebaseelan, "Efficient adaptive deep neural network model for securing demand side management in IoT enabled smart grid," *Renew. Energy Focus*, vol. 42, pp. 277–284, Sep. 2022.

[99] S. Cakir, S. Toklu, and N. Yalcin, "RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning," *IEEE Access*, vol. 8, pp. 183678–183689, 2020.

[100] S. Nayak, N. Ahmed, and S. Misra, "Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things," *Ad Hoc Netw.*, vol. 123, Dec. 2021, Art. no. 102661.

[101] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, p. 39, 2018.
[102] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, "Cyberattacks detection in IoT-based smart city applications using machine learning techniques," *Int. J. Environ. Res. Public Health*, vol. 17, no. 24, p. 9347, Dec. 2020.
[103] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," *Appl. Sci.*, vol. 11, no. 18, p. 8383, Sep. 2021.
[104] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*.
[105] N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. Lira Neto, and V. H. C. de Albuquerque, "Industrial Internet-of-Things security enhanced with deep learning approaches for smart cities," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6393–6405, Apr. 2021.
[106] S. A. Parah, J. A. Kaw, P. Bellavista, N. A. Loan, G. M. Bhat, K. Muhammad, and V. H. C. de Albuquerque, "Efficient security and authentication for edge-based Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15652–15662, Nov. 2021.
[107] M. Fahim and A. Sillitti, "Anomaly detection, analysis and prediction techniques in IoT environment: A systematic literature review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019.
[108] S. Bulusu, B. Kailkhura, B. Li, P. K. Varshney, and D. Song, "Anomalous example detection in deep learning: A survey," *IEEE Access*, vol. 8, pp. 132330–132347, 2020.
[109] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
[110] T. Alam, "Blockchain and its role in the Internet of Things (IoT)," 2019, *arXiv:1902.09779*.
[111] T. Faika, T. Kim, J. Ochoa, M. Khan, S.-W. Park, and C. S. Leung, "A blockchain-based Internet of Things (IoT) network for security-enhanced wireless battery management systems," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, Sep. 2019, pp. 1–6.
[112] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[113] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, Jan. 2021.
[114] A. M. C. Souza and J. R. A. Amazonas, "An outlier detect algorithm using big data processing and Internet of Things architecture," *Proc. Comput. Sci.*, vol. 52, pp. 1010–1015, 2015.
[115] K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, "SDN-enabled secure IoT architecture," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6549–6564, Apr. 2021.
[116] K. C. Ravikumar, P. Chiranjeevi, N. M. Devarajan, C. Kaur, and A. I. Taloba, "Challenges in Internet of Things towards the security using deep learning techniques," *Measurement: Sensors*, vol. 24, Dec. 2022, Art. no. 100473.
[117] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022.
[118] G. Pattewar, N. Mahamuni, H. Nikam, O. Loka, and R. Patil, "Management of IoT devices security using blockchain," in *Proc. Sentimental Anal. Deep Learning ICSADL*, 2021, pp. 735–743.
[119] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, "Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions," *Electronics*, vol. 11, no. 4, p. 630, Feb. 2022.
[120] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, Aug. 2022.
[121] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem, A. Basuhail, and M. Yamin, "Hierarchical blockchain-based multi-chaincode access control for securing IoT systems," *Electronics*, vol. 11, no. 5, p. 711, Feb. 2022.
[122] 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.
[123] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101470.
[124] R. Vilalta, R. Ciungu, A. Mayoral, R. Casellas, R. Martinez, D. Pubill, J. Serra, R. Munoz, and C. Verikoukis, "Improving security in Internet of Things with software defined networking," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

MUMIN ADAM received the B.Sc. degree in computer science and engineering from Hodeidah University, Yemen, in 2014, and the M.Sc. degree in computer engineering from the King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2020, where he is currently pursuing the Ph.D. degree with the Computer Engineering Department. His research interests include the Internet of Things (IoT), wireless sensor networks (WSN), FL-enabled IoT, the IoT security, and AI applications in cybersecurity.



MOHAMMAD HAMMOUDEH (Senior Member, IEEE) received the B.Sc. degree in computer communications from Arts Sciences and Technology University, in 2004, the M.Sc. degree in advanced distributed systems from the University of Leicester, in 2006, and the Ph.D. degree in computer science from the University of Wolverhampton, in 2008. He is currently a Saudi Aramco Chair Professor of cybersecurity with the King Fahd University of Petroleum and Minerals. His research interests include the applications of zero trust security to internet-connected critical national infrastructures, blockchains, and other complex highly decentralized systems.

RANA ALRAWASHDEH received the B.Sc. degree in computer science from Albalqa Applied University, Jordan, in 2009, and the M.Sc. degree from Jordan University of Science and Technology, Jordan, in 2019. She is currently pursuing the Ph.D. degree with the Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Saudi Arabia. Her research interests include machine learning and data mining.

BASIL ALSULAIMY received the B.Sc. degree in computer science and information security from the Royal Holloway, University of London, in 2020. He is currently pursuing the M.Sc. degree in computer science specializing in information assurance and security with the King Fahd University of Petroleum and Minerals. With years of experience at Aramco, he is a Cybersecurity Expert at Saudi Aramco and excels in the development of cybersecurity solutions, blockchain, red teaming, and incident response. His research interests include enhancing cybersecurity frameworks, safeguarding critical energy systems and vital industrial infrastructures, and AI implementation in cybersecurity.