IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 January 2024, accepted 9 February 2024, date of publication 13 February 2024, date of current version 22 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3365634

SURVEY

Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey

MAMOONA HUMAYUN[1], NOSHINA TARIQ[2], MAJED ALFAYAD[1], MUHAMMAD ZAKWAN[2], GHADAH ALWAKID[3], AND MOHAMMED ASSIRI[4]

[1]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia
[2]Department of Avionics Engineering, Air University, Islamabad 44000, Pakistan
[3]Department of Computer Sciences, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia
[4]Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, P.O. BOX 16273, Al-Kharj 3963, Saudi Arabia

Corresponding author: Mamoona Humayun (mahumayun@ju.edu.sa)

This work was funded by the Deanship of Scientific Research at Jouf University.

ABSTRACT The Internet of Things (IoT) has revolutionized various domains, enabling interconnected devices to communicate and exchange data. The integration of Artificial Intelligence (AI) in IoT systems further enhances their capabilities and potential benefits. Unfortunately, in the era of AI, ensuring the privacy and security of the IoT faces novel and specific challenges. IoT security is imperative, necessitating comprehensive strategies, including comprehension of IoT security challenges, implementation of AI methodologies, adoption of resilient security frameworks, and handling of privacy and ethical concerns to construct dependable and secure IoT systems. It is vital to note that the term 'security' encompasses a more comprehensive view than cyberattacks alone. Therefore, with an emphasis on securing against cyberattacks, this comprehensive survey also includes physical security threats on the IoT. It investigates the complexities and solutions for IoT systems, placing particular emphasis on AI-based security techniques. The paper undertakes a categorization of the challenges associated with ensuring IoT security, investigates the utilization of AI in IoT security, presents security frameworks and strategies, underscores privacy and ethical considerations, and provides insights derived from practical case studies. Furthermore, the survey sheds light on emerging trends concerning IoT security in the AI era. This survey provides significant contributions to the understanding of establishing dependable and secure IoT systems through an exhaustive examination of the present condition of IoT security and the ramifications of AI on it.

INDEX TERMS Artificial intelligence, cyberattack, Internet of Things, privacy, security.

I. INTRODUCTION

The Internet of Things (IoT) has witnessed exponential growth in recent years, transforming various sectors such as healthcare, transportation, manufacturing, and smart cities [1]. It refers to a network of interconnected devices that collect, exchange, and analyze data to facilitate automation, improve efficiency, and enhance decision-making processes. However, the rapid proliferation of IoT devices has also exposed significant security vulnerabilities, making IoT systems attractive targets for cybercriminals [2]. The integration of Artificial Intelligence (AI) techniques in IoT systems has emerged as a promising approach to address these security challenges and safeguard the IoT ecosystem. The integration of AI and IoT brings together two transformative technologies that complement each other's capabilities [3], [4]. AI techniques, such as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP), enable IoT systems to analyze vast amounts of data, derive insights, and make intelligent decisions. These techniques empower IoT systems to adapt to dynamic environments, detect anomalies, and automate security operations against cyberattacks. By leveraging AI, IoT systems can enhance cyberattacks detection, secure communication, and protect data privacy, ultimately creating a more robust and resilient IoT ecosystem [5]. The numerical values depicted on the

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

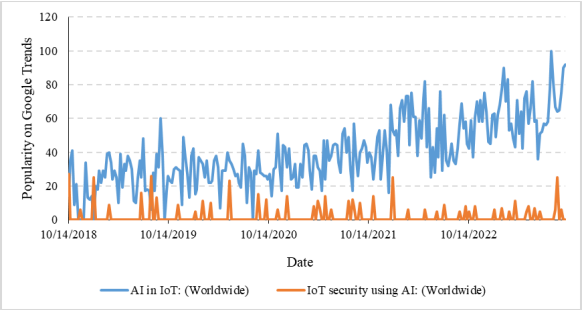

FIGURE 1. Trends in AI-based IoT Research.

chart (in Fig. 1) represent the degree of search interest relative to the peak point attained within a timeframe of the last five years from 2018 to the present. A value of 100 indicates the maximum level of popularity. However, a zero value indicates that an inadequate amount of data is accessible for that particular phrase.

Many industries have gained substantially from the increased automation, efficiency, network optimization, resource allocation, and decision-making capabilities due to the wide adoption of AI in IoT. For instance, AI has a particularly large influence on optimizing throughput in mobile wireless-powered IoT networks. It has played a crucial role in solving difficult problems with energy management and network efficiency. There is potential for significant improvements in network performance via AI-driven algorithms for throughput maximization, controlling data transfer, and improving energy utilization [6]. In addition, the throughput maximization in wireless-powered communication networks demonstrates how AI may improve the operational efficiency of IoT systems by tackling complex optimization challenges like the double near-far effect [7]. However, securing IoT in the AI era presents unique challenges that must be addressed. The diverse and distributed nature of IoT deployments, coupled with resource-constrained devices like wireless-powered networks, introduces complexities in implementing effective security measures [8].

Moreover, AI techniques themselves can be vulnerable to adversarial attacks, raising concerns about the reliability and integrity of AI-enabled security solutions. Therefore, it is crucial to comprehensively explore the intersection of IoT and AI security, identify the challenges and opportunities, and develop strategies to ensure the security and trustworthiness of IoT systems. This survey aims to provide a systematic analysis of the security landscape in the context of IoT systems empowered by AI techniques. It categorizes IoT security challenges into device-level, network-level, data-level, and privacy-related challenges. These challenges encompass aspects such as physical security [9], firmware vulnerabilities [10], secure communication protocols [11], and privacy protection [12]. Understanding these challenges is the foundation for developing effective security solutions that mitigate risks and protect IoT deployments.

AI techniques play a pivotal role in enhancing IoT security. Therefore, it is inevitable to explore the application of AI in addressing IoT security [13], [14], [15] challenges. This paper categorizes AI techniques into cyberattacks and threat detection and prevention, secure communication and authentication, and predictive security analytics. These techniques encompass anomaly detection, behavioral analysis, cryptographic mechanisms, authentication algorithms, and predictive maintenance models. Exploring these AI techniques helps understand their potential to fortify the security posture of IoT systems. Building on the understanding of IoT security challenges and AI techniques, this survey examines security frameworks and approaches tailored for IoT environments. It explores defense-in-depth architectures, secure software development practices, and secure data management strategies. These frameworks encompass layered security mechanisms, secure coding practices, secure firmware updates, data classification, access control, and secure data storage and processing. By adopting these frameworks, organizations can establish a holistic and resilient security infrastructure for their IoT deployments.

Privacy and ethical considerations are vital components of IoT security. Thus, this paper discusses privacy challenges associated with IoT data collection and processing, consent management, and privacy-preserving techniques. Additionally, it addresses the ethical use of AI in IoT security, including transparency, fairness, and accountability. Integration of privacy and ethical considerations into IoT systems can foster user trust and ensure responsible deployment of AI-enabled IoT security solutions. To provide practical insights, we present real-world case studies and use cases that highlight the application of AI in securing IoT systems. These case studies span diverse domains, such as healthcare, smart homes, and industrial IoT. These examples provide a deeper understanding of the real-world impact of AI-enabled security solutions and their effectiveness in mitigating IoT security risks. Finally, it identifies future research directions and emerging trends in securing IoT in the AI era. It also discusses advancements in AI for IoT security, including federated learning, edge AI, and self-defending IoT systems. Additionally, it highlights standardization and regulatory efforts aimed at establishing industry standards, legal frameworks, and interoperability for secure IoT deployments.

II. CONTRIBUTIONS OF THE SURVEY

This survey is a valuable resource for researchers, practitioners, and decision-makers in the field of AI and IoT security, guiding future research and fostering innovation in securing the interconnected IoT world. This exhaustive survey makes a number of significant contributions to the field:

- It classifies and analyzes the most significant security challenges encountered by IoT systems, such as device-level vulnerabilities, network security threats, data security concerns, and concerns regarding privacy.

- It discusses AI techniques that can improve the security of IoT systems, such as cyberattacks and threat detection and prevention algorithms, secure communication and authentication mechanisms, and predictive security analytics.
- It details various security frameworks and approaches that are tailored for IoT environments, including defense-in-depth architectures, secure software development practices, and secure data management strategies, especially, against cyberattacks.
- It addresses the privacy challenges associated with IoT data collection and processing, as well as the ethical use of AI in IoT security.
- It presents real-world case studies and use cases that demonstrate the application of AI in securing IoT systems across diverse domains, including healthcare, smart homes, and industrial IoT.
- It identifies future and emerging trends in securing IoT in the era of AI, such as federated learning, edge AI, and self-defending IoT systems. Additionally, it discusses standardization and regulatory efforts aimed at establishing industry standards and legal frameworks for secure IoT deployments.

A. MAIN CONTENTS OF THE PAPER

This paper proposes a taxonomy of this survey and a comparison with related surveys in Sections II-B and II-C. The significance of this survey is provided in Section III. Section IV discusses the security challenges of IoT. Section V highlights the AI techniques used for IoT security. IoT security frameworks and approaches are provided in Section VI. Privacy and ethical considerations in IoT are discussed in Section VII. Section VIII presents real-world case studies and use cases. In Section IX, future directions and research challenges are delineated, and the conclusion is drawn in Section X.

B. THE PROPOSED TAXONOMY OF THE SURVEY

The taxonomy shown in Fig. 2 derived from the sections on "Case Studies and Use Cases" categorizes AI applications in securing IoT systems into two main branches: "Industry-specific use cases" and "Real-world deployment scenarios." Under "Industry-specific use cases," it explores how AI enhances security in healthcare IoT, smart home systems, and industrial IoT. Meanwhile, the "Real-world deployment scenarios" branch showcases AI's practicality in securing smart cities, connected vehicles, and agricultural IoT. This taxonomy helps organizations understand diverse applications of AI in IoT security, from protecting patient data to securing smart city infrastructure, providing a comprehensive framework for exploring tailored security solutions across various domains.

C. RELATED SURVEYS

The comparative analysis between this survey and state-of-the-art surveys is presented in Table 1. It quantified

TABLE 1. Comparison of state-of-the-art cybersecurity approaches.

Ref.	Threat Detection and Prevention	Secure Communication and Authentication	Security Challenges	Predictive Security Analytics	Security Frameworks	Privacy and Ethical Considerations	Case Studies and Use Cases	Future Directions and Research Challenges
This survey	✓	✓	✓	✓	✓	✓	✓	✓
[16]	×	✓	✓	×	×	×	×	✓
[17]	✓	✓	✓	×	×	✓	×	✓
[18]	✓	×	×	×	✓	✓	×	✓
[19]	✓	×	✓	×	✓	×	×	×
[20]	✓	✓	✓	✓	×	×	×	✓
[21]	×	✓	✓	×	✓	×	×	✓
[22]	✓	×	✓	×	×	✓	×	✓

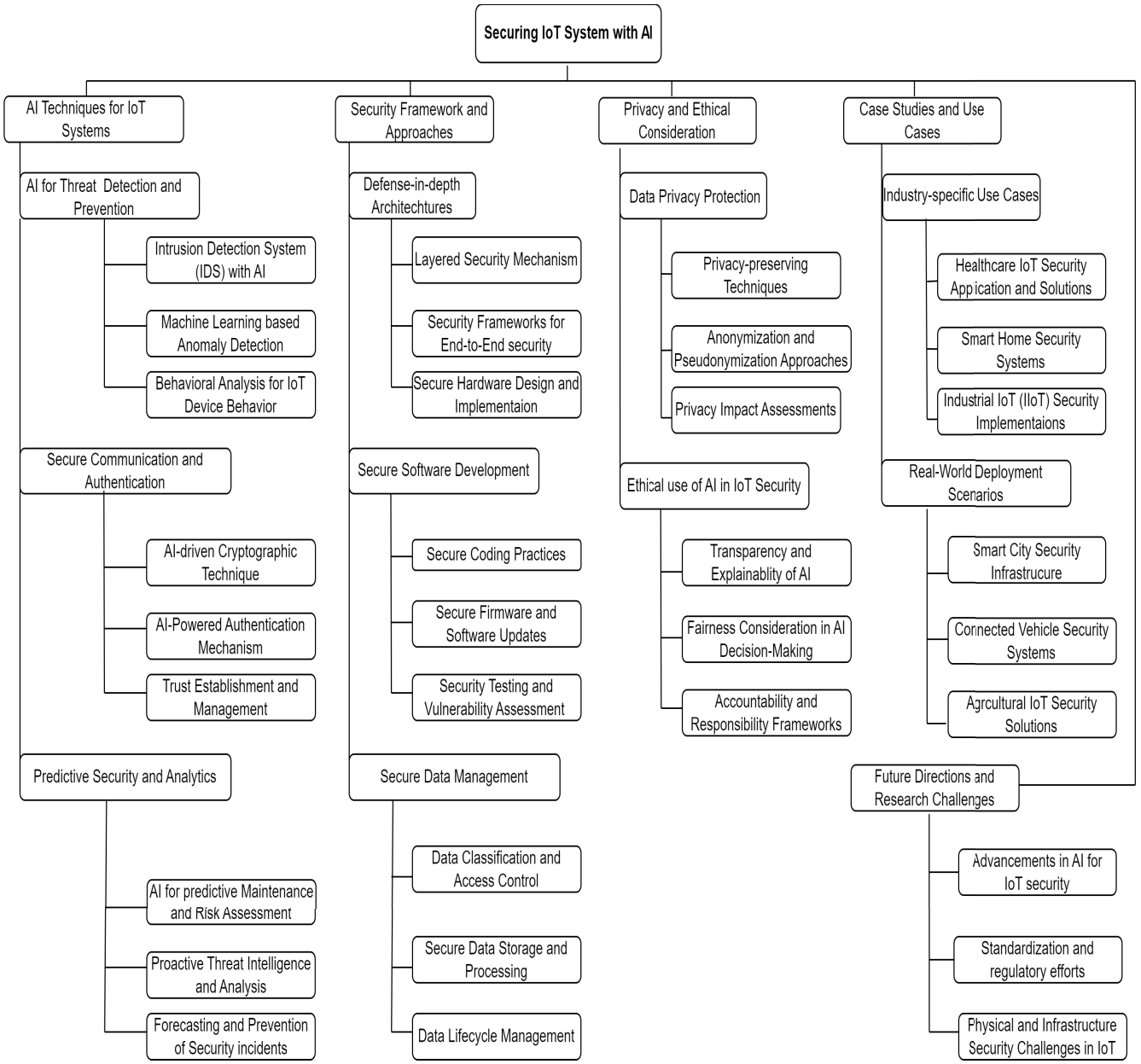

FIGURE 2. The Proposed Taxonomy of IoT system with AI.

each surveyed reference according to the key aspects of IoT cybersecurity. The results highlight the comprehensive nature of this survey, achieving a perfect 100% coverage across all aspects, indicating a thorough exploration of IoT cybersecurity topics. In contrast, the state-of-the-art surveys exhibit varying levels of coverage, ranging from 25% to 62.5%. While some references excel in specific areas, such as secure communication or specific security challenges, our survey stands out as the most comprehensive resource, reflecting a well-rounded approach that encompasses a wide spectrum of aspects. It offers readers a holistic understanding of IoT cybersecurity and the role of AI.

III. SIGNIFICANCE OF THE SURVEY

This survey on securing IoT in the era of AI is of significant importance due to the rapid growth and adoption of IoT devices in various domains. As AI continues to play a crucial role in enhancing IoT capabilities, it is essential to understand the security challenges and potential solutions. By providing a comprehensive analysis of IoT security challenges, AI techniques, security frameworks, privacy considerations, and real-world case studies, this survey contributes to the body of knowledge in securing IoT systems and guides future research and industry practices.

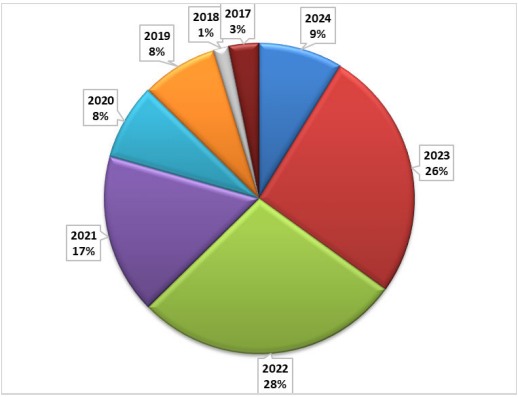

FIGURE 3. Trends in IoT Security and AI Research.

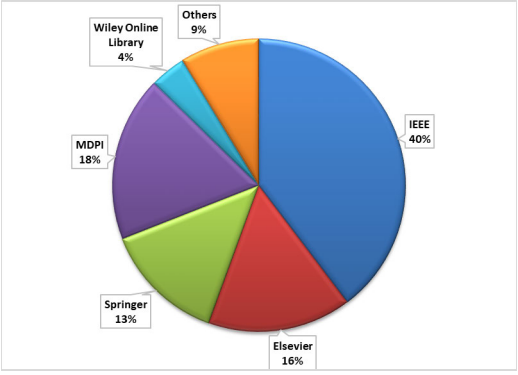

FIGURE 4. Publisher Distribution of Appearances in IoT Security and AI Research.

A. DATA ANALYSIS AND KEY METRICS

This section delves into the statistical analysis of our research findings, identifying significant metrics and insights gained from our dataset. The number of references in Fig. 3 indicates that research in the fields of IoT security and AI has grown significantly in recent years. The chart depicts the growing interest and focus on IoT security and AI integration, demonstrating the dynamic landscape of research and development in this subject.

As part of our comprehensive analysis, we also looked at the distribution of research publications in the field of IoT security and AI across different publishers. Fig. 4 summarizes the publisher distribution and proportion of appearances in our research collection. This distribution emphasizes substantial contributions from IEEE, MDPI, Springer, Elsevier, Wiley Online Library,and other publishers, demonstrating the diversity of research sources in this sector.

Table 2 gives a complete keyword analysis of the IoT security and AI research landscape, identifying the most prominent terms and their patterns. It depicts the incidence, frequency, and trend of significant phrases in the study literature. As demonstrated, terms such as 'Internet of Things,' 'Security,' 'Blockchain,' and 'Artificial Intelligence' are among the most often mentioned keywords, with clear increase trends over time. This co-occurrence analysis illuminates the interconnection of these terms, emphasizing their significance and impact in the area.

B. TOP 10 MUST-READ PAPERS

Some academic publications have made notable contributions and provided valuable insights into the ever-changing area of IoT security. In the context of Generative AI (GenAI) and AI, the following table lists the top ten publications that have significantly influenced the discussion around the security of the IoT. Our selection process for these articles was focused on their originality, influence, and capacity to provide light on the state of the art and potential future developments in IoT security. They consist of significant investigations that conform to the most recent IEEE and other industry standards. These surveys provide the groundwork and research at the cutting edge of GenAI's application to cybersecurity. Each work addresses the complicated issues of protecting IoT systems and provides distinct viewpoints and answers. Therefore, they serve as essential resources for scholars and professionals working in this field and are pretty instructive. A summary of these 10 papers is provided in Table 3.

IV. IoT SECURITY CHALLENGES

Securing IoT systems poses unique challenges that need to be addressed to ensure the integrity, confidentiality, and availability of IoT services [32], [33]. This survey paper categorizes these challenges into several dimensions:

A. DEVICE-LEVEL SECURITY CHALLENGES

Device-level security challenges encompass a range of vulnerabilities and risks associated with individual IoT devices. These challenges must be addressed to ensure the overall security and integrity [34] of the IoT system. Key considerations in device-level security include:

- Physical security of IoT devices: Protecting IoT devices from physical tampering, theft, and unauthorized access is paramount. Physical security measures may include secure enclosures, tamper-evident seals, or physical locks to prevent unauthorized physical access to devices. By safeguarding the physical integrity of devices, the system can maintain the confidentiality and availability of data and prevent malicious manipulation or extraction of sensitive information [35], [36].
- Firmware and software vulnerabilities: IoT devices often rely on firmware and software to function properly and execute their intended tasks. However, these software components can contain vulnerabilities that malicious actors may exploit. Identifying and mitigating firmware and software vulnerabilities through regular security assessments, code reviews, and patch management processes is crucial [37]. Promptly applying security patches and updates released by device manufacturers can help address known vulnerabilities and ensure that devices are protected against potential attacks.

TABLE 2. Keyword analysis and trends.

Keyword	Frequency	Trend	Co-Occurrence
Internet of Things	48	Increasing	IoT Security, AI, Blockchain
Security	38	Stable	Blockchain, Privacy, AI
Blockchain	22	Increasing	IoT Security, AI, Cryptography
Artificial Intelligence	39	Increasing	IoT Security, Blockchain, ML
Privacy	20	Stable	Security, IoT, Data Protection
Machine Learning	19	Increasing	IoT Security, AI, Predictive Analytics
Data Protection	15	Stable	Privacy, Security, Compliance
Cryptography	16	Stable	Blockchain, Security, Encryption
Predictive Analytics	12	Increasing	IoT Security, AI, ML

- Authentication and access control mechanisms: Robust authentication and access control mechanisms are essential to prevent unauthorized access to IoT devices [38]. It is crucial to implement strong authentication protocols, such as two-Factor Authentication (2FA) [39] or biometric authentication [40], to ensure that only authorized entities can access and interact with the devices. Access control mechanisms [41], such as Role-Based Access Control (RBAC) [42], or Attribute-Based Access Control (ABAC) [43], can be implemented to regulate the level of access granted to different users or entities based on their roles or attributes. These mechanisms help prevent unauthorized configuration changes, data breaches, or unauthorized device control by malicious actors.

By addressing these device-level security challenges, organizations can significantly enhance the security of IoT devices, reducing the risk of unauthorized access, data breaches, cyberattacks, and physical tampering. Implementing physical security measures, ensuring the integrity of firmware and software, and deploying robust authentication and access control mechanisms form the foundation for securing IoT devices in the AI era.

B. NETWORK SECURITY CHALLENGES

Network security challenges in the context of IoT deployments revolve around ensuring a secure and reliable communication infrastructure that connects IoT devices and enables data exchange. These challenges need to be addressed to protect against unauthorized data access, data tempering, and maintaining the privacy and integrity of transmitted data. Key considerations for network security in IoT include:

- Secure communication protocols for IoT devices: Implementing secure communication protocols, such as Transport Layer Security (TLS) [44] or Datagram Transport Layer Security (DTLS) [23], is crucial to ensure the confidentiality, integrity, and authenticity of data transmitted between IoT devices and backend systems. These protocols employ encryption and digital certificates to establish secure communication channels, preventing unauthorized eavesdropping, tampering, or impersonation.
- Vulnerabilities in the network infrastructure: The network infrastructure supporting IoT deployments, including routers, gateways, and access points, can be vulnerable to various cyberattacks [24]. Identifying and addressing vulnerabilities in the network infrastructure is essential to prevent unauthorized access and data breaches. Regular security assessments, firmware updates, and applying best practices for securing network devices help protect against known vulnerabilities and ensure a resilient network infrastructure.
- Protection against Denial of Service (DoS) attacks: DoS attacks can disrupt IoT services by overwhelming network resources and rendering them unavailable to legitimate users [45]. Implementing mechanisms to detect and mitigate DoS attacks is crucial to ensure the availability and reliability of IoT services. These mechanisms may include network traffic monitoring, anomaly detection algorithms, rate limiting, or traffic filtering to identify and mitigate malicious traffic or excessive resource consumption.

Addressing these network security challenges is vital to establishing a robust and secure communication infrastructure for IoT deployments. By implementing secure communication protocols, ensuring the integrity of network infrastructure, and protecting against DoS attacks, organizations can mitigate risks associated with unauthorized access, data breaches, and service disruptions. Securing the network infrastructure

TABLE 3. Top 10 must-read papers in IoT security.

Ref.	Contribution and Significance
[5]	A survey highlighting the integration of AI and IoT with 5G, pivotal for smart grid development.
[23]	Presents advancements in IIoT communications, emphasizing efficiency and security.
[24]	Provides foundational understanding of IoT architectures, essential for IoT security.
[25]	Discusses behavior-based attack recognition in industrial control systems within IoT.
[26]	Addresses the critical area of firmware updates for IoT devices.
[27]	Surveys collaborative data-access enablers in IIoT, vital for secure and efficient data handling.
[28]	A forward-looking survey that discusses the role of machine learning and GenAI in IoT security.
[29]	Evaluates cyber threats in Industrial IoT and discusses the relevant standards.
[30]	Aligns industrial standards with reference architectures, key for IoT security standardization.
[31]	Highlights the relationship between GenAI and cybersecurity, reflecting the latest trends in the field.

enhances the overall security posture of IoT systems and safeguards the privacy and integrity of transmitted data.

C. DATA SECURITY CHALLENGES

Data security challenges in IoT systems revolve around ensuring the confidentiality, integrity, and privacy of IoT data. Given the sensitive nature of the data collected and transmitted by IoT devices, robust data security measures are essential. Key considerations for data security in IoT include:

- Data confidentiality and encryption techniques: IoT data often contain sensitive information that needs to be protected from unauthorized access. Employing encryption techniques, such as Advanced Encryption Standard (AES) [46] or Elliptic Curve Cryptography (ECC) [47], ensures that IoT data remains confidential and unreadable by unauthorized entities. Encryption techniques convert the data into an encrypted format that can only be deciphered with the appropriate decryption key, mitigating the risk of data exposure.
- Data integrity and prevention of tampering: Ensuring the integrity of IoT data is crucial to maintaining its accuracy and trustworthiness. Implementing techniques such as digital signatures [48] or hash functions [49] helps verify the integrity of IoT data and detect any unauthorized modifications. Digital signatures provide a way to validate the authenticity and integrity of data by using cryptographic techniques to bind the data to the identity of the sender, ensuring that it has not been tampered with during transmission or storage.
- Secure storage and transmission of IoT data: Protecting the storage and transmission of IoT data is vital to prevent unauthorized access or interception. Utilizing secure storage mechanisms, such as encrypted databases or Hardware Security Modules (HSMs), ensures that IoT data remains protected at rest. Encrypted communication channels, such as secure protocols (e.g., HTTPS or MQTT with TLS) [44], [50], establish secure end-to-end communication between IoT devices and backend systems, preventing unauthorized entities from eavesdropping or tampering with the data during transmission.

By addressing these data security challenges, organizations can maintain the confidentiality, integrity, and privacy of IoT data. Implementing encryption techniques, ensuring data integrity through digital signatures or hash functions, and securing data storage and transmission mechanisms provide a robust foundation for protecting sensitive IoT data. These measures mitigate the risk of unauthorized access, data breaches, tampering, and interception, ensuring that IoT data remains secure throughout its life cycle.

D. PRIVACY CHALLENGES

Privacy challenges in IoT systems revolve around addressing concerns related to data collection, processing, and user consent. Protecting user privacy is crucial to ensure trust, compliance with regulations, and respect for individual preferences. Key considerations for privacy in IoT include:

- Protection of user privacy in IoT data collection and processing: IoT systems collect vast amounts of data, including personal and sensitive information. Protecting user privacy while enabling valuable data analysis is essential. Implementing privacy-enhancing technologies, such as differential privacy [51] or data anonymization techniques [52], helps protect user privacy by minimizing the risk of reidentification and unauthorized tracking. These techniques introduce noise or anonymize data to provide aggregate insights without compromising individual privacy.
- Consent management and data ownership: Obtaining user consent and clarifying data ownership rights are crucial aspects of privacy in IoT systems. Establishing transparent mechanisms for obtaining informed and granular consent ensures that users have control over the collection, use, and sharing of their data. Clearly defining data ownership rights and responsibilities between IoT device manufacturers, service providers, and end-users helps establish accountability and ensures compliance with privacy regulations.
- Adoption of privacy-preserving techniques in IoT systems: Privacy-preserving techniques play a vital role in IoT systems by enabling data analysis while preserving the privacy of sensitive information. Techniques such as secure multiparty computation [53] or federated learning [54] allow data analysis to be performed without exposing raw data to third parties. By distributing the computation or learning process across multiple devices or parties, privacy-preserving techniques safeguard the confidentiality of data while still enabling collaborative analysis or machine learning models.

Table 4 shows a comprehensive summary of the key security and privacy challenges faced in the realm of IoT systems. It is organized into four distinct categories, beginning with ''Device-level Security Challenges,'' which encompasses measures to secure individual IoT devices, addressing physical security, firmware/software vulnerabilities, and authentication methods. The ''Network Security Challenges'' section delves into issues regarding secure communication protocols, network infrastructure vulnerabilities, and protection against DoS attacks. ''Data Security Challenges'' focuses on safeguarding the confidentiality, integrity, and privacy of IoT data, covering encryption, data integrity, and secure data storage/transmission. Lastly, the ''Privacy Challenges'' segment explores concerns surrounding data collection, processing, and user consent, highlighting privacy-enhancing techniques, consent management, and privacy-preserving methods.

The table also includes an ''Additional Features'' section, emphasizing extra considerations such as security auditing, incident response planning, user education, and compliance with privacy regulations, all aimed at enhancing the

TABLE 4. IoT security and privacy challenges.

Ref.	Area/Field	Description	Key Measures	Solutions
[34]–[38], [40]	Device-level Security Challenges	Measures to secure individual IoT devices.	- Physical security of IoT devices - Firmware and software vulnerabilities - Authentication and access control mechanisms	- Secure enclosures, tamper-evident seals, physical locks - Regular security assessments, code reviews, patch management - Strong authentication protocols (e.g., 2FA, biometrics), access control mechanisms (e.g., RBAC, ABAC)
[23], [24], [44], [45]	Network Security Challenges	Challenges in securing the communication infrastructure connecting IoT devices.	- Secure communication protocols for IoT devices - Vulnerabilities in the network infrastructure - Protection against Denial of Service (DoS) attacks	- TLS, DTLS - Regular assessments, firmware updates, best practices - Monitoring, anomaly detection, rate limiting, traffic filtering
[46]–[50]	Data Security Challenges	Challenges related to ensuring the confidentiality, integrity, and privacy of IoT data.	- Data confidentiality and encryption techniques - Data integrity and prevention of tampering - Secure storage and transmission of IoT data	- AES, ECC - Digital signatures, hash functions - Encrypted databases, secure communication channels (e.g., HTTPS, MQTT with TLS)
[51]–[54]	Privacy Challenges	Challenges associated with data collection, processing, and user consent in IoT systems.	- Protection of user privacy in IoT data collection and processing - Consent management and data ownership - Adoption of privacy-preserving techniques in IoT systems	- Differential privacy, data anonymization - Transparent consent mechanisms, clear data ownership definitions - Secure multiparty computation, federated learning
[55]	Additional Features	Additional considerations for addressing IoT security and privacy challenges.	- Security Auditing - Incident Response Plan - User Education - Legal & Regulatory Compliance	- Regular audits and assessments to identify vulnerabilities - A plan to respond to security incidents promptly - Educating users about IoT security and privacy best practices - Compliance with relevant privacy laws and regulations (e.g., GDPR, CCPA)

security and privacy of IoT systems. This comprehensive table serves as a valuable reference for understanding and mitigating the multifaceted challenges within IoT security and privacy. Addressing these privacy challenges is crucial for building trust, respecting user preferences, and ensuring compliance with privacy regulations in IoT systems. Implementing privacy-enhancing technologies, establishing transparent consent mechanisms, and adopting privacy-preserving techniques empower individuals to have control over their data while still benefiting from the insights and functionality offered by IoT deployments. By prioritizing privacy, organizations can enhance user trust and ensure the responsible and ethical use of IoT data.

V. AI TECHNIQUES FOR IoT SECURITY

AI techniques have the potential to significantly enhance the security of IoT systems [13], [15]. Leveraging AI algorithms and models can enable intelligent threat detection, robust authentication mechanisms, and proactive security analytics. We classify these techniques into the following categories:

A. THREAT DETECTION AND PREVENTION

AI techniques play a crucial role in detecting and preventing threats in IoT systems by identifying anomalous patterns and behaviors that may indicate potential security breaches. These techniques leverage machine learning algorithms and data analysis to enhance the security posture of IoT deployments. Key techniques for threat detection and prevention in IoT systems include:

- Intrusion detection systems (IDS) using AI algorithms: IDS powered by AI algorithms, such as anomaly detection [56] or behavior-based models [25], can identify potential security breaches and mitigate cyberattacks. These IDS systems continuously monitor network traffic, device activities, and system logs to detect deviations from normal behavior [57]. By learning from historical data and real-time observations, AI algorithms can identify patterns associated with known cyberattacks or detect abnormal activities that may indicate new and emerging threats.
- Machine learning-based anomaly detection in IoT data streams: AI algorithms can analyze real-time data streams generated by IoT devices to detect abnormal patterns, signaling potential security threats or unauthorized activities. By training on historical data and establishing a baseline of normal behavior, machine learning models can identify deviations and raise alerts

when anomalous activities occur. It enables proactive identification of potential cyberattacks, enabling timely response and mitigation measures to prevent security breaches [58].

- Behavioral analysis for identifying abnormal patterns in IoT device behavior: AI techniques can be employed to build models of normal behavior for IoT devices [59]. These models capture the typical usage patterns, communication patterns, and device interactions within an IoT system. By comparing the observed behavior of devices against these models, AI algorithms can identify deviations and flag suspicious activities. Behavioral analysis enables the detection of subtle anomalies that may not be captured by traditional rule-based systems, enhancing the overall threat detection capabilities of IoT security solutions.
- Modern AI Tools for IoT Security: Modern AI techniques, including DL, Stochastic and bayesian learning, transformers, and GenAI [31], are essential in enhancing IoT security against advanced cyber threats in the fast-changing IoT systems. DL is ideal for intrusion protection and anomaly detection because of its processing power and ability to recognize complicated patterns in big datasets. For example, network security systems use DL algorithms to spot suspicious patterns that might be signs of an attack. Similarly, stochastic and bayesian learning play a crucial role in situations requiring decision-making in the face of uncertainty. Adapting security mechanisms based on probabilistic reasoning, these technologies provide resilience against emerging threats in the dynamic environment of IoT. However, IoT Cybersecurity is making more use of transformers, which are well-known for their efficiency in processing sequential data. With their help, we can proactively protect ourselves against security breaches by analyzing time-series data from IoT devices. Likewise, there are significant consequences for cybersecurity in the IoT from GenAI like ChatGPT. It helps create security model training data, sophisticated protection techniques, and simulating cyber attacks. This technology is quickly becoming a crucial component of advanced cybersecurity systems that are proactive.

By utilizing AI techniques for threat detection and prevention in IoT systems, organizations can proactively identify and respond to potential security threats. IDS powered by AI algorithms, machine learning-based anomaly detection, and behavioral analysis techniques provide advanced capabilities to detect emerging threats, mitigate cyberattacks, and safeguard IoT deployments. These techniques enhance the overall security posture of IoT systems by enabling timely detection, response, and prevention of security breaches.

B. SECURE COMMUNICATION AND AUTHENTICATION

AI techniques play a vital role in enhancing the security of communication and authentication mechanisms in IoT systems. By leveraging intelligent algorithms and models, these techniques enhance the confidentiality, integrity, and authenticity of data transmission and strengthen the authentication process. Key techniques for secure communication and authentication in IoT systems include:

- AI-driven cryptographic techniques for secure data transmission: AI algorithms can improve cryptographic protocols [60] and key management schemes [61] to ensure secure and robust communication between IoT devices. These algorithms can optimize encryption algorithms, establish secure key exchange mechanisms, and enhance the overall security of data transmission in IoT systems. By leveraging AI techniques, organizations can address the challenges associated with secure and efficient cryptographic operations in resource-constrained IoT devices.
- AI-powered authentication mechanisms, such as biometrics or behavior-based authentication: AI techniques can enhance authentication mechanisms in IoT systems, moving beyond traditional username-password schemes. For instance, biometric identification algorithms can utilize facial recognition [62], voice recognition [63], palm print recognition [64], or fingerprint scanning [65] to ensure secure and convenient authentication for IoT devices. AI algorithms can also analyze user behavior patterns for continuous authentication, enabling a dynamic and adaptive authentication process. By incorporating AI into authentication mechanisms, organizations can enhance the security and user experience of IoT systems.
- Trust establishment and management using AI algorithms: AI algorithms can be utilized to establish trust relationships between IoT devices and manage trust in dynamic and evolving IoT environments. These algorithms can assess the reputation, behavior, and context of IoT devices to determine the level of trustworthiness. By continuously evaluating trust [66], AI algorithms can dynamically adjust access privileges and permissions, enabling secure and granular control over device interactions. It enhances the security and integrity of IoT systems by preventing unauthorized access and malicious activities.

By leveraging AI techniques for secure communication and authentication, organizations can strengthen the security posture of IoT systems. AI-driven cryptographic techniques enhance data transmission security, AI-powered authentication mechanisms provide robust and user-friendly authentication processes, and AI-based trust establishment and management enable dynamic and adaptive control over device interactions. These techniques enhance the overall security and trustworthiness of IoT systems, ensuring the confidentiality, integrity, and authenticity of data and interactions in the interconnected IoT ecosystem.

C. PREDICTIVE SECURITY ANALYTICS

AI techniques leverage the power of data analysis to provide predictive security analytics for IoT systems [67]. By analyzing large amounts of data, these techniques can enable organizations to proactively identify and mitigate security risks, assess potential vulnerabilities, and prevent security incidents. Key techniques for predictive security analytics in IoT systems include:

- AI for predictive maintenance and risk assessment in IoT deployments: AI models can analyze sensor data collected from IoT devices to predict maintenance needs and assess potential risks. By identifying patterns and anomalies in sensor readings, AI algorithms can predict when a device is likely to fail or require maintenance [68]. It enables organizations to proactively address maintenance needs, reducing the risk of system failures or security breaches. Additionally, AI models can assess potential risks [69] in IoT deployments by analyzing historical data and environmental factors, helping organizations prioritize security measures and allocate resources effectively.
- Proactive threat intelligence and analysis using AI algorithms: AI techniques can analyze diverse data sources, including security logs, threat intelligence feeds, and network traffic data, to identify potential threats and vulnerabilities. By leveraging machine learning algorithms, AI models can detect patterns and indicators of compromise that may signal an imminent security threat. It enables organizations to respond to emerging threats proactively, update security measures, and strengthen their defense against potential cyberattacks. AI-powered threat intelligence and analysis provide valuable insights and enable organizations to stay one step ahead of cyberattacks [70].
- Forecasting and prevention of security incidents using AI models: AI models can analyze historical data to identify patterns that precede security incidents. By learning from past incidents and associated data, AI algorithms can identify indicators that indicate a potential security breach or attack. It enables organizations to take proactive measures to prevent future incidents, such as implementing security patches, updating configurations, or strengthening access controls [71]. By forecasting and preventing security incidents, organizations can minimize the impact of cyberattacks and ensure the ongoing security of their IoT systems.

Table 5 provides a comprehensive overview of how AI techniques can significantly bolster the security of IoT systems. It categorizes these techniques into three key areas: ''Threat Detection and Prevention,'' ''Secure Communication and Authentication,'' and ''Predictive Security Analytics.'' In the first category, AI is harnessed for identifying and thwarting cyberattacks by utilizing techniques such as IDS, machine learning-based anomaly detection, and behavioral analysis. The second category highlights AI's role in enhancing communication security and authentication mechanisms through cryptographic techniques, biometrics, and dynamic trust management. Finally, the third category discusses how AI empowers IoT systems with predictive security analytics, enabling predictive maintenance, proactive threat intelligence, and forecasting of security incidents. Additionally, the table includes an ''Additional Features'' section, emphasizing the importance of security auditing, incident response planning, user education, and legal and regulatory compliance [55]. These AI-driven measures and solutions collectively fortify IoT security, mitigating vulnerabilities and ensuring the integrity of connected systems.

By utilizing AI techniques for predictive security analytics, organizations can proactively identify and address security risks, anticipate maintenance needs, and prevent security incidents. Predictive maintenance and risk assessment using AI, proactive threat intelligence and analysis, and forecasting and prevention of security incidents enable organizations to strengthen the security posture of their IoT systems. By leveraging the power of data and AI algorithms, organizations can make informed decisions, allocate resources effectively, and take proactive measures to ensure the security and resilience of their IoT deployments.

VI. SECURITY FRAMEWORKS AND APPROACHES

Securing IoT systems requires comprehensive frameworks and approaches. We categorize these frameworks based on their core principles and implementation strategies:

A. DEFENSE-IN-DEPTH ARCHITECTURES

Defense-in-depth architectures aim to provide layered security mechanisms for IoT systems, ensuring robust protection against various attack vectors. These architectures involve implementing multiple layers of security, considering the entire IoT ecosystem, and incorporating secure hardware design and implementation strategies. Key aspects of defense-in-depth architectures for IoT security include:

- Layered security mechanisms for protecting IoT devices and networks: Defense-in-depth architectures employ multiple layers of security to protect IoT devices and networks. It includes implementing physical security measures, such as secure enclosures and tamper-evident seals, to prevent unauthorized access to IoT devices. Network segmentation techniques, such as Virtual Local Area Networks (VLANs) or firewalls [72], can be deployed to isolate IoT devices and prevent lateral movement within the network. Access control mechanisms, such as strong authentication and authorization protocols, ensure that only authorized entities can interact with IoT devices and systems. By layering these security mechanisms, organizations create multiple barriers for attackers, increasing the overall security resilience of their IoT deployments.
- Security frameworks designed for end-to-end security in IoT systems: Defense-in-depth architectures consider

TABLE 5. AI techniques for IoT security.

Reference	Category	Description	Key Measures	Solutions
[13], [15]	Threat Detection and Prevention	AI techniques for identifying cyberattacks in IoT.	- Intrusion detection systems (IDS) using AI algorithms - Machine learning-based anomaly detection in IoT data streams - Behavioral analysis for identifying abnormal patterns in IoT device behavior	- Anomaly detection, behavior-based models - Real-time data analysis, anomaly detection - Building models of normal behavior, behavioral analysis
[60]–[63], [65]	Secure Communication and Authentication	AI techniques for enhancing communication security and authentication in IoT.	- AI-driven cryptographic techniques for secure data transmission - AI-powered authentication mechanisms (e.g., biometrics) - Trust establishment and management using AI algorithms	- Encryption optimization, secure key exchange - Facial recognition, voice recognition, behavior-based authentication - Dynamic trust assessment, context-based access control
[68]–[70]	Predictive Security Analytics	AI techniques for predictive security analytics in IoT.	- AI for predictive maintenance and risk assessment in IoT deployments - Proactive threat intelligence and analysis using AI algorithms - Forecasting and prevention of security incidents using AI models	- Sensor data analysis, risk assessment - Threat pattern detection, proactive response - Incident pattern recognition, preventive measures
[55]	Additional Features	Additional considerations for enhancing IoT security.	- Security Auditing - Incident Response Plan - User Education - Legal & Regulatory Compliance	- Regular audits and assessments - A plan for responding to security incidents - Educating users about IoT security best practices - Compliance with privacy laws and regulations

the entire IoT ecosystem, encompassing devices, networks, and backend systems. This approach ensures a holistic and comprehensive approach to security. Security frameworks designed for end-to-end security in IoT systems define security policies, protocols, and best practices to be followed throughout the life cycle of IoT deployments. These frameworks address security at different levels, including device security [73], network security [74], data security [75], and access control [76]. By adopting such frameworks, organizations can ensure that security measures are consistently applied across the entire IoT ecosystem, minimizing vulnerabilities and potential attack surfaces.

- Secure hardware design and implementation strategies: Defense-in-depth architectures also incorporate secure hardware design and implementation strategies. It involves incorporating security features into the design of IoT device hardware, such as tamper-resistant chips [77], secure elements, or secure boot mechanisms [78]. Secure hardware design aims to protect the integrity of the device, prevent unauthorized access or tampering, and ensure that only trusted firmware and software can be loaded onto the device. By incorporating security into the hardware design and implementing secure manufacturing and supply chain practices, organizations can establish a strong foundation for IoT device security.

By adopting defense-in-depth architectures, organizations can significantly enhance the security of their IoT systems. Layered security mechanisms protect IoT devices and networks from various attack vectors. Security frameworks ensure end-to-end security across the IoT ecosystem, and secure hardware design and implementation strategies provide a robust foundation for device security. These approaches minimize vulnerabilities, reduce the impact of potential cyberattacks, and strengthen the overall security resilience of IoT deployments.

B. SECURE SOFTWARE DEVELOPMENT

Secure software development practices are crucial for building resilient IoT systems that are resistant to cyberattacks. By following secure coding practices, implementing secure update mechanisms, and conducting thorough security testing, organizations can minimize vulnerabilities and enhance the overall security of IoT software. Key considerations for secure software development in IoT systems include:

- Secure coding practices for IoT devices and applications: Following secure coding guidelines and best practices is essential to minimize the introduction of vulnerabilities during the development process. It includes practices such as input validation [79], output encoding [80], and proper handling of user input to prevent common attack vectors such as injection attacks or cross-site scripting [81]. By incorporating secure coding practices into the development life cycle of IoT devices and applications, organizations can reduce the risk of security vulnerabilities and improve the overall resilience of their software.

- Secure firmware and software update mechanisms: Implementing secure over-the-air (OTA) update mechanisms is crucial to ensure that IoT devices can receive and install security patches and updates securely. It involves implementing cryptographic protocols to secure the update process, verifying the integrity and authenticity of updates, and securely distributing updates to IoT devices. Secure update mechanisms enable organizations to address newly discovered vulnerabilities and mitigate potential risks without requiring physical access to devices, enhancing the overall security and maintainability of IoT deployments [26], [82].
- Security testing and vulnerability assessment techniques for IoT systems: Conducting thorough security testing is essential to identify and address vulnerabilities in IoT software components. It includes techniques such as penetration testing, code audits, and vulnerability scanning [83] to identify weaknesses and potential entry points for attackers. Security testing helps organizations identify vulnerabilities before deployment and validate the effectiveness of security measures [84]. By incorporating security testing as an integral part of the software development process, organizations can proactively identify and remediate security issues, reducing the likelihood of successful cyberattacks.

By embracing secure software development practices, organizations can significantly enhance the security of their IoT systems. Secure coding practices reduce the risk of introducing vulnerabilities, secure update mechanisms enable timely patching of security flaws, and security testing ensures the identification and remediation of vulnerabilities. Collectively, these practices contribute to building resilient and secure IoT software, reducing the attack surface and enhancing the overall security posture of IoT deployments.

C. SECURE DATA MANAGEMENT

Effective data management is crucial for maintaining the security and privacy of IoT data. Secure data management practices encompass data classification, access control mechanisms, secure data storage, secure data processing techniques, and appropriate data life cycle management. Key aspects of secure data management in IoT systems include:

- Data classification and access control mechanisms: Applying data classification labels to IoT data helps organizations understand the sensitivity and criticality of the data they collect. By implementing fine-grained access control mechanisms, such as role-based access control [85] or attribute-based [86] access control, organizations can ensure that IoT data is accessed only by authorized entities. Access control mechanisms should consider user authentication, authorization policies, and secure communication channels to protect the confidentiality and integrity of IoT data.
- Secure data storage and processing techniques for IoT environments: Secure storage mechanisms are vital to protect IoT data at rest. Employing encryption techniques, such as strong symmetric or asymmetric encryption algorithms [87], ensures that data remains confidential even if it is compromised or stolen. Secure enclaves or hardware security modules (HSMs) can provide additional protection by isolating sensitive data and cryptographic operations from the underlying system. Similarly, secure data processing techniques, such as secure multiparty computation [88], enable collaborative data analysis [27] without exposing the raw data, ensuring the confidentiality of IoT data during processing.
- Data life cycle management considerations in IoT systems: Managing IoT data throughout its life cycle is essential to ensure its security. It includes establishing appropriate data retention policies that determine how long data should be stored and defining secure data disposal procedures [89] to minimize the risk of data breaches. Organizations should consider data anonymization or pseudonymization techniques to protect the privacy of individuals and comply with data protection regulations. Implementing robust data backup and recovery strategies also contributes to secure data management, ensuring the availability and integrity of IoT data.

Table 6 outlines essential security frameworks and approaches for safeguarding IoT systems. It categorizes these approaches into three key areas: defense-in-depth architectures, secure software development, and secure data management. Defense-in-depth architectures emphasize layered security mechanisms, holistic security frameworks, and secure hardware design to fortify IoT deployments against diverse attack vectors. Secure software development practices encompass secure coding, over-the-air update mechanisms, and rigorous security testing, reducing vulnerabilities and bolstering IoT software resilience. Secure data management entails data classification, access controls, secure storage, and life cycle management, ensuring the confidentiality, integrity, and compliance of IoT data. Each approach offers distinct key measures and benefits, collectively contributing to comprehensive IoT security strategies.

By embracing secure data management practices, organizations can protect the confidentiality, integrity, and privacy of IoT data. Data classification and access control mechanisms ensure that data is accessed only by authorized entities, secure storage, and processing techniques protect data at rest and during processing, and data life cycle management considerations minimize the risk of data breaches. Collectively, these practices contribute to building a secure and compliant data management framework for IoT systems, enabling organizations to derive value from IoT data while maintaining data security and privacy.

TABLE 6. Security frameworks and approaches.

Ref.	Security Frameworks and Approaches	Key Measures	Benefits
[72], [73], [75], [76]	Defense-in-depth architectures	• Layered security mechanisms • Security frameworks for end-to-end security • Secure hardware design and implementation	• Enhanced protection against various attack vectors • Comprehensive approach to IoT security • Strong foundation for device security
[26], [79], [80], [83]	Secure software development	• Secure coding practices • Secure firmware and software update mechanisms • Security testing and vulnerability assessment techniques for IoT systems	• reduced risk of introducing vulnerabilities • Timely patching of security flaws • Improved software maintainability • Proactive identification and remediation of vulnerabilities
[27], [85], [88], [89]	Secure data management	• Data classification and access control mechanisms • Secure data storage and processing techniques for IoT environments • Data life cycle management considerations in IoT systems	• Controlled and authorized access to IoT data • Protection of data confidentiality and integrity • Confidentiality of data at rest and during processing • Compliance with data protection regulations • Minimized risk of data breaches

VII. PRIVACY AND ETHICAL CONSIDERATIONS

Preserving privacy and ensuring ethical practices in IoT systems are critical for user trust. We categorize these considerations as follows:

A. DATA PRIVACY PROTECTION

Protecting user privacy is a fundamental requirement in IoT systems. Key considerations include:

B. PRIVACY CHALLENGES

Ensuring privacy in IoT systems is crucial to address concerns related to data collection, processing, and user consent. Privacy challenges arise due to the sensitive nature of IoT data and the need to protect individual privacy rights. Effective privacy measures involve privacy-preserving techniques, anonymization and pseudonymization approaches, and privacy impact assessments. Key aspects of privacy challenges in IoT systems include:

- Privacy-preserving techniques for IoT data collection and processing: Privacy-preserving techniques, such as differential privacy or secure multi-party computation, enable data analysis while preserving the privacy of individual users. Differential privacy introduces controlled noise or perturbation to data to provide aggregate insights without revealing sensitive individual information [90], [91]. Secure multi-party computation enables collaboration and data analysis across multiple parties without sharing raw data. By employing these techniques, organizations can derive valuable insights from IoT data while ensuring the privacy and confidentiality of personal information [92], [93].
- Anonymization and pseudonymization approaches for protecting user identities: Anonymization and pseudonymization techniques play a vital role in protecting the identities of individuals in IoT data sets. Anonymization involves removing or altering Personally Identifiable Information (PII) from data, making it impossible to link the data back to an individual [94]. Pseudonymization replaces identifying information with pseudonyms, allowing for data analysis while preserving the privacy of individuals. By applying these approaches, organizations can minimize the risk of re-identification and unauthorized disclosure of personal information in IoT data.
- Privacy impact assessments to identify and mitigate privacy risks: Conducting privacy impact assessments help organizations identify potential privacy risks in IoT systems and implement appropriate measures to mitigate them. These assessments evaluate the impact of data collection and processing on privacy rights and identify potential vulnerabilities or risks. By conducting privacy impact assessments, organizations can proactively address privacy concerns, implement privacy-by-design principles, and ensure compliance with privacy regulations and standards [95].

Addressing privacy challenges in IoT systems requires the adoption of privacy-preserving techniques, anonymization and pseudonymization approaches, and privacy impact

assessments. By implementing these measures, organizations can protect the privacy of individuals, maintain compliance with privacy regulations, and foster trust among users. Privacy-preserving techniques enable valuable data analysis while safeguarding sensitive information, anonymization and pseudonymization approaches protect user identities, and privacy impact assessments ensure that privacy risks are identified and mitigated. By prioritizing privacy in IoT systems, organizations can achieve a balance between data utilization and individual privacy rights.

C. ETHICAL USE OF AI IN IoT SECURITY

Ensuring the ethical use of AI in IoT security is essential to maintain transparency, fairness, and accountability. Ethical considerations help address potential biases, ensure transparency and explainability of AI algorithms, and establish frameworks for accountability and responsibility. Key aspects of the ethical use of AI in IoT security include:

- Transparency and explainability of AI algorithms used in IoT security: Making AI algorithms and decision-making processes transparent and explainable helps build user trust and ensures accountability. Users and stakeholders should have visibility into how AI algorithms are trained, the data used, and the decision-making criteria employed. Explainability techniques, such as model interpretability and algorithmic transparency, can provide insights into how AI models arrive at their decisions. Transparent and explainable AI fosters trust and enables individuals to understand the rationale behind security measures and potential limitations [96], [97].
- Fairness considerations to mitigate bias in AI decision-making: Addressing biases in AI algorithms and models used in IoT security is crucial to prevent discriminatory outcomes and ensure fair treatment of individuals. Bias can arise from biased training data, flawed algorithms, or inherent societal biases. Organizations should strive to identify and mitigate biases through rigorous data preprocessing, algorithmic fairness techniques, and continuous monitoring [98]. By actively addressing bias, organizations can enhance the fairness and equity of AI-enabled security systems, promoting equal treatment and reducing the risk of disparate impacts.
- Accountability and responsibility frameworks for AI-enabled IoT security systems: Establishing frameworks to govern the responsible use of AI in IoT security is essential. It includes defining clear accountability and liability frameworks that assign responsibilities [99] to organizations, developers, and operators of AI-enabled IoT security systems. Organizations should ensure compliance with applicable laws, regulations, and ethical standards [100]. They should also consider the potential risks and unintended consequences associated with AI deployments and establish mechanisms for redress and recourse in the event of system failures or misuse. By implementing accountability and responsibility frameworks, organizations can promote ethical practices, enhance user trust, and mitigate potential risks.

Table 7 summarizes essential privacy and ethical considerations in IoT systems, emphasizing the need for safeguarding user privacy and ensuring responsible AI deployment. It begins with "Data Privacy Protection," encompassing privacy-preserving techniques like differential privacy and secure multi-party computation, anonymization, pseudonymization approaches, and privacy impact assessments. "Ethical Use of AI" explores transparency, fairness, and accountability in AI-enabled IoT security. "Privacy Challenges" delves into challenges related to data collection, processing, and user consent. The table underscores the importance of transparent AI algorithms and decision-making processes, fairness to mitigate bias, and accountability and responsibility frameworks for AI in IoT. By referencing notable works in each category, this table serves as a valuable resource for organizations aiming to navigate the intricate landscape of privacy and ethics in IoT systems.

By prioritizing the ethical use of AI in IoT security, organizations can build transparency, fairness, and accountability into their systems. Transparent and explainable AI algorithms foster trust, fairness considerations mitigate bias, and accountability frameworks ensure responsible practices. These ethical considerations promote the adoption of AI technologies in a manner that aligns with societal values, respects individual rights, and enhances the overall security and trustworthiness of IoT systems.

VIII. CASE STUDIES AND USE CASES

We present real-world case studies and use cases that highlight the application of AI in securing IoT systems:

A. INDUSTRY-SPECIFIC USE CASES

In addition to the general application of AI techniques for IoT security, there are specific industries where AI is applied to enhance the security of IoT systems. These industry-specific use cases showcase how AI techniques can address the unique security challenges and requirements in various sectors. Some notable industry-specific use cases include:

- Healthcare IoT security applications and solutions: The healthcare industry relies heavily on IoT devices to monitor patients, deliver personalized care, and streamline medical operations [19], [102]. AI techniques are employed to secure medical devices, protect patient privacy, and ensure the integrity of healthcare IoT systems. For example, AI-powered anomaly detection algorithms can continuously monitor patient data, identify abnormal patterns that may indicate unauthorized access or tampering, and trigger timely alerts for healthcare providers. AI can also enable secure and privacy-preserving data sharing and analysis for medical

TABLE 7. Privacy and ethical considerations in IoT systems.

Ref.	Consideration	Description
[94], [95], [101]	Data Privacy Protection	Measures to protect user privacy in IoT, including privacy-preserving techniques (e.g., differential privacy, secure multi-party computation), anonymization and pseudonymization approaches, and privacy impact assessments.
[96]–[100]	Ethical Use of AI	Ensuring the ethical use of AI in IoT security, focusing on transparency and explainability of AI algorithms, fairness considerations to mitigate bias, and accountability and responsibility frameworks for AI-enabled IoT security systems.
[94], [95], [101]	Privacy Challenges	Addressing privacy challenges in IoT systems, including data collection, processing, and user consent, through privacy-preserving techniques, anonymization and pseudonymization approaches, and privacy impact assessments.
[96], [97]	Transparency	Making AI algorithms and decision-making processes transparent and explainable, enabling users and stakeholders to understand how AI models are trained and make decisions.
[98]	Fairness	Mitigating biases in AI decision-making by addressing issues arising from training data, algorithms, and societal biases to ensure fair treatment of individuals.
[99], [100]	Accountability	Establishing accountability and responsibility frameworks for AI-enabled IoT security systems, assigning responsibilities, ensuring compliance, and addressing potential risks and consequences.

research, enabling collaboration while safeguarding sensitive patient information [103].

- Smart City security: Surveillance and CCTV systems equipped with AI have significantly improved security in smart cities. Modern video analysis tools use sophisticated machine learning algorithms (e.g., Convolutional Neural Networks (CNNs) [104], [105], Recurrent Neural Networks (RNNs) [106], [107], Support Vector Machines (SVMs) [108], [109], Decision Trees (DT) [110], and Random Forests (RF) [111]) to identify anomalies, analyze behavior, and recognize facial features in real-time. These technologies can detect suspicious behavior or possible dangers and immediately notify. For example, AI-powered smart surveillance systems in cities efficiently and accurately sift through mountains of video footage to keep residents safe and deter criminals. For example, a smart city program used artificial intelligence to power a state-of-the-art CCTV monitoring system that increased public safety and reduced crime. Using algorithms for face recognition and behavioral analysis, this system allowed for the real-time surveillance of public locations via a network of cameras. After training, the AI algorithms can identify suspicious behavior and notify the proper authorities immediately in case of a possible security danger. This proactive strategy may result in a considerable drop in crime rates. There can be an improvement in both public safety and trust in urban security measures.
- Smart home security systems leveraging AI techniques: With the increasing adoption of smart home devices and automation systems, ensuring the security of these interconnected devices is crucial [112]. AI-based intrusion detection systems [113] and anomaly detection algorithms [114] are utilized to protect smart homes from unauthorized access and potential cyberattacks. AI algorithms can learn the normal behavior patterns of smart home devices and identify deviations that may indicate unauthorized activities. For example, AI algorithms can detect anomalies in device communication patterns, identify potential security breaches, and send alerts to homeowners or security providers. AI can also enable intelligent authentication mechanisms, such as behavior-based authentication or facial recognition, to ensure secure access to smart home systems.
- Industrial IoT (IIoT) security implementations in manufacturing and critical infrastructure: The industrial sector, including manufacturing facilities and critical infrastructure, heavily relies on IoT systems to optimize operations, improve efficiency, and monitor equipment performance. However, these systems are often prime targets for cyberattacks [115], [116]. AI techniques are employed to secure industrial control systems, detect anomalies [114] in operational data, and mitigate cyberattacks in critical infrastructure. AI algorithms can analyze vast amounts of data generated by IIoT devices, such as sensors and industrial machinery, to identify abnormal patterns that may indicate cyberattacks or equipment malfunctions. By leveraging AI-powered threat detection and predictive maintenance capabilities, organizations can enhance the security and resilience of their industrial IoT deployments.

These industry-specific use cases demonstrate the diverse applications of AI in enhancing the security of IoT systems. In the healthcare industry, AI enables secure and privacy-preserving healthcare IoT solutions. For instance, smart home security systems leverage AI for intrusion detection and secure access control. In the industrial sector, AI techniques enhance the security of IIoT deployments and enable proactive threat detection. By understanding these use cases, organizations can explore tailored approaches to securing IoT systems in their specific industry, addressing industry-specific challenges and requirements while harnessing the power of AI for enhanced security.

B. REAL-WORLD DEPLOYMENT SCENARIOS

Real-world deployment scenarios highlight successful implementations of AI-based security solutions in IoT systems, showcasing how AI and IoT technologies work together to enhance security. These deployment scenarios demonstrate

the practical applications of AI techniques in securing various domains. Some notable real-world deployment scenarios include:

- Smart city security infrastructure leveraging AI and IoT technologies: Smart cities rely on interconnected IoT devices and systems to enhance urban living, but they also present unique security challenges. AI algorithms are utilized to monitor and detect potential security incidents in smart city infrastructure, such as video surveillance systems, smart grids, or public transportation networks [117], [118]. AI techniques can analyze real-time data from various sensors and sources to identify anomalies, detect suspicious activities, and trigger immediate responses. For example, AI algorithms can analyze video feeds to detect unusual behavior patterns or identify potential security breaches, enabling quick intervention and proactive security measures.
- Connected vehicle security systems using AI algorithms for threat detection: The increasing connectivity and autonomy of vehicles introduce new security risks. Connected vehicle security systems leverage AI algorithms for threat detection and mitigation. AI-based anomaly detection algorithms are applied to analyze vehicle sensor data, network traffic, and communication patterns to detect potential cyberattacks or tampering attempts [119]. By continuously monitoring vehicle behavior and identifying abnormal patterns, AI algorithms can trigger alarms, initiate countermeasures, and alert vehicle owners or security authorities. AI-enabled connected vehicle security systems contribute to safer transportation and protect against potential cyberattacks targeting vehicle systems and data [120].
- Agricultural IoT security solutions to protect crop monitoring and management systems: Agricultural IoT systems play a crucial role in improving crop yield, optimizing resource utilization, and enabling precision farming [121]. However, these systems also face security risks that can impact crop management and data integrity. AI techniques are used to secure agricultural IoT systems, ensuring the integrity of data collected from sensors and protecting against unauthorized access. AI algorithms can analyze sensor data to identify anomalies that may indicate environmental threats, crop diseases, or potential tampering [122], [123]. By leveraging AI-based security solutions, farmers and agricultural organizations can detect and mitigate risks, safeguard crop monitoring and management systems, and ensure the productivity and sustainability of agricultural operations.

These real-world deployment scenarios highlight successful implementations of AI-based security solutions in IoT systems shown in Table 8. From securing smart city infrastructure to protecting connected vehicles and agricultural IoT systems, AI techniques demonstrate their effectiveness in enhancing security, detecting anomalies, and enabling proactive measures. By understanding these real-world scenarios, organizations can gain insights into the practical applications of AI in IoT security and explore opportunities to deploy similar solutions in their respective domains.

IX. FUTURE DIRECTIONS AND RESEARCH CHALLENGES

This section highlights emerging trends and research challenges in securing IoT in the era of AI:

A. ADVANCEMENTS IN AI FOR IoT SECURITY

Advancements in AI have opened up new possibilities for enhancing IoT security. These emerging advancements leverage AI techniques to address the unique challenges of IoT security, enabling distributed security intelligence, on-device security processing, and adaptive and self-defending IoT systems. Some notable advancements in AI for IoT security include:

- Federated learning for distributed security intelligence in IoT systems: Federated learning is a privacy-preserving machine learning technique that enables collaborative model training across multiple IoT devices while preserving data privacy. Federated learning can be applied to IoT security to create distributed security intelligence. Instead of centralizing data in a single location, federated learning allows models to be trained on IoT devices themselves. This approach enables IoT devices to learn from their local data while sharing aggregated knowledge with a central server or among other devices. By leveraging federated learning, IoT systems can benefit from collective intelligence while preserving data privacy and addressing data ownership concerns.
- Edge AI for on-device security processing and decision-making: Edge AI refers to the deployment of AI algorithms directly on IoT devices or at the edge of IoT networks, enabling real-time security processing and decision-making without relying on cloud-based services. By bringing AI capabilities to the edge, IoT devices can analyze and respond to cyberattacks locally, minimizing latency and dependence on external connectivity. Edge AI enables efficient data processing, immediate response to security incidents, and reduced reliance on cloud resources. With on-device security processing, IoT devices can identify and mitigate security threats autonomously, enhancing the overall security and resilience of IoT deployments.
- AI-powered adaptive and self-defending IoT systems: AI techniques can enable IoT systems to adapt to evolving cyberattacks, dynamically adjust security measures, and autonomously respond to potential attacks. AI algorithms can continuously monitor IoT data, analyze patterns, and identify emerging cyberattacks or vulnerabilities. By learning from past incidents, AI-powered IoT systems can proactively adjust security

TABLE 8. AI applications in securing IoT systems: use cases and real-world deployment.

Ref.	Industry/Application	AI Techniques Used	Key Outcomes and Benefits
[19], [102], [103]	Healthcare IoT Security Solutions	Privacy-preserving techniques, AI-based anomaly detection	Secure medical devices, protect patient privacy, detect unauthorized access, enable privacy-preserving data sharing
[112]–[114]	Smart Home Security Systems	AI-based intrusion detection, anomaly detection, secure access control	Protect smart homes from unauthorized access, identify security breaches, enable intelligent authentication mechanisms
[114]–[116]	Industrial IoT (IIoT) Security	AI-based anomaly detection, predictive maintenance	Enhance the security of IIoT deployments, detect equipment malfunctions, mitigate cyberattacks, improve operational resilience
[117], [118]	Smart City Security Infrastructure	AI-based anomaly detection, real-time monitoring	Monitor smart city infrastructure, detect security incidents, analyze video feeds, enable quick intervention
[119], [120]	Connected Vehicle Security Systems	AI-based anomaly detection, threat detection	Enhance vehicle cybersecurity, detect cyberattacks, ensure vehicle data integrity, protect against tampering
[121]–[123]	Agricultural IoT Security Solutions	AI-based anomaly detection, data integrity protection	Secure agricultural IoT systems, detect environmental threats, safeguard crop monitoring, ensure data integrity

measures, such as updating access controls, modifying encryption algorithms, or blocking suspicious activities. This adaptive and self-defending capability helps IoT systems stay resilient and responsive in the face of evolving security challenges, reducing the likelihood of successful cyberattacks and minimizing the impact of security breaches.

- Role and Future Vision of GenAI in Cybersecurity: Tools like ChatGPT, which fall under the umbrella of GenAI, have emerged over the past few years and are reshaping several industries, including cybersecurity [28]. GenAI has revolutionized threat detection and system protection, which is essential for the security of the IoT. Its capacity to learn and duplicate complicated data patterns sets it apart. Integrating GenAI into cybersecurity signifies a notable departure from conventional reactive, defensive mechanisms and adopting a more proactive approach. These AI algorithms ace the art of finding and forecasting possible breaches by sifting through mountains of data on cybersecurity concerns. Thanks to GenAI's superior threat detection, thorough data analysis, and risk prediction capabilities, cybersecurity is now more efficient. On the other hand, there are obstacles specific to implementing such technologies. Addressing challenges such as the necessity for large-scale computing resources, the risk of hackers abusing AI capabilities, and ethical concerns about data protection and control is crucial. Several cutting-edge cybersecurity products demonstrate the use of GenAI. In addition, there have been notable breakthroughs in AI-native security analyst tools, such as CrowdStrike's Charlotte AI [31], which provides practical and easy methods for managing cybersecurity risks. The Hiroshima AI Process of the G7 and China's Global AI Governance Initiative are two examples of worldwide attempts to control artificial intelligence [124]. In delicate domains such as cybersecurity, these regulatory frameworks play a pivotal role in molding the proper use of AI. There are immediate ramifications for IoT security from incorporating GenAI into cybersecurity. Now more than ever, with IoT devices pervasive and essential to many industries, it is critical that these AI models can anticipate and proactively manage risks. To guarantee the security and dependability of IoT systems, it is crucial to use and regulate GenAI with care as we continue to tap into its potential.

These advancements in AI for IoT security offer promising opportunities to enhance the security and resilience of IoT systems. Federated learning enables distributed security intelligence, on-device security processing leverages edge AI for real-time decision-making, and AI-powered adaptive and self-defending IoT systems autonomously respond to cyberattacks. By embracing these advancements, organizations can leverage the power of AI to enhance the security posture of their IoT deployments, enabling proactive threat detection, efficient security processing, and adaptive defense mechanisms.

B. STANDARDIZATION AND REGULATORY EFFORTS

Standardization and regulatory efforts play a crucial role in ensuring the security and trustworthiness of IoT systems. As the adoption of IoT continues to expand across industries and sectors, the need for consistent security measures and legal frameworks becomes increasingly important. Standardization efforts focus on developing IoT security frameworks, industry standards, and best practices, while regulatory efforts address legal and compliance considerations specific to IoT security and privacy. Key aspects of standardization and regulatory efforts in IoT security include:

- IoT security frameworks and industry standards: Developing standardized frameworks and industry standards

for IoT security is essential to ensure consistent security measures across different IoT deployments. These frameworks and standards provide guidelines and best practices for securing IoT devices, networks, and data. They address various aspects of IoT security, including device-level security, network security, data security, and privacy. By adhering to these frameworks and standards, organizations can establish a common baseline for IoT security, facilitate interoperability, and promote good security practices throughout the IoT ecosystem. Examples of IoT security frameworks and standards include the Industrial Internet Consortium (IIC) Security Framework, the NIST Cybersecurity Framework, and the ISO/IEC 27000 series [29]. Using AI/IoT standards established by international organizations, industrial plants should update systems in line with global norms. The UN/ITU defines secure and interoperable IIoT systems [125]. For the same reason, IEEE standards provide a structure for incorporating AI into the IIoT [30]. The industries adhered to these requirements to guarantee that their improved systems were technologically modern and aligned with best practices and regulations worldwide.

For instance, a manufacturing company encountered difficulties due to its outdated infrastructure and lack of sophisticated monitoring capabilities in a real-life situation. Stochastic learning methods provide a practical and economical way to upgrade manufacturing-related IoT devices that lack intelligence [126]. Integrating stochastic learning into existing frameworks may save the system's rebuilding cost. This method incorporates AI models that can process the newly acquired data by equipping older machinery with sensors. The manufacturing industry may launch a predictive maintenance program by integrating AI into its IIoT framework. Attached to vital machinery, this system's sensors gathered real-time data on equipment performance. By analyzing this data, AI systems could spot irregularities that may indicate that equipment was about to break down. With the help of predictive maintenance technology, maintenance crews could act before a costly breakdown happened, preventing a crucial failure in a critical production line. Significant cost reductions and the avoidance of major production downtime were both achieved by this action. The successful adoption showcased the practical advantages of AI in industrial environments, further solidifying the plant's standing as a leader in technical advancement.

- Legal and regulatory considerations for IoT security and privacy: Addressing legal and regulatory challenges in IoT security is crucial to establishing a solid legal foundation for secure and privacy-preserving IoT systems. IoT deployments often involve the collection, processing, and storage of large amounts of data, including personal and sensitive information. Legal and regulatory considerations encompass data protection regulations, privacy laws, and liability frameworks. Organizations must comply with applicable regulations and ensure that IoT systems meet legal requirements related to data privacy, consent management, data breach notification, and user rights. Governments and regulatory bodies are actively working to update existing laws or introduce new regulations specific to IoT security and privacy, aiming to strike a balance between innovation and the protection of individual rights.
- Interoperability and certification frameworks for IoT security solutions: Developing interoperability standards and certification frameworks for IoT security solutions is crucial to ensure that different security components can seamlessly work together and meet established security requirements. Interoperability standards define protocols and interfaces that enable the integration and interaction of diverse IoT devices and systems. These standards help establish secure communication, ensure consistent authentication mechanisms, and facilitate the exchange of security-related information. Certification frameworks provide a means to verify and validate the security capabilities of IoT devices, networks, or solutions. Through third-party evaluation and certification, organizations can demonstrate compliance with established security standards and gain confidence in the security of their IoT deployments. Examples of interoperability standards and certification frameworks for IoT security include the Zigbee Alliance, the Thread Group, and the Common Criteria for Information Technology Security Evaluation.

Standardization and regulatory efforts in IoT security are essential for establishing consistent security measures, ensuring legal compliance, and promoting interoperability. IoT security frameworks and industry standards guide the implementation of effective security measures, legal and regulatory considerations address privacy and liability concerns, and interoperability and certification frameworks ensure the compatibility and trustworthiness of IoT security solutions. By embracing these standardization and regulatory efforts, organizations can enhance the security posture of their IoT systems, foster trust among users and stakeholders, and drive the widespread adoption of secure and privacy-preserving IoT deployments.

C. PHYSICAL AND INFRASTRUCTURE SECURITY CHALLENGES IN IoT

The protection of IoT systems requires physical and infrastructure considerations in addition to digital ones. A significant challenge within this domain is the minimization of risks associated with unauthorized physical intrusions into IoT infrastructure or devices. It is paramount to prevent any tampering with these devices to ensure their continued functionality and integrity.

- Saving IoT devices against physical theft: Ensuring the security of IoT devices and the sensitive data they

contain from theft is crucial. Additionally, physical resilience is a key aspect, necessitating that infrastructure components and IoT devices be designed to withstand environmental challenges, including but not limited to extreme temperatures, humidity, and other adverse conditions. It is critical to exercise caution when selecting deployment sites to mitigate susceptibility to physical hazards. To mitigate the risk of tampering or compromise throughout the life cycle of IoT devices, including their production, transportation, and installation, supply chain security is of equal importance.

- Environmental conditions: Environmental considerations comprise a range of challenges associated with adverse conditions such as severe weather, pollution, and physical harm. It is imperative to protect IoT devices from intentional physical interference that may disrupt their operations or compromise the integrity of data.
- Safeguarding against physical tampering and Ensuring uninterrupted power supply: Ensuring security against physical tampering is also important. We must pay attention to the dependability of the power supply for IoT devices. Both physical tampering and power supply loss can result in interrupted communication and sensitive data loss. It is also important to protect the physical infrastructure of data centers or cloud servers that store and process IoT data, in addition to the network infrastructure that facilitates IoT communication. It includes protecting physical threats against routers, switches, and gateways. In light of the various physical and infrastructure security challenges that these systems entail and the diverse threats they may encounter in practical deployments, an all-encompassing strategy must be adopted to ensure the security of the IoT.

X. CONCLUSION

Securing IoT in the AI era requires a comprehensive and multidimensional approach. By addressing the challenges, leveraging AI techniques, adhering to security frameworks, and considering privacy and ethical implications, it can build robust and resilient IoT systems that enhance security, protect user privacy, and foster trust. This survey paper examined the challenges that arise in securing IoT systems and explored various AI techniques that can be employed to enhance their security. Through the categorization of device-level security challenges, network security challenges, data security challenges, privacy challenges, and ethical considerations, it highlighted the multifaceted nature of securing IoT in the context of AI. It discussed the importance of physical security, firmware and software vulnerabilities, authentication, and access control mechanisms at the device level.

Additionally, data security and privacy challenges were explored, along with the ethical considerations for transparency and explainability of AI algorithms. It also provided industry-specific use cases and real-world deployment scenarios to illustrate how AI techniques are applied in securing IoT systems across various domains. Lastly, it discussed the ongoing standardization and regulatory efforts in IoT security, which encompass the development of IoT security frameworks, industry standards, legal and regulatory considerations, as well as interoperability and certification frameworks. As IoT continues to evolve and expand, future research directions should focus on addressing emerging security challenges, exploring new AI techniques, and ensuring the responsible and ethical use of AI in IoT security.

REFERENCES

[1] M. Shen, A. Gu, J. Kang, X. Tang, X. Lin, L. Zhu, and D. Niyato, "Blockchains for artificial intelligence of things: A comprehensive survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14483–14506, Aug. 2023.

[2] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, p. 1788, Apr. 2019.

[3] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma'a, "Machine learning and the Internet of Things security: Solutions and open challenges," *J. Parallel Distrib. Comput.*, vol. 162, pp. 89–104, Apr. 2022.

[4] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022.

[5] R. Singh and S. S. Gill, "Edge AI: A survey," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 71–92, Mar. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000196

[6] K. Zheng, R. Luo, Z. Wang, X. Liu, and Y. Yao, "Short-term and long-term throughput maximization in mobile wireless-powered Internet of Things," *IEEE Internet Things J.*, Early Access, Oct. 23, 2023, doi: 10.1109/JIOT.2023.3326440.

[7] X. Liu, B. Xu, K. Zheng, and H. Zheng, "Throughput maximization of wireless-powered communication network with mobile access points," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4401–4415, Jul. 2023.

[8] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT," *J. Parallel Distrib. Comput.*, vol. 134, pp. 198–206, Dec. 2019.

[9] M. H. Panahi Rizi and S. A. Hosseini Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet Things*, vol. 20, Nov. 2022, Art. no. 100584.

[10] S. A. Baho and J. Abawajy, "Analysis of consumer IoT device vulnerability quantification frameworks," *Electronics*, vol. 12, no. 5, p. 1176, Feb. 2023.

[11] S. E. Ali, N. Tariq, F. A. Khan, M. Ashraf, W. Abdul, and K. Saleem, "BFT-IoMT: A blockchain-based trust mechanism to mitigate Sybil attack using fuzzy logic in the Internet of Medical Things," *Sensors*, vol. 23, no. 9, p. 4265, Apr. 2023.

[12] S. A. Moqurrab, A. Anjum, N. Tariq, and G. Srivastava, "Instant_Anonymity: A lightweight semantic privacy guarantee for 5G-enabled IIoT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 951–959, Jan. 2023.

[13] M. Hanif, H. Ashraf, Z. Jalil, N. Z. Jhanjhi, M. Humayun, S. Saeed, and A. M. Almuhaideb, "AI-based wormhole attack detection techniques in wireless sensor networks," *Electronics*, vol. 11, no. 15, p. 2324, Jul. 2022.

[14] S. A. Moqurrab, N. Tariq, A. Anjum, A. Asheralieva, S. U. R. Malik, H. Malik, H. Pervaiz, and S. S. Gill, "A deep learning-based privacy-preserving model for smart healthcare in Internet of Medical Things using fog computing," *Wireless Pers. Commun.*, vol. 126, no. 3, pp. 2379–2401, Oct. 2022.

[15] C. S. Kalutharage, X. Liu, C. Chrysoulas, N. Pitropakis, and P. Papadopoulos, "Explainable AI-based DDOS attack identification method for IoT networks," *Computers*, vol. 12, no. 2, p. 32, Feb. 2023.

[16] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of IoT security challenges and its solutions using artificial intelligence," *Brain Sci.*, vol. 13, no. 4, p. 683, Apr. 2023.

[17] A. K. Abed and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," *Secur. Privacy*, vol. 6, no. 3, p. e285, May 2023.

[18] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial intelligence-based cyber security in the context of Industry 4.0—A survey," *Electronics*, vol. 12, no. 8, p. 1920, Apr. 2023.

[19] S. S. Gopalan, A. Raza, and W. Almobaideen, "IoT security in healthcare using AI: A survey," in *Proc. Int. Conf. Commun., Signal Process., Appl. (ICCSPA)*, Mar. 2021, pp. 1–6.

[20] H. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing Internet of Things security: A survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020.

[21] 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.

[22] M. Kuzlu, C. Fair, and O. Guler, "Role of artificial intelligence in the Internet of Things (IoT) cybersecurity," *Discover Internet Things*, vol. 1, no. 1, pp. 1–14, 2021.

[23] A. Atutxa, J. Astorga, M. Barcelo, A. Urbieta, and E. Jacob, "Improving efficiency and security of IIoT communications using in-network validation of server certificate," *Comput. Ind.*, vol. 144, Jan. 2023, Art. no. 103802.

[24] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018.

[25] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, "Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," *IEEE Access*, vol. 8, pp. 104956–104966, 2020.

[26] S. El Jaouhari and E. Bouvet, "Secure firmware over-the-air updates for IoT: Survey, challenges, and discussions," *Internet Things*, vol. 18, May 2022, Art. no. 100508.

[27] D. Sun, J. Hu, H. Wu, J. Wu, J. Yang, Q. Z. Sheng, and S. Dustdar, "A comprehensive survey on collaborative data-access enablers in the IIoT," *ACM Comput. Surv.*, vol. 56, no. 2, pp. 1–37, Sep. 2023, doi: 10.1145/3612918.

[28] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet Things Cyber-Physical Syst.*, vol. 4, pp. 167–185, Jan. 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000585

[29] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap," *Sensors*, vol. 21, no. 11, p. 3901, Jun. 2021.

[30] P. Leitão, S. Karnouskos, T. I. Strasser, X. Jia, J. Lee, and A. W. Colombo, "Alignment of the IEEE industrial agents recommended practice standard with the reference architectures RAMI4.0, IIRA, and SGAM," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 98–111, 2023.

[31] P. Dhoni and R. Kumar, "Synergizing generative AI and cybersecurity: Roles of generative AI entities, companies, agencies, and government in enhancing cybersecurity," *TechRxiv*, Aug. 2023, doi: 10.36227/techrxiv.23968809.v1.

[32] T. U. Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, "CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 3, p. e4224, Mar. 2021.

[33] M. Javed, N. Tariq, M. Ashraf, F. A. Khan, M. Asim, and M. Imran, "Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled Gini index framework," *Sensors*, vol. 23, no. 23, p. 9372, Nov. 2023.

[34] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *J. Sensor Actuator Netw.*, vol. 8, no. 1, p. 16, Feb. 2019.

[35] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4319–4330, Jul. 2022.

[36] S. Chakkaravarthy Sethuraman, A. Mitra, K.-C. Li, A. Ghosh, M. Gopinath, and N. Sukhija, "Loki: A physical security key compatible IoT based lock for protecting physical assets," *IEEE Access*, vol. 10, pp. 112721–112730, 2022.

[37] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on deep learning approaches for IoT security," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100389.

[38] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[39] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[40] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and Industry 4.0," *IEEE Consum. Electron. Mag.*, vol. 11, no. 2, pp. 51–56, Mar. 2022.

[41] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[42] Q. Liu, H. Zhang, J. Wan, and X. Chen, "An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing Internet of Things," *IEEE Access*, vol. 5, pp. 7001–7011, 2017.

[43] 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.

[44] P. Li, J. Su, and X. Wang, "ITLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6828–6841, Aug. 2020.

[45] Q. Chen, H. Chen, Y. Cai, Y. Zhang, and X. Huang, "Denial of service attack on IoT system," in *Proc. 9th Int. Conf. Inf. Technol. Med. Educ. (ITME)*, Oct. 2018, pp. 755–758.

[46] M. Al-Mashhadani and M. Shujaa, "IoT security using AES encryption technology based ESP32 platform," *Int. Arab J. Inf. Technol.*, vol. 19, no. 2, pp. 214–223, 2022.

[47] A. S. Reegan and V. Kabila, "Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT," *Wireless Pers. Commun.*, vol. 118, no. 2, pp. 1313–1329, May 2021.

[48] M. R. Alagheband and A. Mashatan, "Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: Taxonomy, capabilities, and objectives," *Internet Things*, vol. 18, May 2022, Art. no. 100492.

[49] U. Farooq, M. Asim, N. Tariq, T. Baker, and A. I. Awad, "Multi-mobile agent trust framework for mitigating internal attacks and augmenting RPL security," *Sensors*, vol. 22, no. 12, p. 4539, Jun. 2022.

[50] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Appl. Sci.*, vol. 9, no. 5, p. 848, Feb. 2019.

[51] M. A. Husnoo, A. Anwar, R. K. Chakrabortty, R. Doss, and M. J. Ryan, "Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey," *IEEE Access*, vol. 9, pp. 153276–153304, 2021.

[52] F. Neves, R. Souza, J. Sousa, M. Bonfim, and V. Garcia, "Data privacy in the Internet of Things based on anonymization: A review," *J. Comput. Secur.*, vol. 31, no. 3, pp. 261–291, May 2023.

[53] T. Geng, L. Njilla, and C.-T. Huang, "Delegated proof of secret sharing: A privacy-preserving consensus protocol based on secure multiparty computation for IoT environment," *Network*, vol. 2, no. 1, pp. 66–80, Jan. 2022.

[54] T. Alam and R. Gupta, "Federated learning and its role in the privacy preservation of IoT devices," *Future Internet*, vol. 14, no. 9, p. 246, 2022.

[55] S. Hadzovic, S. Mrdovic, and M. Radonjic, "A path towards an Internet of Things and artificial intelligence regulatory framework," *IEEE Commun. Mag.*, vol. 61, no. 7, pp. 90–96, Jul. 2023.

[56] P. Dixit, P. Bhattacharya, S. Tanwar, and R. Gupta, "Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey," *Exp. Syst.*, vol. 39, no. 5, Jun. 2022, Art. no. e12754.

[57] J. Kipongo, T. G. Swart, and E. Esenogho, "Design and implementation of intrusion detection systems using RPL and AOVD protocols-based wireless sensor networks," *Int. J. Electron. Telecommun.*, vol. 69, pp. 309–318, Dec. 2022.

[58] A. Yahyaoui, H. Lakhdhar, T. Abdellatif, and R. Attia, "Machine learning based network intrusion detection for data streaming IoT applications," in *Proc. 21st ACIS Int. Winter Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. (SNPD-Winter)*, Jan. 2021, pp. 51–56.

[59] C. M. V. Wong, R. Y.-Y. Chan, Y. N. Yum, and K. Wang, "Internet of Things (IoT)-enhanced applied behavior analysis (ABA) for special education needs," *Sensors*, vol. 21, no. 19, p. 6693, Oct. 2021.

[60] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100075.

[61] S. Bettayeb, M.-L. Messai, and S. M. Hemam, "A robust and efficient vector-based key management scheme for IoT networks," *Ad Hoc Netw.*, vol. 149, Oct. 2023, Art. no. 103250.

[62] H. Meddeb, Z. Abdellaoui, and F. Houaidi, "Development of surveillance robot based on face recognition using raspberry-PI and IoT," *Microprocess. Microsyst.*, vol. 96, Feb. 2023, Art. no. 104728.

[63] P. Spachos, S. Gregori, and M. J. Deen, "Voice activated IoT devices for healthcare: Design challenges and emerging applications," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 7, pp. 3101–3107, Jul. 2022.

[64] A. S. Martey, A. Ali, and E. Ebenezer, "AI-based palm print recognition system for high-security applications," in *Proc. IEEE AFRICON*, Sep. 2023, pp. 1–6.

[65] C. Annadurai, I. Nelson, K. Devi, R. Manikandan, N. Jhanjhi, M. Masud, and A. Sheikh, "Biometric authentication-based intrusion detection using artificial intelligence Internet of Things in smart city," *Energies*, vol. 15, no. 19, p. 7430, Oct. 2022.

[66] J. Guo, A. Liu, K. Ota, M. Dong, X. Deng, and N. N. Xiong, "ITCN: An intelligent trust collaboration network system in IoT," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 203–218, Jan. 2022.

[67] Z. Rehman, N. Tariq, S. A. Moqurrab, J. Yoo, and G. Srivastava, "Machine learning and Internet of Things applications in enterprise architectures: Solutions, challenges, and open issues," *Exp. Syst.*, vol. 41, no. 1, Jan. 2024, Art. no. e13467.

[68] S. Ayvaz and K. Alpay, "Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time," *Exp. Syst. Appl.*, vol. 173, Jul. 2021, Art. no. 114598.

[69] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani, A. Hosseinian-Far, and A. Daneshkhah, "Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*. London, U.K.: IEEE, 2021, pp. 47–64.

[70] S. Samtani, Y. Chai, and H. Chen, "Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep structured semantic model," *MIS Quart.*, vol. 46, no. 2, pp. 911–946, May 2022.

[71] M. Chen and W. Du, "The predicting public sentiment evolution on public emergencies under deep learning and Internet of Things," *J. Supercomput.*, vol. 79, no. 6, pp. 6452–6470, Apr. 2023.

[72] D. Tomar, "A network architecture for secure traffic management for the Internet of Things using virtual local area network," *Int. J. Comput. Trends Technol.*, vol. 68, no. 12, pp. 11–14, Dec. 2020.

[73] G. Pattewar, N. Mahamuni, H. Nikam, O. Loka, and R. Patil, "Management of IoT devices security using blockchain—A review," in *Sentimental Analysis and Deep Learning*. Singapore: Springer, 2022, pp. 735–743.

[74] N. Sambandam, M. Hussein, N. Siddiqi, and C.-H. Lung, "Network security for IoT using SDN: Timely DDoS detection," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Dec. 2018, pp. 1–2.

[75] A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, and A. Ghosh, "Blockchain-based model for expanding IoT device data security," in *Advances in Applications of Data-Driven Computing*. Singapore: Springer, 2021, pp. 61–71.

[76] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access control for IoT: A survey of existing research, dynamic policies and future directions," *Sensors*, vol. 23, no. 4, p. 1805, Feb. 2023.

[77] S. Alyahya, W. U. Khan, S. Ahmed, S. N. K. Marwat, and S. Habib, "Cyber secure framework for smart agriculture: Robust and tamper-resistant authentication scheme for IoT devices," *Electronics*, vol. 11, no. 6, p. 963, 2022.

[78] Z. Ling, H. Yan, X. Shao, J. Luo, Y. Xu, B. Pearson, and X. Fu, "Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT nodes," *J. Syst. Archit.*, vol. 119, Oct. 2021, Art. no. 102240.

[79] O. I. Khalaf, M. Sokiyna, Y. Alotaibi, A. Alsufyani, and S. Alghamdi, "Web attack detection using the input validation method: DPDA theory," *Comput., Mater. Continua*, vol. 68, no. 3, pp. 3167–3184, 2021.

[80] A. Basati and M. M. Faghih, "APAE: An IoT intrusion detection system using asymmetric parallel auto-encoder," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 4813–4833, Mar. 2023.

[81] J. Kaur, U. Garg, and G. Bathla, "Detection of cross-site scripting (XSS) attacks using machine learning techniques: A review," *Artif. Intell. Rev.*, vol. 56, no. 11, pp. 12725–12769, Nov. 2023.

[82] W.-J. Tsaur, J.-C. Chang, and C.-L. Chen, "A highly secure IoT firmware update mechanism using blockchain," *Sensors*, vol. 22, no. 2, p. 530, Jan. 2022.

[83] A. Fatima, T. A. Khan, T. M. Abdellatif, S. Zulfiqar, M. Asif, W. Safi, H. A. Hamadi, and A. H. Al-Kassem, "Impact and research challenges of penetrating testing and vulnerability assessment on network threat," in *Proc. Int. Conf. Bus. Analytics Technol. Secur. (ICBATS)*, Mar. 2023, pp. 1–8.

[84] M. Rak, G. Salzillo, and D. Granata, "ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107721.

[85] M. Rashid, S. A. Parah, A. R. Wani, and S. K. Gupta, "Securing e-health IoT data on cloud systems using novel extended role based access control model," in *Internet of Things (IoT)*. Cham, Switzerland: Springer, 2020, pp. 473–489.

[86] S. Ameer, J. Benson, and R. Sandhu, "An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach," *Information*, vol. 13, no. 2, p. 60, Jan. 2022.

[87] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," in *Proc. Int. Conf. IoT Appl. (ICIOT)*, May 2017, pp. 1–4.

[88] H. Goyal and S. Saha, "Multi-party computation in IoT for privacy-preservation," in *Proc. IEEE 42nd Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2022, pp. 1280–1281.

[89] A. Mohiyuddin, A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, "Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system," *Int. J. Fuzzy Syst.*, vol. 24, no. 2, pp. 1203–1215, Mar. 2022.

[90] M. A. Hashmi and N. Tariq, "An efficient substitution box design with a chaotic logistic map and linear congruential generator for secure communication in smart cities," *EAI Endorsed Trans. Smart Cities*, vol. 7, no. 1, p. e5, Mar. 2023.

[91] J. S. Khan, S. K. Kayhan, I. S. Tawfic, and N. Tariq, "Chaos-based secured modified strong recovery conditions for least support orthogonal matching pursuit in the noisy case," in *Proc. Int. Conf. Commun., Comput. Digit. Syst. (C-CODE)*, 2023, pp. 1–4.

[92] Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1333–1345, May 2018.

[93] M. Hao, H. Li, G. Xu, S. Liu, and H. Yang, "Towards efficient and privacy-preserving federated deep learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[94] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system," *Int. J. Environ. Res. Public Health*, vol. 16, no. 9, p. 1490, Apr. 2019.

[95] M. Azimeh and H. Friborg, "Privacy in smart homes using privacy impact assessment to inspect privacy issues in a smart home," M.S. thesis, Fac. Eng. Sci., Dept. Inf. Commun. Technol., Univ. Agder, Kristiansand, Norway, 2022.

[96] I. Kök, F. Y. Okay, Ö. Muyanli, and S. Özdemir, "Explainable artificial intelligence (XAI) for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14764–14779, Aug. 2023.

[97] M. H. Kabir, K. F. Hasan, M. K. Hasan, and K. Ansari, "Explainable artificial intelligence for smart city application: A secure and trusted platform," in *Explainable Artificial Intelligence for Cyber Security: Next Generation Artificial Intelligence*. Cham, Switzerland: Springer, 2022, pp. 241–263.

[98] U. A. Usmani, A. Happonen, and J. Watada, "Human-centered artificial intelligence: Designing for user empowerment and ethical considerations," in *Proc. 5th Int. Congr. Human-Comput. Interact., Optim. Robotic Appl. (HORA)*, 2023, pp. 01–05.

[99] R. El-Haddadeh, A. Fadlalla, and N. M. Hindi, "Is there a place for responsible artificial intelligence in pandemics? A tale of two countries," *Inf. Syst. Frontiers*, vol. 25, no. 6, pp. 2221–2237, Dec. 2023.
[100] D. Tjondronegoro, E. Yuwono, B. Richards, D. Green, and S. Hatakka, "Responsible AI implementation: A human-centered framework for accelerating the innovation process," 2022, *arXiv:2209.07076*.
[101] R. Canetti, U. Feige, O. Goldreich, and M. Naor, "Adaptively secure multi-party computation," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 639–648.
[102] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare Internet of Things," *Wireless Netw.*, vol. 27, no. 8, pp. 5503–5509, Nov. 2021.
[103] 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.
[104] J. Kukade and P. Panse, "Advanced deep learning model for anomaly detection based video surveillance system," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 5, pp. 477–485, 2024.
[105] A. Mumtaz, A. B. Sargano, and Z. Habib, "AnomalyNet: A spatiotemporal motion-aware CNN approach for detecting anomalies in real-world autonomous surveillance," *Vis. Comput.*, vol. 9, pp. 1–22, Jan. 2024.
[106] X. Li, H. Zhao, Y. Feng, J. Li, Y. Zhao, and X. Wang, "Research on key technologies of high energy efficiency and low power consumption of new data acquisition equipment of power Internet of Things based on artificial intelligence," *Int. J. Thermofluids*, vol. 21, Feb. 2024, Art. no. 100575.
[107] H. Nguyen, D. Nawara, and R. Kashef, "Connecting the indispensable roles of IoT and artificial intelligence in smart cities: A survey," *J. Inf. Intell.*, pp. 2–73, Jan. 2024.
[108] J. R. Madhukaro and D. Rao, "SVM-GA based a novel technique for the detection of the vehicle in an optimized overlapped multi-camera system," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 1, pp. 810–818, 2024.
[109] J. Prakash, L. Murali, N. Manikandan, N. Nagaprasad, and K. Ramaswamy, "A vehicular network based intelligent transport system for smart cities using machine learning algorithms," *Sci. Rep.*, vol. 14, no. 1, p. 468, Jan. 2024.
[110] M. Schnieder, "Using explainable artificial intelligence (XAI) to predict the influence of weather on the thermal soaring capabilities of sailplanes for smart city applications," *Smart Cities*, vol. 7, no. 1, pp. 163–178, Jan. 2024.
[111] P. Elamparithi, S. Kalaivani, S. Vijayalakshmi, E. Keerthika, S. Koteswari, and R. S. Raaj, "A machine learning approach for detecting DDOS attack in IoT network using random forest classifier," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 2s, pp. 495–502, 2024.
[112] W. Yan, Z. Wang, H. Wang, W. Wang, J. Li, and X. Gui, "Survey on recent smart gateways for smart home: Systems, technologies, and challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4067, Jun. 2022.
[113] C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, "An enhanced AI-based network intrusion detection system using generative adversarial networks," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2330–2345, Feb. 2023.
[114] M. Das Nath and T. Bhattasali, "Anomaly detection using machine learning approaches," *Azerbaijan J. High Perform. Comput.*, vol. 3, no. 2, pp. 196–206, Dec. 2020.
[115] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: A survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, Mar. 2021.
[116] N. Priya, "Cybersecurity considerations for industrial IoT in critical infrastructure sector," *Int. J. Comput. Org. Trends*, vol. 12, no. 1, pp. 27–36, Apr. 2022.
[117] C. Zhao, Y. Lv, J. Jin, Y. Tian, J. Wang, and F.-Y. Wang, "DeCAST in TransVerse for parallel intelligent transportation systems and smart cities: Three decades and beyond," *IEEE Intell. Transp. Syst. Mag.*, vol. 14, no. 6, pp. 6–17, 2022.
[118] H. Herath and M. Mittal, "Adoption of artificial intelligence in smart cities: A comprehensive review," *Int. J. Inf. Manag. Data Insights*, vol. 2, no. 1, Apr. 2022, Art. no. 100076.
[119] C. I. Nwakanma, L. A. C. Ahakonye, J. N. Njoku, J. C. Odirichukwu, S. A. Okolie, C. Uzondu, C. C. N. Nweke, and D.-S. Kim, "Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review," *Appl. Sci.*, vol. 13, no. 3, p. 1252, Jan. 2023.
[120] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842.
[121] A. Vangala, A. K. Das, V. Chamola, V. Korotaev, and J. J. P. C. Rodrigues, "Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges," *Cluster Comput.*, vol. 26, no. 2, pp. 879–902, Apr. 2023.
[122] Y. Zhou, Q. Xia, Z. Zhang, M. Quan, and H. Li, "RETRACTED ARTICLE: Artificial intelligence and machine learning for the green development of agriculture in the emerging manufacturing industry in the IoT platform," *Acta Agriculturae Scandinavica, Sect. B-Soil Plant Sci.*, vol. 72, no. 1, pp. 284–299, Dec. 2022.
[123] N. N. Misra, Y. Dixit, A. Al-Mallahi, M. S. Bhullar, R. Upadhyay, and A. Martynenko, "IoT, big data, and artificial intelligence in agriculture and food industry," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6305–6324, May 2022.
[124] T. Jelinek, A. Bhave, N. Buchoud, M. M. Bühler, P. Glauner, O. Inderwildi, M. Kraft, C. Mok, K. Nübel, and A. Voss, "International collaboration: Mainstreaming artificial intelligence and cyberphysical systems for carbon neutrality," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 2, pp. 26–34, 2024.
[125] F. Atsu and P. S. Adams, "New insights in the ICT and environmental degradation: Accounting for policy uncertainty and ICT quality," Elsevier, Amsterdam, The Netherlands, 2024. [Online]. Available: https://ssrn.com/abstract=4688541
[126] G. Wu, X. Chen, Y. Shen, Z. Xu, H. Zhang, S. Shen, and S. Yu, "Combining Lyapunov optimization with actor-critic networks for privacy-aware IIoT computation offloading," *IEEE Internet Things J.*, early access, Jan. 22, 2024, doi: 10.1109/JIOT.2024.3357110.