Received 22 June 2025; accepted 24 July 2025. Date of publication 28 July 2025; date of current version 26 August 2025.

*Digital Object Identifier 10.1109/OJCOMS.2025.3593311*

# Securing AIoT Surveillance: Techniques, Challenges, and Solutions

**KIRAN KHURSHID [1], KHAWAR KHURSHID [2] (Member, IEEE), MUHAMMAD USMAN HADI [3] (Member, IEEE), MOHAMMAD AL BATAINEH [4,5] (Member, IEEE), AND NASIR SAEED [5] (Senior Member, IEEE)**

[1]Department of Computer and Software Engineering, National University of Sciences and Technology, Islamabad 44000, Pakistan
[2]Department of Computer Science, Namal University, Mianwali 42250, Pakistan
[3]School of Engineering, Ulster University (Belfast), BT15 1AP Belfast, U.K.
[4]Department of Electrical and Communication Engineering, UAE University, Al-Ain, UAE
[5]Telecommunications Engineering Department, Yarmouk University, Irbid 21163, Jordan

CORRESPONDING AUTHOR: N. SAEED (e-mail: mr.nasir.saeed@ieee.org)

This work was supported by the Research and Sponsored Projects Office at United Arab Emirates University (UAEU).

**ABSTRACT** The fusion of Artificial Intelligence (AI) and the Internet of Things (IoT) in surveillance systems, known as the Artificial Intelligence of Things (AIoT), represents a major leap in security technology, enabling advanced monitoring and real-time data processing. However, this integration also presents a new frontier of complex security challenges. This comprehensive survey examines the evolving landscape of AIoT security in surveillance, focusing on critical issues such as the integration of heterogeneous devices, vulnerabilities inherent in edge computing and distributed processing, and the increasing threat of adversarial attacks on AI algorithms. We also address regulatory and compliance challenges that arise in this domain. The survey highlights the urgent need for robust security frameworks and proposes cutting-edge solutions, including advanced encryption mechanisms, lightweight communication protocols, and specialized Intrusion Detection and Prevention Systems (IDPS). Furthermore, we emphasize the significance of ethical considerations, particularly the implementation of zero-trust architectures and the necessity for ethical oversight to maintain user trust and ensure regulatory compliance. By synthesizing the latest research and identifying future directions, this paper provides essential insights for advancing AIoT security in surveillance and offers valuable guidance for researchers and industry practitioners navigating this rapidly evolving field.

**INDEX TERMS** Artificial Intelligence of Things, data security, Internet of Things, privacy, surveillance.

## I. INTRODUCTION

THE RAPID evolution of Artificial Intelligence of Things (AIoT) is significantly expanding its role across diverse domains. This advancement is enhancing both everyday life and professional activities. From smart homes and healthcare to smart transportation [1], AIoT is seamlessly integrating into various aspects of life, making them more efficient and convenient. Beyond these applications, AIoT is gaining traction in fields such as environmental sustainability, climate change, and urban development [2], [3], thereby supporting a sustainable future.

By incorporating artificial intelligence (AI) into conventionally non-intelligent devices and connecting them through the Internet and advanced communication networks, AIoT is revolutionizing industries. This integration optimizes resource utilization, enhances productivity, and transforms processes on an unprecedented scale. Mohamed et al. have explored the intersection of AI, Big Data, and IoT, highlighting their collective impact on data management, analytics, and human-machine interaction [4]. The convergence of these technologies enables AIoT systems to gather vast amounts of data from diverse sources, which can then be processed and analyzed through advanced AI techniques

to predict patterns, identify trends, and support decision-making [5].

Recent advancements in AIoT offer transformative opportunities to enhance the functionality of smart cities. Smart cities employ advanced infrastructure to promote sustainability, improve residents' quality of life, and optimize urban services such as public safety, energy management, transportation, waste management, and communication [6]. Among the critical components of smart cities is video surveillance, which equips residents with advanced tools for monitoring their environment while strengthening the city's security framework, thereby contributing to overall safety and stability [7].

The use of surveillance cameras for visual monitoring has become indispensable in today's world, forming a cornerstone of law enforcement and security measures in smart cities to enhance public safety. Traditional digital video surveillance systems primarily focused on public safety, crime prevention, traffic management, building security, and environmental monitoring. However, their capabilities were limited to video capture, storage, and distribution, with threat detection relying heavily on labor-intensive human efforts.

To overcome these limitations, the development of smart video surveillance systems leveraging AIoT represents a significant advancement. This approach integrates advanced AI technologies with IoT to enhance visual surveillance, garnering considerable interest within the computer vision community. The term "smart surveillance" [8], introduced by Langheinrich et al., defines surveillance systems that harness advancements in networking, sensors, cloud computing, and intelligent data processing algorithms. These systems enable the extraction of application-specific intelligence from recorded data, facilitating the sharing, storage, correlation, and analysis of information for informed decision-making [8].

Another definition describes smart surveillance systems as those enhanced by advanced hardware and software technologies to extract and analyze application-specific information from video streams, enabling automated or semi-automated real-time decisions [9]. Key advantages of smart surveillance include:

1) Enhanced Threat Detection: AI improves the speed and accuracy of threat detection compared to human operators, resulting in better overall security.
2) Reduction in False Alarms: AI filters out irrelevant information, such as movements by pets or shadows, significantly reducing false alarms.
3) Immediate Responses: AI can trigger immediate actions, such as activating lights or sirens, enabling faster reactions to security incidents.
4) Data-Driven Insights: Collected data can be analyzed to identify trends, refine security measures, and enhance overall strategies.

A common challenge associated with surveillance is the massive generation of data. Surveillance videos produce significant volumes of unstructured data; however, modern big data infrastructures now enable effective storage and retrieval, adhering to the 9Vs of big data [10]. Recent advancements in signal processing have further enhanced intelligent video surveillance systems, enabling dynamic adjustment of video data collection rates and improved handling of complex datasets.

While integrating AI technologies into IoT infrastructures has shown promising results, AIoT systems still face substantial challenges. These systems inherit vulnerabilities from both IoT and AI technologies. Key issues include inefficiencies, security and privacy concerns, low trust levels, and insufficient incentives [11]. Among these, security and privacy are particularly critical, as the networked nature of AIoT systems increases susceptibility to breaches and attacks. The interconnected devices and continuous data exchanges present numerous potential entry points for malicious actors. Additionally, reliance on cloud services for data processing and storage introduces further vulnerabilities, especially if security protocols are inadequate.

Malicious actors can exploit weaknesses in IoT devices, communication protocols, and AI algorithms to gain unauthorized access, manipulate data, or launch cyberattacks. To address these risks and ensure the integrity and confidentiality of AIoT systems, it is essential to adopt stronger security measures, implement robust encryption techniques, and enforce stringent data privacy regulations.

In this article, we explore the current landscape of AIoT security in surveillance by framing the discussion around the following core research questions: (i) What are the predominant security challenges in AIoT-based surveillance systems? (ii) In what ways do these challenges differ from those encountered in traditional IoT environments? (iii) Which solutions have emerged as the most promising, and how do they compare against existing security solutions in terms of effectiveness? To address these questions, we analyze the security and privacy landscape through the lens of established standards such as ISO 27001, review case studies of significant security breaches, and discuss the specific vulnerabilities and technical challenges unique to AIoT surveillance environments. Furthermore, we propose potential strategies for enhancing system resilience and outline directions for future research and development.

### A. CONTRIBUTIONS OF THIS SURVEY

While existing reviews offer various perspectives on AI and IoT in surveillance, this work addresses a critical gap by focusing specifically on the security challenges and solutions in AIoT-based surveillance systems. The key contributions of this paper are:

1) To the best of our knowledge, this is the first survey that provides an in-depth analysis of the unique challenges, solutions, and future research directions in AIoT-based surveillance systems. Unlike previous works that either address IoT or AI challenges in isolation or focus on specific monitoring systems, this

paper offers a holistic view of the security landscape in AIoT surveillance.
2) We present a detailed investigation into the security and privacy risks inherent in AIoT surveillance. This includes the complexities of integrating heterogeneous devices, vulnerabilities in edge computing environments, data privacy concerns, the susceptibility of AI algorithms to adversarial attacks, and the challenges of regulatory compliance.
3) We conduct a critical analysis of current security standards, such as ISO 27001, in the context of AIoT surveillance. By leveraging real-world case studies, we demonstrate practical challenges and security breaches, offering a grounded perspective on the limitations of existing frameworks in addressing AIoT-specific threats.
4) We propose cutting-edge security solutions tailored to the needs of AIoT surveillance systems. These include advanced encryption methods, lightweight communication protocols, and bespoke Intrusion Detection and Prevention Systems (IDPS). Additionally, we identify the limitations of current research and propose actionable future research directions aimed at enhancing the security, scalability, and efficiency of AIoT surveillance systems.

### B. RELATED WORK

The existing literature on AIoT has explored various aspects of this technology, yet several critical areas, particularly concerning security and privacy in AIoT-based surveillance remain underdeveloped. Several studies have investigated the individual components of AI and IoT within surveillance systems. For instance, early works have discussed the role of IoT in enabling real-time data collection and monitoring in urban environments [12], [13], [14], [15], [16], [17]. Similarly, researchers have investigated the use of AI algorithms in video analytics [18], [19], [20], [21], [22], [23], [24] to improve the detection of suspicious activities. However, these works often treat AI and IoT as distinct entities.

A significant body of research has addressed security concerns in IoT systems. Various extensive reviews have highlighted IoT vulnerabilities [25], [26], [27], [28], [29], [30], including challenges related to device heterogeneity, insecure communication protocols, and inadequate authentication mechanisms. While these studies offer valuable insights, they do not fully consider the additional complexities and security issues introduced when AI is integrated into IoT environments. The integration of AI amplifies security risks due to the need for constant data analysis and model updates, which can be exploited by attackers. For example, AI algorithms used in surveillance systems could be tricked by adversarial inputs, compromising security outcomes. In addition, the increased data flow between devices and AI models expands the attack surface, making these systems more vulnerable to breaches.

The application of AI in surveillance has been extensively studied in the literature [31], [32], [33]. Researchers have also raised ethical and privacy issues about AI-driven decision-making in surveillance contexts [34], [35]. However, again these studies often overlook the integration between AI and IoT within AIoT systems.

Several surveys have started to examine the intersection of AI and IoT, particularly in healthcare and industrial domains [36], [37], [38], [39], [40], [41], [42]. For example, some researchers have provided a comprehensive review of AIoT in healthcare, emphasizing the advantages of integrating AI's analytical capabilities with IoT's connectivity [43], [44]. Other surveys have concentrated on AIoT's impact in smart cities [45], [46], [47].

To our knowledge, no existing survey has specifically addressed security challenges, proposed solutions, and future research directions for AIoT-based surveillance systems. To fill this critical gap, we present the first comprehensive survey that offers an in-depth, holistic analysis of the intricate security landscape, encompassing unique challenges, cutting-edge solutions, and actionable future research directions specifically tailored to AIoT-based surveillance systems.

Table 1 presents a comparison between our survey and existing literature, highlighting that while numerous surveys address various aspects of AI, IoT, or general security, most concentrate on isolated areas or specific domains. Crucially, it demonstrates that no prior survey comprehensively targets the integrated security challenges and solutions within AIoT-based surveillance systems.

### C. METHODOLOGY

Our systematic literature review conducted across prominent academic databases including IEEE Xplore, ACM Digital Library, Scopus, and Web of Science. The searches were conducted using combinations of keywords, focusing primarily on

- AIoT, AI of Things
- Surveillance, Monitoring Systems
- Security, Privacy, Vulnerability, Challenges, Solution
- Adversarial Attacks, Anomaly Detection, ISO 20071
- IDPS for AIoT, Ethical Considerations

We focused on peer-reviewed articles published between January 2018 and May 2025, yielding approximately 2,500 initial results. Our inclusion criteria specifically selected peer-reviewed journal articles, conference papers, and comprehensive surveys that directly addressed security and privacy within AIoT-based systems. Conversely, exclusion criteria filtered out short papers (e.g., workshop abstracts) or those focusing on general IoT/AI security without explicit relevance to AIoT systems. A rigorous two-phase screening process was then implemented, with three researchers independently reviewing titles and abstracts and identifying approximately 450 potentially relevant papers. This was followed by a full-text assessment of these papers against our detailed criteria, ultimately leading to the selection of

**TABLE 1.** Comparative analysis of key features in AIoT security and surveillance survey papers.

| Feature / Aspect Covered | This Survey | IoT Security Surveys ( [25], [26], [27], [28], [29], [30]) | AI in Surveillance ( [31], [32], [33], [34], [35]) | AIoT Reviews ( [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51]) |
|---|---|---|---|---|
| **Primary Focus** | AIoT-based surveillance system security | Broad IoT security | AI in video analytics / surveillance | General AIoT applications (e.g., healthcare, smart city) |
| **Holistic Security View of AI-IoT Integration in Surveillance** | ✓(Comprehensive, unique to AIoT surveillance) | × (IoT only) | × (AI only) | ✓ (General AIoT, but not surveillance-specific security) |
| **Detailed Security & Privacy Risks in AIoT Surveillance** | ✓(Heterogeneous devices, edge vulnerabilities, data privacy, adversarial attacks, regulatory) | Partial (General IoT vulnerabilities) | Partial (AI privacy/ethics) | Partial (General AIoT risks) |
| **Susceptibility of AI Algorithms to Adversarial Attacks (AIoT Surveillance Context)** | ✓(In-depth analysis) | × / Limited | ✓(General AI, not AIoT specific) | Limited / General AIoT |
| **Critical Analysis of Security Standards (e.g., ISO 27001) in AIoT Surveillance Context** | ✓(With case studies) | × / General IoT standards | × | × (Very few emphasize security and privacy standards but lack explicit mention of surveillance data compliance frameworks.) |
| **Real-World Case Studies / Practical Challenges (AIoT Surveillance-specific)** | ✓(Grounded perspective on limitations) | × / General IoT incidents | Limited / General AI incidents | Limited to their specific domains (e.g., healthcare) |
| **Proposed Cutting-Edge Security Solutions Tailored to AIoT Surveillance** | ✓(Advanced encryption, lightweight protocols, bespoke IDPS) | General IoT solutions | General AI defenses | General AIoT solutions |
| **Detailed Discussion on IDPS Tailored for AIoT Surveillance** | ✓ | × | × | × |
| **Actionable Future Research Directions (AIoT Surveillance-specific)** | ✓(Comprehensive, identifying gaps) | General IoT security future directions | General AI security future directions | General AIoT future directions |

250 core papers for synthesis. The extracted key data points included security challenges, proposed solutions, identified vulnerabilities, and future research directions. Subsequently, papers were iteratively categorized based on their primary thematic contributions, directly aligning with the survey's main sections.

### D. ORGANIZATION

The remainder of this paper is organized as follows: Section II examines the current landscape of AIoT security, offering an in-depth discussion of the ISO 27001 domains related to Information Security Management Systems (ISMS). This section also reviews several case studies that illustrate the practical implications of these security standards in AIoT surveillance. Section III addresses the unique security challenges specific to AIoT surveillance systems. These include the integration of heterogeneous devices and protocols, which introduces vulnerabilities, and the security challenges posed by edge computing and distributed processing. Data privacy concerns related to surveillance footage are also explored, along with the risks of adversarial attacks on AI algorithms. Additionally, regulatory and compliance issues in managing surveillance data are discussed. Section IV presents proposed solutions and innovations to address these challenges. This includes advanced encryption methods, standardization efforts in AIoT surveillance, and the development of cutting-edge AI algorithms. The section further explores the adoption of zero-trust security models, the role of specialized security expertise, and the design of IDPS tailored to AIoT surveillance. Ethical considerations and the importance of fostering collaboration among stakeholders are also highlighted. Section V provides a comprehensive discussion of our findings, summarizing the current state of AIoT surveillance security and identifying the gaps that persist. Finally, Section VI concludes with a summary of the key findings and proposes directions for future research in this critical field. Figure 1 offers a concise overview of the key content presented in the paper. Solid boxes denote main contents, while the dotted boxes, color-matched to the solid ones, highlight specific

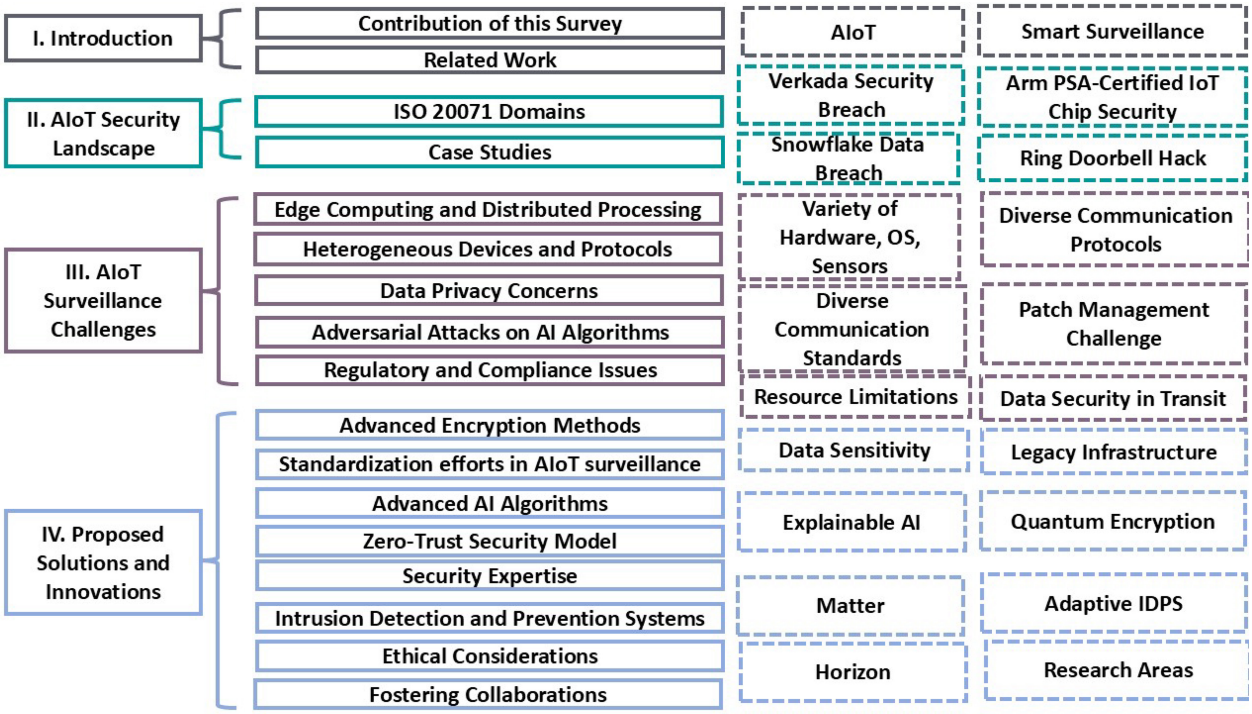



**FIGURE 1.** Overview of the contents of this article.

key areas or examples explored within each respective topic.

## II. CURRENT LANDSCAPE OF AIOT SECURITY

ISO-27001, the international standard for ISMS, outlines essential security specifications across multiple domains to ensure robust protection of information systems [52], [53], [54], [55], [56], [57], [58], [59]. Among these, the most prominent domains include:

### A. COMPANY SECURITY POLICY

This domain emphasizes the need for a well-defined set of guidelines, protocols, and metrics to achieve information security goals. These policies must be clearly established, endorsed by management, and effectively communicated to employees and third-party users. Documentation should cover all procedures, resources, and methods required to meet the project objectives, regardless of the organization's size. Special emphasis should be placed on data protection and data retention regulations. Essential documentation includes risk assessments, log files, scope documentation, and other relevant records. Table 2 provides an overview the required documentation to meet this standard.

### B. ASSET MANAGEMENT

According to this domain, it is crucial for an organization to identify, protect, and manage its assets effectively. Asset management encompasses every phase of the asset lifecycle, including acquisition, utilization, and disposal. It is essential to document the individuals responsible for each asset, track its location, and monitor its condition throughout its lifecycle [60]. Effective asset management contributes to improved performance, lower costs, and reduced risks related to asset ownership and utilization.

**TABLE 2.** Mandatory documentation requirement.

| No. | Documentation Type |
|---|---|
| 1 | ISMS Scope Documentation |
| 2 | Risk Assessment Policy Documentation |
| 3 | Information Security Policy Documentation |
| 4 | Relevant Logs Documentation |
| 5 | Internal Audit Documentation |
| 6 | Training Plans Documentation |
| 7 | Statement of Applicability |
| 8 | Definition of Security Roles and Responsibilities |
| 9 | Information Classification Policy Documentation |
| 10 | Corrective Action Plans Documentation |

### C. PHYSICAL AND ENVIRONMENTAL SECURITY

International ISMS guidelines place significant emphasis on physical security. It is critical in protecting the organization's assets, including as buildings, computers, machines, servers, data, and employees, against unauthorized physical access, theft, or sabotage. Secure areas must be designed to protect valuable equipment and sensitive data from unauthorized access. Environmental security is similarly crucial because unplanned incidents such as power outages or abrupt surges, fires or water leaks, rain, and so on can all pose threats [61]. Environmental security controls safeguard assets against unintentional, intentional, and natural disasters. Both

environmental and physical security are necessary to fortify the defense against vulnerabilities and threats.

### D. ACCESS CONTROL

Access control is intended to protect buildings, individuals, machines, data, and assets by reducing unauthorized access while providing convenience to authorized users. Access is granted based on specific privileges, and managing this process effectively is crucial. A strong access management system is required in order to efficiently manage permissions in organizations. The system should not only permit and revoke access, but also ensure that everything runs smoothly. This system should include regular audits to monitor who has access. Furthermore, it must include automated procedures for managing permissions. The system should have clear guidelines for dealing with exceptions and emergencies.

Apart from this, a formal process for registering and de-registering of users is also crucial [62]. To effectively manage user IDs, strategies should associate IDs with specific users rather than using shared access IDs. If shared IDs are required, they must be approved and documented to ensure accountability.

### E. CRYPTOGRAPHY

Cryptography and encryption are two critical security components that work together to protect data. Cryptography is a field of mathematics that uses algorithms to secure and decipher information [63]. It is the practice of ensuring secure communication in the presence of other parties, whereas encryption is the process of converting readable information into an unreadable format. Its purpose is to prevent unauthorized access to data. If data is not properly secured, it can be easily accessed by anyone outside the organization. To comply with regulatory requirements and meet the expectations of customers who provide sensitive information, organizations must be adaptable and willing to implement the best information security practices. Cryptography is employed to securely share necessary information and identify users, ensuring the exchange of private data. It is the most essential tool for maintaining data integrity and confidentiality. The ISO 27001 standard outlines the criteria for selecting and implementing security controls in Annex A.10 [64].

### F. INCIDENT MANAGEMENT

According to ISO 27001, a security incident is any unwanted event that threatens the availability, confidentiality, or integrity of information. Examples include malware attacks, data breaches, and similar threats. Effective incident management requires thorough preparation, including detection and analysis, eradication, and post-incident activities. To mitigate the impact of security incidents, advanced methods for identifying, analyzing, responding to, and managing these events must be implemented. Additionally, compliance with legal requirements such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 is crucial [65], [66]. These rules require that certain security incidents involving personal data be reported to the relevant authorities. Consequently, security controls should be designed to meet these legal obligations and prevent duplication of efforts or gaps in incident management.

### G. REGULATORY COMPLIANCE

Regulatory compliance refers to an organization adhering to the regulations and laws that govern its activities and operations. Organizations must comply with all applicable local, national, and international legal obligations in order to build customer trust, defend themselves from penalties, and prevent their products and services from being used illegally Furthermore, complying with all of the requirements, whether legislative, regulatory, or contractual, protects firms across all industries from reputational damage. Annex A.18.1 of ISO 27001 focuses on managing legal and contractual responsibilities [67]. Its primary aim is to ensure that all information security obligations, whether they are legal, statutory, regulatory, or contractual, are met to prevent any violations.

In line with current cyberphysical systems (CPS) standards, ISO 27001 encourages a holistic approach to information security management, including the evaluation of people, policies, equipment and technology [50]. An organization may set up systems with enhanced cyber resilience, and efficiency, as well as better risk management, data and asset protection, and overall optimization, by following this standard. The GDPR focuses primarily on personal data protection and privacy, whereas ISO 27001 aims to build information security management. Other well-known security standards include ISO 27002, ISO/IEC 15408, ISO 38500, Control Objectives for Information and Related Technology (COBIT)-5, PRojects IN Controlled Environments (PRINCE)2, Platform Security Architecture (PSA), IEC 62443 (Security for Industrial Automation and Control Systems), and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). NIST 800-53 is a U.S. government standard for information security controls, whereas ISO 27002 is an international standard that gives guidance on implementing and maintaining an ISMS. COBIT framework offers a tool to managers in domains such as risk management, compliance, and value delivery [68], while the NIST Cybersecurity Framework focuses solely on cybersecurity risk management and due to its complex nature can become a difficult tool for small organizations to implement. Some critics claim that the implementation of ISO / IEC 27002 may be too general and lack specificity [69].

In IoT systems, hardware security is extremely critical. In 2019, Arm along with other chip security research organizations developed the PSA certification program to assure the security of IoT chips [70]. The program aims to

improve IoT security by certifying chips that meet industry requirements.

Although there are a number of security standards, AIoT is still a relatively new and emerging field, thus putting these established standards and rules into practice is difficult for such systems. Traditional security techniques frequently struggle to accommodate the inherent complexity of AIoT systems. For example, AIoT often includes a network of interconnected devices with varied security postures, resulting in a greater attack surface. Furthermore, processing data at the source (edge computing) raises significant security concerns as compared to centralized cloud storage. Also, the opacity of some AI algorithms makes it difficult to find and patch embedded vulnerabilities. These variables need a multi-layered security approach tailored to the specific complexities of AIoT systems, which goes beyond mere adherence to existing standards and necessitates a more in-depth understanding of the unique security landscape inside this rapidly changing technological sector.

**Case Studies:**

#### 1) VERKADA SECURITY BREACH

Verkada, a tech company in San Mateo, California, offers cloud-based building security systems. Their technology combines security cameras, door access controls, and even environmental sensors with powerful AI and image analysis software in the cloud. This creates a comprehensive video surveillance system using artificial intelligence. But in 2021, a major security flaw was discovered in Verkada's system, allowing attackers to exploit the vulnerability. Over 150,000 cameras were compromised, exposing sensitive data from all sorts of places like prisons, schools, hospitals, and even companies like Tesla and Nissan [71]. The hackers were also able to download sensitive data from critical organizations including video footage from Verkada's cameras and customer information consisting of names, email addresses, and phone numbers The attackers bypassed the security checks altogether and gained complete control of the cameras remotely. The Verkada attack is an alarming reminder of the risks associated with the AI-powered surveillance systems.

To improve its security, Verkada has now acquired cybersecurity and privacy certifications for the following ISO standards: ISO 27001:2022 for information security management systems; ISO 27017:2015 for cloud service information security controls; and ISO 27018:2019 for personally identifiable information (PII) in public cloud privacy controls [72].

#### 2) ARM PSA-CERTIFIED IOT CHIP SECURITY

An important part of AIoT system includes the IoT chips. Fei Chen et al., investigated the security of an IoT chip certified at PSA Level 2 [70]. Their investigation revealed a critical vulnerability in which the chip leaked a part of the encryption key, significantly compromising its security. They used readily available equipment to gather electromagnetic traces emitted by the chip during its operation. By applying a statistical T-test, they confirmed the presence of physical leakage during the chip's Advanced Encryption Standard (AES) encryption process. Further analysis, employing correlation analysis, pinpointed the specific timeframe within the collected data where the encryption happened. This allowed them to exploit this weakness and recover approximately half (8 bytes) of the 16-byte AES encryption key through a technique called intermediate value correlation analysis.

The experiment was repeated three times with consistent results, highlighting the chip's vulnerability despite its PSA Level 2 certification. This research underscores the need for additional security measures beyond certification standards to safeguard sensitive data in IoT chips.

#### 3) SNOWFLAKE DATA BREACH

Cloud technology is an integral component of AIoT systems. Snowflake, a prominent cloud storage provider, enables businesses to store extensive datasets on its servers. However, it was discovered that criminal hackers attempted to compromise its clients' accounts by using stolen login credentials. This breach is believed to be one of the largest ever, affecting an undisclosed number of client databases and resulting in additional breaches at several other companies, including Ticketmaster and Santander [73].

According to TechCrunch, attackers have gained access to hundreds of Snowflake customer credentials that were found online. These credentials were obtained through infostealing malware that infected the computers of employees with access to their company's (Snowflake) environment [74].

Snowflake reported that hackers specifically targeted customers using single-factor authentication, acquiring their credentials via malware. The company does not enforce multi-factor authentication (MFA), instead allowing users to manage their own security. As Snowflake is a cloud-based product so anyone can sign up for an account at any time. If a threat actor obtains customer credentials, they could potentially access the account [75].

#### 4) RING DOORBELL HACK (MULTIPLE INCIDENTS)

A recent CBS News report (August 2023) highlighted the critical need for cybersecurity in smart home devices like Ring doorbells, following multiple resident reports of hacked devices [76]. Hackers may exploit vulnerabilities to gain unauthorized access to live video feeds, potentially using the two-way talk feature to impersonate visitors or misusing unconfirmed object recognition capabilities for targeted surveillance.

These concerns reflect a growing trend within the security industry, as research by Siwakoti [77] reveals the increasing exploitation of vulnerabilities in Internet-connected devices for domestic intrusion. This example underscores the significant risks associated with the widespread use of AIoT devices in personal spaces.

#### 5) AMAZON FRANCE LOGISTIQUE FINE

The €32 million fine imposed by the French data protection authority (CNIL) on Amazon France Logistique on

December 27, 2023, serves as a pivotal case highlighting the intersection of GDPR, AIoT surveillance, and employee monitoring. The CNIL found that Amazon's system for tracking employee activity and performance in their warehouses was excessively intrusive and violated several aspects of the GDPR. Specifically, the investigation cited violations related to video surveillance conducted without adequate information or sufficient security. Furthermore, the CNIL ruled it illegal to implement a system that measured work interruptions with such precision, potentially compelling employees to justify every break or pause. The authority also deemed the measurement of scanning speed excessive, particularly an indicator that flagged if an item was scanned in less than 1.25 seconds after the previous one, deeming it disproportionate to the stated goals.

More generally, the CNIL deemed the 31-day retention of all collected data and resulting statistical indicators for all employees and temporary workers to be excessive [78]. This landmark fine underscores the critical importance of proportionality and transparency in deploying AIoT-driven monitoring systems, even in high-performance environments.

The above incidents demonstrate weaknesses of AIoT devices. They show that usage of AI for object detection further adds complexity and raises privacy concerns. These incidents expose vulnerabilities in IoT chips, cloud infrastructure, and AI algorithms, while demonstrating the potential consequences of data breaches in AIoT systems. However, it is also important to acknowledge that overly stringent interpretations or enforcement of regulations like GDPR and CCPA can inadvertently stifle innovation and the beneficial deployment of AIoT solutions by creating excessive compliance burdens or discouraging necessary data processing. To mitigate these risks, it is essential to implement robust security measures for AIoT surveillance devices. Furthermore, users must be well-informed about both the advantages and potential risks associated with deploying AIoT devices for surveillance.

## III. UNIQUE SECURITY CHALLENGES IN AIOT SURVEILLANCE

The attributes that make IoT devices ideal for surveillance, such as their compact size and wireless connectivity, also pose significant security risks. Traditional security technologies are often too resource-intensive for these lightweight devices, leaving them vulnerable to hacking. This is particularly concerning because they connect directly to networks. Key factors such as processing power, memory, and battery life are crucial for IoT devices [79]. This creates a fundamental trade-off, as incorporating more advanced security features often comes at the cost of reduced functionality. This lack of security is particularly concerning for surveillance applications, since hackers might exploit these weaknesses to disrupt monitoring, manipulate data, or steal sensitive footage, jeopardizing both security and privacy.

As the preceding real-world examples demonstrate, despite the hype surrounding AIoT devices, vulnerabilities exist throughout the complex network. Each element, from the chip and camera to sensors, networks, and the cloud, presents a potential entry point. Furthermore, AI algorithms themselves can be susceptible to manipulation. Hackers can exploit biases in training data or manipulate data streams to trigger false positives, creating a false sense of security or wasting valuable resources.

Some of the security challenges unique to AIoT surveillance are as follows:

### A. INTEGRATION OF HETEROGENEOUS DEVICES AND PROTOCOLS

The emergence of AIoT has revolutionized surveillance, allowing for extensive monitoring via interconnected sensors and cameras. However, integrating these sensors and cameras into a cohesive AIoT surveillance system is a substantial problem due to the heterogeneity of the devices and protocols [80] and such heterogeneity raises some security concerns as well. First, we will examine the device and protocol heterogeneity in detail, followed by a discussion of the security issues associated with this variability.

#### 1) DEVICE HETEROGENEITY

1) Variety of hardware: Surveillance systems employ a diverse range of devices, from high-resolution cameras with advanced AI processing to simple motion sensors [6]. These variety of hardware components are built for different purposes and integrating them in a heterogeneous arrangement poses different problems as mentioned below:

1) Low-power sensors may need to send data to a central hub with more computing capacity in order to do real-time on-device AI analysis. To achieve the high level of automation required by modern smart IoT applications, sensors integrated into nodes must be effective, intelligent, context aware, dependable, precise, and interconnected [38].
2) Devices have varying storage capacities for captured footage, impacting how long video data can be stored locally before needing transfer. Furthermore, a video has several features that influence its encoding, transmission, and overall quality of experience [81], all of which have an impact on storage.

2) Operating systems: Cameras and sensors often run on different operating systems (e.g., proprietary OS, embedded Linux, and Windows Embedded) [82], which can impact infrastructure efficiency. The advent of smaller operating systems explicitly designed for IoT, such as FreeRTOS, TinyOS, and Contiki, has introduced significant changes [83]. However, these variations make it challenging to manage configurations and updates across the network.

3) Sensors types: The type of sensors used e.g., thermal cameras, facial recognition cameras, license plate readers, create variations in the data collected. This data needs to

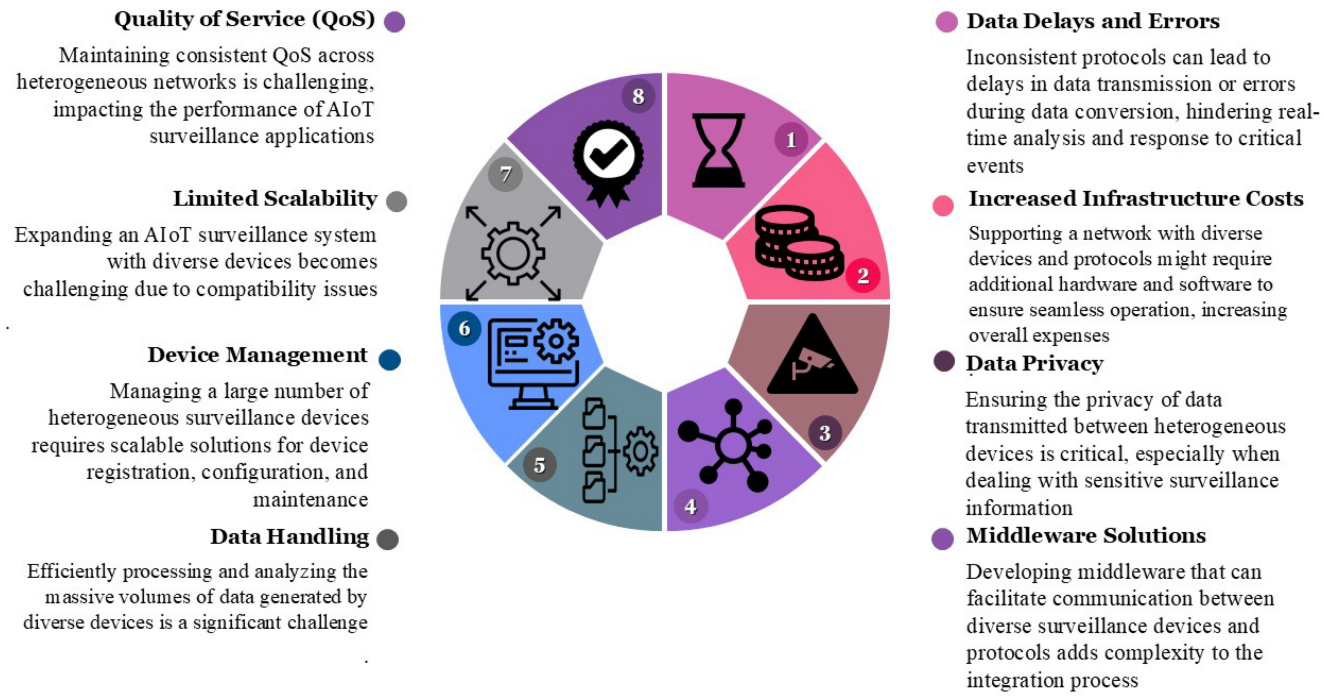



**FIGURE 2.** Adverse effects of system heterogeneity in surveillance system.

be understood and interpreted by the central AI system for effective analysis. Cameras and sensors may generate data in different formats e.g., MJPEG, H.264, H.265, VP9, RTSP, etc., requiring conversion for compatibility with the central AI system. Inconsistent formats can hinder real-time analysis and response [84]. To integrate data from disparate sources, complex transformation processes are required. Ensuring accurate interpretation across all systems demands a common framework or ontology for the exchanged data.

### 2) PROTOCOL HETEROGENEITY

1) Communication standards: A multitude of communication protocols exist for AIoT systems, such as Wi-Fi, cellular networks, Bluetooth Low Energy, LoRaWAN, NB-IoT, etc., for transmitting video footage and sensor data. Additionally, Ultra-Wideband (UWB) is often used for high-speed multimedia communication, while various WPAN standards like Zigbee, IEEE 802.15.4, and Near Field Communication (NFC) are widely used for low-power, short-range communication in Wireless Sensor Networks (WSNs) [85]. These protocols have varying bandwidth limitations, affecting the speed and efficiency of data transfer.

2) Diverse communication protocols: Surveillance devices, such as cameras, sensors, and alarms, often use different communication protocols e.g., MQTT, CoAP, HTTP. Ensuring that these devices can communicate seamlessly is challenging as certain protocols prioritize real-time data delivery for live monitoring, while others are optimized for efficient transmission of large video files after recording. MQTT messages include headers that add some overhead, which can be an issue for very constrained devices or networks [86]. CoAP is designed for constrained environments and uses a lightweight approach that may not provide the reliability needed for some applications [87]. Lack of universal standards for device communication leads to compatibility issues, making it difficult for devices from different manufacturers to work together.

Figure 2 highlights the various adverse effects associated with system heterogeneity.

### 3) SECURITY VULNERABILITIES

1) Exploiting weakest link: MQTT is excellent for lightweight, low-bandwidth communication but can suffer from security and scalability issues [88]. Similarly, CoAP is well-suited for constrained environments but can face challenges with server scalability [89]. HTTP is highly interoperable and widely adopted but can be too heavy and resource-intensive for many IoT applications [90]. As AIoT devices differ in hardware capabilities such as power consumption, connectivity, and transmission coverage, it is difficult to identify appropriate communication mediums and protocols for use within AIoT device boundaries.

The architecture, hardware, sensors, cameras, energy approaches, and all the layers from physical to application/business have so many variants, linking one architecture to another can differ significantly. These inconsistencies create vulnerabilities that can be exploited for unauthorized access, data breaches, or manipulation of surveillance footage. A single device with a weak security protocol can become the entry point for attackers. Hackers can exploit these vulnerabilities to gain access to the entire network, steal sensitive data, or manipulate surveillance footage.

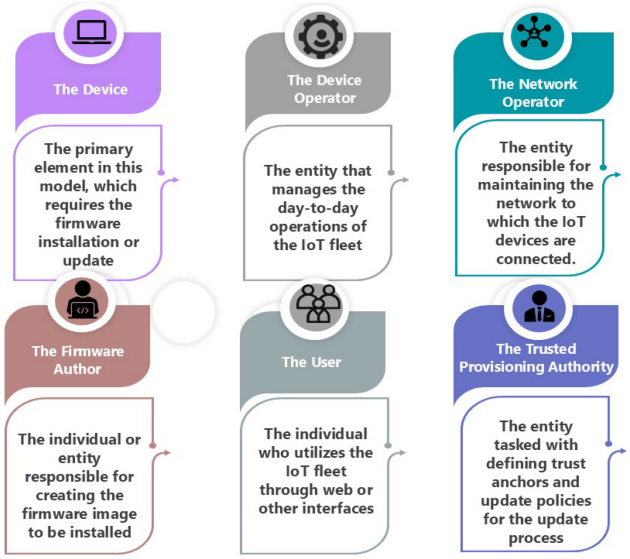



**FIGURE 3.** Key stakeholders involved in the firmware update process.

If the surveillance footage contains PII or facial recognition, it demands strong privacy protection. However, the security protocols may differ across all the devices. This increases the risk of unauthorized access and misuse of sensitive information. The overall security system must be strong e.g., if one camera has strong encryption but another sensor uses weaker protocol it can result in vulnerabilities. This inconsistency in design can leave gaps in protection of sensitive information.

2) Patch management challenges: Each device in AIoT surveillance system operates with its own unique system, firmware, and software application. Keeping all these updates with the latest security patches becomes very difficult. In order to secure the overall system, it is essential to ensure that every device receives latest security updates. Different update schedules and mechanisms make this procedure very complex. The IETF Software Updates for Internet of Things (SUIT) group has identified six key stakeholders involved in the firmware update process [91]. Figure 3 illustrates these stakeholders and their roles in the process.

The identified stakeholders represent the minimal set typically present in an IoT deployment. However, in some instances, certain roles may be consolidated within a single entity; for example, the network operator and device operator might be the same organization.

Coordinating firmware updates across a large-scale AIoT surveillance system is often logistically complex and time-consuming. A critical aspect of designing and deploying a secure firmware update system is the clear definition of the security properties that must be ensured, along with any associated deployment constraints. An insecure update system can introduce greater security risks than the vulnerabilities it seeks to address [91].

Managing security patch updates across AIoT devices presents substantial issues particularly when devices have limited processing power or storage capacity, making it difficult to install large software updates. Neglecting patch management can lead to severe consequences. Unpatched vulnerabilities create openings for attackers, potentially resulting in unauthorized access, data breaches, and system disruptions. In surveillance systems this can lead to compromised video footage, enable surveillance abuse, or even allows attackers to manipulate the system for malicious purposes.

3) Real-time threat detection: AIoT surveillance systems rely on a sophisticated network of interconnected devices and protocols to provide a comprehensive view of the monitored locations. While diversity improves the system's capabilities, it also brings weaknesses. Delays induced by data conversion and compatibility concerns can result in a large time lag between a real-world event and its analysis by the central AI system. Such delay can have major effects, such as failing to notice critical security incidents in a timely manner, limiting the ability to respond to threats efficiently and compromising overall security. For example, delays in processing data due to heterogeneity can result in missing crucial real-time events [92], such as a suspicious individual entering a restricted area or someone brandishing a weapon. Even a slight delay in threat identification can severely impact the security team's response effectiveness. By the time the system issues an alert, the perpetrator may have already fled or inflicted harm. Real-time surveillance data analysis is vital for security personnel to make informed decisions based on the most recent information. However, delays caused by data inconsistency can force reliance on outdated information, increasing the likelihood of poor decision-making that could escalate a situation.

Additionally, existing surveillance systems often rely on older, less secure infrastructure that may struggle to integrate with newer AIoT devices and protocols. This incompatibility can create significant security vulnerabilities that must be addressed [93].

### B. EDGE COMPUTING AND DISTRIBUTED PROCESSING VULNERABILITIES

In contrast to using distant and centralized cloud data center resources, fog/edge computing is an emerging computing paradigm that leverages decentralized resources at the network's edge to process data closer to user devices, such as smartphones and tablets [94]. Edge-based AIoT systems use less bandwidth for data transfers, avoiding potential delays in data analysis. The incorporation of edge computing and distributed processing into AIoT surveillance systems provides numerous benefits, including faster response times, reduced network load, and increased privacy by keeping some data analysis local. However, these advancements also introduce specific security challenges. In this section, the vulnerabilities in edge computing will first be examined, followed by those in distributed processing, and finally, the unique security challenges arising

from these, specific to AIoT surveillance systems, will be addressed.

### 1) EDGE COMPUTING VULNERABILITIES

1) Resource limitations: Edge devices often have lower processing power, storage, and memory than centralized servers, making them more vulnerable to a variety of security threats. These include brute-force attacks, where attackers attempt to gain access through repeated trial-and-error; overprivileged attacks, where an app or device is given excessive access rights beyond what is necessary; jamming attacks, a type of denial-of-service (DoS) attack that disrupts communication; distributed denial-of-service (DDoS) attacks, which can overwhelm and drain resources from edge nodes; and zero-day attacks, which exploit previously unknown vulnerabilities in the device's code. Additionally, non-network side-channel attacks can compromise edge nodes by extracting critical information even when data is not being transmitted, potentially hindering their ability to enforce robust security measures [95], [96].

Smith et al. demonstrated the impact of various battery-draining attacks on edge nodes, including hello flooding, packet flooding, selective forwarding, rank attacks, and versioning attacks [97]. Their findings showed that these attacks could significantly increase energy consumption and disrupt device operations. Notably, their research highlighted the stretch attack, which alters packet headers to force longer travel routes, draining the device's battery within 60 minutes even with a relatively small number of packets.

2) Physical access: Edge devices are often physically located on-site, making them more susceptible to tampering and theft. This can compromise sensitive data stored locally or give attackers a foothold in the network [98]. Attackers can then modify the operating system or software, interfere with the circuit, or extract sensitive and valuable cryptographic data. Tempering the device may cause it to malfunction or provide the attacker with a backdoor into the system. Another attack is differential power analysis (DPA). DPA can involve statistically analyzing a device's power consumption in order to potentially extract encryption information. In some cases, physical access may be required to connect the monitoring equipment to the device. DPA is a more effective and advanced approach, where a larger number of traces are statistically analyzed to obtain encryption information [99]. Edge devices are more susceptible to hardware trojans and DoS attacks. DoS attacks aim to block legitimate users from accessing resources. For example, attackers might force devices out of low-power sleep mode, draining their batteries, or jam radio signals to disrupt communication. Additionally, attackers can tamper with the physical packaging of the device itself. This could involve stealing cryptographic keys, modifying software to make malicious nodes appear legitimate, or even attempting to reverse engineer the device's communication protocols to understand how it works and potentially gain access to user data [99]. The aim of hardware attackers is to steal, alter, or expose information on an IoT device, bypassing security measures. They can do this remotely or directly access the device. There are three main types of hardware attacks, differing in how they interact with the device [100], [101], [102]:

1) Invasive: Requires significant expertise and equipment to physically damage the device's core components, like reverse engineering, cloning, battery drainage, or tampering.
2) Semi-invasive: Analyzes the device's functionality and tests its security circuits without causing harm, often focusing on the chip's surface e.g., imaging attacks, hardware trojans, etc.
3) Non-invasive: Targets the device physically but avoids destruction. This might involve side-channel attacks that exploit unintentional information leaks.

3) Software vulnerabilities: The rapidly growing field of edge computing promises real-time data processing and localized decision-making. However, a critical vulnerability exists beneath the surface, i.e., software running on edge devices. Unlike traditional servers housed in secure data centers, edge devices are frequently deployed on-site, closer to the data source. This deployment strategy emphasizes efficiency, which frequently results in the use of specialized operating systems designed for low power consumption and limited processing power [103]. However, this emphasis on efficiency may come at a cost of security. Similarly, edge device operating systems may not receive security updates as frequently as their server counterparts [104], and this update gap leaves them exposed to known vulnerabilities that attackers can readily exploit.

According to the Kratos report [105], on April 24, 2024, Cisco Talos identified two vulnerabilities in Cisco Adaptive Security Appliances. In a campaign known as "ArcaneDoor," nation-state actors exploited these vulnerabilities to conduct espionage on government entities. Researchers observed a trend of attacks targeting edge network devices over the last two years, highlighting the impact that these exploits can have on businesses.

4) Limited security expertise: Organizations deploying edge devices may not have the in-house expertise to properly configure and secure these devices, increasing the risk of misconfigurations and security gaps [106]. Lack of trained workers is the reason most of the organizations and people avoid implementing IoT and most of the companies with active IoT initiatives are trying to cope with a shortage of skilled laborers [3].

### 2) DISTRIBUTED PROCESSING VULNERABILITIES

The AIoT architecture is distributed, which promotes scalability, flexibility, reliability, and robustness. It decentralizes data processing and decision-making, resulting in more efficient device management across numerous sites. This architecture also allows for real-time processing in multiple locations, lowering latency and improving responsiveness. It promotes improved resource allocation and energy efficiency,

allowing AIoT systems to adapt to a variety of applications while also providing faster response times. However, despite the benefits, there are some risks connected with distributed processing, which are outlined below:

1) Single point of failure (SPOF): If a central processing hub or communication channel fails, real-time data processing suffers, potentially leading to delays in critical decision-making [107]. Furthermore, Xu et al. [108] investigated the security implications of SPOFs in AIoT. A central hub failure could masked security personnel to crucial events, creating a window of opportunity for cyberattacks to go undetected [109]. This emphasizes the need for more resilient AIoT architectures that can tolerate failures without compromising system functionality or security posture.

2) Data security in transit: Data transmitted between edge devices and the central processing unit is vulnerable to interception if proper encryption methods are not used. Man-in-the-middle attacks may compromise sensitive surveillance footage or sensor data. Data must be protected even when attacks like DoS and eavesdropping are taking place. In 2020, a vulnerability known as "Ripple20" was discovered, affecting millions of IoT devices from a variety of industries, including edge computing. This vulnerability enabled attackers to run malicious code remotely, resulting in data breaches or system compromise [110], [111].

Generally cryptographic protocols do not always meet the growing security demands. These motivations are primarily linked to maintaining compatibility with middleboxes, backward compatibility with older systems, a lower availability of the chosen protocol version, and some recent attacks [112].

Attackers can flood the central processing unit with requests, exhausting its resources and preventing it from processing legitimate data from edge devices. The distribution of processing tasks across multiple locations raises concerns about data privacy. Ensuring data anonymization and access control throughout the processing chain is critical for preventing unauthorized access or misuse of personal information.

### 3) UNIQUE CHALLENGES FOR AIOT SURVEILLANCE

1) Data sensitivity: The GDPR's privacy regulation for personal data, and the protection and supervision of personal information has reached new heights. AIoT data often contains personal privacy information, such as a camera on a smart home door lock or body status information collected by smart health devices. As a result, traditional centralized learning and parallel distributed learning in the cloud have data privacy vulnerabilities and are no longer suitable for AIoT model learning [108].

There is a significant global debate about granting access to personal data, even for security reasons. Surveillance data, which includes video footage and potentially identifiable information, is extremely sensitive. People are understandably concerned about unauthorized parties accessing their personal information. Unauthorized access or breaches may result in significant legal and privacy ramifications [109].

2) Privacy concerns at the edge: Tags, sensors, actuators, and embedded devices enable edge devices to interact directly with the physical environment. As a vital component of every IoT program, the edge layer is an exposed target for attackers, who can obtain access and compromise or bring down the entire system [113]. Edge devices deployed for video surveillance are often physically accessible, making each camera with edge processing capabilities a potential entry point. Attackers no longer need to target a central server; compromising a single camera can disrupt the entire system. This vulnerability allows attackers to tamper with the device itself, potentially altering its functionality, such as manipulating camera angles or stealing sensitive data like encryption keys used to secure video streams.

Furthermore, video data analysis often occurs directly on edge devices, raising privacy concerns. Robust data governance frameworks and strong encryption are crucial to ensure user privacy is protected throughout the processing pipeline, especially when dealing with PII captured in video feeds.

3) Exploiting streaming vulnerabilities: The reliance on real-time video streaming opens up new attack vectors. Attackers could use vulnerabilities in communication protocols (e.g., RTSP, RTP) to intercept or manipulate video streams [114], potentially resulting in false alarms or missed threats. In addition, compromised or outdated video compression codecs may pose security risks. Conventional cryptographic protocols like TLS/SSL may not always meet the increasing security requirements of cloud communications [115], [116]. Securing video transmission while adhering to the requirements for real-time transmission remains a significant challenge.

4) Legacy infrastructure: AIoT video surveillance systems often integrate cameras and edge devices from multiple vendors, each utilizing distinct security protocols, bit rates, and configurations. Furthermore, the use of diverse video compression techniques, encoding methods, AI model deployment strategies, decision-making algorithms, video players, chunking, latency rates, and segmentation techniques further complicates system interoperability [117]. This heterogeneity, unlike traditional systems with standardized components, poses challenges in maintaining a unified security posture across the network. It also hinders the timely distribution of security updates, particularly for legacy devices that may no longer be supported by their manufacturers.

Many existing surveillance systems may rely on older, less secure infrastructure, such as analog cameras or proprietary video management systems. These legacy systems might not be easily integrated with edge computing and distributed processing architectures [118]. This lack of integration can create compatibility issues and security gaps between the old and new systems. Additionally, organizations deploying

AIoT video surveillance systems may lack the in-house expertise to properly secure these complex, distributed architectures. This can lead to misconfigurations, vulnerabilities, and a higher risk of cyberattacks, especially when dealing with integrating disparate systems.

### C. PRIVACY CONCERNS RELATED TO SURVEILLANCE FOOTAGE

Smart devices, such as personal cameras, smartphones, and intelligent personal assistants, constantly produce images, videos, and audio recordings. These unstructured data are frequently shared with untrusted parties, raising significant privacy concerns [119]. Surveillance footage, in particular, contains highly sensitive information, including voiceprints, human faces, individual identities, vehicle license plates, and personal health records. Once exposed, these unique identifiers can lead to permanent privacy breaches.

A data protection impact assessment (DPIA) is essential for facial recognition technology (FRT) in order to demonstrate and achieve privacy by design. In Europe and the United States, using FRT and implementing DPIA present significant challenges [120]. In Europe, the GDPR requires the use of DPIAs to identify and mitigate risks linked with personal data processing, especially for technologies such as FRT. DPIA is a process devised for helping organizations to identify and minimize the data protection risks of a project by ensuring privacy by design. For example, the city of Nice in France has experimented using FRT for safety reasons [121], but such projects must undergo stringent DPIAs to address privacy issues. Problems include maintaining GDPR compliance, coping with public skepticism, and minimizing the danger of abuse or overreach by authorities. In the United States, there is no federal regulation equivalent to GDPR, resulting in a patchwork of state and local laws governing FRT. For example, San Francisco and Berkeley banned the use of FRT by city agencies, citing privacy and civil liberties concerns [120]. The lack of a standardized requirement for DPIAs means that privacy impact assessments are not conducted consistently, resulting in inconsistent personal data protection. Both regions face common challenges, including bias in FRT algorithms, surveillance overreach, and retaining public trust. The controversial use of FRT at public events in the UK has raised privacy and efficacy concerns. In the USA, the deployment of FRT by law enforcement agencies without clear oversight has raised alarms about potential abuse and discrimination. These examples highlight the ongoing struggle to balance security benefits with privacy rights in the deployment of FRT and the necessity of robust DPIA practices.

Given the complexity of using FRT, it is critical to consider the additional degree of differential privacy introduced by GDPR. Differential privacy tries to give stringent privacy assurances by introducing noise into data, thereby protecting individual identities even when the data is shared with untrustworthy parties. However, implementing differential privacy for unstructured data like images and videos presents significant challenges. These include balancing the trade-off between data utility and privacy, ensuring that additional noise does not significantly degrade data quality, and safeguarding against sophisticated AI attacks that could reverse the obfuscation and re-identify individuals [122].

Beyond public and commercial applications, data privacy concerns also extend to home surveillance systems. When considering home surveillance, the data privacy concerns become even more pronounced. Smart home devices, including cameras and voice assistants, continuously collect vast amounts of personal information, capturing intimate details of individuals' lives [123]. This footage can reveal daily routines, personal habits, and sensitive interactions, making it a prime target for unauthorized access and data breaches. Despite the implementation of differential privacy, DPIA, and other security measures, threats persist [124]. Hackers can still gain control of devices, unauthorized parties may view live feeds or stored footage, and personal data can be misused for identity theft or other malicious activities.

### D. POTENTIAL FOR ADVERSARIAL ATTACKS TARGETING AI ALGORITHMS

There are four key aspects related to AI algorithms and processing in smart surveillance:

1) Data Preprocessing
2) Data Training
3) AI Model Selection
4) Autonomous Decision Making

Preprocessing data is a key part of preparing it for analysis. It involves cleaning the data to remove errors and irrelevant information. This ensures that data is accurate and ready for use. The data is then standardized so that it is consistent and comparable. Feature engineering is a crucial step where raw data is transformed into more meaningful pieces. This step helps the model understand the problem in a better way. In these missing values are handled too, ensuring that incomplete data does not mess with the model's performance. Good preprocessing improves model accuracy and efficiency. Training the model is the next step after preprocessing. During training, the model identifies patterns in the data. The model receives a subset of the preprocessed data known as the training set. This allows the model to refine and improve its predictions or classifications. Training consists of repeated cycles in which the model's predictions are compared to known outcomes. Backpropagation and gradient descent are techniques for reducing errors. The goal is that the model should perform well with new, previously unseen data in real-world applications. Once the AI models are trained on historical data, they are deployed to edge devices or cloud servers. Inference is the process where trained AI models are applied to fresh, real-time data to generate predictions or insights. This enables AIoT systems to quickly adapt and respond to dynamic conditions and events. The next crucial aspect is autonomous decision-making which is the ultimate goal of AIoT, i.e., to create systems that can make informed decisions without human intervention [117].

Data preprocessing is a critical step in AI-driven video surveillance. It is required to transform raw data into actionable insights. Data preparation is such an important step that gathering data, cleaning it, and making it suitable for machine learning (ML) training takes 45% or even 80–90% [125], [126], [127] of the entire time. Even the best ML algorithms cannot perform adequately in the absence of good data [127]. However, this stage is also susceptible to several threats, such as adversarial attacks. Malicious actors can introduce intentionally corrupted or manipulated data, e.g., deepfakes into the training dataset [128], leading to biased or compromised models that generate false positives, i.e., flagging harmless activity as a threat or negatives, i.e., failing to detect actual threats. Ali Aliev devised a method for producing deepfakes in real time [129]. To test the technology, he joined a random Zoom conference and successfully pretended to be Elon Musk.

Noise can also be introduced to manipulate data, remove crucial information, or alter labels to significantly impact model performance and accuracy. Data preprocessing might also unintentionally expose sensitive information, such as facial features, license plates, or unique identifiers, leading to privacy breaches. In addition, improper handling of training data can also result in accidental exposure of sensitive information, compromising individuals' privacy. Biased data can lead to biased models, which can impact both accuracy and fairness. For instance, a dataset with limited representation of certain demographics can result in biased decision-making by the AI system. Hence, insufficient or imbalanced datasets can limit the effectiveness of AI models, particularly in detecting rare events or anomalies. Data preprocessing can also be computationally demanding, necessitating significant processing power and memory. Inefficient algorithms and suboptimal hardware can have a negative impact on the overall performance of the surveillance system. Additionally, huge volumes of video data necessitate significant storage capacity. Insufficient storage can cause data loss or selective data processing, potentially compromising the model's accuracy.

AIoT-based surveillance systems face significant threats related to the manipulation of training data, especially involving video footage and facial recognition. One such threat is AI trojans, where a trained AI model is altered to perform specific actions only when given certain inputs [130]. For instance, an image classification model could be manipulated to fail in detecting a particular type of weapon, severely compromising the security managed by the AI system. A realistic attack scenario involves hackers breaching the model hosting server and uploading Trojan models. This threat is particularly plausible because many AI solutions rely on pre-trained models, making them susceptible to such manipulations. Rakin et al. [131] demonstrate a method for inserting Trojans into a neural network to achieve misclassification without the need for retraining. Attackers need to know the neural network's architecture and parameters, but not necessarily the training process.

Similarly, AI backdoors pose a significant threat. These are implemented during the model training stage by the model's authors. For example, a facial recognition vendor might train a model to recognize a particular face as a universal key, allowing unauthorized access to numerous facilities [132]. Identifying these backdoors is incredibly challenging. AI systems, often based on deep neural networks, are complex, and understanding their behavior under normal circumstances is already difficult. Detecting malicious manipulations, especially those involving subtle changes to training data, adds an extra layer of complexity.

Recognizing inappropriate human activities in surveillance applications is essential to prevent potential theft, harm, and other destructive actions. Effectively evaluating human activity is a critical yet challenging task for computer vision researchers. This difficulty arises due to factors such as camera movement, interactions between individuals, visual similarities, interactions between humans and objects, facial actions involving objects, and the identical viewpoints of different activities [133]. It is also quite difficult to provide a standard definition for an abnormal event because multiple types of such events exist that correspond to different scenarios. One significant problem in AIoT surveillance systems is the selection of appropriate AI models. Choosing the wrong algorithm can lead to substantial losses. AI models require large amounts of training data to perform effectively, and insufficient data can result in underfitting, where the model does not capture the data patterns well, leading to high bias and low variance. Conversely, overfitting occurs when the model is trained excessively on specific data, causing it to perform well on training data but poorly on new data, resulting in low bias but high variance [134].

AI algorithms are categorized based on learning styles and similarities. Learning styles include supervised, unsupervised, and semi-supervised learning [135]. Similarity-based algorithms group similar data and include methods like instance-based learning, regression, regularization, clustering, decision trees, and Bayesian algorithms. Challenges arise when integrating hybrid systems that combine two or more algorithms to leverage their combined strengths for enhanced performance [136]. Similarly, a model that may operate at 99.9% accuracy but takes too long to make a classification decision is rendered useless and is similar to a 0% accuracy model in the context of time-critical applications, such as proactive monitoring [137]. Table 3 shows the algorithms that are used for surveillance purpose.

CNNs, while highly accurate in image recognition, present significant challenges due to their computational intensity and substantial resource requirements for both training and inference [164], rendering them less suitable for real-time surveillance on resource-constrained edge devices. They also demand large amounts of labeled data, which can be difficult to obtain, and are prone to overfitting when the training dataset is small or lacks diversity, leading to poor generalization. Moreover, CNNs are vulnerable to adversarial attacks, where minor perturbations can cause

**TABLE 3.** Algorithms and their use in video surveillance.

| Algorithm | Use in Video Surveillance |
|---|---|
| Convolutional Neural Networks (CNNs) | Widely used for image and video analysis tasks, such as object detection, facial recognition, and activity recognition [138], [139]. YOLO (You Only Look Once), Faster R-CNN, and SSD (Single Shot MultiBox Detector) are popular CNN-based models for object detection. Recently, 3D CNN has been used for anomaly recognition from surveillance videos [140]–[143]. |
| Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) Networks | Used for tasks involving sequential data, such as activity recognition and behavior prediction from video sequences [133]. LSTMs are often combined with CNNs for analyzing video data where temporal relationships are important [114]–[147]. |
| Support Vector Machines (SVMs) | Used for classification tasks, such as distinguishing between different types of activities or recognizing specific patterns in video data. SVMs can be used for anomaly detection in surveillance footage [147]–[149]. |
| K-Means Clustering | Used for segmenting video data into different groups, such as separating different moving objects in a scene. K-Means can be used for background subtraction and object tracking [150], [151]. |
| Decision Trees and Random Forests | Used for classification and regression tasks, offering interpretable results and relatively fast training times. Random forests can be used for recognizing specific activities or events in surveillance footage [152]–[154]. |
| Autoencoders | Used for anomaly detection by learning a compressed representation of normal behavior and identifying deviations from this norm. Autoencoders have been applied to detect unusual activities or objects in video streams [155]–[158]. |
| Optical Flow Algorithms | Used for motion detection and tracking by analyzing the flow of pixels between consecutive frames in a video [159]. Optical flow can be used for tracking moving objects and understanding motion patterns in surveillance footage [160], [161]. |
| Gaussian Classifier | Deep autoencoder networks and single-class image-level classification techniques have been proposed to detect anomalies in surveillance videos [140]. |
| Ada-Net | An attention-based autoencoder leveraging contentious learning has been proposed for detecting anomalies in videos. This approach enhances the model's focus on critical regions and events within the video [162]. |
| Asymptotic Bounds | The crowd escape anomaly is detected through statistical and deep learning algorithms that assess pixel coordinates directly [163]. |

incorrect classifications. Other Artificial Neural Networks (ANNs) share similar drawbacks, such as long training times and the necessity for substantial data, alongside their black-box nature which complicates the interpretability of their decision-making processes, a crucial aspect in security-sensitive applications like surveillance. Scaling ANNs to handle complex datasets requires sophisticated architectures and greater computational power. Traditional ML algorithms also face hurdles with extensive feature engineering, bias-variance trade-offs, and the challenge of selecting appropriate models, all of which require significant experimentation and tuning. Many advanced ML models, like ensemble methods, are difficult to interpret, reducing trust in their decisions [165].

The complexity of deep learning models and some shallow ML models, such as random forests and SVMs, makes their performance in specific contexts unpredictable and their decision-making processes opaque, thereby diminishing user trust in these intelligent systems. The Zillow case which led to a $6 billion drop in the company's valuation, highlights the severe consequences of mismanaging ML models. As a result, Zillow had to lay off 25% of workforce and sell 7,000 homes with a total asset value exceeding $2.8 billion [166]. This failure underscores a critical point that ML applications, by their very nature, are tasked with making smarter and more critical decisions than traditional software. As a result, when these systems fail, the consequences are much more severe.

In general, AI algorithms need computational resources and memory. Their complexity may limit their use on edge devices in AIoT surveillance systems. The collection and processing of massive amounts of data by these systems

**TABLE 4.** Performance metrics of AI models in AIoT surveillance under diverse adversarial attacks.

| Year | AI Model | AIoT Application | Attack Type | Adversary Knowledge | Metrics | Key Findings |
|---|---|---|---|---|---|---|
| 2022 [168] | Various DNNs | Image Classification (General Surveillance Principles) | Universal Adversarial Perturbations (UAPs) | Black-box | Attack Success Rate (ASR) | **ASR:** 40-90% against several model architectures. |
| 2023 [168] | LSTM | Time Series Classification (Traffic Anomaly) | Custom Black-box Attack | Black-box | ASR, Detection Success Rate (IDS) | **LSTM ASR:** Improved from 19.3% to 27.3%. **IDS Detection Success Rate:** Decreased from 90.9% to 6.8%. |
| 2024 [169] | ML Classifier | IoT Network Intrusion Detection | Evasion | White-box | Accuracy Drop, Evasion Rate | **Accuracy Drop:** Significant reduction in detection accuracy. **Evasion Rate:** High percentage of malicious samples undetected. |
| 2025 [170] | YOLOv5 | Object Detection (Smart Retail) | Adversarial Patch (Hiding) | Black-box (Physical) | Mean Average Precision (mAP), Misclassification Rate | **mAP drop:** From 0.996 (no attack) to 0.079 (gray patch). **Misclassification Rate:** ∼91% for specific hidden objects. |
| 2025 [171] | EfficientNet, ResNet, MobileNet | Smart Surveillance (Video Streams) | Multi-Pixel Deception (MPD) | Black-box | Accuracy, ASR | **EfficientNet Accuracy:** Dropped from 87.45% to 61.23% (ASR: 29.10%). **MobileNet Accuracy:** Dropped from 81.40% to 55.17% (ASR: 32.60%). |
| 2025 [172] | Federated Learning Models | Distributed AIoT (e.g., Smart Home IDS) | Backdoor (Data Poisoning) | White-box (Malicious Client) | Backdoor Accuracy / Misclassification Rate | **Backdoor Accuracy:** >90% on triggered inputs. **Overall Accuracy:** Degradation on clean data due to poisoning. |

on edge devices may also raise privacy concerns. Scaling these algorithms to handle complex tasks is also difficult and requires ongoing updates and improvements. Al algorithms are also vulnerable to a variety of security threats, such as data poisoning, model inversion attacks, and adversarial attacks. These problems risk the integrity and reliability of surveillance systems. To ensure reliable and efficient AIoT surveillance, AI algorithms must be carefully selected and implemented.

Table 4 provides a quantitative overview of the vulnerability of the AI model within AIoT surveillance systems. It shows how different AI models, employed in different AIoT applications, react to various types of adversarial attacks such as adversarial patches, data poisoning, and evasion techniques. The data quantifies this vulnerability through key metrics such as accuracy drop, misclassification rates, detection rate degradation, perturbation size, and attack success rates (ASR), often differentiating between black-box attack scenarios, where the adversary has no knowledge of the model's internals, and white-box attack scenarios, where full model information is available. Collectively, the findings demonstrate that AI models in AIoT surveillance are indeed susceptible to adversarial manipulation, exhibiting measurable performance degradation and successful attack outcomes in a range of simulated real-world conditions.

### E. REGULATORY AND COMPLIANCE ISSUES IN SURVEILLANCE DATA HANDLING

Regulatory and compliance issues present significant challenges for AIoT surveillance security. AIoT surveillance systems gather, process, and analyze vast amounts of surveillance data in real time, which raises substantial privacy and security concerns. Key regulatory frameworks, such as the GDPR in Europe and the California Consumer Privacy Act (CCPA) in the United States, impose strict guidelines on handling surveillance data. Compliance requires strong data protection measures like encryption and secure storage. These safeguards help prevent unauthorized access and

data breaches. The CCPA grants consumers rights over their personal information, including the right to know what data is collected, who is selling it, and how they can access and delete it [173]. The GDPR and CCPA require explicit consent, transparent data handling practices, and stringent data protection. When using biometric data such as facial recognition or fingerprints, additional legal considerations and robust security measures are required to protect individuals' rights.

Another important consideration is that AI models must be explainable and bias-free. This will lead to fair and legal data processing. Regular testing and validation of AI models is critical for detecting and mitigating biases. This ensures fair treatment and protects against discrimination. This also helps maintain accountability and makes it easier to meet legal obligations.

AIoT surveillance systems require robust encryption to protect data in transit and at rest. This protects against unauthorized access and data breaches. To ensure security, encryption methods should be tested for vulnerabilities on a regular basis. Organizations must establish clear data retention policies and securely delete data when it is no longer required or when individuals request it. Explicit consent must be obtained for data collection and processing, and individuals should be able to withdraw it easily.

Surveillance data is governed by specific regulations in various sectors, including healthcare, finance, and law enforcement. Financial institutions' surveillance systems, for example, must follow strict data privacy and security standards, such as the Payment Card Industry Data Security Standard (PCI DSS) [174]. Organizations are responsible for ensuring that sector-specific regulations are followed. Furthermore, having a comprehensive incident response plan in place to deal with data breaches and promptly notify affected parties and regulatory bodies is critical.

Some countries have strict data localization laws requiring data to be stored within their borders, which can complicate compliance for multinational organizations. Organizations must ensure that data transfers between countries adhere to relevant regulations and international data transfer agreements. Adopting ethical AI practices is essential to ensure that AIoT surveillance systems are used responsibly, respecting individual rights and societal norms. A notable recent example involves Clearview AI, a facial recognition technology company. In 2022, Clearview AI faced substantial regulatory backlash for its use of facial recognition technology [175], which involved scraping billions of images from the Internet, including social media, without consent. Authorities in multiple countries, including the United Kingdom, Australia, and France, took action against Clearview AI, citing violations of privacy laws. For instance, the French data protection authority Commission Nationale de L'informatique et des Libertés (CNIL) fined Clearview AI €20 million and mandated that the company delete data of French citizens and cease further data collection activities [176], [177]. This case highlights the critical importance of obtaining explicit consent, ensuring transparency, and adhering to stringent data protection regulations in AIoT surveillance.

Organizations deploying AIoT surveillance systems must navigate complex regulatory and compliance requirements. Failure to do so can lead to heavy fines, reputational harm, and legal issues [178]. Balancing public safety with individual privacy is challenging. It is crucial to protect privacy while ensuring effective surveillance.

### F. SCALABILITY CHALLENGES

Large-scale AIoT surveillance deployments face significant scalability challenges driven primarily by the immense data volume and velocity generated by thousands or millions of networked sensors. Ingesting, transmitting, processing, and storing this continuous stream of video, audio, and other sensor data in real-time, especially at the edge, can quickly overwhelm existing network bandwidth, storage, and computational capabilities. The integration of AI algorithms, such as object detection and facial recognition, further compounds this, as these are inherently computationally intensive, demanding substantial processing power that must be efficiently balanced between resource-constrained edge devices and more powerful cloud infrastructure. Moreover, ensuring low latency for real-time alerts and responses becomes a critical network challenge, while managing power consumption across countless, often battery-powered, edge AI devices is crucial for sustainable operation.

Beyond raw technical capacity, scalability in AIoT surveillance is complicated by the inherent heterogeneity and interoperability issues across a vast ecosystem of diverse hardware, operating systems, and communication protocols from various vendors. This fragmentation makes uniform security management, software updates, and seamless data exchange incredibly difficult to orchestrate at scale. The management and orchestration of deploying, monitoring, and maintaining an ever-growing number of AIoT devices and their associated AI models across a wide geographical area presents formidable logistical hurdles. Effectively securing each device as a potential entry point, maintaining data privacy throughout the distributed system, and updating sophisticated AI models across an extensive and diverse fleet are all profound challenges that must be comprehensively addressed for truly scalable AIoT surveillance.

## IV. PROPOSED SOLUTIONS AND INNOVATIONS

Innovative approaches and technologies are required to effectively address AIoT surveillance security challenges. Some suggestions for overcoming complex challenges are discussed below.

### A. ADVANCED ENCRYPTION METHODS

In the rapidly evolving field of AIoT, various encryption standards face unique challenges that can impact their effectiveness and suitability, potentially compromising the security and integrity of the system. Symmetric

**TABLE 5.** Comparison of encryption methods in AIoT ([179], [180], [181], [183], [184], [186], [187], [188], [190], [191], [192], [193]).

| Method | Latency | Overhead | Security | AIoT Suitability |
|---|---|---|---|---|
| AES-128 (Symmetric) | Low (1–2 ms) | Low | Medium | High (real-time, lightweight) |
| RSA-2048 (Asymmetric) | High (100× AES) | High | High | Low (resource intensive) |
| Hybrid (AES+RSA) | Medium | Medium | High | Medium–High (balanced) |
| Homomorphic (CKKS/BFV) | Very High (1000×) | Very High | Very High | Low (non-real-time) |
| Quantum (QKD) | Low (theoretical) | Very High | Very High | Experimental (not practical yet) |
| Post-Quantum (Kyber) | Medium (2–3× RSA) | Medium | High | Emerging (future-ready) |

encryption, such as AES, is efficient and ideal for resource-constrained IoT devices due to its speed and simplicity [179]. AES-128, for instance, offers low latency and minimal computational overhead, making it well-suited for embedded hardware [180]. However, it suffers from key management issues, especially in large-scale deployments where secure key distribution and storage become complex [181].

Asymmetric encryption, such as Rivest–Shamir–Adleman (RSA), provides enhanced security using public and private key pairs, offering better authentication and integrity [182]. However, RSA-2048 requires significantly higher processing power due to its higher computational complexity, resulting in considerable delays on resource-limited AIoT nodes [183]. This overhead limits its practicality for real-time AIoT surveillance and control systems.

Hybrid encryption, which combines the speed of symmetric encryption with the secure key exchange of asymmetric encryption, has gained traction for AIoT systems. It improves overall security and key management efficiency [184]. However, this approach still requires moderate computational resources and memory allocation, especially on edge devices [185]. Research demonstrates that hybrid cryptographic implementations increase computational overhead by 28% on average, with key generation time increasing from 0.8 ms to 1.2 ms on standard IoT processors [186].

Homomorphic encryption (HE) allows computations on encrypted data without decryption, which is particularly beneficial for sensitive AIoT applications such as healthcare and finance. Currently, HE is challenging to scale, making it impractical for real-world use. Additionally, execution is very sluggish in comparison to plaintext analysis. Thereby, training an ML model is not feasible, but as research evolves, it may become more practical in the future [187]. Nevertheless, schemes like BFV and CKKS typically introduce a 1000× slowdown compared to unencrypted computation, posing a significant barrier to real-time deployment without dedicated hardware acceleration [187], [188].

Quantum encryption offers unprecedented theoretical security based on quantum key distribution (QKD), protecting data from both classical and quantum attacks [189]. Despite its advantages, it remains largely experimental and requires specialized quantum infrastructure, which makes it currently impractical for widespread AIoT use [190]. As a forward-looking solution, post-quantum cryptographic algorithms (PQC) are being standardized to resist quantum computing threats. However, an analysis of network performance reveals that the implementation of post-quantum cryptography results in an approximate 189-millisecond increase in end-to-end authentication time in typical IoT environments. The higher computational complexity of quantum-resistant protocols contributes to a 47% reduction in network throughput, primarily due to the additional processing time required for key generation and validation [186], [191]. Recent research highlights that CRYSTALS-Kyber and CRYSTALS-Dilithium, the NIST-approved PQC, offer strong resistance against quantum attacks while maintaining execution times comparable to classical cryptographic methods. However, their large-scale adoption may present practical challenges such as the need for infrastructure upgrades, interoperability issues, compliance with evolving regulations, and increased implementation costs [192], [193]. Table 5 summarizes the computational trade-offs, latency characteristics, and overall suitability of key encryption techniques in AIoT environments.

As AI capabilities continue to evolve, encryption standards must also advance to counteract potential AI-driven threats and system vulnerabilities. Each encryption method represents a trade-off between performance, resource consumption, and security. Therefore, the design and deployment of AIoT systems must carefully consider these factors based on their operational context: real-time requirements, scalability, and data sensitivity. Future-proof encryption strategies should incorporate post-quantum resilience, lightweight implementations, and adaptability to constrained environments to maintain long-term system trustworthiness.

### B. STANDARDIZATION EFFORTS IN AIOT SURVEILLANCE

In AIoT surveillance, the lack of universal communication protocols and standardized data formats creates significant hurdles. Many systems rely on proprietary protocols and data formats, which impede seamless interoperability and effective data sharing. For instance, the concept of data normalization, as discussed in [194], aims to make data uniform and complete, addressing issues like noise isolation, redundancy, and data size adjustments to speed up processing. Additionally, the use of proprietary protocols leads to integration issues and increased complexity [195].

While industry initiatives like the IoT Security Foundation's guidelines and Open Connectivity Foundation (OCF) standards have made progress, adoption remains uneven. According to a Gartner report, as of 2024, only about 30% of AIoT devices fully comply with these standards, which hinders effective data sharing and integration. For example, the TabDoc system, mentioned in [196], demonstrates an advancement in knowledge discovery by requiring documents to be formatted in XML, DTD, or XSD standards, integrating these with ontology approaches to enhance semantic understanding.

Adopting the Matter standard (formerly known as Project CHIP) developed by the Connectivity Standards Alliance (CSA-IoT) offers a promising solution [197], [198]. Matter provides a unified communication protocol and standardized data formats, designed to streamline device integration and enhance interoperability. With backing from major tech companies and support for end-to-end encryption, Matter addresses critical integration challenges [199]. According to an ABI report [200], over 5.5 billion smart home Matter-compliant devices are expected to be shipped between 2022 and 2030. As Matter is still in its early stages, it is crucial to evaluate whether it can handle the demanding performance requirements for real-time processing of high-resolution video streams while maintaining low latency. Additionally, adapting to evolving security threats and ensuring robust, long-term protection are significant concerns. Addressing these challenges effectively is vital for Matter to realize its potential in standardizing AIoT surveillance systems.

### C. ADVANCED AI ALGORITHMS

In the context of AIoT surveillance, the application of certain deep learning and ML algorithms presents a range of challenges that can impact their effectiveness. Deep neural networks (DNNs), while recognized for their robust performance in various tasks, often encounter difficulties in real-time surveillance scenarios. Their computational complexity requires substantial processing power and memory, which can be a significant drawback in resource-constrained IoT environments [201]. This limitation can result in delays and inefficiencies, making DNNs less suitable for applications where immediate analysis and response are crucial. LSTM networks, designed primarily for sequence prediction tasks, also face challenges when applied to surveillance tasks. The high computational cost and slow training times associated with LSTMs can hinder their performance in real-time video stream analysis [202], [203]. LSTMs are optimized for handling long sequences and temporal dependencies, such as those found in natural language processing, but may struggle with the demands of continuous, high-resolution video analysis required in surveillance systems.

Generative adversarial networks (GANs) are used to generate realistic data and enhance image quality. However, they may not be suitable for real-time surveillance. GANs are complex and resource-intensive. This makes them impractical for real-time use. Their computing needs may slow down network traffic processing and analysis. This can create problems with scalability and threat detection. GANs also have high processing latency. This may not meet the demands of real-time applications and may result in exposure of networks to emerging attacks [204], [205]. They are better at data generation than at immediate object detection or classification, which are crucial for effective surveillance.

Another technique applied in research for video analysis involves using CNNs [206], [207], [208]. But despite their widespread use in image and video analysis, they can encounter limitations in the context of AIoT surveillance. Traditional CNNs require impressive and robust hardware resources like GPUs for effective CNN training [203]. The demand for significant computational power and memory can be a constraint for edge devices with limited resources. Additionally, CNNs may struggle with contextual understanding and processing varied visual inputs in real-time, which are essential for effective surveillance.

Recent research is addressing some of these challenges by focusing on optimizing algorithms for real-time performance and resource efficiency [209]. Techniques such as quantization and pruning are being employed to reduce the computational complexity and memory requirements of deep learning models [210], [211], [212], [213] making them more suitable for deployment on edge devices. To solve the problem of embedding CNN into edge devices for inference which is a very challenging task, lightweight CNN architectures, such as MobileNet and EfficientNet, have evolved. These are specifically suitable for resource-constrained environments, offering a balance between performance and computational efficiency [214], [215], [216].

Advances in edge computing and federated learning are also improving IoT devices' ability to process data locally and collaboratively, reducing the need for large computational resources and improving real-time analysis [217], [218]. However, training AI models collaboratively in multiple locations at the same time necessitates a significant amount of communication bandwidth. This is especially true if data hosts train their local models on the device. To address the bandwidth and computing constraints of federated learning, some proposed efficiency measures include pruning and compressing the locally trained model before it is sent to the central server. Transparency is another challenge for federated learning [219]. Because training data is kept private, there must be a system in place to test the model's outputs for accuracy, fairness, and potential bias. However, this is still in its early stages and will evolve with the passage of time.

Another advancement in the AI field is the development of explainable AI (XAI) techniques [220], [221], [222]. XAI is crucial for building trust in AIoT surveillance systems. XAI provides insights into how AI models make decisions, ensuring transparency and accountability. This is particularly important for compliance with stringent data protection regulations and for maintaining public trust in surveillance technology. By making AI systems more interpretable,

XAI helps address concerns about the black-box nature of AI models, fostering greater acceptance and reliability in their deployment for surveillance purposes. However, the efficacy and adequacy of explainability as a tool for AI safety may be limited in some cases. For example, AI systems used by malicious human actors can pose significant challenges to explainability [223], [224]. Researchers must further investigate this area in order to provide a balanced solution to the problems.

Ongoing research and development aim to address issues such as computational demands, real-time processing capabilities, and resource constraints by optimizing algorithms, leveraging advanced techniques, and incorporating XAI to improve their suitability and trustworthiness for real-time surveillance tasks in AIoT environments.

### D. ZERO-TRUST SECURITY MODEL

The zero-trust security model [225], [226] operates on the principle of not trusting any entity by default. This applies to both internal and external entities within the network. This approach necessitates continuous authentication and authorization checks throughout the system. It recognizes that threats can emerge from both internal and external sources so, the zero-trust model ensures that security is maintained at every level of the organization. Organizations can improve the security of their environmentally friendly operations by rigorously verifying the identity of individuals. They must also ensure the integrity of devices, sensors, and systems [227]. This can be achieved through the application of zero-trust principles. In AIoT surveillance, adopting a zero-trust security model is essential to protect systems from advanced cyber threats. This model ensures that every entity is constantly monitored. It helps maintain strong security, even against complex and sophisticated attacks. This model requires constant verification of both users and devices trying to access resources. It ensures that only authenticated and authorized entities are granted access.

The zero-trust approach addresses key challenges in AIoT surveillance systems. These systems contain a large number of interconnected devices, each of which poses a potential vulnerability. The information gathered and transmitted by these systems is critical. Continuous authentication and authorization checks help to avoid unauthorized access and data breaches. This offers strong protection against potential intrusions.

Implementing zero-trust in AIoT surveillance demands precise technical considerations that extend beyond traditional network perimeters. Robust Identity and Access Management (IAM) is paramount, where each AIoT device establishes a unique, immutable identity often rooted in hardware security modules (HSMs) or secure boot processes, verified via certificates. User access requires stringent multi-factor authentication (MFA) and dynamic, context-aware access policies, such as Attribute-Based Access Control (ABAC), which continuously assess device health, location, and user behavior. Furthermore, micro-segmentation becomes critical, utilizing technologies like Software-Defined Networking (SDN) or VLANs to create logical isolation for different device types (e.g., cameras, edge gateways), thereby limiting lateral movement even if one component is compromised. This foundational security posture is continuously reinforced by real-time device posture assessment and network behavioral analytics, which monitor for anomalies or deviations from established security policies.

Zero-trust system requires monitoring network traffic for unusual activity. All devices and users must be regularly authenticated. Continuous verification not only enhances security but ensures compliance with regulations. This model helps to build public trust in surveillance technologies. One major issue is the difficulty of integrating zero-trust principles with legacy systems not designed for this model [228]. The growing volume of data and the increasing number of devices in AIoT environments also make continuous monitoring and verification resource-intensive. In current era, cyber threats are constantly evolving which requires security protocols to adapt in real time. Maintaining this level of adaptability can be challenging.

XAI techniques are crucial for reinforcing zero-trust security. XAI reveals how AI models make decisions. This is important for transparency and accountability of systems. It is essential to complying with strict data protection regulations to maintain public trust in surveillance technologies. XAI supports this by clarifying AI decision-making processes. Technically, XAI mechanisms provide auditable insights into AI decisions, such as why a specific object was detected or an anomaly flagged, which is crucial for maintaining transparency within the zero-trust framework. It helps organizations spot and fix biases in AI models. This ensures that surveillance system decisions are fair and justifiable [229].

Advances in ML and AI are enhancing continuous monitoring and anomaly detection. For instance, federated learning allows AI models to be trained across multiple decentralized devices while keeping raw data private and secure. This aligns with the principle of least privilege for data access, allowing model updates to be exchanged securely without exposing raw data. Blockchain technology is also being investigated to create immutable logs of all access requests and transactions. This improves the auditability and trustworthiness of AIoT systems [230], [231]. Moreover, zero-trust in AIoT necessitates robust data protection, including secure key management systems for encryption of data at rest and in transit, leveraging capabilities like HSMs on devices.

Implementing a zero-trust security model is critical for AIoT surveillance. It reduces risks and improves system security. Organizations can safeguard sensitive data by continuously verifying identities. Enforcing strict access controls helps to meet regulatory requirements. Patch management and multi-factor authentication must be performed on a

timely basis. Integrating XAI techniques improves resilience and reliability. Finally, maintaining zero-trust requires secure orchestration and lifecycle management for AIoT devices, ensuring secure provisioning, automated deployment, and verifiable over-the-air (OTA) updates, thereby enforcing a continuous state of trust validation from device inception to decommissioning. This approach is critical in an increasingly connected world.

### E. SECURITY EXPERTISE

As AIoT devices advance, organizations must invest in training personnel or hiring security specialists to manage the growing complexity of securing AIoT surveillance systems. One of the most significant challenges in this area is the rapidly evolving landscape of cyber threats [232]. AIoT surveillance systems are particularly susceptible to sophisticated attacks because of their interconnected nature and because of handling vast amounts of sensitive data. It is crucial for organizations to stay ahead of potential threats by ensuring that their security measures are constantly updated and robust [233].

Ensuring the security of each connected component of the system, as well as the overall surveillance system, requires a deep understanding of both AI and IoT technologies. This necessitates specialized security expertise that can navigate the unique vulnerabilities and attack vectors associated with AIoT systems.

Organizations should meet this problem by devoting resources for continuous training of their employees. Such training must include cybersecurity policies, methods of threat scanning, and the latest AI and IoT technological advancements. Keeping oneself abreast on such issues helps security experts in the comprehension and possible management of attacks. Further, employing dedicated security experts that are AIoT literate will strengthen the organization's effort in maintaining the safety of its surveillance systems.

Recent research has focused on developing automated security frameworks for AIoT systems [234], [235], [236]. These frameworks employ AI technologies to monitor the security state of the system at all times. In case any potential threat is identified within the system, preconfigured actions are taken in order to address the threat. This increases the efficiency within the system while minimizing the need for manual intervention. As a result, security professionals can concentrate on more strategic tasks.

The other area which is being investigated is the application of blockchain technology as a way of improving AIoT surveillance system security. By utilizing the blockchain, the level of confidence in the AIoT surveillance system used by the organizations can be reinforced. Investment in ongoing training is essential for protecting against new cyber threats. Hiring dedicated security specialists further boosts this defense. Advanced solutions like ML, automated security frameworks, and blockchain can greatly enhance the security of AIoT surveillance systems. Recent studies show promising progress in these technologies. These efforts help ensure that AIoT surveillance systems stay secure and reliable.

### F. IDPS TAILORED FOR AIOT SURVEILLANCE

IDPS are essential for protecting AIoT surveillance systems from different cyber-attacks. However, in AIoT environments traditional IDPS frameworks frequently prove inadequate. This is because of various complexities such as: numerous interconnected devices, diverse network architectures, and continuous data flow. Consequently, there is a need for AIoT tailored IDPS solutions for AIoT surveillance systems.

Recent AIoT-based IDPS implementations now use advanced technologies like AI and ML to improve threat detection and response [237], [238]. These systems use intelligent algorithms to analyze the large amounts of data from AIoT devices, identifying patterns and anomalies that may indicate security breaches.

Some existing solutions use edge computing, where intrusion detection happens on edge devices near the data source [239], [240]. This approach reduces latency and bandwidth consumption by processing data locally. It is especially useful for time-sensitive surveillance applications. Edge-based IDPS can detect and mitigate threats quickly without relying on constant communication with centralized servers. This enhances efficiency, resilience, and reduces latency in the surveillance system.

The concept of collaborative IDPS frameworks has also emerged recently [241]. In this arrangement AIoT devices exchange security information to jointly detect and neutralize threats. This distributed method offers a more complete security posture. It makes understanding of the network an easier task as the insights are available from different devices and nodes. In large-scale surveillance deployments, where threats can spread quickly across interconnected devices such cooperation is crucial.

Despite advances in IDPS technology, there are several challenges in the development and deployment of effective IDPS for AIoT surveillance. One of the major challenges is the scalability of AIoT systems. With the growing AIoT networks, IDPS must manage increasing data volumes and more devices without compromising performance. IDPS must maintain high detection accuracy and low false-positive rates to produce secure AIoT surveillance networks.

Another significant challenge is to design IDPS for diverse and heterogeneous AIoT environment. AIoT networks include a wide range of devices with different processing capabilities. It becomes very difficult to design IDPS for AIoT surveillance systems having different communication protocols and security needs. The need of time is to design flexible and adaptable IDPS solutions for securing such diverse ecosystems.

To detect and eliminate threats instantly, AIoT surveillance needs real-time processing. However, handling massive data volumes in real-time can strain system resources. This may lead to performance bottlenecks, especially with complex

**TABLE 6.** Performance evaluation of various AI-powered IDS.

| Model | Dataset | Accuracy (%) | Detection Rate (%) | FPR (%) | F1-Score |
|---|---|---|---|---|---|
| CNN-LSTM [244] | CICIoT2023 | 99.16 | 86.64 | N/A | 91.81 |
| CNN-BiLSTM [245] | UNSW-NB15 | 97.28 | 96.4 | 1.94 | 97.43 |
| Bidirectional Encoder Representations from Transformers (BERT) [244] | CICIoT2023 | 98.94 | 87.41 | N/A | 88.03 |
| Gated Recurrent Unit (GRU) with Self-Attention [246] | ToN-IoT | 99.00 | 99.00 | N/A | 99.00 |
| Feedforward Neural Network (FFNN) [247] | CIC-IoT22 | 99.93 | 99.93 | N/A | 99.93 |
| Random Forest [248] | UNSW-NB15 | 99.57 | 100 | 0.009 | 1 |

AI algorithms. Combining strong security measures with computational efficiency remains a constant challenge.

In centralized server systems, sensitive surveillance data is often send to central servers. This increases risk of data breaches and unauthorized access. Protecting data privacy while carrying out intrusion detection adds another layer of complexity to the IDPS design for AIoT surveillance systems. Innovative research is required to address these challenges and improve IDPS effectiveness. One promising direction is integrating federated learning into IDPS frameworks. It can help in developing robust IDPS by minimizing data exposure risks and learning from diverse data sources.

Incorporating blockchain technology can also offer a way to enhance the performance of AIoT-based IDPS. As blockchain provides a decentralized and immutable ledger that records security events and transactions transparently [242]. This simplifies audit processes and ensures that all intrusion detection activities are verifiable. It also improves trust and accountability [243]. To further improve security, blockchain smart contracts have the ability to automate response mechanisms and security protocols.

According to previous studies, it is possible to design more sophisticated self-adaptive IDPS systems based on ML methods such as reinforcement learning which improves the learning process and also enhances the performance of the intrusion detection systems [249], [250], [251]. Such systems incorporate real-time adjustment of the detection modalities in accordance with the feedback received and the detected threats. They adapt to the new forms of vulnerability and therefore prune new strategies. It is also evident that through systemic self-improvement, adaptive IDPS applies more robust defense tactics and also prevents new strains of security threats. Table 6 presents performance evaluation results of various AI-powered IDS tested on different datasets. AI-powered IDS models achieve remarkably high performance across different datasets, with accuracy, detection rates, and F1-scores consistently exceeding 97% in many cases. This demonstrates the strong capability of diverse AI models, ranging from deep learning architectures like CNN-LSTM, CNN-BiLSTM, BERT, and GRU, to traditional ML methods such as Random Forest, in effectively identifying network intrusions and anomalies. However, a significant observation is the frequent absence of False Positive Rate (FPR) data for several entries, which is a crucial metric to assess the practical suitability of an IDS in real-world scenarios, as high detection often comes at the cost of increased false alarms.

To address these concerns about practical suitability and further enhance the reliability of intrusion detection, integrating context-sensitive security mechanisms [252] becomes crucial. By understanding factors such as device roles, user behaviors, and environmental conditions, IDPS can make better decisions about potential threats. This reduces false positives and ensures that resources are focused on genuine security concerns.

Moreover, collaborative research and development are crucial for advancing novel IDPS solutions for AIoT surveillance. Cross-disciplinary efforts that involve cybersecurity experts, AI researchers, system engineers, and policy makers can create comprehensive security frameworks. These partnerships can also help establish standardized protocols and best practices. This guarantees that the solutions offered by the IDPS are cutting-edge technology and adhere to the ethical and regulatory environment.

### G. ETHICAL CONSIDERATIONS IN AIOT SURVEILLANCE

As AIoT surveillance is evolving, it is becoming more complicated to address ethical challenges. Two major concerns in AIoT surveillance are transparency of AI algorithm and data protection consent taken from user. Mostly AI systems work in ways that are difficult for people to understand. How AI decisions are made is a question that often remains unanswered. The users and stakeholders are often left in the dark about this. This lack of understanding can lead to real issues such as bias or discrimination. It can make people less trusting of AI systems overall. An ethical concern is to bring more transparency and fairness in system designs. It is important to build trust of people using these systems.

To address these concerns, AI models must be effective and explainable. This helps users understand the decision-making process and ensures accountability. Fairness is also important. AI algorithms require careful design and testing to avoid biases. Training AI systems on diverse and balanced data is critical for preventing bias. Regular testing is essential for detecting and correcting new biases. Ensuring fairness involves both technical and moral responsibilities. This helps assure that technologies are not supporting social injustice.

Data privacy is also a major concern in AIoT surveillance. AIoT surveillance systems often handle large amounts of personal data. Traditional AI approaches require centralizing data which can heighten the risks of misuse or theft. One

solution to this problem is Federated learning. Federated learning protects data privacy by keeping data local and reduces the risks of breaches. This aligns with ethical standards and legal requirements.

An important ethical dilemma is striking a balance between privacy rights and cybersecurity. It is critical to protect AIoT surveillance systems while upholding privacy as they become more common. A fundamental right and an essential component of democratic societies is privacy. It protects freedoms like speech and limits excessive government surveillance. Developing strategies that guarantee robust security without sacrificing privacy is a challenge. People and organizations are often left vulnerable as laws and regulations frequently fall behind the swift advancement of technology and cyber threats. For instance, regulations like GDPR were created before the widespread use of AI and IoT technologies. These technologies now present new challenges for data protection and cybersecurity [253], [254]. As technology advances, it is essential for laws and regulations to evolve accordingly, ensuring that privacy and security are effectively safeguarded in AIoT surveillance systems. Table 7 highlights the work of researchers focused on regulatory and compliance aspects within the AIoT domain.

Another key ethical concern in AIoT surveillance is obtaining informed consent from individuals whose data is collected. It is critical to develop transparent consent mechanisms. Users need to understand what data is collected and how it will be used. They should also be aware of their rights regarding data access and deletion. Sometimes explicit consent is not possible, such as in public surveillance. In such cases clear signage should inform people about the surveillance activities. It is also essential to communicate the goals of surveillance. Allowing users to opt out or anonymize their information can enhance trust in AIoT systems [264].

Because of the ongoing advancements of the technologies associated with AI and the IoT, it is imperative that there is persistent ethical governance [265]. Ethical governance can be obtained from independent ethics boards that have been created within the organizations. These boards monitor adherence to standards of ethics and recommend corrections as technology advances. Outreach to external stakeholders such as civil society organizations and the public are critical as well. In this way, coming up with ways of using AIoT surveillance ethically is possible.

Surveillance systems must not be deployed without an understanding of how they may affect different sections of society, especially those that are most vulnerable. Conducting social impact assessments helps identify these effects and design systems that are beneficial while minimizing harm. This approach ensures that surveillance serves everyone positively and equitably.

As AIoT technologies become more widespread it is crucial to establish internationally recognized ethical standards. A global consortium of experts, policymakers, researchers, and industry leaders should collaborate to develop and promote these standards. They must address key ethical concerns like privacy, bias, transparency, and accountability. By setting these guidelines, a framework for responsible AIoT use worldwide can be created. Organizations that align with these standards can ensure their AIoT surveillance systems meet ethical expectations and support a fairer and more equitable society.

### H. ADDRESSING DATA HETEROGENEITY

Addressing data heterogeneity is a critical concern for large-scale AIoT surveillance deployments, where data originates from a multitude of diverse sensors and devices. This heterogeneity manifests in various forms, including differences in data format, such as raw video feeds, structured sensor readings, audio, and logs. It also involves varying temporal characteristics, for instance, asynchronous arrivals and differing sampling rates, alongside semantic interpretations, which include diverse units or contextual meanings. Such disparity poses significant challenges for effective data integration, real-time analysis, and AI model training in surveillance systems. To mitigate this, solutions often begin at the edge by leveraging intelligent gateways or edge processors for initial data normalization and standardization, converting disparate raw inputs into common formats or adhering to shared data models. This early-stage processing is crucial for streamlining data flow and ensuring interoperability across the vast and varied AIoT network.

Beyond the edge, comprehensive solutions involve robust data integration and transformation layers, often residing in fog or cloud infrastructure, that employ advanced ETL/ELT pipelines. These pipelines, which stand for Extract, Transform, and Load (or Extract, Load, and then Transform), are used to unify and align data from disparate AIoT sources into a consistent, usable format for large-scale analytics. Furthermore, semantic interoperability is key, achieved through the use of structured vocabularies, knowledge graphs, and rich metadata management to imbue heterogeneous data with shared context and meaning, allowing AI models to correctly interpret and fuse information from diverse streams. Finally, specialized AI/ML architectures designed for heterogeneous data, such as multimodal learning or domain adaptation techniques, enable surveillance systems to process and derive insights from a combination of visual, auditory, and environmental sensor data, ultimately enhancing the accuracy and reliability of AI-powered detection and analysis. Despite these advancements, effectively managing the vast and continuously evolving data heterogeneity remains a significant ongoing challenge for truly scalable and robust AIoT surveillance, warranting further dedicated research in future work.

### I. FOSTERING COLLABORATION

Working together is key to solving problems in AIoT surveillance. Bringing in experts from different areas like cybersecurity, ethics, data science, and law can help to come up with better solutions. Different viewpoints aid creating

**TABLE 7.** Research contributions in AIoT with limited focus on regulatory, compliance, or ethical aspects.

| Ref. | Year | Brief Summary/Focus Area and Ethical/Regulatory/Compliance Focus | |
|---|---|---|---|
| | | **Brief Summary/Focus Area** | **Ethical/Regulatory/Compliance Focus** |
| [236] | 2021 | Reviews AIoT research, focusing on sensing, computing, and networking. Highlights ethical and legal considerations, emphasizing responsible design to protect user rights. | Emphasizes the necessity for ethical compliance and legal obligations in AIoT deployments. |
| [259] | 2022 | Discusses the need for AI and IoT regulatory frameworks and their adoption across countries, particularly in the EU and developing nations. | Focuses on the creation of AI and IoT regulatory frameworks in developing countries. |
| [245] | 2022 | Discusses how blockchain and AI can enhance IoT security, focusing on securing IoT data and privacy. | Mentions privacy and security challenges but lacks regulatory and compliance-specific discussion. |
| [50] | 2023 | Covers existing cybersecurity standards (ISO-27001, NIST CSF) and their application in AIoT networks. Discusses privacy and security solutions for CPS. | Detailed on ISO-27001 and other relevant standards applicable to AIoT systems. No specific mention for surveillance data; focus is more on general cybersecurity. |
| [256] | 2023 | Explores AIoT's role in energy efficiency and renewable integration, including challenges as data privacy and cybersecurity. | Brief mention of regulatory frameworks related to AIoT in smart grids, including privacy concerns. |
| [11] | 2023 | This survey discusses integrating blockchain with AIoT to enhance efficiency, security, privacy, trust, and incentives. Reviews solutions and addresses challenges in AIoT systems. | Highlights the need for regulatory frameworks to ensure secure and efficient integration but does not specify existing regulations. |
| [178] | 2023 | Discusses the balance between innovation and security in cloud environments, addressing regulations like GDPR, CCPA, and HIPAA. | Strong focus on regulatory compliance for cloud security, particularly GDPR, HIPAA, and other data privacy laws. |
| [257] | 2023 | Addresses AIoT's potential in improving networking performance, security, and productivity, including ethical concerns. | Brief mention of security and compliance in networking but lacks focus on regulatory frameworks. |
| [258] | 2023 | Examines privacy concerns of smart speaker users under China's Personal Information Protection Law (PIPL), using a socio-technical system approach. | Detailed analysis of PIPL and its impact on privacy and personal information protection. |
| [241] | 2023 | Addresses challenges in the metrology sector, proposing AI and Big Data solutions. Advocates for a National Digital Grid for Metrology and stakeholder interoperability. | Highlights the need for regulatory frameworks in metrology to adapt to digital transformations. |
| [226] | 2023 | Examines advancements in AI and IoT, focusing on their transformative effects on technology and society. Covers surveillance and healthcare while addressing challenges like privacy and ethical concerns. | Discusses ethical considerations and data privacy in the context of AI and IoT. |
| [259] | 2023 | Addresses privacy and data protection challenges in healthcare due to digital transformation. Explores the growth of telehealth, IoT-enabled medical devices, and online healthcare platforms. | Focuses on regulatory and compliance challenges related to privacy and data protection for IoT-enabled healthcare solutions in the EU context. |
| [260] | 2024 | Proposes a secure IoT-based ML system using WSNs and cloud computing for detecting viruses, emphasizing privacy, data integrity, and infectious disease detection. | Focuses on compliance with healthcare regulations like HIPAA and GDPR for secure data management. |
| [261] | 2024 | Examines how integrating Intelligent Systems with IIoT improves waste management and recycling using AIoT for advanced monitoring. | Discusses implications for regulatory compliance related to waste management and sustainability. |
| [254] | 2024 | Reviews the evolution of data privacy regulations, emphasizing challenges posed by AI and IoT. | Discusses the need for flexible and adaptable regulations to address complexities introduced by AI and IoT. |
| [262] | 2024 | Explores AIoT and Distributed Ledger Technologies (DLT) for decentralized energy trading, enhancing energy sharing and addressing market challenges. | Discusses the need for regulations to support decentralized energy trading mechanisms and ensure privacy. |
| [209] | 2024 | Explores AI's transformative role in information security, evaluating algorithms and their strengths/weaknesses. | Discusses ethical AI practices and implications of deploying AI in security. |
| [263] | 2024 | Presents an AIoT-based aviation health monitoring system utilizing cloud architecture and 6G technology to enhance predictive accuracy and safety. | No direct focus on specific regulatory or compliance standards; emphasizes strategic investment in AIoT technologies. |
| [48] | 2024 | Focuses on AIoT in healthcare cybersecurity, addressing sensitive data protection and regulatory implications. | Addresses regulations in healthcare (e.g., sensitive data protection) and cybersecurity best practices. |
| [51] | 2024 | Explores vulnerabilities in AIoT systems, improved encryption, secure protocols, and privacy-preserving strategies like anonymization, differential privacy, and federated learning. | Emphasizes security and privacy standards but lacks explicit mention of surveillance data compliance frameworks. |

strong and reliable surveillance systems. These systems can then be advanced, ethical, and legally sound. Partnerships between industry, academia, and government can also help develop standards and best practices faster. This makes sure that surveillance systems are secure, transparent, and aligned with what society values.

Although the Horizon Europe program, building on Horizon 2020, has advanced cross-disciplinary collaboration and innovation in AI and IoT [266], [267], some gaps remain. One area for improvement is integrating real-time ethical oversight within AIoT systems. While the program promotes collaboration, it often emphasizes technological advancements over continuous ethical monitoring of deployed systems.

An innovative approach is to develop a dynamic ethical assessment framework for AIoT surveillance systems. This framework would monitor and evaluate ethical implications in real-time. It would adjust system behavior to prevent

ethical breaches. Continuous checks would identify biases, privacy violations, and unauthorized data usage. This ensures compliance with ethical standards throughout operation.

Additionally, the framework could use decentralized, blockchain-based governance models. This would enhance transparency and accountability. Stakeholders from various fields could audit AIoT surveillance activities. They would contribute to ethical oversight, ensuring the technology is both effective and aligned with societal values. By addressing these gaps and implementing such innovations, future collaborations can build on the foundations laid by Horizon 2020. This will drive the development of AIoT surveillance systems that are both advanced and ethically responsible.

## V. DISCUSSION

Despite several advantages offered by AIoT based surveillance, there are plethora of challenges in its development and deployment. These critical areas need to be addressed to ensure that these systems are both effective and ethically sound. The following points are the crux of this article.

1) Standardization is the most crucial aspect due to universal nature of AIoT systems. The major issue in these systems is the interoperability. There are no worldwide accepted standards for communications protocols, security measures, and data formats. The available standards like GDPR and CCPA are a starting point, however, there is a need for them to be harmonized with international technological advancements. Once harmonized it will ensure that they keep pace with technological advancements. At present, the standards often trail behind which necessitates frequent updates to address evolving threats and advancements in AIoT surveillance.
2) AIoT surveillance systems comprise of different interconnected devices. All these devices have unique operating systems, battery requirements, communication techniques, and computational capacities. To create an efficient system each component must ensure robust security measures. However, this must be done such that performance of the system is not compromised. Surveillance systems not only process massive data but also real-time data, which compounds the problem. Such massive processing in real-time can strain resources, increase risk of performance problems as well as security risks.
3) AI algorithms are an integral part of AIoT surveillance systems. However, they face challenges like biased decision-making and a lack of transparency. For surveillance systems, advanced AI algorithms are needed that prioritize transparency and fairness. In addition, these advanced algorithms must also be efficient on edge devices, as these have limited computational and energy resources. Lightweight and robust AI models that reduce energy consumption and ensure faster processing are the need of the hour. Such efficiency is vital for effective surveillance applications.
4) The effectiveness of AIoT security frameworks is significantly constrained by the inherent limitations of edge computing environments, demanding rigorous analysis. Edge devices, such as smart cameras and sensor nodes, typically possess limited computational power, memory, storage, and power supply. These fundamental constraints directly impact the ability to implement complex cryptographic operations, run sophisticated on-device AI for anomaly detection, store extensive audit logs, or perform frequent, rigorous security checks. Consequently, security frameworks must often resort to lightweight algorithms, rely more heavily on hardware security features, or intelligently offload intensive tasks to fog/cloud layers, forcing critical trade-offs between desired security levels and a device's operational capabilities, battery life, or overall performance. Beyond computational and power limitations, edge computing introduces further security challenges due to constrained network bandwidth and reliability, complicating the timely transmission of large security updates, telemetry data, or continuous authentication checks critical for dynamic security models. The physical vulnerability of devices deployed in exposed or remote locations necessitates robust hardware-based security measures and tamper detection, which themselves consume precious resources. Moreover, the vast heterogeneity of AIoT devices, spanning diverse hardware platforms, operating systems, and firmware presents a formidable hurdle for applying uniform security policies, managing patching cycles, and ensuring consistent integrity across an entire surveillance ecosystem. Collectively, these edge computing constraints underscore the need for highly optimized, resource-aware, and adaptable security frameworks that can pragmatically address real-world deployment limitations.
5) Encryption methods are crucial to protecting surveillance data. Advanced algorithms are needed to secure sensitive footage. Encryption should cover both data at rest and data in transit. Traditional encryption techniques, such as AES, primarily secure data at rest and in transit by transforming it into an unreadable format, guaranteeing confidentiality and integrity against unauthorized access; however, the encryption and decryption processes themselves introduce computational latency. For AI model training or analysis, this data typically needs to be decrypted, which further exposes sensitive raw information during processing. In contrast, federated learning and differential privacy are privacy-preserving techniques designed to protect individual privacy during data computation. However, federated learning still faces challenges with potential data leakage through model updates, significant communication overhead, and the resultant

impact on overall system latency. Differential privacy on the other hand, provides mathematically rigorous privacy guarantees by introducing controlled statistical noise to datasets or algorithm outputs, making it virtually impossible to infer information about any single individual's data contribution; nevertheless, this often involves a fundamental trade-off between privacy strength and the utility or accuracy of the resulting model or data analysis, and the complex computations required for noise addition can also introduce additional latency. Overall, balancing efficient data processing with strong encryption and privacy-preserving techniques is a significant challenge, and these algorithms must also continuously address inherent vulnerabilities, such as those arising from patch update failures, to maintain robust security.

6) Regulations like the CCPA and GDPR pose challenges for AIoT surveillance. These laws impose strict guidelines on collecting, storing, and processing surveillance data. Penalties for noncompliance can be significant. Organizations need to consider privacy when using surveillance systems. Meeting legal requirements alone is not enough. Data privacy is crucial because AIoT can lead to misuse of surveillance footage. Addressing privacy concerns alongside regulatory compliance is important.
7) Several solutions have been proposed in order to overcome these obstacles. One of the most innovative of them is Security by Design, which implies incorporating security into an AIoT infrastructure at the start. Such measures include processes to ensure secure bootup, authentication and authorization procedures, regular system/software updates and latest encryption techniques for edge and distributed devices. Recent research also highlights federated learning as a key solution. It employs edge devices for AI model training instead of centralized cloud systems. It also enhances security since less data is moved and stored.
8) The need for zero-trust security in AIoT surveillance has emerged. No one in the network is considered trustable in the zero-trust security model. The security model demands constant checks on the users for authorization and authentication. Zero-trust security model ensures that there is no unauthorized access practically with each request being validated. It also helps in minimizing threats from the internal networks as well.
9) To overcome the challenges posed by AIoT security, a triad comprising of industry, academia, and government needs to be involved. There have been programs like the EU's Horizon 2020, which assisted these collaborations, although they tend to be very general with regard to AI technologies. There is a need for more careful targeting of these programs to the diverse security aspects of AIoT surveillance systems. An area that seems worth exploring in the future is the development of specific IDPS for AIoT environment.
10) One area that needs further research is XAI for AIoT surveillance security. XAI focusses on transparency and understandable decision-making processes. Transparency is an essential element to create trust of users in AIoT surveillance systems. It ensures compliance with strict data protection regulations.
11) Emerging technologies like quantum encryption and post-quantum cryptography are changing security. Quantum encryption uses quantum mechanics to create very strong encryption keys. This offers strong protection against advanced cyber threats. Post-quantum cryptography focuses on encryption that can resist future quantum computers. These computers might break today's cryptographic systems. Both technologies help tackle key security challenges. They provide better protection as threats evolve. AIoT surveillance systems should consider using these technologies.
12) In ongoing research for AIoT surveillance, ethical considerations are crucial. Frameworks must balance security with privacy rights. This involves developing strong consent mechanisms and conducting social impact assessments before deploying AIoT systems. Continuous ethical oversight within organizations is also essential. Addressing these concerns ensures that AIoT surveillance systems are both effective and respectful of individual rights.
13) Lastly, it is critical to create international ethical guidelines for AIoT surveillance. As AIoT technologies are adopted globally, uniform standards are needed to address key ethical concerns. These concerns include accountability, transparency, and bias. Establishing these standards will help ensure that AIoT systems are implemented ethically and responsibly.

## VI. CONCLUSION

The rapidly advancing landscape of AIoT security in surveillance offers both significant challenges and transformative opportunities. As AIoT systems continue to integrate a diverse range of devices and leverage cutting-edge technologies, the need for robust security and privacy safeguards becomes paramount. Critical challenges include managing the complexity of heterogeneous device integration, mitigating vulnerabilities in edge computing and distributed processing, defending against adversarial attacks on AI algorithms, addressing legacy infrastructure limitations, securing real-time data streams, and ensuring effective patch management and regulatory compliance. While standards like ISO-27001 provide a foundational framework for ISMS, the rapid evolution of AIoT technologies demands continual updates to these standards to keep pace with emerging threats. High-profile breaches, such as the Verkada incident, underscore the real-world consequences of security lapses

and highlight the urgent need for more proactive and dynamic security measures.

Innovative solutions, such as quantum encryption, XAI, federated learning, and context-aware adaptive IDPS, are essential to protect data both in transit and at rest. The development of lightweight protocols and enhanced AI algorithms is crucial for improving the performance of AIoT surveillance systems while reducing their vulnerability to cyberattacks. Ethical considerations, such as the adoption of zero-trust architectures and rigorous ethical oversight, are vital to maintaining user trust and ensuring compliance with legal frameworks. Furthermore, the collaboration between industry, academia, and government will be indispensable in the development of resilient and secure AIoT surveillance systems. As AIoT surveillance technology continues to evolve, addressing these multifaceted security challenges through innovative, adaptive solutions and cross-sector collaboration will be key. Ongoing research and a proactive approach are necessary to stay ahead of technological advancements and emerging security threats, ensuring the secure, ethical, and efficient deployment of AIoT in surveillance systems.

## REFERENCES


[1] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 1–24, Jan. 2022.

[2] S. E. Bibri, J. Krogstie, A. Kaboli, and A. Alahi, "Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review," *Environ. Sci. Ecotechnol.*, vol. 19, Oct. 2023, Art. no. 100330.

[3] K. Khurshid, A. Danish, M. U. Salim, M. Bayram, T. Ozbakkaloglu, and M. A. Mosaberpanah, "An in-depth survey demystifying the Internet of Things (IoT) in the construction industry: Unfolding new dimensions," *Sustainability*, vol. 15, no. 2, p. 1275, Jan. 2023.

[4] E. Mohamed, "The relation of artificial intelligence with Internet of Things: A survey," *J. Cybersecurity Inf. Manag.*, vol. 1, no. 1, pp. 30–34, Jan. 2020.

[5] S. E. Bibri, A. Alexandre, A. Sharifi, and J. Krogstie, "Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: An integrated approach to an extensive literature review," *Energy Inf.*, vol. 6, no. 1, p. 9, Apr. 2023.

[6] Y. Myagmar-Ochir and W. Kim, "A survey of video surveillance systems in smart city," *Electronics*, vol. 12, no. 17, pp. 3567–3567, Aug. 2023.

[7] M. A. Ezzat, M. A. A. E. Ghany, S. Almotairi, and M. A.-M. Salem, "Horizontal review on video surveillance for smart cities: Edge devices, applications, datasets, and future trends," *Sensors*, vol. 21, no. 9, p. 3222, May 2021.

[8] M. Langheinrich, R. Finn, V. C. Coroama, and D. Wright, *Quo Vadis Smart Surveillance? How Smart Technologies Combine and Challenge Democratic Oversight*. Heidelberg, Germany: Springer, Oct. 2013, pp. 151–182.

[9] S. Gutwirth, R. Leenes, and P. Hert, *Reloading Data Protection*. Dordrecht, The Netherlands: Springer, 2014.

[10] K. Khurshid, A. Khan, H. Siddique, and I. Rashid, "Big data-9Vs, challenges and solutions," *Tech. J.*, vol. 23, no. 3, pp. 28–34, Nov. 2018. [Online]. Available: https://tj.uettaxila.edu.pk/index.php/technical-journal/article/view/632

[11] M. Shen et al., "Blockchains for artificial intelligence of things: A comprehensive survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14483–14506, Aug. 2023.

[12] M. M. Rathore, A. Paul, W. H. Hong, H. Seo, I. Awan, and S. Saeed, "Exploiting IoT and big data analytics: Defining smart digital city using real-time urban data," *Sustain. Cities Soc.*, vol. 40, pp. 600–610, Jul. 2018.

[13] M. I. Ali et al., "Real-time data analytics and event detection for IoT-enabled communication systems," *J. Web Semantics*, vol. 42, pp. 19–37, Jan. 2017.

[14] A. Estebsari, P. R. Mazzarino, L. Bottaccioli, and E. Patti, "IoT-enabled real-time management of smart grids with demand response aggregators," *IEEE Trans. Ind. Appl.*, vol. 58, no. 1, pp. 102–112, Oct. 2021.

[15] R. Rajavel, S. K. Ravichandran, K. Harimoorthy, P. Nagappan, and K. R. Gobichettipalayam, "IoT-based smart healthcare video surveillance system using edge computing," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 6, pp. 3195–3207, Jun. 2022.

[16] A. Čolaković, S. Čaušević, A. Kosovac, and E. Muharemović, "A review of enabling technologies and solutions for IoT based smart warehouse monitoring system," in *Proc. New Technol. Develop. Appl.*, vol. 6, 2020, pp. 630–637.

[17] J. Shah and B. Mishra, "IoT enabled environmental monitoring system for smart cities," in *Proc. Int. Conf. Internet Things Appl. (IOTA)*, 2016, pp. 383–388.

[18] A. Zaman, X. Liu, and Z. Zhang, "Video analytics for railroad safety research: An artificial intelligence approach," *Transp. Res. Rec.*, vol. 2672, no. 10, pp. 269–277, Dec. 2018.

[19] M. T. Nguyen, L. H. Truong, T. T. Tran, and C. F. Chien, "Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5," *Comput. Ind. Eng.*, vol. 148, Oct. 2020, Art. no. 106671.

[20] Q. Zhang, H. Sun, X. Wu, and H. Zhong, "Edge video analytics for public safety: A review," *Proc. IEEE*, vol. 107, no. 8, pp. 1675–1696, Jul. 2019.

[21] H. R. Aradhya, "Object detection and tracking using deep learning and artificial intelligence for video surveillance applications," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, p. 19, 2019.

[22] T. Lian, B. P. Loo, and Z. Fan, "Advances in estimating pedestrian measures through artificial intelligence: From data sources, computer vision, video analytics to the prediction of crash frequency," *Comput. Environ. Urban Syst.*, vol. 107, Jan. 2024, Art. no. 102057.

[23] S. Afzal et al., "Visualization and visual analytics approaches for image and video datasets: A survey," *ACM Trans. Interact. Intell. Syst.*, vol. 13, no. 1, pp. 1–41, Mar. 2023.

[24] P. Bellavista, R. D. Penna, L. Foschini, and D. Scotece, "Machine learning for predictive diagnostics at the edge: An IIoT practical example," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–7.

[25] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[26] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2019.

[27] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10102–10110, Oct. 2020.

[28] P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, "IoVT: Internet of Vulnerable Things? Threat architecture, attack surfaces, and vulnerabilities in Internet of Things and its applications towards smart grids," *Energies*, vol. 13, no. 18, p. 4813, Sep. 2020.

[29] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics," *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, Art. no. 102761.

[30] H. Pourrahmani, A. Yavarinasab, and A. M. Monazzah, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the blockchain," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100888.

[31] C. Fontes, E. Hohma, C. C. Corrigan, and C. Lütge, "AI-powered public surveillance systems: Why we (might) need them and how we want them," *Technol. Soc.*, vol. 71, Nov. 2022, Art. no. 102137.

[32] G. Arora, J. Joshi, R. S. Mandal, N. Shrivastava, R. Virmani, and T. Sethi, "Artificial intelligence in surveillance, diagnosis, drug discovery and vaccine development against COVID-19," *Pathogens*, vol. 10, no. 8, p. 1048, Aug. 2021.

[33] A. A. Ahmed and M. Echi, "Hawk-eye: An AI-powered threat detector for intelligent surveillance cameras," *IEEE Access*, vol. 9, pp. 63283–63293, 2021.

[34] C. Shachar, S. Gerke, and E. Y. Adashi, "AI surveillance during pandemics: Ethical implementation imperatives," *Hastings Center Rep.*, vol. 50, no. 3, pp. 18–21, May 2020.

[35] A. Borda, A. Molnar, C. Neesham, and P. Kostkova, "Ethical issues in AI-enabled disease surveillance: Perspectives from global health," *Appl. Sci.*, vol. 12, no. 8, p. 3890, Apr. 2022.

[36] D. Zeng, Z. Cao, and D. B. Neill, "Artificial intelligence—Enabled public health surveillance—From local detection to global epidemic monitoring and control," in *Proc. Artif. Intell. Med.*, 2021, pp. 437–453.

[37] J. S. Brownstein, B. Rader, C. M. Astley, and H. Tian, "Advances in artificial intelligence for infectious-disease surveillance," *New England J. Med.*, vol. 388, no. 17, pp. 1597–1607, Apr. 2023.

[38] S. C. Mukhopadhyay, S. K. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial intelligence-based sensors for next generation IoT applications: A review," *IEEE Sensors J.*, vol. 21, no. 22, pp. 24920–24932, Jan. 2021.

[39] Z. Jan et al., "Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities," *Exp. Syst. Appl.*, vol. 216, Apr. 2023, Art. no. 119456.

[40] S. Zhu, K. Ota, and M. Dong, "Green AI for IIoT: Energy efficient intelligent edge computing for Industrial Internet of Things," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 79–88, Mar. 2022.

[41] M. Abouelyazid, "Advanced artificial intelligence techniques for real-time predictive maintenance in industrial IoT systems: A comprehensive analysis and framework," *J. AI Assist. Sci. Disc.*, vol. 3, no. 1, pp. 271–313, Feb. 2023.

[42] P. Fraga-Lamas, S. I. Lopes, and T. M. Fernández-Caramés, "Green IoT and edge AI as key technological enablers for a sustainable digital transition towards a smart circular economy: An industry 5.0 use case," *Sensors*, vol. 21, no. 17, p. 5745, Aug. 2021.

[43] A. Pise, B. Yoon, and S. Singh, "Enabling Ambient Intelligence of Things (AIoT) healthcare system architectures," *Comput. Commun.*, vol. 198, pp. 186–194, Jan. 2023.

[44] S. Baker and W. Xiang, "Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1261–1293, 2nd Quart., 2023.

[45] Y. Marine, "A review: Application of AIOT in smart cities in industry 4.0 and society 5.0," *Int. J. Smart Syst.*, vol. 1, no. 1, pp. 1–4, Feb. 2023.

[46] V. Santhi, Y. N. Sabareesh, P. P. Sudheer, and V. P. Krishna, "Trends and challenges in AIoT implementation for smart home, smart buildings, and smart cities in cloud platforms," in *Proc. Artif. Intell. Things (AIoT) Prod. Org. Trans.*, 2024, pp. 240–319.

[47] B. K. Kuguoglu, H. van der Voort, and M. Janssen, "The giant leap for smart cities: Scaling up smart city artificial intelligence of things (AIoT) initiatives," *Sustainability*, vol. 13, no. 21, 2021, Art. no. 12295.

[48] M. Vijarania, S. Gupta, A. Agrawal, and S. Misra, *Achieving Sustainable Development Goals in Cyber Security Using AIoT for Healthcare Application*. Cham, Switzerland: Springer, Sep. 2024, pp. 207–231.

[49] S. Doss, "AIoT and the governance of security," in *Information Security Governance Using Artificial Intelligence of Things in Smart Environments*. Boca Raton, FL, USA: CRC Press, 2025.

[50] U. Ahmad, H. Zaib, and K. N. Qureshi, "Cybersecurity standards for AIoT networks," in *Artificial Intelligence of Things (AIoT)*. Boca Raton, FL, USA: CRC Press, 2024, pp. 179–197.

[51] M. I. Mihailescu and S. L. Nita, *Securing Web Data and Privacy in AIoT Systems*. London, U.K.: IGI Global, 2024, pp. 128–172.

[52] A. Calder, *Nine Steps to Success: An ISO 27001 Implementation Overview*. London, U.K.: IT Governance Ltd., 2017.

[53] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector," *Sustainability*, vol. 15, no. 7, p. 5828, Mar. 2023.

[54] J. Jevelin and A. Faza, "Evaluation the information security management system: A path towards ISO 27001 certification," *J. Inf. Syst. Inf.*, vol. 5, no. 4, pp. 1240–1256, Nov. 2023.

[55] Y. Kamil, S. Lund, and M. S. Islam, "Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden," *Inf. Syst. e-Bus. Manag.*, vol. 21, no. 3, pp. 699–722, Sep. 2023.

[56] M. Alshar'e, "Cyber security framework selection: Comparison of NIST and ISO27001," *Appl. Comput. J.*, vol. 3, pp. 245–255, Feb. 2023.

[57] A. A. Alrehili and O. H. Alhazmi, "ISO/IEC 27001 standard: Analytical and comparative overview," in *Proc. Int. Conf. Adv. Data Driven Comput. Intell. Syst.*, 2023, pp. 143–156.

[58] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, "Information security and value creation: The performance implications of ISO/IEC 27001," *Comput. Ind.*, vol. 142, Nov. 2022, Art. no. 103744.

[59] T. S. Junaid. "ISO 27001: Information security management systems." 2020. [Online]. Available: https://doi.org/10.13140/RG.2.2.36267.52005

[60] P. E. Pais, J. T. Farinha, A. J. Cardoso, and H. Raposo, "Optimizing the life cycle of physical assets—A review," *WSEAS Trans. Syst. Control*, vol. 15, pp. 417–430, Oct. 2020.

[61] R. Damaševičius, N. Bacanin, and S. Misra, "From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management," *J. Sensor Actuator Netw.*, vol. 12, no. 3, p. 41, May 2023.

[62] K. Imran, N. Anjum, A. Alghamdi, A. Shaikh, M. Hamdi, and S. Mahfooz, "A secure and efficient cluster-based authentication scheme for internet of things (IoTs)," *Comput. Mater. Continua*, vol. 70, no. 1, pp. 1033–1052, Jan. 2022.

[63] M. I. Bhat and K. J. Giri, "Impact of computational power on cryptography," in *Multimedia Security: Algorithm Development, Analysis and Applications*. Singapore: Springer, 2021, pp. 45–88.

[64] E. Koza, "Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security," *Med. Eng. Themes*, vol. 2, no. 3, pp. 26–39, 2022.

[65] T. Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (and Why it Matters)*, New York Times, New York, NY, USA, Sep. 2021.

[66] N. B. Sureani, A. S. Qurni, A. H. Azman, M. B. Othman, and H. S. Zahari, "The adequacy of data protection laws in protecting personal data in Malaysia," *Malaysian J. Soc. Sci. Humanities*, vol. 6, no. 10, pp. 488–495, Oct. 2021.

[67] ISMS.online. "Annex a.18: Compliance." 2012. [Online]. Available: https://www.isms.online/iso-27001/annex-a-18-compliance/#::text=18.1

[68] A. K. Rama, Suharjito, and E. Gunawan, "Evaluation of IT governance implementation using COBIT 5 framework and ISO 38500 at telecommunication industries," in *Proc. Int. Conf. Inf. Manag. Technol. (ICIMTech)*, 2020, pp. 453–457.

[69] J. P. K. Kouassi. "ISO/IEC 27002: Strength and weakness." Accessed: Aug. 1, 2024. [Online]. Available: https://www.linkedin.com/pulse/isoiec-27002-strength-weakness-jean-paul-k-kouassi-mk4he/

[70] F. Chen, D. Luo, J. Li, V. C. M. Leung, S. Li, and J. Fan, "Arm PSA-certified IoT chip security: A case study," *Tsinghua Sci. Technol.*, vol. 28, no. 2, pp. 244–257, Apr. 2023.

[71] A. A. Allaf and W. Totonji. "Exploring IoT security threats and forensic challenges: A literature review and survey study." 2023. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1764110

[72] Verkada. "Security update." Accessed: Aug. 1, 2024. [Online]. Available: https://www.verkada.com/security-update

[73] Wired. "LendingTree, advanced auto parts hit in snowflake data breach." Accessed: Aug. 1, 2024. [Online]. Available: https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/

[74] C. Page. "Snowflake customer passwords found online after infostealing malware attack." Accessed: Aug. 15, 2024. [Online]. Available: https://techcrunch.com/2024/06/05/snowflake-customer-passwords-found-online-infostealing-malware/

[75] Snowflake Community. "Detecting and preventing unauthorized user access." 2024. Accessed: Aug. 16, 2024. [Online]. Available: https://community.snowflake.com/s/question/0D5VI00000Emyl00AB/detecting-and-preventing-unauthorized-user-access

[76] CBS News 8. "Prevent your doorbell camera from being hacked: Here's how." 2024. Accessed: Aug. 16, 2024. [Online]. Available: https://www.cbs8.com/article/news/local/prevent-doorbell-camera-from-being-hacked-heres-how/509-8867ce7e-3786-420e-b5ab-5b3887210835

[77] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. C. Johnson, "Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11224–11239, Jul. 2023.

[78] CNIL. "Employee monitoring: CNIL fined AMAZON FRANCE LOGISTIQUE 32 million." Dec. 27, 2023. [Online]. Available: https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million

[79] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges, and solutions," *J. Ambient Intell. Humanized Comput.*, vol. 15, pp. 1625–1642, Feb. 2024.

[80] V. D. Gowda, M. Kaur, D. Srinivas, K. D. Prasad, and R. Shekhar, "AIoT integration advancements and challenges in smart sensing technologies for smart devices," in *AIoT and Smart Sensing Technologies for Smart Devices*. London, U.K.: IGI Global, 2024, pp. 42–65.

[81] B. Jedari, G. Premsankar, G. Illahi, M. D. Francesco, A. Mehrabi, and A. Ylä-Jääski, "Video caching, analytics, and delivery at the wireless edge: A survey and future directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 431–471, 1st Quart., 2021.

[82] A. Antony and S. Sarika, "A review on IoT operating systems," *Int. J. Comput. Appl.*, vol. 176, pp. 33–40, May 2020.

[83] K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, and C. de Vaulx, "Trends and challenges in AIoT/IIoT/IoT implementation," *Sensors*, vol. 23, no. 11, p. 5074, May 2023.

[84] S. S. Albouq, A. A. A. Sen, N. Almashf, M. Yamin, A. Alshanqiti, and N. M. Bahbouh, "A survey of interoperability challenges and solutions for dealing with them in IoT environment," *IEEE Access*, vol. 10, pp. 36416–36428, 2022.

[85] G. Yang, M. A. Jan, A. U. Rehman, M. Babar, M. M. Aimal, and S. Verma, "Interoperability and data storage in Internet of Multimedia Things: Investigating current trends, research challenges and future directions," *IEEE Access*, vol. 8, pp. 124382–124401, 2020.

[86] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, and S. Karuppayah, "MQTT vulnerabilities, attack vectors and solutions in the Internet of Things (IoT)," *IETE J. Res.*, vol. 69, no. 6, pp. 3368–3397, Aug. 2023.

[87] F. A. Alhaidari and E. J. Alqahtani, "Securing communication between fog computing and IoT using constrained application protocol (CoAP): A survey," *J. Commun.*, vol. 15, no. 1, pp. 14–30, Jan. 2020.

[88] M. Amoretti, R. Pecori, Y. Protskaya, L. Veltri, and F. Zanichelli, "A scalable and secure publish/subscribe-based framework for Industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 3815–3825, Jun. 2021.

[89] E. Al-Masri et al., "Investigating messaging protocols for the Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 94880–94911, 2020.

[90] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A general overview between architectures, protocols and applications," *Information*, vol. 12, no. 2, p. 87, Feb. 2021.

[91] L. Catuogno and C. Galdi, "Secure firmware update: Challenges and solutions," *Cryptography*, vol. 7, no. 2, p. 30, Jun. 2023.

[92] K. A. Alaghbari, M. H. Saad, A. Hussain, and M. R. Alam, "Complex event processing for physical and cyber security in data centres-recent progress, challenges and recommendations," *J. Cloud Comput.*, vol. 11, no. 1, p. 65, Oct. 2022.

[93] T. Mazhar et al., "Analysis of IoT security challenges and its solutions using artificial intelligence," *Brain Sci.*, vol. 13, no. 4, p. 683, Apr. 2023.

[94] C. H. Hong and B. Varghese, "Resource management in fog/edge computing: A survey on architectures, infrastructure, and algorithms," *ACM Comput. Surveys*, vol. 52, no. 5, pp. 1–37, Sep. 2019.

[95] E. Fazeldehkordi and T. M. Grønli, "A survey of security architectures for edge computing-based IoT," *IoT*, vol. 3, no. 3, pp. 332–365, Jun. 2022.

[96] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2205–2224, Apr. 2019.

[97] R. Smith, D. Palin, P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "Battery draining attacks against edge computing nodes in IoT networks," *Cyber Phys. Syst.*, vol. 6, no. 2, pp. 96–116, Apr. 2020.

[98] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing assisted Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021.

[99] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[100] M. Vidaković and D. Vinko, "Hardware-based methods for electronic device protection against invasive and non-invasive attacks," *Electronics*, vol. 12, no. 21, p. 4507, Nov. 2023.

[101] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Proc. ICCCIOT*, 2021, pp. 213–222.

[102] A. Roy, J. Kokila, N. Ramasubramanian, and B. S. Begum, "Device-specific security challenges and solution in IoT edge computing: A review," *J. Supercomputing*, vol. 79, no. 18, pp. 20790–20825, Dec. 2023.

[103] M. Silva, D. Cerdeira, S. Pinto, and T. Gomes, "Operating systems for Internet of Things low-end devices: Analysis and benchmarking," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10375–10383, Dec. 2019.

[104] F. Bruschi, M. Zanghieri, M. Terziani, and D. Sciuto, "Decentralized updates of IoT and edge devices," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.*, Apr. 2024, pp. 161–170.

[105] "Attacks on edge devices surge: Multiple critical vulnerabilities identified." 2024, Accessed: Aug. 19, 2024. [Online]. Available: https://www.kratosdefense.com/constellations/articles/attacks-on-edge-devices-surge-multiple-critical-vulnerabilities-identified

[106] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *Proc. IEEE Symp. Security Privacy (SP)*, 2019, pp. 1362–1380.

[107] H. F. Atlam and G. B. Wills, "Intersections between IoT and distributed ledger," in *Advances in Computers*, vol. 115. Amsterdam, The Netherlands: Elsevier, 2019, pp. 73–113.

[108] H. Xu, K. P. Seng, L. M. Ang, and J. Smith, "Decentralized and distributed learning for AIoT: A comprehensive review, emerging challenges and opportunities," *IEEE Access*, vol. 12, pp. 125678–125692, 2024.

[109] Z. Wang, Y. Hu, S. Yan, Z. Wang, R. Hou, and C. Wu, "Efficient ring-topology decentralized federated learning with deep generative models for medical data in e-healthcare systems," *Electronics*, vol. 11, no. 10, p. 1548, May 2022.

[110] J. Röckl, A. Wagenhäuser, and T. Müller, "Veto: Prohibit outdated edge system software from booting," in *Proc. Int. Conf. Inf. Syst. Security Privacy*, Lisbon, Portugal, Feb. 2023, pp. 46–57.

[111] J. Larsson, "Are modern smart cameras vulnerable to yesterday's vulnerabilities? A security evaluation of a smart home camera," M.S. thesis, School Elect. Eng. Comput. Sci., KTH, Stockholm, Sweden, 2021. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?dswid=510&pid=diva2

[112] P. Mahadevappa, R. Al-Amri, G. Alkawsi, A. A. Alkahtani, M. F. Alghenaim, and M. Alsamman, "Analyzing threats and attacks in edge data analytics within IoT environments," *IoT*, vol. 5, no. 1, pp. 123–154, Mar. 2024.

[113] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-computing architectures for Internet of Things applications: A survey," *Sensors*, vol. 20, no. 22, p. 6441, Nov. 2020.

[114] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of IP-based video surveillance systems," *Sensors*, vol. 20, no. 17, p. 4806, Aug. 2020.

[115] K. Nandakumar et al., "Securing data in transit using data-in-transit defender architecture for cloud communication," *Soft Comput.*, vol. 25, pp. 12343–12356, Jun. 2021.

[116] S. Sadoudi, C. Tanougast, B. Bouteghrine, H. Chen, and S. Mihoub, "Video cryptosystem using chaotic systems," in *Recent Advances in Image Security Technologies: Intelligent Image, Signal, and Video Processing*. Cham, Switzerland: Springer Int., 2023, pp. 127–162.

[117] K. Khan and W. Goodridge, "A comprehensive taxonomy for AIoT video streaming systems: Components, connectivity, and applications," *Int. J. Multidiscipl. Res. Publications*, vol. 6, no. 2, pp. 133–145, 2023.

[118] A. Behrendt, E. D. Boer, T. Kasah, B. Koerber, N. Mohr, and G. Richter. "Leveraging industrial IoT and advanced technologies for digital transformation." Feb. 2021. [Online]. Available: https://sightmachine.com/leveraging-industrial-iot-and-advanced-technologies-for-digital-transformation/

[119] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Comput. Surveys*, vol. 54, no. 10s, pp. 1–28, Sep. 2022.

[120] D. Almeida, K. Shmarko, and E. Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of U.S., E.U., and U.K. regulatory frameworks," *AI Ethics*, vol. 2, no. 3, pp. 377–387, Aug. 2022.

[121] C. Jasserand, "Experiments with facial recognition technologies in public spaces: In search of an EU governance framework," in *Handbook on the Politics and Governance of Big Data and Artificial Intelligence*, E. Elgar, Ed. Cheltenham, U.K.: Edward Elgar, 2023, pp. 315–357.

[122] H. Xue, "A study on image privacy protection in response to artificial intelligence technology," Ph.D. dissertation, Elect. Eng., Univ. Technol., Sydney, Sydney, NSW, Australia, 2023.

[123] N. Guhr, O. Werth, P. P. Blacha, and M. H. Breitner, "Privacy concerns in the smart home context," *SN Appl. Sci.*, vol. 2, pp. 1–2, Feb. 2020.

[124] V. Wylde et al., "Cybersecurity, data privacy and blockchain: A review," *SN Comput. Sci.*, vol. 3, no. 2, p. 127, Mar. 2022.

[125] Datanami. "Data prep still dominates data scientists' time, survey finds." Accessed: Aug. 20, 2024. [Online]. Available: https://www.datanami.com/2020/07/06/data-prep-stilldominates-data-scientists-time-survey-finds/

[126] M. Stonebraker and E. K. Rezig, "Machine learning and big data: What is important?" *IEEE Data Eng. Bull.*, vol. 42, no. 4, pp. 3–7, Jun. 2019.

[127] S. E. Whang et al., "Data collection and quality challenges in deep learning: A data-centric AI perspective," *VLDB J.*, vol. 32, no. 4, pp. 791–813, Jul. 2023.

[128] M. Westerlund, "The emergence of deepfake technology: A review," *Technol. Innov. Manag. Rev.*, vol. 9, no. 11, p. 23, 2019.

[129] T. Greene. "Watch: Fake ELON musk zoom-bombs meeting using real-time deepfake AI." Accessed: Aug. 20, 2024. [Online]. Available: https://thenextweb.com/neural/2020/04/21/watch-fake-elon-musk-zoom-bombs-meeting-using-real-time-deepfake-ai/

[130] Y. Liu et al., "A survey on neural trojans," in *Proc. 21st Int. Symp. Qual. Electron. Design (ISQED)*, Mar. 2020, pp. 33–39.

[131] A. S. Rakin et al., "TBT: Targeted neural network attack with bit trojan," 2019, *arXiv:1909.05193*.

[132] F. T. Council. "Supply chain attacks on AI." Apr. 2022. Accessed: Aug. 21, 2024. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2022/04/11/supply-chain-attacks-on-ai/

[133] T. Ahmad et al., "Human activity recognition based on deep-temporal learning using convolution neural networks features and bidirectional gated recurrent unit with features selection," *IEEE Access*, vol. 11, pp. 33148–33159, 2023.

[134] M. S. Santos et al., "Cross-validation for imbalanced datasets: Avoiding overoptimistic and overfitting approaches [research frontier]," *IEEE Comput. Intell. Mag.*, vol. 13, no. 4, pp. 59–76, Nov. 2018.

[135] B. Kiran et al., "An overview of deep learning based methods for unsupervised and semi-supervised anomaly detection in videos," *J. Imag.*, vol. 4, no. 2, p. 36, 2018.

[136] A. I. Khan and S. Al-Habsi, "Machine learning in computer vision," *Procedia Comput. Sci.*, vol. 167, pp. 1444–1451, 2020.

[137] C. Janiesch et al., "Machine learning and deep learning," *Electron. Markets*, vol. 31, no. 3, pp. 685–695, 2021.

[138] Y. Zhu et al., "Hidden two-stream convolutional networks for action recognition," in *Proc. Asian Conf. Comput. Vis.*, 2018, pp. 363–378.

[139] M. Sabokrou, M. Fayyaz, M. Fathy, Z. Moayed, and R. Klette, "Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes," *Comput. Vis. Image Understand.*, vol. 172, pp. 88–97, Jul. 2019.

[140] R. Maqsood et al., "Anomaly recognition from surveillance videos using 3-D convolution neural network," *Multimedia Tools Appl.*, vol. 80, pp. 18693–18716, Feb. 2021.

[141] J. W. Lee and H. S. Kang, "Three-stage deep learning framework for video surveillance," *Appl. Sci.*, vol. 14, no. 1, p. 408, 2024.

[142] V. Akula and I. Kavati, "Human violence detection in videos using key frame identification and 3-D CNN with convolutional block attention module," *Circuits Syst. Signal Process.*, vol. 43, pp. 7924–7950, Aug. 2024.

[143] E. A. Mahareek et al., "Detecting anomalies in security cameras with 3-D-convolutional neural network and convolutional long short-term memory," *Int. J. Elect. Comput. Eng.*, vol. 14, no. 1, pp. 993–1004, 2024.

[144] J. Chen et al., "CNN-LSTM model for recognizing video-recorded actions performed in a traditional Chinese exercise," *IEEE J. Transl. Eng. Health Med.*, vol. 11, pp. 351–359, 2023.

[145] M. Woźniak et al., "Recurrent neural network model for IoT and networking malware threat detection," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5583–5594, Aug. 2021.

[146] W. Ullah et al., "An efficient anomaly recognition framework using an attention residual LSTM in surveillance videos," *Sensors*, vol. 21, no. 8, p. 2811, 2021.

[147] R. Raja et al., "Analysis of anomaly detection in surveillance video: Recent trends and future vision," *Multimedia Tools Appl.*, vol. 82, no. 8, pp. 12635–12651, 2023.

[148] G. Wu et al., "SVM-based fast CU partitioning algorithm for VVC intra coding," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2021, pp. 1–5.

[149] X. Huang and L. Du, "Fire detection and recognition optimization based on virtual reality video image," *IEEE Access*, vol. 8, pp. 77951–77961, 2020.

[150] F. H. Awad et al., "Robust classification and detection of big medical data using advanced parallel K-means clustering, YOLOv4, and logistic regression," *Life*, vol. 13, no. 3, p. 691, 2023.

[151] Y. Chang et al., "Video anomaly detection with spatio-temporal dissociation," *Pattern Recognit.*, vol. 122, Feb. 2022, Art. no. 108213.

[152] Z. Su et al., "A traffic event detection method based on random forest and permutation importance," *Mathematics*, vol. 10, no. 6, p. 873, 2022.

[153] A. K. Langroodi et al., "Activity recognition of construction equipment using fractional random forest," *Autom. Construct.*, vol. 122, Feb. 2021, Art. no. 103465.

[154] R. Vijeikis et al., "Efficient violence detection in surveillance," *Sensors*, vol. 22, no. 6, p. 2216, 2022.

[155] N. Li et al., "Spatial-temporal cascade autoencoder for video anomaly detection in crowded scenes," *IEEE Trans. Multimedia*, vol. 23, pp. 203–215, Apr. 2020.

[156] S. Mishra and S. Jabin, "Anomaly detection in surveillance videos using deep autoencoder," *Int. J. Inf. Technol.*, vol. 16, no. 2, pp. 1111–1122, Feb. 2024.

[157] K. V. Joshi and N. M. Patel, "Anomaly detection in surveillance scenes using autoencoders," *SN Comput. Sci.*, vol. 4, no. 6, p. 804, Oct. 2023.

[158] M. Yan, Y. Xiong, and J. She, "Memory clustering autoencoder method for human action anomaly detection on surveillance camera video," *IEEE Sensors J.*, vol. 23, no. 18, pp. 20715–20728, Sep. 2023.

[159] N. Varshney and B. Bakariya, "Deep convolutional neural model for human activities recognition in a sequence of video by combining multiple CNN streams," *Multimedia Tools Appl.*, vol. 81, pp. 42117–42129, Aug. 2022. [Online]. Available: https://doi.org/10.1007/s11042-021-11220-4

[160] A. B. Mabrouk and E. Zagrouba, "Spatio-temporal feature using optical flow-based distribution for violence detection," *Pattern Recognit. Lett.*, vol. 92, pp. 62–67, Jun. 2017.

[161] A. Ladjailia, I. Bouchrika, H. F. Merouani, N. Harrati, and Z. Mahfouf, "Human activity recognition via optical flow: Decomposing activities into basic actions," *Neural Comput. Appl.*, vol. 32, pp. 16387–16400, Jun. 2020.

[162] H. Song, C. Sun, X. Wu, M. Chen, and Y. Jia, "Learning normal patterns via adversarial attention-based autoencoder for abnormal event detection in videos," *IEEE Trans. Multimedia*, vol. 22, no. 8, pp. 2138–2148, Aug. 2020.

[163] K. Doshi and Y. Yilmaz, "Online anomaly detection in surveillance videos with asymptotic bound on false alarm rate," *Pattern Recognit.*, vol. 114, Jun. 2021, Art. no. 107865.

[164] S. Zhang, S. Zhang, Z. Qian, J. Wu, Y. Jin, and S. Lu, "DeepSlicing: Collaborative and adaptive CNN inference with low latency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 9, pp. 2175–2187, Sep. 2021.

[165] A. Chatzimparmpas, R. M. Martins, I. Jusufi, K. Kucher, F. Rossi, and A. Kerren, "The state-of-the-art in enhancing trust in machine learning models with the use of visualizations," *Comput. Graph. Forum*, vol. 39, no. 3, pp. 713–756, Jun. 2020.

[166] Statsig. "In defense of Zillow's besieged data scientists." Nov. 2021. Accessed: Aug. 2, 2024. [Online]. Available: https://www.statsig.com/blog/in-defense-of-zillows-data-scientists

[167] K. Koga and K. Takemoto, "Simple black-box universal adversarial attacks on deep neural networks for medical image classification," *Algorithms*, vol. 15, no. 5, p. 144, 2022.

[168] D. Ding, M. Zhang, F. Feng, Y. Huang, E. Jiang, and M. Yang, "Black-box adversarial attack on time series classification," in *Proc. AAAI Conf. Artif. Intell.*, vol. 37, 2023, pp. 7358–7368.

[169] H. Khazane, M. Ridouani, F. Salahdine, and N. Kaabouch, "A holistic review of machine learning adversarial attacks in IoT networks," *Future Internet*, vol. 16, no. 1, p. 32, 2024.

[170] H. Na, W. Lee, S. Roh, S. Park, and D. Choi, "Robustness analysis against adversarial patch attacks in fully unmanned stores," 2025, *arXiv:2505.08835*.

[171] S. Hina, Q. Abbas, and K. Ahmed, "Adversarial attacks on Artificial Internet of Things-based operational technologies in theme parks," *Internet Things*, vol. 32, Jul. 2025, Art. no. 101654.

[172] Q. Tan, Y. Li, and B.-S. Shin, "Defending against backdoor attacks in federated learning by using differential privacy and OOD data attributes," *Comput. Model. Eng. Sci.*, vol. 143, no. 2, pp. 2417–2428, 2025. [Online]. Available: http://www.techscience.com/CMES/v143n2/61439

[173] N. D. Lucca, G. M. Martins, and R. C. Queiroz, "Brazilian general data protection law (LGPD) and California consumer privacy act (CCPA): A critical analysis of consumer personal data protection in Brazil and the state of California (USA)," *Brazil. J. Law Technol. Innov.*, vol. 1, no. 1, pp. 38–57, Feb. 2023.

[174] M. N. Bhutta et al., "Towards secure IoT-based payments by extension of payment card industry data security standard (PCI DSS)," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, p. 14, Jan. 2022.

[175] C. Dul, "Facial recognition technology vs privacy: The case of Clearview AI," *Queen Mary Law J.*, vol. 2022, no. 1, pp. 1–24, 2022.

[176] M. Kohn, "Clearview AI, TikTok, and the collection of facial images in international law," *Chicago J. Int. Law*, vol. 23, no. 1, p. 195, 2022.

[177] E. K. Cortez and N. Maslej, "Adjudication of artificial intelligence and automated decision-making cases in Europe and the USA," *Eur. J. Risk Regul.*, vol. 14, no. 3, pp. 457–475, Sep. 2023.

[178] R. Sundar, P. B. Srikaanth, D. A. Naik, V. P. Murugan, M. Karumudi, and S. Boopathi, "Achieving balance between innovation and security in the cloud with artificial intelligence of things: Semantic Web control models," in *Semantic Web Technologies and Applications in Artificial Intelligence of Things*. London, U.K.: IGI Global, 2024, pp. 1–26.

[179] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices," *Sensors*, vol. 24, no. 12, p. 4008, Jun. 2024.

[180] P. Thaenkaew, B. Quoitin, and A. Meddahi, "Leveraging larger AES keys in LoRaWAN: A practical evaluation of energy and time costs," *Sensors*, vol. 23, no. 22, p. 9172, 2023.

[181] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, p. 1083, Mar. 2022.

[182] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of Internet of Things based on cryptographic algorithms: A survey," *Wireless Netw.*, vol. 27, no. 2, pp. 1515–1555, Feb. 2021.

[183] O. Popoola, M. A. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security," *Internet Things*, vol. 27, Oct. 2024, Art. no. 101314.

[184] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control," *Alexandria Eng. J.*, vol. 84, pp. 275–284, Dec. 2023.

[185] "Hybrid encryption approaches and key management." Accessed: Aug. 25, 2024. [Online]. Available: https://forum.huawei.com/enterprise/en/encryption-protocols-and-the-best-practices/thread/693474328018042880-667213854934970368

[186] A. Awasthi, "Quantum-resistant security for IoT systems: Challenges and implementation strategies," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 1, no. 1, pp. 671–678, 2025.

[187] F. Firouzi et al., "Fusion of IoT, AI, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in Healthcare and medicine," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 3686–3705, Mar. 2023.

[188] W. J. Buchanan and H. Ali, "Evaluation of privacy-aware support vector machine (SVM) learning using homomorphic encryption," 2025, *arXiv:2503.04652*.

[189] E. S. Alu, K. Yunana, and M. U. Ogah, "Secured cloud data storage encryption using post-quantum cryptography," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 11, no. 7, p. 24, Jul. 2022.

[190] H. U. Khan, N. Ali, F. Ali, and S. Nazir, "Transforming future technology with quantum-based IoT," *J. Supercomput.*, vol. 80, pp. 22362–22396, Jun. 2024.

[191] J. Bozhko, Y. Hanna, R. Harrilal-Parchment, S. Tonyali, and K. Akkaya, "Performance evaluation of quantum-resistant TLS for consumer IoT devices," in *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, 2023, pp. 230–235.

[192] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1748–1774, 3rd Quart., 2024.

[193] E. D. Demir, B. Bilgin, and M. C. Onbasli, "Performance analysis and industry deployment of post-quantum cryptography algorithms," 2025, *arXiv:2503.12952*.

[194] M. Babar and F. Arif, "Smart urban planning using big data analytics to contend with the interoperability in Internet of Things," *Future Gener. Comput. Syst.*, vol. 77, pp. 65–76, Dec. 2017.

[195] J. Tournier, F. Lesueur, F. L. Mouël, L. Guyon, and H. Ben-Hassine, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet Things*, vol. 16, Dec. 2021, Art. no. 100264.

[196] S. Yang and R. Wei, "Semantic interoperability through a novel cross-context tabular document representation approach for smart cities," *IEEE Access*, vol. 8, pp. 70676–70692, 2020.

[197] D. Belli, P. Barsocchi, and F. Palumbo, "Connectivity standards alliance matter: State of the art and opportunities," *Internet Things*, vol. 25, Nov. 2023, Art. no. 101005.

[198] A. Ansari, M. Nazir, and K. Mustafa, "Smart homes App vulnerabilities, threats, and solutions: A systematic literature review," *J. Netw. Syst. Manag.*, vol. 32, p. 29, Feb. 2024.

[199] C. Loreck. "How does the new IoT standard matter? Innovation through Standardization in smart home ecosystems." 2024. [Online]. Available: https://www.edit.fis.uni-hamburg.de/ws/files/54825461/EURAS_2024_Loreck_Matter.pdf

[200] PR Newswire. "More than 5.5 billion smart home matter-compliant devices will ship between 2022 and 2030." Accessed: Aug. 26, 2024. [Online]. Available: https://www.prnewswire.com/news-releases/more-than-5-5-billion-smart-home-matter-compliant-devices-will-ship-between-2022-and-2030–301477876.html

[201] Y. Zhao, Y. Yin, and G. Gui, "Lightweight deep learning based intelligent edge surveillance techniques," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 4, pp. 1146–1154, Dec. 2020.

[202] R. Chalapathy and S. Chawla. "Deep learning for anomaly detection: A survey." 2019. [Online]. Available: https://arxiv.org/abs/1901.03407

[203] L. Alzubaidi et al., "Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions," *J. Big Data*, vol. 8, pp. 1–74, Mar. 2021.

[204] T. Das, R. M. Shukla, and S. Sengupta, "What could possibly go wrong? Identification of current challenges and prospective opportunities for anomaly detection in Internet of Things," *IEEE Netw.*, vol. 37, no. 3, pp. 194–200, Nov./Jun. 2023.

[205] W. Lim, K. Y. Chek, L. B. Theng, and C. T. Lin, "Future of generative adversarial networks (GAN) for anomaly detection in network security: A review," *Comput. Security*, vol. 139, Apr. 2024, Art. no. 103733,

[206] S. Dey, A. K. Singh, D. K. Prasad, and K. D. McDonald-Maier, "IronMAN: An approach to perform temporal motionless analysis of video using CNN in MPSoC," *IEEE Access*, vol. 8, pp. 137101–137115, 2020.

[207] M. R. Bhuiyan et al., "Hajj pilgrimage video analytics using CNN," *Bull. Elect. Eng. Inf.*, vol. 10, no. 5, pp. 2598–2606, Oct. 2021.

[208] R. Sharma and A. Sungheetha, "An efficient dimension reduction based fusion of CNN and SVM model for detection of abnormal incident in video surveillance," *J. Soft Comput. Paradigm*, vol. 3, no. 2, pp. 55–69, May 2021.

[209] E. Hashmi, M. M. Yamin, and S. Y. Yayilgan, "Securing tomorrow: A comprehensive survey on the synergy of artificial intelligence and information security," *AI Ethics*, vol. 5, pp. 1911–1929, Jul. 2024.

[210] T. Liang, J. Glossner, L. Wang, S. Shi, and X. Zhang, "Pruning and quantization for deep neural network acceleration: A survey," *Neurocomputing*, vol. 461, pp. 370–403, Oct. 2021.

[211] T. Choudhary, V. Mishra, A. Goswami, and J. Sarangapani, "A comprehensive survey on model compression and acceleration," *Artif. Intell. Rev.*, vol. 53, pp. 5113–5155, Oct. 2020.

[212] A. Kuzmin et al., "Pruning vs. quantization: Which is better?" in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 36, Feb. 2024, pp. 1–8.

[213] G. Menghani, "Efficient deep learning: A survey on making deep learning models smaller, faster, and better," *ACM Comput. Surveys*, vol. 55, no. 12, pp. 1–37, Mar. 2023.

[214] R. A. Aral, C. Zalluhoglu, and E. A. Sezer, "Lightweight and attention-based CNN architecture for wildfire detection using UAV vision data," *Int. J. Remote Sens.*, vol. 44, no. 18, pp. 5768–5787, Sep. 2023.

[215] C. C. Wang, C. T. Chiu, and J. Y. Chang, "EfficientNet-elite: Extremely lightweight and efficient CNN models for edge devices by network candidate search," *J. Signal Process. Syst.*, vol. 95, no. 5, pp. 657–669, May 2023.

[216] F. Chen et al., "Review of lightweight deep convolutional neural networks," *Arch. Comput. Methods Eng.*, vol. 31, no. 4, pp. 1915–1937, May 2024.

[217] J. Wen et al., "A survey on federated learning: Challenges and applications," *Int. J. Mach. Learn. Cybern.*, vol. 14, no. 2, pp. 513–535, Feb. 2023.

[218] M. Ye et al., "Heterogeneous federated learning: State-of-the-art and research challenges," *ACM Comput. Surveys*, vol. 56, no. 3, pp. 1–44, Oct. 2023.

[219] T. Awosika, R. M. Shukla, and B. Pranggono, "Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection," *IEEE Access*, vol. 12, pp. 123456–123467, 2024.

[220] I. Kök et al., "Explainable artificial intelligence (XAI) for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14764–14779, Aug. 2023.

[221] R. Dwivedi et al., "Explainable AI (XAI): Core ideas, techniques, and solutions," *ACM Comput. Surveys*, vol. 55, no. 9, pp. 1–33, Jan. 2023.

[222] G. Rjoub et al., "A survey on explainable artificial intelligence for cybersecurity," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 4, pp. 5115–5140, Dec. 2023.

[223] W. J. Murdoch et al., "Definitions, methods, and applications in interpretable machine learning," *Proc. Nat. Acad. Sci. USA*, vol. 116, no. 44, pp. 22071–22080, Oct. 2019.

[224] M. Juric, A. Sandic, and M. Brcic, "AI safety: State of the field through quantitative lens," in *Proc. 43rd Int. Conv. Inf. Commun. Electron. Technol. (MIPRO)*, Sep. 2020, pp. 1254–1259.

[225] B. Desai, K. Patil, I. Mehta, and A. Patil, "A secure communication framework for smart city infrastructure leveraging encryption, intrusion detection, and blockchain technology," *Adv. Comput. Sci.*, vol. 7, no. 1, p. 12, Jan. 2024.

[226] S. F. Mallo, "A review on feasibility of web technology and cloud computing for sustainable ES: Leveraging AI, IoT, and security for green operations," *J. Inf. Technol. Inform.*, vol. 3, no. 2, p. 125, Aug. 2024.

[227] J. Jayadatta, "A study on latest developments in artificial intelligence (AI) and Internet of Things (IoT) in current context," *J. Appl. Inf. Sci.*, vol. 11, no. 2, pp. 21–28, 2023.

[228] A. I. Weinberg and K. Cohen. "Zero trust implementation in the emerging technologies era: Survey." Jan. 2024. [Online]. Available: https://arxiv.org/abs/2401.09575

[229] A. Berber and S. Srećković, "When something goes wrong: Who is responsible for errors in ML decision-making?" *AI Soc.*, vol. 38, no. 1, pp. 1–3, Feb. 2023.

[230] I. T. Javed and K. N. Qureshi, "Role of blockchain models for AIoT communication systems," in *Artificial Intelligence of Things (AIoT)*. Boca Raton, FL, USA: CRC Press, 2024, pp. 122–139.

[231] Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang, "Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1159–1175, Oct. 2021.

[232] A. Isakov, F. Urozov, S. Abduzhapporov, and M. Isokova, "Enhancing cybersecurity: Protecting data in the digital age," *Innov. Sci. Technol.*, vol. 1, no. 1, pp. 40–49, Mar. 2024.

[233] S. I. Siam et al., "Artificial intelligence of things: A survey," *ACM Trans. Sensor Netw.*, vol. 21, no. 1, pp. 1–75, 2025.

[234] P. Chakraborty, R. N. Dizon-Paradis, and S. Bhunia, "ARTS: A framework for AI-rooted IoT system design automation," *IEEE Embedded Syst. Lett.*, vol. 14, no. 3, pp. 151–154, Sep. 2022.

[235] S. Rangaraju, "AI sentry: Reinventing cybersecurity through intelligent threat detection," *EPH Int. J. Sci. Eng.*, vol. 9, no. 3, pp. 30–35, Dec. 2023.

[236] S. O. Olabanji, Y. Marquis, C. S. Adigwe, S. A. Ajayi, T. O. Oladoyinbo, and O. O. Olaniyi, "AI-driven cloud security: Examining the impact of user Behavior analysis on threat detection," *Asian J. Res. Comput. Sci.*, vol. 17, no. 3, pp. 57–74, 2024.

[237] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[238] J. Li et al., "AI-based two-stage intrusion detection for software defined IoT networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2093–2102, Apr. 2019.

[239] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020.

[240] E. Gyamfi and A. Jurcut, "Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, May 2022.

[241] D. Rupanetti and N. Kaabouch, "Combining edge computing-assisted Internet of Things security with artificial intelligence: Applications, challenges, and opportunities," *Appl. Sci.*, vol. 14, no. 16, p. 7104, Aug. 2024.

[242] M. Tauseef, M. R. Kounte, A. H. Nalband, and M. R. Ahmed, "Exploring the joint potential of blockchain and AI for securing Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, p. 98, 2023.

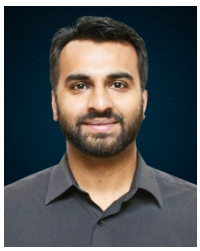
[243] P. Verma, "Potential role of metrology in digital transformation for quality infrastructure," *MAPAN*, vol. 39, no. 1, pp. 111–118, Mar. 2024.

[244] S. Elouardi, A. Motii, M. Jouhari, A. N. H. Amadou, and M. Hedabou, "A survey on hybrid-CNN and LLMs for intrusion detection systems: Recent IoT datasets," *IEEE Access*, vol. 12, pp. 180009–180033, 2024.

[245] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based intrusion detection systems for resource-constrained IoT devices," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2024, pp. 1558–1563.

[246] M. L. Mutleg, A. M. Mahmood, and M. M. Jawad Al-Nayar, "Deep learning based intrusion detection system of IoT technology: Accuracy versus computational complexity," *Int. J. Safety Security Eng.*, vol. 14, no. 5, pp. 1547–1558, 2024.
[247] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered intrusion detection system," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100936.
[248] G. Kocher and G. Kumar, "Analysis of machine learning algorithms with feature selection for intrusion detection using UNSW-NB15 dataset," in *Proc. SSRN*, 2021, Art. no. 3784406.
[249] K. Sethi, E. S. Rupesh, R. Kumar, P. Bera, and Y. V. Madhav, "A context-aware robust intrusion detection system: A reinforcement learning-based approach," *Int. J. Inf. Security*, vol. 19, pp. 657–678, Dec. 2020.
[250] P. H. Durole and M. Agarwal, "A comprehensive review of advanced artificial intelligence techniques to enhance intrusion detection systems," in *Proc. IEEE Int. Conf. Elect. Electron. Comput. Sci. (SCEECS)*, Bhopal, India, 2024, pp. 1–7.
[251] K. X. Kan et al., "A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network," *Inf. Sci.*, vol. 568, pp. 147–162, Aug. 2021.
[252] P. Khanpara, K. Lavingia, R. Trivedi, S. Tanwar, A. Verma, and R. Sharma, "A context-aware Internet of Things-driven security scheme for smart homes," *Security Privacy*, vol. 6, no. 1, p. e269, Jan. 2023.
[253] N. Allahrakha, "Balancing Cyber-security and privacy: Legal and ethical considerations in the digital age," *Legal Issues Digit. Age*, vol. 2023, no. 2, pp. 78–121, 2023.
[254] A. Agustina, M. O. Cahyania, and M. Syaoqibihillah, "Data privacy and the law: Balancing security and individual rights," *Law Stud. Justice J.*, vol. 1, no. 1, pp. 15–24, Mar. 2024.
[255] 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, Apr. 2023.
[256] F. A. Alaba, U. Sani, E. G. Dada, and B. H. Mohammed, *AIoT-Enabled Smart Grids: Advancing Energy Efficiency and Renewable Energy Integration*. Cham, Switzerland: Springer, Sep. 2024, pp. 59–79.
[257] C. S. Babu, M. S. Saltonya, S. Ganapathi, and A. Gunasekar, *AIoT Revolution: Transforming Networking Productivity for the Digital Age*. London, U.K.: IGI Global, 2024, pp. 108–143.
[258] Y. L. Liu, L. Huang, W. Yan, X. Wang, and R. Zhang, "Privacy in AI and the IoT: The privacy concerns of smart speaker users and the personal information protection law in China," *Telecommun. Policy*, vol. 46, no. 7, Aug. 2022, Art. no. 102334.
[259] R. R. Rak. "Internet of healthcare (LAW): Privacy and data protection aspects in an Internet of Everything." 2023. [Online]. Available: https://amsdottorato.unibo.it/id/eprint/10715/1/RichardRudolfRak_DoctoralThesis_final.pdf
[260] C. L. Stergiou, A. P. Plageras, V. A. Memos, M. P. Koidou, and K. E. Psannis, "Secure monitoring system for IoT healthcare data in the cloud," *Appl. Sci.*, vol. 14, no. 1, p. 120, Feb. 2023.
[261] J. V. Arputharaj, J. M. Varkey, R. Vagadia, and R. K. Ayyasamy, *Leveraging Intelligent Systems and the AIoT/IIoT for Enhanced Waste Management and Recycling Efficiency*. Boca Raton, FL, USA: CRC Press, 2024, pp. 266–291.
[262] B. A. Jnr, "Decentralized AIoT based intelligence for sustainable energy prosumption in local energy communities: A citizen-centric prosumer approach," *Cities*, vol. 152, p. 1962, Jan. 2024.
[263] I. Kabashkin and L. Shoshin, "Artificial intelligence of things as new paradigm in aviation health monitoring systems," *Future Internet*, vol. 16, no. 8, p. 276, Feb. 2024.
[264] P. Sun, S. Shen, Y. Wan, Z. Wu, Z. Fang, and X. Gao, "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 1105–1123, Nov. 2024.
[265] G. Singh, A. Mishra, C. Pattanayak, A. Priyadarshini, and R. C. Das, "Artificial intelligence and the institutional ethics committee: A balanced insight into pros and cons, challenges, and future directions in ethical review of clinical research," *J. Integr. Med. Res.*, vol. 1, no. 4, pp. 164–168, Oct. 2023.
[266] M. Strauss, G. Kent, and N. Flour. "Horizon Europe: The EU's research and innovation program." Accessed: Sep. 6, 2024. [Online]. Available: https://www.researchgate.net/profile/Gisele-Kent-2/publication/381272723_Horizon_Europe_The_EUs_Research_and_Innovation_Program/links/66645f6fa54c5f0b9456da3b/Horizon-Europe-The-EUs-Research-and-Innovation-Program.pdf
[267] *What Is Horizon Europe*, Eur. Commission, Brussels, Belgium, 2022.

**KIRAN KHURSHID** received the B.E. degree in information and communication systems engineering, and the M.S. and Ph.D. degrees in wireless communication and signal processing from the National University of Sciences and Technology (NUST), Pakistan. She was a recipient of the NUST merit scholarship for her undergraduate and postgraduate studies. She has extensive teaching experience and currently serves as an Assistant Professor with the Department of Computer and Software Engineering, College of Electrical and Mechanical Engineering, NUST. Her research interests include MIMO systems, massive MIMO systems, 5G and beyond, wireless channel modeling, IoT, AIoT, and big data mining.



**KHAWAR KHURSHID** (Member, IEEE) received the Ph.D. degree from Michigan State University, USA, in the field of medical image processing using ML algorithms. He is an Academic and a Researcher of Machine Learning and Computer Vision, currently holding the position of Professor with the Department of Computer Science, Namal University. Prior to joining Namal University, he served with SEECS, NUST for more than 13 years in the capacity of an Assistant Professor and an Associate Professor. He was also the head of the Institute of Applied Electronics and Computing, SEECS for six years. He has published over 50 research papers. His interests include medical imaging, computer vision, machine learning, and the Internet of Things.

**MUHAMMAD USMAN HADI** (Member, IEEE) received the M.S. and Ph.D. degrees from the University of Bologna, Italy. He was a Postdoctoral Researcher with Aalborg University, Denmark, in close collaboration with Nokia. He was a Visiting Researcher with ESIEE Paris, France, and Nokia Bell Laboratories. He is currently an Assistant Professor with the School of Engineering, Ulster University, Belfast, U.K. He has authored more than 60 journal articles and transactions. As a Principal Investigator, he has received EPSRC DTNET+, Innovate U.K., British Council Going Global Partnerships, Garfield Weston Trust, R&I funds and EPSRC, DFE, and ISPF research grants as a Co-Investigator. His research interests include machine learning for engineering applications, unmanned aerial vehicles, fiber wireless communication, microwave photonics, and devices for telecommunications. He has been included in top 2% of researchers for consecutive three years since 2021.

**MOHAMMAD AL BATAINEH** (Member, IEEE) the B.S. degree (Hons.) in telecommunications engineering from Yarmouk University, Jordan, in 2003, and the M.S. and Ph.D. degrees in electrical engineering from the Illinois Institute of Technology, USA, in 2006 and 2010, respectively. Following his academic pursuits, he held notable positions at several institutions, including Yarmouk University, where he was promoted to an Associate Professor in 2018, as well as roles with Argonne National Laboratories and MicroSun Technologies. He is currently working as an Assistant Professor with United Arab Emirates University, Al-Ain, UAE. His research interests include the application of communication theory, coding theory, and information theory to the interpretation and understanding of information flow in biological systems, particularly gene expression. His other research areas encompass machine learning, network information theory, and optimization.

**NASIR SAEED** (Senior Member, IEEE) received the B.Sc. degree in telecommunication from the University of Engineering and Technology, Peshawar, Pakistan, in 2009, the M.Sc. degree in Satellite Navigation from the Polito di Torino, Italy, in 2012, and the Ph.D. degree in Electronics and Communication Engineering from Hanyang University, Seoul, South Korea, in 2015. He was an Assistant Professor with the Department of Electrical Engineering, IQRA National University, Peshawar, from 2015 to 2017. From July 2017 to December 2020, he was a Postdoctoral Research Fellow with the Communication Theory Laboratory, King Abdullah University of Science and Technology, Saudi Arabia. He is currently an Associate Professor with the Department of Electrical and Communication Engineering, United Arab Emirates University, Al Ain, UAE. He has published more than 80 international journal and conference articles. His research interests include nonconventional communication networks, heterogeneous vertical networks, multidimensional signal processing, and localization. He is also an Associate Editor of IEEE WIRELESS COMMUNICATIONS LETTERS.