Computers, Materials &
Continua

Tech Science Press

Doi:10.32604/cmc.2025.070189

REVIEW

Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework

Inam Ullah Khan[1], **Fida Muhammad Khan**[1,*], **Zeeshan Ali Haider**[1] **and Fahad Alturise**[2,*]

[1]Department of Computer Science, Qurtuba University of Science & Information Technology, Peshawar, 25000, Pakistan
[2]Department of Cybersecurity, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia

*Corresponding Authors: Fida Muhammad Khan. Email: fida5073@gmail.com; Fahad Alturise. Email: falturise@qu.edu.sa

Received: 10 July 2025; Accepted: 12 September 2025; Published: 23 October 2025

ABSTRACT: The rapid expansion of the Internet of Things (IoT) has introduced significant security challenges due to the scale, complexity, and heterogeneity of interconnected devices. The current traditional centralized security models are deemed irrelevant in dealing with these threats, especially in decentralized applications where the IoT devices may at times operate on minimal resources. The emergence of new technologies, including Artificial Intelligence (AI), blockchain, edge computing, and Zero-Trust-Architecture (ZTA), is offering potential solutions as it helps with additional threat detection, data integrity, and system resilience in real-time. AI offers sophisticated anomaly detection and prediction analytics, and blockchain delivers decentralized and tamper-proof insurance over device communication and exchange of information. Edge computing enables low-latency character processing by distributing and moving the computational workload near the devices. The ZTA enhances security by continuously verifying each device and user on the network, adhering to the "never trust, always verify" ideology. The present research paper is a review of these technologies, finding out how they are used in securing IoT ecosystems, the issues of such integration, and the possibility of developing a multi-layered, adaptive security structure. Major concerns, such as scalability, resource limitations, and interoperability, are identified, and the way to optimize the application of AI, blockchain, and edge computing in zero-trust IoT systems in the future is discussed.

KEYWORDS: Internet of Things (IoT); artificial intelligence (AI); blockchain; edge computing; zero-trust-architecture (ZTA); IoT security; real-time threat detection

1 Introduction

The Internet of Things (IoT) has dramatically changed the way devices communicate, making it easier for physical objects to interact with virtual environments. However, the rapid expansion of IoT networks, which now involve billions of devices interconnected across various networks, has introduced significant security challenges. One of the biggest issues is that some of these IoT devices, especially those designed so far, lack high-security levels or inherent security. As an example, research conducted by the European Union Agency for Cybersecurity (ENISA) in 2020 notes that approximately 70% of IoT devices are affected by security threats, and many of these vulnerabilities are linked to their poor design or insufficient security features [1,2]. The scale, diversity, and sophistication of current IoT security requirements have rendered current models of centralized security inadequate. Models are typically designed with a focus on centralizing information, making them susceptible to single points of failure, delays, and scalability issues when managing millions of instruments across various networks. In 2016, the Mirai botnet exploited the insufficient security of IoT devices, leading to what is believed to be one of the largest distributed denial-of-service (DDoS) attacks in history, which took down popular websites like Twitter and Netflix [3]. This type of incident is believed to exemplify the inadequacy of centralized security models to cope with the dynamism and scale of the IoT ecosystems. These issues have prompted the emergence of decentralized security infrastructures that incorporate blockchain and edge computing applications along with AI-based threat detection. Blockchain offers a viable system of securing IoT data since the transactions are verifiable and transparent, as there is no way of altering the data. As an example, blockchain technology has been considered in healthcare regarding secure medical record sharing; the medical records could not be changed since this would bypass the security and transparency characteristics of blockchain [4,5]. Edge computing is considered a complement to blockchain, as it helps move the computing part closer to IoT devices, thereby decreasing latency and limiting the locations of failure. This is particularly important for applications with low latency, such as autonomous vehicles, where decisions must be made in real time. As an example, edge computing enables autonomous cars to compute data internally, making faster decisions and reducing reliance on centralized cloud servers, which introduce unacceptable delays [6,7]. The other IoT security emerging model is the ZTA, which is based on the following maxim: "never trust, always verify". Unlike traditional security models, which presume trust within a network perimeter, ZTA requires regular authentication and validation of all users and devices attempting to access the network. This model works very well in the IoT ecosystems where devices are typically communicating over distributed networks all the time. The scenario of incorporating ZTA into blockchain enables IoT systems to employ a dual-layered protection strategy, where every transaction is registered and permanently stored on the blockchain, thereby enhancing the integrity and traceability of interactions [8,9].

In recent years, a combination of AI, blockchain, and Zero-Trust Architecture (ZTA) in IoT security systems has become an area of increased study among professionals. AI, specifically machine learning (ML), is employed to detect anomalies quickly and perform predictive analytics, enabling real-time adaptation and overcoming of changes. Indicatively, AI-enabled systems in smart homes monitor atypical activity patterns that can lead to breaches, e.g., abnormal energy use, or unauthorized access, to identify and prevent possible violations before they materialize [10,11]. Blockchain augments these AI-based systems by decentralizing verification procedures, in which every decision of the AI model is safely stored and trackable. This distributed setting ensures that unauthorized activity cannot pass without being noticed. Nevertheless, the interplay of these technologies has also been hindered by several challenges, including scale, interoperability, and resource limitations. Many IoT devices are resource-limited and may lack the processing power required to run blockchain and AI applications. For instance, a standard IoT device often lacks sufficient CPU, memory, and power to support a battery, making it challenging to implement computationally intensive blockchain protocols and AI models. Alternatively, the latest developments in edge computing technology are striving to overcome these security issues by reallocating the processing load among numerous devices placed at the edge of the network. There are also new blockchain protocols that are designed to operate in IoT environments. To ensure high-level security, these protocols are built to be ultra-specific with low resource requirements [12]. Recent research has focused on lightweight blockchain protocols in IoT devices in the Journal of IoT Security. It has been shown that lightweight blockchain protocols are set to decrease the overhead caused by such IoT protocols at the expense of performance security [13]. The road to IoT ecosystem security is now concentrated on the embracement of AI, blockchain, and ZTA as a way of establishing a nimble and responsive security infrastructure. The necessity to have security models that dynamically adjust to new threats becomes even more urgent as the variety of IoT networks continues to grow. This review addresses recent works in this direction, highlighting gaps and future research on integrating AI, blockchain, and ZTA to enhance IoT infrastructure security [14,15]. Fig. 1 illustrates the key components of the IoT network and how AI, Blockchain, Edge Computing, and ZTA work synergistically to create a secure, resilient IoT ecosystem.

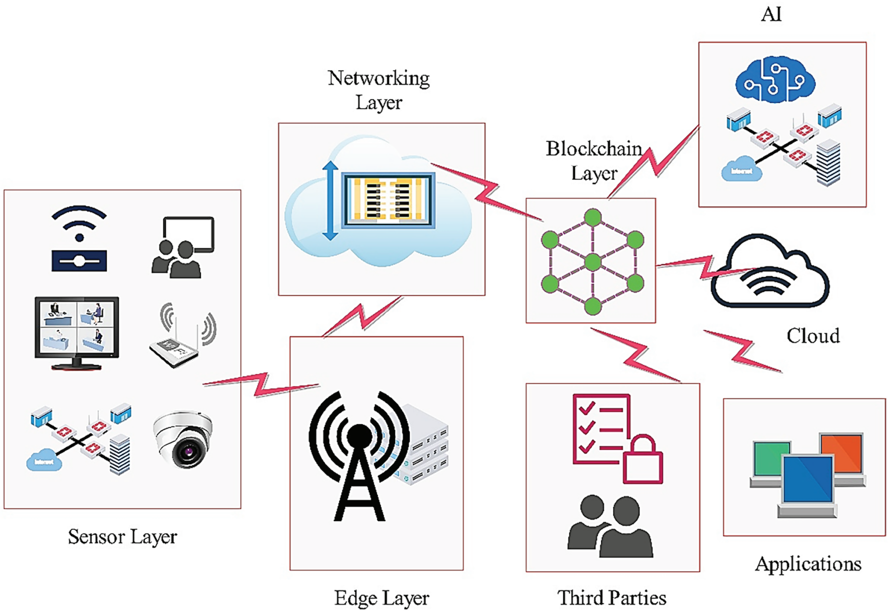

Figure 1: Multi-Layer IoT architecture with blockchain, AI, and cloud integration components

1.1 Motivation

The deployment of Internet of Things systems in infrastructure areas, including smart cities, healthcare, transportation, and industrial plants, has increased the necessity of effective cybersecurity mechanisms. The IoT devices are implemented on a massive scale, making them easily prone to cyber-attacks, despite their security features being underdeveloped. For instance, a 2017 ransomware attack on the NHS in the UK disrupted access to healthcare services, while cyber-attacks on connected cars have enabled remote control over vehicles. In transportation, cybercriminals have unlawfully intruded on innovative traffic systems, posing a safety risk. The extent of disruption that can be caused by one compromised device in the IoT systems is significant due to interconnectedness. The recent cyber-attack on the water treatment plant in Florida indicated the potential rise in breaches on interdependent networks, which can affect the infrastructure in general. Centralized traditional models of security are insufficient to address the dynamic and changing nature of these threats, as evidenced by outdated firewalls that fail to identify new attack vectors in real-time. Possible solutions to these problems are AI, blockchain, and edge computing. AI will be able to foresee and react to emerging risks, whereas blockchain will offer decentralization of data transfer, making it safer and more transparent. Edge computing decreases latency by processing the data near the IoT device, which is critical in real-time applications, such as driving an autonomous car or industrial IoT. ZTA also provides a higher level of security due to the continuous authentication process of the devices and users. It thus ensures that there is no unauthorized access. IoT networks incorporate blockchain, AI, and Edge computing, paired with ZTA to be more resilient, scale to meet modern cyber threats, and operate securely in areas of high risk to society, such as healthcare, finance, and transportation.

1.2 Methodology

This section specifies the research methodology that will be utilized in reviewing the implementation of AI, blockchain, edge computing, and zero-trust architectures in IoT cybersecurity platforms. The main aim of the review is to develop thorough knowledge of the capabilities of such technologies in enhancing security systems of the IoT-based networks, emphasizing the capacities of these technologies to counter the emerging cyberattacks and to boost system resilience. The methodology is organized so that it could answer the following research questions:

- **RQ1:** What are the current cybersecurity threats to IoT systems, particularly in decentralized and dynamic environments?
- **RQ2:** How can AI, blockchain, and edge computing be integrated to mitigate these cybersecurity risks in IoT ecosystems?
- **RQ3:** What are the challenges and limitations associated with implementing these technologies in IoT security frameworks?
- **RQ4:** How do zero-trust architectures enhance the overall security and adaptability of IoT systems when combined with AI, blockchain, and edge computing?

A systematic literature review search was conducted to address the research questions by using well-established, peer-reviewed literature databases (Web of Science, Scopus, Google Scholar, IEEE Xplore, and Science Direct). The search strategy was detailed to make sure that the chosen studies encompassed the latest and most appropriate literature. The works published after 10 years were filtered out to maintain the currency of the reviews with the current developments and trends in IoT security. The relevant articles were identified with the help of a set of keywords, such as the following: IoT security, AI-driven cybersecurity, blockchain in IoT, edge computing in cybersecurity, and zero-trust architecture. The literature selected through these keywords was explicitly related to the nexus of these technologies and their application in ensuring the security of the IoT. The 150 studies have been identified in terms of their relevance to the research questions and their contribution to the knowledge of AI, blockchain, edge computing, and zero-trust security in IoT ecosystems. It has been ensured that both conceptual inventions and practical findings are supported by rigorous screening to determine whether the studies provide empirical or theoretical contributions. The process of selection entailed abstract, full-text, and methodology review to establish the appropriateness of the studies to the review. Exclusion criteria were established to ensure the quality and relevance of the studies. Some articles were too old (published over 10 years ago), or the analysis was not seriously done on them. Also, observations with methodological limitations or those that did not discuss the main themes of the review (AI-based threat detection, blockchain in decentralized security, real-time data processing based on edge computing, and the introduction of Zero-Trust-Architecture into the context of IoT) were excluded. The selected studies were subsequently divided into several central themes, using the contribution that they made to the field as a basis for categorization: AI-based threat detection, decentralized IoT security via blockchain, edge computing to process data in real-time, and the Zero-Trust-Architecture applied to IoT security. This practice ensured the literature review was extensive, providing a solid basis for establishing the current state of the research and demonstrating how new technologies can enhance IoT security. Table 1 presents a summary of the significant academic databases utilized in the systematic literature review of this study. These databases, Web of Science, Scopus, Google Scholar, IEEE Xplore, and ScienceDirect, have been chosen because of their wide coverage of scholarly work in IoT security, AI, blockchain, and edge computing. In turn, these databases have distinct strengths, including technical depth, multidisciplinary scope, and comprehensive indexing of grey literature. They allowed a wide range and variety of high-quality and recent studies.

Table 1: Overview of academic databases used for the systematic literature review on IoT security technologies

Database name	Description	Special focus
Web of Science	A comprehensive database with over 100 million scientific articles.	Includes Springer journals.
Scopus	A multidisciplinary bibliographic database covering over 71 million scholarly items.	Broad academic scope, includes Springer journals.
Google Scholar	A search engine that indexes scholarly literature from across the web.	Inclusive of diverse sources, both formal and informal.
IEEE Xplore	A database focused on engineering and computer science articles.	Strong in technical fields; includes Springer content.
ScienceDirect	A multidisciplinary database featuring articles from top academic publishers globally.	Emphasis on scientific research; includes Springer.

1.3 Contribution

This review makes several significant and original contributions to the field of cybersecurity in IoT ecosystems, particularly through the synergistic integration of Artificial Intelligence (AI), Blockchain, Edge Computing, and ZTA. The main contributions of this review are as follows:

- This review provides an in-depth examination of how AI, Blockchain, and Edge Computing seamlessly integrate to address the complex security challenges faced by IoT networks. It explores the unique roles of each technology AI in real-time threat detection, Blockchain for decentralizing authentication and ensuring data integrity, and Edge Computing for reducing latency and enhancing local decision-making, and how their complementary functions strengthen the overall security of IoT systems. This analysis is crucial for advancing the understanding of how these technologies can work together to protect IoT ecosystems in decentralized environments.
- The review identifies and highlights the technical challenges that arise when deploying these technologies in resource-constrained IoT systems. These challenges include computational limitations, scalability issues, and the need for real-time data processing. In response, this review discusses practical solutions, such as the development of lightweight blockchain protocols, the use of distributed AI models, and the optimization of edge computing to enhance efficiency and performance in IoT networks. By presenting these solutions, the review provides valuable insights into how to overcome key barriers to implementing AI, blockchain, and edge computing in IoT security frameworks.
- One of the key contributions of this review is demonstrating how ZTA can be seamlessly integrated with AI and Blockchain to enhance the overall security and resilience of IoT networks. By enforcing the "never trust, always verify" principle, ZTA ensures that every interaction within the IoT network is continuously verified. This review outlines how ZTA enforces continuous authentication and authorization for both devices and users, thereby preventing unauthorized access and improving system resilience against cyberattacks. The integration of AI for real-time threat detection and blockchain for secure data verification creates a robust and adaptive security model for IoT environments.
- The review offers insights into future research directions by identifying emerging trends and integration strategies for these technologies. These include the development of advanced AI algorithms for real-time threat detection, the application of blockchain in securing autonomous devices, and the potential of Edge AI for decentralized processing. The exploration of these future trends lays the groundwork for

innovative solutions to the evolving security challenges in IoT ecosystems. The review encourages future research into these cutting-edge technologies and how they can be further optimized for IoT security.

By focusing on these key areas, this review not only contributes to the current body of knowledge but also lays a solid foundation for future research and real-world applications. It highlights the critical role of AI, Blockchain, Edge Computing, and Zero-Trust Architecture in building secure, scalable, and resilient IoT ecosystems. In doing so, it sets the stage for the next wave of cybersecurity solutions for IoT networks.

1.4 Organization

In this research study, the following sections are divided, which jointly give a detailed review of next-generation cyber defense strategies in IoT security. Section 1 will highlight the need to integrate AI, blockchain, edge computing, and zero-trust architectures to address emerging threats in the IoT domain effectively. Section 2 presents the literature review of the state of current studies about the shortcomings of the traditional cybersecurity frameworks and their relevance in terms of adaptive, decentralized security approaches to IoT systems. In Section 3, a discussion is held on how AI, blockchain, and edge computing can strengthen IoT security through the detection of real-time threats, increase stability, and ensure data integrity. In Section 4, we shall look at the application of zero-trust architectures (ZTA) to these technologies to provide continuous verification and protection within an IoT network. Section 5 presents issues with the implementation of these technologies, such as computational limitations and scalability problems. In Section 6, the authors explain why zero-trust IoT security is implemented using AI, blockchain, and edge computing, and what the synergistic benefits of these technologies are in securing the IoT ecosystem against security challenges that are specific to IoT. Section 7 proposes avenues of future research, whereas Section 8 assesses the effect of these technologies on the security frameworks of IoT. Section 9 ends with an overview of significant findings and suggestions on where future research on the study should be directed. This structure will make the flow of ideas logical. It will offer readers not only an overview of an analytical process but also valuable insights into enhancing cybersecurity in IoT.

2 Related Work

To date, there has been no comprehensive review that integrates explicitly AI, blockchain, edge computing, and zero-trust architectures to address IoT cybersecurity challenges. Although individual studies have explored the security role of these technologies in IoT, none have combined them into a unified framework for understanding how they can collectively enhance IoT security. Several studies have provided overviews of AI in cybersecurity, focusing particularly on its potential for threat detection and anomaly recognition [16,17]. However, these studies primarily focus on conventional Information technology systems and do not address the unique requirements of IoT systems, such as real-time processing needs and the constrained computational resources of IoT devices [18,19]. The real reason behind this disjuncture is that IoT systems are both distributed and resource-constrained, meaning that they need security mechanisms that are fundamentally different than those employed in more traditional IT infrastructures [20,21]. Comparatively, blockchain studies in IoT security have emphasized its capacity to deliver data integrity, decentralized authentication, and secure data exchange [22,23]. Nevertheless, most of these studies have been reduced to targeted applications such as supply chain management or device authentication [24,25]. This selective emphasis is restrictive to the broader adoption of blockchain in securing dynamic and distributed IoT environments. The implication is that the potential of blockchain as a more integrated security solution, when paired with AI and edge computing, is not yet fully explored. The literature on edge computing emphasizes its ability to reduce latency and bandwidth use by processing data closer to IoT devices [26–28]. However, many studies view edge computing as an isolated solution and do not explore its integration with AI and blockchain to enhance IoT security. This lack of integration reflects a missed opportunity to develop a more robust, multi-layered security system. The implication here is that while edge computing can alleviate some IoT challenges, its true potential lies in combining it with other technologies for a more holistic approach to security. Research on ZTA points to its effectiveness in ensuring continuous validation of all interactions, ensuring that default [29,30] trusts no device or user. However, most studies on ZTA in IoT security are theoretical, focusing on the principles of the model without addressing its integration with other technologies like AI and blockchain [31–33]. The underutilization of ZTA, especially in combination with AI and blockchain, limits its application in real-world, dynamic IoT environments. The implication is that a unified, adaptable security framework combining ZTA with AI, blockchain, and edge computing could offer a more resilient defense against emerging threats. Moreover, the challenges related to scalability and interoperability in IoT security are widely acknowledged. Theoretical papers addressing blockchain scalability in IoT and the computational workload of AI emphasize the major constraints [34–36], yet the solutions to the issues remain at the initial phase. These issues mitigated by including lightweight blockchain mechanisms and distributed AI models [37–39]. The constraints are attributed to the nature of the IoT devices, which are usually complex and diverse and do not have standardized security protocols, thus making it difficult to come up with an integrated security solution capable of ensuring continuity and interoperability of the various industries [40,41]. This review will provide these gaps by presenting a full comprehension of how AI, blockchain, edge computing, and Zero-Trust Architecture (ZTA) can be incorporated into IoT security. It looks at why research is so varied, why certain applications or technology receive attention and how this has affected the development of a unified and multi-layered security system on IoT. The collective study of these technologies will help us define the direction of future research, which will help to create more resilient, scalable, and adaptable IoT security solutions. Table 2 offers an extensive comparative evaluation of the associated literature about the combination of AI, Blockchain, Edge Computing, and Zero-Trust Architectures to IoT cybersecurity.

Table 2: Comparative analysis of related work on the integration of AI, blockchain, edge computing, and zero-trust architectures in IoT cybersecurity

Ref.	Year	AI	Blockchain	Edge computing	Zero trust	IoT integration	Cybersecurity focus	Key challenges	Future directions	Remarks (Focused on)
[16,22]	2021	√	×	×	×	×	√	√	√	Overview of AI in cybersecurity, transparency, and trustworthiness of models
[17,21,23,32]	2023	×	√	×	×	√	√	×	×	Data mining in cybersecurity is focused on traditional IT environments
[13,24]	2021	×	×	√	×	√	×	×	×	IoT architecture and services, excluding cybersecurity
[15,25,31]	2023	×	×	√	×	√	×	×	×	IoT data handling with limited focus on cybersecurity
[19,26]	2024	×	×	√	×	×	×	×	×	IoT system designs without AI-driven cybersecurity focus
[27]	2024	√	×	√	√	√	×	×	×	Explaining anomalies detected in IoT networks, limited in comprehensive AI-blockchain integration

(Continued)

Table 2 (continued)

Ref.	Year	AI	Blockchain	Edge computing	Zero trust	IoT integration	Cybersecurity focus	Key challenges	Future directions	Remarks (Focused on)
[20,28]	2025	×	√	√	×	√	√	×	×	Smart city analytics with partial focus on cybersecurity
[18,29,30]	2025	√	×	√	√	√	√	×	×	Deep learning applications in IoT security, limited to specific areas like intrusion detection
Our study	2025	√	√	√	√	√	√	√	√	Comprehensive integration of AI, blockchain, edge computing, and zero-trust for IoT cybersecurity

3 The Role of AI, Blockchain, and Edge Computing in IoT Security

Artificial Intelligence (AI), blockchain, and edge computing are ever-changing technologies that have radically changed IoT security models, allowing a very dynamic, decentralized, and intelligent security architecture [42–44]. All of these technologies can overcome the most relevant security issues within the IoT systems, i.e., scalability, real-time threat detection, data privacy, and optimal usage of computational resources. Fig. 2 shows an AI-strengthened blockchain-based approach to security in IoT of a smart city. It illustrates how data sensed at the edge layer is processed to demonstrate legitimacy, blockchain approval, and the detection of abnormalities, and then transfers these values to the cloud layer for storage. It has the capacity to analyze the paths of events in real-time to verify questionable actions and sound security alerts. This layered architecture is used to enhance the protection of information, integrity, and time responses to threats in a Zero-Trust system.

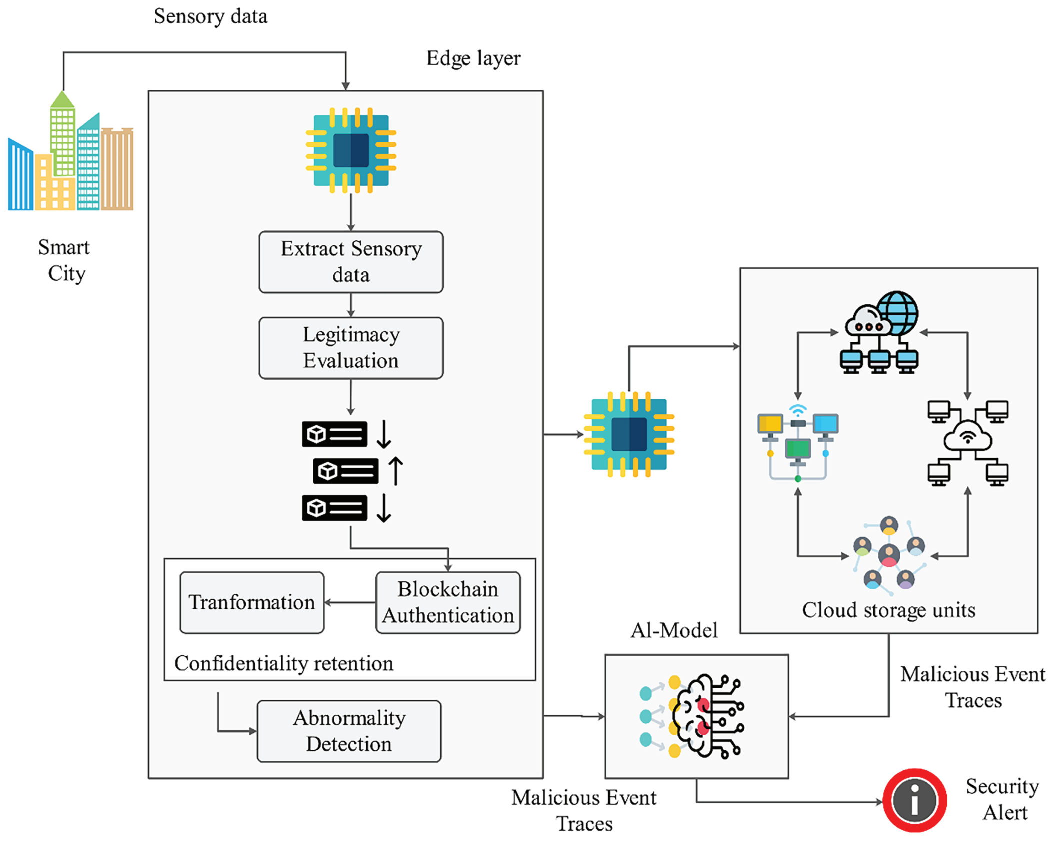

Figure 2: AI-enabled blockchain framework for smart city IoT security using edge and cloud layers

3.1 Artificial Intelligence (AI) in IoT Security

Artificial intelligence is necessary to detect threats and analyze abnormalities in IoT networks in real-time. Conventional IoT systems, which rely on predefined security rules and signatures, are no longer effective due to the rapid evolution of cyberattacks. Machine learning (ML) and deep learning (DL) models are AI-based systems capable of processing large volumes of data generated by IoT devices in real time and identifying patterns and anomalies that can be indicative of a security breach [45,46]. Compared to traditional systems that are built around rules, these models are flexible and can evolve to identify emerging risks, which makes them more efficient. AI was also used to detect anomalies through traffic patterns and to detect irregularities in the processing of JSON that could indicate malicious intent. To detect zero-day attacks, emphasis is no longer on signature-based detection, but on methods such as unsupervised learning and clustering algorithms. The predictive and detection capabilities to identify potential threats before they have fully evolved lead to the opportunity to intervene proactively, which can reduce the effect of a cyberattack on IoT systems [47]. Moreover, AI automation will reduce the need for human involvement in monitoring and responding to threats, enabling security systems to detect and react to potential events promptly. Since IoT networks consist of large amounts of data, AI-based intrusion detection systems (IDS) will be suitable to process large volumes of data to identify abnormalities in real time [48].

3.2 Blockchain for Decentralized IoT Security

Blockchain offers a decentralized and irreversible platform that enhances the security of IoT systems, where the information cannot be interfered with or altered without central authorization. In its simplest form, blockchain is based on a distributed ledger (DLT), which forms a transparent and trustless network encompassing IoT devices capable of securely sharing data. Blockchain immutability implies that once data is placed on the ledger, it cannot be altered or removed [49]. Device authentication is one of the main applications of blockchain in IoT security. The distributed ledger can provide a unique identifier to every device on the IoT network, enabling checking of the authenticity of a particular device before it communicates with the network [50]. This process significantly reduces the risk of unauthorized or malicious devices gaining access to the network. Also, the security protocols may be automated by the use of smart contracts, which are self-executing contracts, where the terms of an agreement are directly or implicitly defined in their code, and therefore ensure in real-time that the security policy is followed, removing the human element of error. Blockchain also increases data privacy since the communication between the IoT devices is cryptographically secured. Blockchain is decentralized and can thus limit the effects of single-point failures, which are often attacked in a centralized system [51]. Moreover, the blockchain's decentralized nature presents the benefit of making all data transactions accessible, which is also helpful for auditing and forensics after an incident.

3.3 Edge Computing for Low-Latency IoT Security

Edge computing boosts IoT security by bringing data processing closer to where the data is generated, which helps reduce latency and bandwidth demands typically associated with cloud-based systems. In traditional IoT setups, data is sent to the cloud for processing, often leading to significant delays and potential security risks, especially for sensitive data. By shifting data processing to the IoT devices themselves, edge computing enables real-time threat detection and rapid response, improving the ability to detect and address security issues as they arise [52]. IoT systems can reduce sensitivity to latency in security concerns by offloading the data processing at the edge, opening up many possibilities in deployment to areas such as autonomous vehicles and healthcare monitoring, in addition to smart cities, where the safety of life applications cannot go more than a few seconds without deciding [53]. With edge computing, security attacks can be identified and thwarted virtually in real-time, without any necessity to deliver data to a central machine. The possibility to distributing the computational load among several edge nodes is another advantage of edge computing, making it more straightforward to scale IoT networks without jeopardizing security. The edge devices can analyze threats at the local level and send only essential information or security warnings to central servers or blockchain networks for processing. This also applies to data privacy, where sensitive information will be restricted in the local network [54].

3.4 The Synergy Between AI, Blockchain, and Edge Computing

Such a complex of AI, blockchain, and edge computing will provide a secure and versatile system of security measures to IoT environments. Security systems with implemented AI can be made smarter by predicting and identifying threats in real-time. The blockchain can be utilized due to its immutability and decentralization options, which help preserve data integrity and ensure secure data transfer among various devices. By enabling local data processing, edge computing enhances the efficiency of both AI and blockchain, reduces latency, and significantly increases the system's scalability and resilience to threats [55]. Blockchain and AI complement each other, as the former can be applied to identify anomalies, while the latter ensures the safety and openness of data. About minimizing the risks posed by its security, smart contracts can automate the security approach (i.e., threat identification) based on AI threats today, which creates a more reactive and self-sustainable IoT security system. Additionally, utilizing edge computing to decentralize data storage and processing helps mitigate scalability and resource-constrained issues associated with deploying AI and blockchain on resource-limited IoT devices [56]. Collectively, the technologies have been shown to address the issue of scalability, real-time processing, and security of data in a resource-limited IoT system to form a complete picture of security frameworks within distributed IoT systems, which guarantees integrity, confidentiality, and the availability of data transmitted through distributed IoT networks.

4 Zero-Trust Architectures (ZTA) for IoT Security

ZTA represents a revolutionary shift in cybersecurity, moving beyond perimeter-focused security models. Devices and users within a network perimeter, such as within an organization's firewall, in a typical security system, are deemed as trusted. In contrast, entities outside the perimeter, such as the external users or devices, are considered untrusted. The model functions on the premise that threats are all external, and thereafter, a device or user within the network is trusted [57]. Contrarily, Zero-Trust-Architecture operates under the principle of a flawed trust, maintaining verifications. This implies that no single device, user, or system, both within and without the network perimeter, is necessarily trusted. Access to the network is continuously authenticated on every action or request, and his/her whereabouts are irrelevant. This enables the eradication of threats posed by attackers who may infiltrate the network through the lateral trust of devices or individuals already within it. As shown in Fig. 3, Zero Trust Security is based on foundational principles and emphasizes the need to secure all elements of an organization's digital environment. The model allows access control and the verification of zero trust, and has six security zones: infrastructure, data, networks, identities, devices, and applications. The implementation of this entire strategy establishes that the ideology of never trust, always verify should be used to help protect the organization against internal or external attacks.

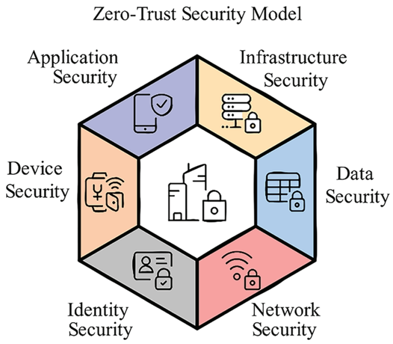

Figure 3: Core components of zero trust security framework

4.1 Why Zero-Trust-Architecture (ZTA) Is Critical for IoT Security

The Internet of Things (IoT) presents significant cybersecurity challenges. IoT devices encompass a wide range of connected objects, from smart home appliances to critical infrastructure elements like medical equipment and industrial sensors [58]. Many of these devices have limited computational resources, making them particularly vulnerable to attacks. Additionally, IoT devices often operate in a decentralized manner and can span multiple network boundaries, which renders traditional perimeter-based security models ineffective [59]. In this context, Zero-Trust Architecture (ZTA) offers a strong alternative by emphasizing continuous verification of all devices, including users, regardless of their location. This approach ensures that security is maintained throughout the IoT network. The zero-trust model works efficiently in IoT ecosystems where many devices connect all the time and share information, as interruptions of possibly unauthorized access can occur. The practice of demanding constant authentication of each device's credentials and permissions, as encompassed by ZTA, prevents a prospective hacker from freely navigating the network of the honeycombed device, even after gaining access through one of their targeted compromised devices [60,61]. Consider an innovative house network, where a smart thermostat has compromised controls. ZTA would prevent attackers from gaining control over additional, more sensitive devices, such as security cameras or personal computers.

4.2 Core Components of ZTA for IoT

- **Identity and Access Management (IAM):** The core of Zero-Trust Architecture (ZTA) lies in Identity and Access Management (IAM). In the Internet of Things (IoT), both devices and users must have a digital identity that is continuously authenticated [62]. During this process, the credentials of all devices are verified before granting access to any network resource. Unlike traditional systems, where credentials are only checked during login, ZTA requires continuous monitoring and re-authentication of credentials [63]. This is especially important in IoT environments, where devices often connect and disconnect from the network. Technologies like blockchain further strengthen ZTA's Identity and Access Management (IAM) systems. Blockchain provides a decentralized ledger that securely records every access attempt and its validation. Actions such as a user logging in or a device requesting data are permanently logged on the blockchain [64]. This creates an auditable history of all communications, allowing any unauthorized interactions to be traced and analyzed to improve future security measures.
- **Continuous Monitoring and Behavioral Analytics:** In Zero-Trust Architecture (ZTA), security is dynamic, not static, with constant monitoring of all activities within the network. Every transaction, data exchange, and interaction is tracked in real time, enabling immediate responses to any unusual or unexpected behaviors [65,66]. This ongoing verification is particularly critical for IoT devices, which regularly operate in a decentralized environment. Machine learning and AI are integral to this process. By leveraging these technologies, it's possible to identify abnormal behavior patterns that may indicate a security breach. AI-driven systems can detect anomalies within the large datasets generated by IoT devices, enabling quicker identification of potential threats and enhancing the overall security of the network [67,68]. As an example, say that there is an AI system controlling a system where certain types of devices usually send data at a specific rate and at a particular time; these devices start sending vast quantities of data that are not within normal parameters, which will be detected as suspicious by the AI system. Such active decision-making will help to identify security risks even before they show signs of a breach.
- **Micro Segmentation:** Partitioning the network into smaller, isolated segments is a key aspect of Zero-Trust Architecture (ZTA). Each segment is equipped with its own security measures, so if one device is compromised, the attacker cannot easily access other parts of the network without undergoing stringent

checks. Micro-segmentation is especially critical in IoT environments, as it limits an attacker's ability to move across a distributed network of devices. For example, in a smart city, traffic light sensors and utility management devices are spread out across different locations. A breach of one device doesn't automatically jeopardize the entire network [69]. ZTA enhances security by isolating devices in distinct spaces, making it much harder for an attacker to gain access to the whole network [70].

  - ○ **Implementation:** Micro-segmentation in the framework of the IoT environment implies the division of virtual network areas, where individual policies are set and access control methods are introduced. An example would be putting smart home devices such as thermostats in one zone, and critical infrastructure sensors such as water treatment facilities in another, a lockdown zone [71]. The risk is mitigated by continuously verifying the network boundary of each segment; therefore, even when one of the devices has been breached, the breach is prevented.
  - ○ **Use Case:** In the case of a smart city, the separation of traffic light sensors can be between sensors that belong to the public utility. In case an attacker accesses the traffic management system, they cannot easily access the water or electricity control systems, which are the public utilities. Micro-segmentation ensures that a breach on a particular segment is not unleashed across the whole infrastructure, leaving essential systems safe.

- **Least Privilege Access:** The other important aspect of Zero-Trust-Architecture (ZTA) is the principle of least privilege, limiting the access of devices and users to only the required minimum to fulfill their roles. In an IoT environment, this implies a scenario where every device or user acquires only those privileges necessary for their operation. For instance, a smart home would not grant a security camera access to the homeowner's personal information or control over other devices unless authorized. This severely limits the chances of malicious users utilizing needless access privileges [72–74]. In Zero-Trust Architecture (ZTA), access is continuously reviewed and updated based on real-time behavior. If a device exhibits behavior that suggests it is compromised, its permission to be accessed can be reduced or removed, thereby preventing further damage.

4.3 ZTA Integration with Blockchain and AI in IoT

The security model of a ZTA builds on the decentralization of Blockchain, where all transactions, access requests, and authorizations are logged and verified on an unrevivable ledger [75]. This decentralized verification lends legitimacy to ZTA by making all IoT device transactions auditable and tamper-proof, which is essential for establishing trust and security. The transparency and continuous updating of blockchain records provide real-time audit trails, which are crucial to the Zero-Trust principle that no internal networked device should be trusted by default. Every access and interaction with each device is meticulously tracked, creating a verifiable chain of actions within the IoT network. This setup makes it easy to detect and trace any security breaches, ensuring that all activities can be thoroughly monitored and analyzed for potential threats. In the IoT environment, where it is necessary to verify millions of devices, decentralized authentication is crucial. Blockchain supports this since every IoT device is supposed to have its own digital identity, which is registered in the blockchain ledger digitally. This identity could not be compromised once it had been authenticated, and therefore, it was argued that only authenticated devices had access to the network [76,77]. For instance, sensors, traffic lights, and surveillance cameras can be classified as IoT devices, each identifiable by a unique identifier that is then indexed in the blockchain within a smart city. After this identity is confirmed, the device is allowed to communicate with other devices and systems. Any unauthenticated device attempting to enter the network will be automatically flagged and blocked in the event of an attack. Zero-Knowledge Proofs (ZKPs) have the potential to improve the authentication process implemented with the help of blockchain in a way that a device can demonstrate its identity without providing any sensitive data. Using ZKPs, devices can verify that they satisfy particular criteria and to identify themselves without revealing superfluous information. To give a few examples, a device can demonstrate that it is entitled to connect to the network without divulging details about its specification and previous interactions. This approach maintains privacy and, at the same time, offers secure authentication, which is one of the main characteristics of Zero-Trust Architecture (ZTA). With immutable blockchain combined with decentralized authentication and the privacy-enhancing features of ZKPs, ZTA establishes a strong validation mechanism that prevents unauthorized devices to gaining access to the network. In addition to being a ledger of authentication information, the blockchain ledger helps to guarantee that once a device identity has been verified, it will never be changed or replicated, which offers an immutable history of all devices and operations within the IoT systems. The additional security and privacy provided by using ZKPs enable devices to authenticate without disclosing any unnecessary information. This upholds the original idea of Zero-Trust: never trust, always verify.

4.3.1 AI's Role in ZTA Integration

Artificial Intelligence (AI), particularly machine learning (ML), plays a vital role in continuous monitoring and behavioral analytics within the Zero-Trust Architecture (ZTA) model. While blockchain handles identity verification and transaction validation, AI provides the intelligent analysis needed to detect and respond to potential security threats in real-time [78]. As IoT devices generate large volumes of data, AI algorithms are trained to recognize the standard behavior patterns of each device. When an anomaly occurs, it could indicate a possible security breach. ZTA leverages AI to monitor the activities of IoT devices, comparing them to established baselines to detect irregularities that may signal an impending threat. In case an anomaly (device unexpectedly sends data to an untrusted endpoint or executes some actions that are not provided by its functionality) is identified, AI may flag the suspicious behavior instantly. This real-time mode of detecting anomalies enables a quick response in cases of rising threats, hence any possible breach is countered before it develops further. When it comes to AI-driven systems, even automated actions, like blocking or quarantining the compromised devices, can be part of the process to prevent lateral movement of the attackers on the network.

4.3.2 Data Flow and Cross-Technology Security Verification

The combination of Zero-Trust-Architecture (ZTA), blockchain, and AI makes the delivery of data through the system as seamless as possible, with all the mentioned technologies interacting in mutually beneficial roles in providing security:

- **Device Registration and Authentication:** During the ingress of a new connected device into the IoT system, the blockchain does the authentication of the device by verifying its digital identity via decentralized verification. The blockchain ledger contains the device's identity, which cannot be altered, and it can only access the network upon verification.
- **Continuous Monitoring:** AI continuously monitors the behavior of the device on an ongoing basis after validating the device. It develops standard behavior groupings of the device and contrasts activities with the standards. If the device behaves suspiciously, such as attempting to communicate with untrusted nodes or displaying unusual data patterns, the AI will immediately raise the red flag.
- **Verification and Response:** In case of an anomaly, the Zero-Trust-Architecture (ZTA) provides the possibility to verify the device further, until sensitive operations are possible. Even after the initial access, the system examines the authenticity of devices on an ongoing basis by using micro-segmentation and access control policies, where only trusted devices can perform a particular action. In a situation where a

device is deemed compromised, AI can trigger a response (e.g., quarantine the machine), and blockchain provides a record of the event, which cannot be changed.

- **Audit and Transparency:** All interactions, whether legal or illegal, are recorded on the blockchain ledger. This creates an open and immutable audit trail that security teams can review at any time. Since blockchain is decentralized, there is no central authority controlling the logs, ensuring that they cannot be tampered with. These records can be audited by any party that is authorized to access them, providing transparency and accountability.

The integration of multiple technologies will create a dynamic security framework, where each technology supports the others. In this system, no device or user can bypass security measures without being detected by another layer of technology. This approach allows the system to adapt to evolving threats while ensuring transparency, accountability, and trust across the entire IoT ecosystem.

4.4 Edge Computing and ZTA Synergy

Edge computing enhances zero-trust architecture (ZTA) by bringing data processing closer to IoT devices. Unlike the use of centralized cloud servers in transferring information, edge computing processes information at the periphery of the network, thus allowing real-time responses to security risks [79,80]. Such proximity is fundamental to situations with time sensitivity, such as autonomous vehicles or other devices that are critical to healthcare, whose delay of device credentials verifications can provoke disastrous consequences. ZTA minimizes latency and network bandwidth by processing security checks at the network edge, which enables faster threat detection and mitigation [81–83]. As an example, when the sensor of an autonomous vehicle is compromised, edge computing allows isolating the compromised sensor without waiting for the cloud-based servers to send a response.

5 Challenges and Limitations in Implementing Emerging Technologies

Emerging technologies like AI, blockchain, edge computing, and Zero-Trust Architectures (ZTA) have significant potential when integrated with IoT security frameworks [84]. However, implementing such technologies in real-life IoT poses numerous challenges and restrictions [85]. The key issues regarding this topic are discussed as follows: namely, scalability, interoperability, computational constraints, real-time performance, security, and energy consumption. Table 3 shows the major technologically daunting issues in the implementation of AI, blockchain, and edge computing into the IoT security systems. It groups the problems under six large areas, including scalability, interoperability, computational constraints, latency and real-time processing, security and privacy-related concerns, and energy efficiency. Each row highlights the uniqueness of these issues in terms of their impact on the corresponding technologies, particularly in resource-constrained, heterogeneous, and large-scale IoT environments. The table can aid in the interpretation of limitations that should be overcome to have an effective and sustainable IoT.

Table 3: Challenges in implementing emerging IoT security technologies

Challenge area	Technology	Key issues
Scalability	AI	High computational demands from large data volumes affect scalability, limiting its applicability in large-scale IoT environments.
	Blockchain	The distributed nature of blockchain limits transaction throughput, which can become a bottleneck in large IoT deployments.

(Continued)

Table 3 (continued)

Challenge area	Technology	Key issues
Interoperability	Edge Computing	Managing and synchronizing distributed edge nodes becomes increasingly difficult as the number of IoT devices grows.
	AI	Diverse device specifications and communication protocols complicate the deployment of AI models across heterogeneous IoT systems.
	Blockchain	Lack of protocol standardization across IoT devices hinders seamless blockchain integration in various IoT systems.
Computational limitations	Edge Computing	Proprietary communication protocols between edge devices limit interoperability, making it difficult for edge nodes to communicate effectively.
	AI	Deep learning models are resource-intensive, making them unsuitable for low-power IoT devices with limited computational capabilities.
	Blockchain	The high resource demand for transaction validation in blockchain networks is often unsuitable for IoT hardware with constrained resources.
Latency & real-time processing	Edge Computing	Balancing the processing load across edge devices is challenging, especially when devices are resource-constrained and require real-time processing.
	AI	AI models can introduce processing delays, which are problematic for time-sensitive IoT applications, such as autonomous vehicles or smart healthcare.
	Blockchain	Blockchain's transaction verification process introduces latency, which can be detrimental to real-time IoT operations like industrial control systems.
Security & privacy concerns	Edge Computing	Ensuring real-time responsiveness across distributed edge nodes is complex, especially in large-scale IoT systems.
	AI	AI models are susceptible to adversarial attacks that manipulate input data, posing significant security risks to IoT systems.
	Blockchain	The transparency of blockchain can inadvertently expose sensitive data permanently, raising privacy concerns in certain IoT applications.

(Continued)

Table 3 (continued)

Challenge area	Technology	Key issues
	Edge Computing	Edge devices, being decentralized and often placed in less-secure environments, are attractive targets for cyberattacks, requiring robust security protocols.
Energy efficiency	AI	AI's energy demands can drain battery-operated IoT devices, reducing their operational lifespan and efficiency in energy-constrained environments.
	Blockchain	Blockchain's consensus and validation mechanisms consume significant energy, which may not be feasible for battery-powered IoT devices.
	Edge Computing	Edge devices, by virtue of processing large volumes of data, often suffer from high energy consumption, necessitating improvements in energy efficiency for sustainability.

In Fig. 4, a comparison was made over the IoT technologies of AI, Blockchain, and Edge Computing as per the demands of the computational resources. Artificial Intelligence is a data analysis game that requires extensive calculations. Blockchain is a highly intensive process that involves approving and recording transactions. Edge Computing strikes a balance between these two aspects, maximizing local computing power while minimizing energy consumption.

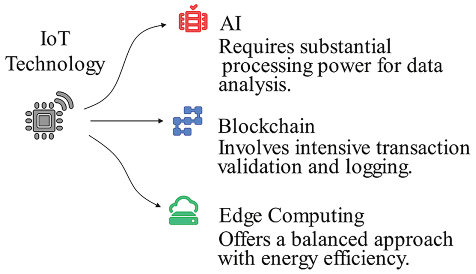
IoT
Technology
AI
Requires substantial processing power for data analysis.
Blockchain
Involves intensive transaction validation and logging.
Edge Computing
Offers a balanced approach with energy efficiency.

Figure 4: IoT technologies categorized by resource intensity requirements

5.1 Scalability

With IoT networks with billions of devices, security frameworks become more complex to scale. Scalability presents a distinct challenge for AI systems when combined with blockchain or edge computing in IoT applications.

- **Scalability of AI:** Systems based on AI assume that they process a large amount of data originating from IoT devices, and in many cases, in real-time. The computational challenge rises exponentially as the volume of linked devices increases, leading to data congestion, as well as a reduction of data processing and threat detection capabilities [86]. The models of AI should handle the growing scale without decreasing performance.
- **Blockchain Scalability:** Achieving decentralized safe system data management, scalability may become an issue with blockchain technology in large-scale IoT implementations since a distributed ledger

limits transaction throughput. Specifically, public blockchains face challenges related to low speed and efficiency due to the high computational costs associated with transaction validations [87]. There are attempts to make blockchain protocols less demanding on resources through scaling solutions to be used in IoT settings.

- **Edge Computing Scalability:** Edge computing is being used to increase the distance data is processed by moving it physically closer to the IoT device. Nevertheless, adding more devices to the network makes it even challenging to spread the computational load across different edge nodes [88]. The process of coordinating, managing, and securing interaction between these nodes while maintaining efficiency and security remains a significant challenge.

5.2 Interoperability

Interoperability plays a crucial role in integrating various IoT systems and devices, particularly when implementing AI, blockchain, and edge computing technologies within a decentralized environment. The communication protocols, data processing formats, and information vary across most IoT devices, creating difficulties when integrating them into a seamless communication framework.

- **AI and Devices Compatibility:** AI models used in maintaining IoT security need to be deployed on numerous devices and support systems with various technical characteristics and protocols of communication [89]. For successful implementations in security deployments, it is vital to ensure that such AI-based systems can analyze and communicate with heterogeneous devices.
- **Blockchain and Protocol Standardization:** A blockchain implementation can be based on particular standards, which are not necessarily compatible with the current IoT infrastructure. There are no unified communication standards to facilitate blockchain-based systems of IoT security [90]. Without cross-platform compatibility, using blockchain in IoT environments would remain fragmented and challenging to implement.
- **Edge Computing and Device Communication:** Data processors on edge devices must be able to connect seamlessly with the centralized cloud solution and other edge nodes. For edge computing to be effectively deployed, smooth interoperability between these layers and the effortless exchange of data are crucial [91,92]. However, the variety of internet-connected devices from different manufacturers, each using its own proprietary protocols, makes integration more challenging.

5.3 Computational Limitations and Resource Constraints

IoT devices are inherently resource-constrained—they have limited processing power, memory, and battery life. As a result, implementing resource-heavy technologies like AI and blockchain on these devices presents a significant challenge.

- **Machine Learning Algorithms and AI:** AI models, particularly newer deep learning models, are computationally intensive. However, most IoT devices lack the processing power to support such demanding requirements, making them unsuitable for running AI-based security systems [93]. To address this, researchers are working on developing lighter AI models and using edge computing to help distribute the workload and ease the strain on these devices.
- **Blockchain Overhead:** It consumes a lot of computational energy to maintain a blockchain network, especially in transaction validation and confirmations. This overhead cannot be supported very well in IoT devices that typically lack sufficient storage and processing power. Even lightweight blockchain protocols, such as those using off-chain solutions, are helpful to some extent, but their implementation still lies at an early stage [94].

- **Resource Allocation:** Edge devices have to make complex calculations with limited resources that are at their disposal [95]. Real-time security analysis on top of energy consumption and processing capacity is also a significant challenge for a resource-constrained IoT device.

5.4 Latency and Real-Time Processing

Time-sensitive IoT systems, such as those used in healthcare and self-driving vehicles, rely on real-time processing. However, technologies like AI and blockchain, which offer significant security benefits, often introduce latency issues, making it challenging to meet the real-time requirements of these systems.

- **AI Processing Lag:** AI-enabled threat detection systems process a lot of information in real-time to reliably detect abnormalities and predict the occurrence of a security threat [96]. Although effective, such processes may also cause delay, especially when the models used are deep learning models. In critical setups like the autonomous vehicle system, even a slight delay in decision-making can lead to disaster.
- **Blockchain Verification Latency:** Such blockchain transaction validation needs time to distribute the transaction information on the network, which poses a problem for real-time IoT security solutions [97]. Although blockchain guarantees information integrity, such a latency may be adverse to the prompt reaction in high-stakes situations, i.e., industrial automation or emergency services.
- **Low Latency Edge Computing:** Low latency can be achieved through edge computing, since it processes the data extremely close to the source, minimizing the number of times communication exists with a cloud server [98]. Nevertheless, making a large-scale IoT network responsive in real-time is a complicated task, particularly in managing a range of edge nodes.

5.5 Security and Privacy Concerns

The emerging technologies, in addition to improving the security of IoT, create new security and privacy risks. New vulnerabilities can arise due to the complexity of AI, blockchain, and edge computing programs.

- **Adversarial Attacks of AI Systems:** AI models, and especially those applied in IoT, can be subject to adversarial attacks, in which minor alterations in input data can make the AI system classify or make an incorrect decision [99]. This weakness presents a serious threat in applications using AIs to detect anomalies and security problems.
- **Blockchain Privacy Problems:** While blockchain ensures data immutability and transparency, privacy concerns can arise. The encrypted data stored on the blockchain is permanent and accessible to all network participants, which means there's a potential risk of sensitive data being exposed. Technologies like zero-knowledge proofs and homomorphic encryption are being explored to enhance privacy, but they have not yet been widely adopted [100].
- **Edge Computing Vulnerabilities:** Decentralization in data processing, brought about by edge computing, increases the risk of vulnerabilities [101]. Each edge node operates independently, making it a potential target for attackers. As a result, the security of data processed at the edge must be closely monitored and encrypted with advanced methods to protect it from breaches.

5.6 Energy Efficiency

In many cases, IoT endpoint devices installed in remote or resource-constrained areas face energy limitations. Implementing power-hungry technologies like AI and blockchain only worsens these challenges, as they require more energy to function effectively.

- **AI Energy Usage:** AI systems, especially the latest deep learning models, are energy-intensive, requiring significant power to process and analyze data [102]. IoT devices, which often rely on low battery power, may not be able to meet these energy demands over time [103]. However, using energy-efficient AI models and leveraging edge computing can help reduce some of these demands, though further optimization is still needed.

- **Blockchain and Energy Costs:** Blockchain, particularly public blockchains, can be very energy-intensive due to the transaction validation and consensus protocols involved [104]. These high-power requirements clash with the low energy needs of IoT devices, highlighting the need for more energy-efficient blockchain solutions that can work seamlessly in IoT environments.
- **Edge Computing and Energy Trade-Off:** While edge computing helps reduce the energy consumption and costs associated with sending data to centralized servers, edge devices themselves are still tasked with processing complex tasks locally, which can drain their energy resources. To ensure sustainable IoT implementations, the key lies in using energy-efficient edge devices and algorithms [105].

6 Application of AI, Blockchain, and Edge Computing for Zero-Trust IoT Security

These combinations of Artificial Intelligence (AI), Blockchain, and Edge Computing in ZTA [106] offer multiple layers of security that are both adaptive and decentralized and are effective in addressing some security challenges inherent in IoT setups. Each of these technologies brings unique strengths to enhancing IoT security. In this section, we explore how combining these methods can strengthen Zero-Trust security, specifically in areas like smart homes, industrial IoT, and autonomous vehicles. Fig. 5 illustrates the key components of a Zero-Trust security framework, emphasizing practices such as early integration of security, continuous authentication, encryption, regular updates, policy enforcement, and user training.

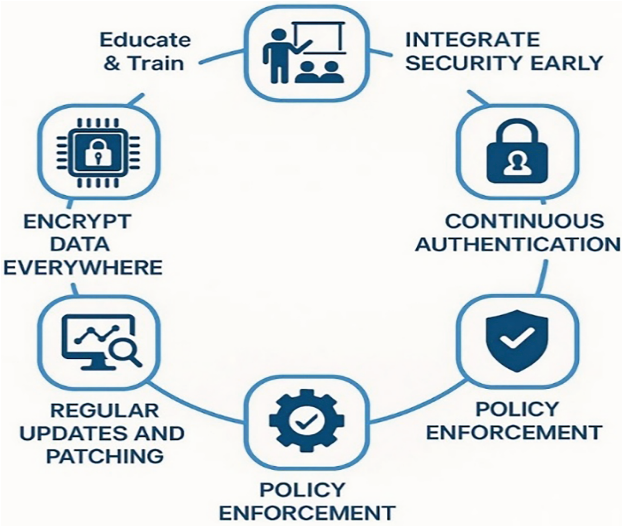

Figure 5: Implementing zero trust in AI applications

6.1 AI for Real-Time Threat Detection and Response

AI plays a vital role in real-time threat monitoring and anomaly detection within IoT networks. The dynamic nature of IoT, where cyber threats frequently emerge, makes traditional rule-based security systems ineffective over time. By leveraging AI, particularly machine learning (ML) and deep learning (DL), these systems can process large datasets generated by IoT devices and identify patterns or anomalies that may signal potential security risks.

Use Case Smart Home Security

Anomaly detection in smart homes driven by AI can monitor the behavior of devices like smart thermostats, cameras, and locks. For example, if a smart lock that is typically used at night suddenly activates during off-hours, AI could flag this as suspicious and immediately send an alert to the homeowner [107].

- **Predictive Analytics:** AI is also capable of predicting the possibility of a security breach based on previous conduct. For instance, AI can identify abnormal behavior patterns in smart appliances and alert homeowners to potential system attacks, such as botnet or data exfiltration attacks [108].
- **Automated Responses:** Anomalous responses to anomalies represent an AI-driven security measure that can facilitate Zero-Trust. For instance, upon detecting an unauthorized access attempt to the smart home device, the device can automatically be isolated from the network and the homeowner notified. Such an automatic response does not require lots of manual involvement, and the reaction time is faster [109].

6.2 Blockchain for Decentralized Security and Data Integrity

Blockchain offers a decentralized platform to secure Internet of Things networks, meaning the completion of any form of transaction involving IoT data transmission or device authentication is unalterable, publicly viewable, and auditable.

Industrial IoT (IIoT) in Manufacturing Use Case

In the context of Decentralized Device Authentication for industrial IoT (IIoT), thousands of devices, such as sensors, actuators, and controllers, are used to monitor and control manufacturing processes. Each device can be assigned a unique digital identity on the blockchain, ensuring that only authorized devices can access and interact with the IIoT network [110].

- **Immutability and Transparency:** Blockchain ensures that once data is recorded on the chain, whether it's temperature readings or machine performance data, it can't be altered. This is especially valuable in IIoT environments, where maintaining data integrity is essential for safety and compliance. For example, in a manufacturing plant, blockchain can track machine maintenance records in a way that prevents tampering with the data, such as ignoring or altering maintenance procedures [111].
- **Utilizing Smart Contracts with Scripts as Presented by Blockchain:** smart contracts could be used to automate security in industrial IoT. As an example, access control regulation may be implemented with smart contracts that permit only devices with a given set of credentials to view sensitive manufacturing systems or data [112], *vice versa*.

6.3 Edge Computing for Low-Latency Security

Edge computing enables real-time data processing by moving computing to the network's edge, bringing the computing system as close to IoT devices as possible. This is crucial for applications where response time is critical for decision-making.

Autonomous Vehicles Use Case

- **Processing of the Real-Time Data:** Autonomous cars depend on the processing of real-time data to make crucial decisions like identifying obstacles or traveling through traffic. The data collected using cameras, sensors, and LiDAR is processed by edge computing, which helps reduce latency and enables quick decisions before accidents happen or in response to a dynamically changing environment [113].
- **Enhanced Edge Security:** Processing is shared and spread over edge nodes, avoiding chances of a single point of failure. Where autonomous vehicles are concerned, in case one edge node was damaged (e.g.,

the sensor node of a car), it is isolated and has no impact on the other nodes of the vehicle. This plays a vital role in ensuring that attacks do not reach across the whole fleet of vehicles [114].

- **Data Privacy and Local Processing:** Edge computing can also increase data privacy by locally processing data that needs to be confidential, like passenger location or driving habits, without transferring it to a central server and preventing data leakage [115].

6.4 Synergizing AI, Blockchain, and Edge Computing for Zero-Trust IoT Security

Integration of AI, blockchain, and edge computing forms a robust and dynamic security ecosystem for IoT systems, with each technology complementing the others in real-time, adapting to new threats, and ensuring a secure environment.

Use Case: Smart City

- **AI and Blockchain Synergy:** AI can be used to detect abnormal behavior by IoT devices in a smart city (such as traffic lights and sensors of public utilities), and blockchain can guarantee the security of all data, which has to be stored and cannot be altered. Consider another scenario: AI detects suspicious operations, such as an intelligent traffic sensor generating illegal data to be sent outside the network to an external server. In this case, blockchain can create an immutable log of the transaction, making all actions transparent and auditable [116].
- **Edge Computing Enabled Technology:** Edge Computing will be critical as it will enable raw blockchain verification and AI analysis on the device level in real-time. An example in the smart city would be to use edge nodes that process traffic sensor data locally to detect threats via AI, which is validated and stored through blockchain in real time. This will minimize the use of one centralized cloud system in case of high response rates and limit single points of failure risks [117].
- **Adaptive Zero-Trust Model:** In a collaborative effort of AI, blockchain, and edge computing, enabling innovations to the Zero-Trust model in IoT networks is possible. AI constantly keeps checking the devices and flagging potentially harmful activity, blockchain provides tried-and-true integrity and traceability of any transaction, and edge computing enables real-time decision-making capabilities. Collectively, they form an IoT ecosystem that is not only secure but also scalable and resilient, with the capacity to react dynamically to emerging threats [118].

7 Why AI, Blockchain, and Edge Computing for Zero-Trust IoT Security

The integration of AI, blockchain, and edge computing into a ZTA provides a robust and adaptive security framework for the Internet of Things (IoT). This approach addresses the limitations of traditional cybersecurity models that struggle to handle the scale, complexity, and dynamic nature of modern IoT networks. This section outlines why these emerging technologies are essential for implementing an effective Zero-Trust IoT security model.

7.1 Dealing with Scalability and Decentralization

Currently, the growth of IoT networks is exponential; billions of devices are already communicating and sharing data in a wide range of apps. The conventional centralized models of security will be unable to match such a pace, and there will be bottlenecks and potential single points of failure [119]. To create a scalable and decentralized IoT security framework, it is essential to apply AI, blockchain, and edge computing.

- **AI to Handle Data Masses:** IoT connections yield vast amounts of data in real-time, and this in turn becomes challenging to manage and analyze using conventional security measures. AI, especially the machine learning algorithms, can effectively operate and analyze significant flows of data, detecting patterns and abnormalities that could point to the possible risk of security breaches. Artificial intelligence can also scale as IoT networks grow in size and evolve alongside new data sources and types of attacks [120].

- **Decentralized Trust:** Blockchain has a decentralized architecture, which makes it a perfect IoT security mechanism. Blockchain spreads trust throughout the network as opposed to relying on a centralized authority to authenticate devices and transactions [121]. This distributed system has no single point of failure, allowing the IoT network to scale without compromising its security. Every transaction or interaction is securely recorded on a distributed ledger, ensuring transparency and building trust within the decentralized network.
- **Edge Computing, a Way of Distributed Processing:** Edge computing complements AI and blockchain by decentralizing tasks and bringing them closer to the devices themselves. This reduces the need to send data to a central server, improving scalability and lowering latency [122]. One of the key benefits of edge computing is that security measures can be implemented directly at the edge, preventing network overloads and enabling a quicker response to threats, especially in large-scale IoT networks.

7.2 Enhancing Real-Time Threat Detection and Response

IoT systems need real-time detection and prevention to ensure the safe operation of critical systems like automotive, healthcare, and industrial control. By combining AI, blockchain, and edge computing, it becomes easier to automate threat analysis, enable decentralized verification, and provide fast, localized responses to potential issues.

- **Artificial Intelligence in Proactive Threat Detection:** Artificial intelligence can help identify potential threats before they even happen, unlike traditional security tools that only respond after an attack occurs. With AI-powered systems, threats can be predicted and detected in advance. IoT systems, for example, analyze historical attack data and use that information to prevent future threats using machine learning models. This ability for real-time detection is crucial in Zero-Trust environments, where devices and data need to be continually validated [123].
- **Blockchain Immutable Security Logs:** Transparency and accountability are central to the Zero-Trust model. The immutable blockchain ledger ensures a permanent record of all transactions and interactions [124]. This boosts data reliability and helps with forensic investigations, allowing the security team to trace the origin of an attack. Additionally, security policies can be automated through smart contracts, and access controls can be applied instantly as new risks are identified, helping to mitigate potential threats.
- **Low-Latency Security through Edge Computing:** The security solution may require millisecond-level decisions, e.g., in self-driving cars or medical devices. By use of edge computing, these decisions can be acted upon at the edge of the network, resulting in latency reduction by a significant margin [125]. Edge computing enables IoT devices to respond in real-time to threats and security breaches by processing threat detection and response locally, rather than relying on cloud-based solutions.

7.3 Overcoming Resource Constraints in IoT Devices

IoT devices have limited processing capabilities, as well as power, memory, and energy. The traditional security solution is frequently not a feasible alternative to implement on such devices because of the computational and energy costs. Edge computing, blockchain, and artificial intelligence provide more scalable, efficient, and unique solutions to IoT devices.

- **AI-Based Efficiency:** AI may be designed to execute on energy-constrained, IoT-based devices. It is possible to use a lightweight AI algorithm to analyze data, leveraging edge AI to identify anomalies locally without straining the device's processing capabilities. This enables even the less powerful IoT gadgets to enjoy sophisticated security features [126].

- **Blockchain Lightweight Security:** Blockchain is resource-intensive; however, newer blockchain protocols that are IoT-focused are resource-light and suitable for use on low-power devices. Methods like sharding, off-chain transactions, and agreements such as Proof of Stake (PoS) eliminate the computational overhead of the traditional blockchain models [127]. That way, IoT devices with limited access to resources can join blockchain networks without depleting their processing power.
- **IoT Data Local Processing:** Edge computing can offload processing of intensive data tasks to neighboring edge computers to spare IoT devices. Compared with the IoT nodes, these edge nodes are more powerful in processing and storage capabilities, in that they can perform complex security processing on behalf of the IoT devices, so that they are focused on their central operations [128]. Such a decentralized system conserves the device's resources and ensures the network has comprehensive security protocols implemented.

7.4 Strengthening the Zero-Trust Model

The core principle of Zero-Trust Architecture is "never trust, always verify." Every machine, participant, and transaction within the network must continuously authenticate and validate itself. By combining AI, blockchain, and edge computing, this model is further reinforced, ensuring that all interactions are secure, verifiable, and immutable.

- **Permanent AI:** AI plays a crucial role in providing continuous monitoring of network activity, ensuring that no device or user is automatically trusted. Machine learning algorithms analyze network traffic, device behavior, and data transfers in real-time, flagging any anomalies that deviate from normal patterns [129]. This constant vigilance helps detect even the smallest security threats before they can escalate into serious issues.
- **Immutable Verification:** Blockchain ensures tamper-proof verification of all transaction assessments within the IoT network. Once data is written to the blockchain, it cannot be erased or altered, providing an auditable record [130]. This is especially important in Zero-Trust environments, where continuous verification is required, and no device or interaction is trusted by default. The transparency feature of blockchain adds an extra layer of accountability, ensuring that every activity within the network can be securely documented and traced.
- **Edge Computing and Real-Time Authentication:** Edge computing takes the Zero-Trust model to the next level by pushing authentication and access validation to the edge of the network, leading to real-time decisions. This local verification ensures that only trusted devices and users can access critical resources [131]. By eliminating delays in processing authentication requests, edge computing improves the overall performance and efficiency of the Zero-Trust model.

7.5 Supporting Future IoT Security Requirements

As IoT systems continue to evolve, there will be an increasing need for adaptive, scalable, and secure architectures, as these systems will have more opportunities to interact with each other and potentially cause harm. Edge computing, blockchain, and AI are uniquely positioned to meet the growing demands of future IoT networks, offering flexible security solutions that can adapt to emerging threats and technological advancements. These technologies can help create security frameworks that evolve alongside the changing landscape of IoT.

- **AI in Evolving Threat Detection:** AI systems are continuously learning and evolving, making them well-suited for detecting new and evolving threats in an IoT environment [132]. As AI models become more advanced, they can be retrained with new data to tackle emerging challenges, helping IoT systems stay ahead of an ever-changing threat landscape.

- **Blockchain to Autonomous IoT Systems:** The decentralized nature of blockchain makes it an ideal solution for securing autonomous IoT systems, such as smart cities and industrial automation [133]. In these environments, where devices must operate autonomously and securely, blockchain provides a transparent and trustless platform. It ensures that all activities are verifiable and unalterable, helping to create self-sustained systems that can function without the need for centralized coordination.
- **Edge Computing in IoT Growth:** As IoT applications expand in areas like 5G, innovative healthcare, and autonomous vehicles, edge computing will play a crucial role in ensuring low-latency and real-time processing [134]. In these critical applications, edge computing improves the ability to respond quickly to security threats by distributing security requirements across edge nodes, enabling faster and more efficient threat detection and response.

8 Regulatory Frameworks and Compliance in IoT Security

As IoT networks expand, integrating technologies like AI, blockchain, and edge computing must comply with multiple data privacy laws and cybersecurity regulations, making it a worthwhile and legal use of technology. Such laws as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) impose rigorous data collection, processing, and storage rules. The laws require adherence by AI on IoT devices in limiting the amount of data used and explainability in decision-making, even though black-box AI models defy such law requirements. The use of blockchain provides permanent data storage, which may contradict the right to be forgotten (GDPR) because it necessitates the removal of certain information after its upload. This problem can be countered through the use of solutions such as off-chain storage or even the use of private blockchains, which do not diminish the level of security afforded by blockchain [133]. Edge computing, which performs local data processing, increases data privacy by reducing the amount of data transferred centrally. Nonetheless, it should also adhere to cross-border data transfer rules, especially where sensitive information is concerned. Legislation such as the NIST Cybersecurity Framework and the IoT Cybersecurity Improvement Act offers fundamental guidance in ensuring the security of IoT devices in the context of cybersecurity. These regulations can be complied with the assistance of AI, blockchain, and edge computing. Through AI, real-time anomaly detection is possible. Blockchain enables secure data storage and protection, as well as decentralized authentication.

Edge computing has the potential to mitigate the consequences of single points of failure by localizing data processing and threat response. The technologies provided by IoT have specific regulations that must be followed in certain industries, such as healthcare and finance. To give an example, when referring to the healthcare sector, HIPAA dictates that patient data is subject to stringent controls, and both AI and blockchain should ensure that health data is secure and transparent. In the finance sector, PSD2 requires secure authentication for financial transactions, and blockchain offers a transparent and secure solution. However, it must meet the stringent security standards of the financial industry. Controversies arise when these technologies intersect with regulatory policies. For example, AI's "black box" nature can limit transparency, and the immutability of blockchain raises concerns about the "right to be forgotten" as outlined in data protection regulations. These issues can be addressed through strategies like implementing explainable AI models or using private blockchains [134]. While edge computing offers benefits for data privacy, it still needs to comply with data sovereignty laws and cross-border data regulations. Such difficulties demand further studies of the harmonization of regulation so that the adoption of innovative IoT security technologies does not interfere with compliance.

9 Future Outlook and Challenges of AI, Blockchain, and Edge Computing in Zero-Trust IoT Security

As IoT ecosystems grow in size and complexity, emerging technologies such as AI, blockchain, and edge computing are becoming critical in addressing the security needs of these networks. These technologies align well with the ZTA model, which is essential for securing decentralized and distributed IoT environments [135]. Together, they provide a robust, layered defense that addresses many of the inherent vulnerabilities of IoT systems. However, the integration of these technologies presents challenges that must be overcome for effective and scalable security solutions [136]. This section discusses the significance of these technologies, the key challenges in their implementation, and potential future directions for IoT security.

9.1 Emergence of AI, Blockchain, and Edge Computing for Zero-Trust IoT Security

IoT security is evolving as the implementation of AI, blockchain, and edge computing impacts the security of devices and networks. The technologies enable IoT systems to adhere to Zero-Trust principles through decentralized, real-time, and replicable security applications.

- **Dynamic Threat Detection with AI:** AI can be used to make dynamic threat detection and predictive analysis possible on IoT products. This is achieved through AI in a Zero-Trust IoT setting, which continuously monitors device behavior and network traffic, addressing potential security breaches at their earliest stages [137]. This is the active side of the Zero-Trust approach, in which nothing, including a device or a user, is trusted by default, and the validation must be ongoing. Immutable and Decentralized Security Blockchain is decentralized, eliminating the need for central authorities. It provides an immutable ledger for securely storing all transactions and communications of the devices [138]. This is a transparent and unalterable verification that is important in Zero-Trust networks, where all interactions have to be verified.
- **Edge Computing to Process in Real-Time:** Edge computing decreases latency because it processes data near the IoT devices. Edge computing as a tool can be used in time-sensitive applications, like in healthcare or autonomous vehicles, where a threat can be recognized and addressed in real-time [139]. It aids the Zero-Trust paradigm by enabling the implementation of security decisions in a decentralized manner within a limited timeframe.

A combination of these technologies enables IoT systems to meet the requirements of the Zero-Trust security approach, thereby addressing scalability, security, and performance issues. Yet, some implementation barriers should be mentioned. The categorization in Fig. 6 into four important technological areas, Blockchain-Based Solutions, Fog Computing-Based Solutions, Edge Computing Solutions, and Machine Learning-Based Solutions, reflects the current IoT security solutions. All these categories contribute to the security, scalability, and protection in real-time within the Internet of Things environment.

9.2 Key Challenges in Implementing AI, Blockchain, and Edge Computing for Zero-Trust-Architecture (ZTA)

Besides the opportunity, the widespread application of AI, blockchain, and edge computing in IoT security systems is hindered by numerous issues. Scalability, resource limitations, interoperability, and energy efficacy are some of the most urgent concerns.

- **Scalability:** The IoT networks will be increasing, which is why scaling AI, blockchain, and edge computing technologies without compromising performance is a problem. The scale of real-time data and the security of millions of transactions carried out by AI algorithms and blockchain networks, respectively, necessitate processing by both blockchain networks and AI algorithms [140]. Greater data traffic would have to be handled by edge computing, and this would cause bottlenecks in a distributed environment.

- **Resource Limitation:** Most IoT devices are limited in processing, storage capacity, and energy, which makes it hard to use computationally expensive AI models or blockchain protocols [141]. There is still much technical work to do in optimizing these technologies for resource-constrained environments.
- **Interoperability:** IoT ecosystems are characterized by heterogeneous devices from different manufacturers, which have their own protocols and standards. It isn't easy to make the communications between these types of devices seamless when introducing AI, blockchain, and edge computing [142]. The lack of standardized protocols makes it challenging to design coherent security frameworks that are applicable across all devices.
- **Energy Efficiency:** The computational power needed by AI and blockchain may draw on the limited energy capacity of IoT devices. Since edge computing may be used to decrease energy costs by processing on-demand content at the edge, the challenge in large-scale IoT systems is to reconcile the computation level with energy efficiency [143].

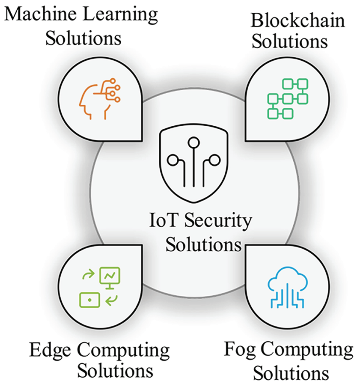

Figure 6: Classification of IoT security solutions

9.3 Future Directions and Perspectives

Some research and development initiatives allow the mitigation of these issues and facilitate the integration of AI, blockchain, and edge computing in Zero-Trust IoT-based systems.

- **Creation of Lightweight AI and Blockchain Protocols:** Research into lightweight AI models and blockchain protocols will be crucial in optimizing these technologies for IoT devices [144]. This will reduce the computational and energy demands of these technologies, making it possible to scale IoT networks securely while maintaining strong performance.
- **Interoperability Standards:** The industry needs to establish a unified standard for IoT devices to facilitate the seamless integration of AI, blockchain, and edge computing. By implementing cross-type communication protocols among devices, IoT security systems can work more efficiently, enabling these technologies to be deployed effectively across various ecosystems [145].
- **Increased AI and Blockchain Interactions:** AI and blockchain together offer the potential to create more effective and transparent security systems. Blockchain enhances AI applications by improving transaction predictions and consensus algorithms [146], while AI can optimize blockchain applications by making device-readable data more accessible and helping to determine and distribute blockchain resources. This mutual benefit strengthens both technologies, enabling them to work seamlessly together.

- **IoT Security Is Increasingly More Edges:** Edge computing is a promising technology for managing latency, real-time awareness, and low latency in IoT networks. As edge AI, which involves local processing of AI algorithms, continues to advance, it will further enhance the security framework of IoT systems, enabling quicker responses and more efficient threat detection [147].
- **AI to Address Evolving Threat Landscapes:** As the threat landscape evolves, AI must be capable of adapting to new and changing threats. Specialized machine learning solutions that can learn independently and adjust to emerging, unknown attack vectors will ensure that IoT systems stay ahead of attackers, neutralizing threats before they cause significant damage [148]. Table 4 outlines how AI, blockchain, and edge computing contribute to enhancing Zero-Trust security in IoT systems, focusing on five key areas.

Table 4: Future directions for enhancing zero-trust iot security using AI, blockchain, and edge computing

Future direction	Description
Lightweight AI and blockchain protocols	Focus on developing resource-efficient models to reduce energy and computational load, enabling secure and scalable IoT deployments.
Interoperability standards	Establish universal communication protocols to enable seamless integration of AI, blockchain, and edge computing across diverse IoT devices.
AI and blockchain synergies	Combine AI for predictive analytics and blockchain for tamper-proof verification to enhance system transparency and automated threat response.
Advances in edge computing	Evolve edge AI capabilities to allow localized, real-time processing and decision-making, reducing latency and improving system resilience.
AI for evolving threat landscapes	Deploy adaptive machine learning models that continuously learn from new data to detect and mitigate sophisticated cyber threats proactively.

The successful integration of AI, blockchain, and edge computing into Zero-Trust IoT architectures will have far-reaching implications for the future of IoT security [149]. These technologies provide the foundation for building adaptive, scalable, and resilient IoT networks capable of withstanding future cyber threats. As IoT expands across various industries, including healthcare, smart cities, and industrial automation, securing these networks with dynamic, decentralized security frameworks will be essential to maintaining their integrity, performance, and reliability [150].

10 Conclusion

The Internet of Things (IoT) has transformed how devices and systems communicate, opening up new possibilities across various sectors. However, this rapid growth has also made IoT networks more vulnerable to sophisticated cyber threats. Traditional perimeter-based security models are no longer suitable for the decentralized and dynamic nature of IoT environments. The question drives the novelty of this study: How can the integration of advanced decentralized security technologies like Artificial Intelligence (AI), blockchain, and edge computing into a Zero-Trust Architecture (ZTA) address the challenges of securing IoT systems? These technologies can be used jointly to improve security by providing real-time detection and response to threats using AI, decentralized device authentication and data integrity using blockchain, and low-latency, real-time processing using edge computing. This composite creates a multi-tiered, Zero-Trust security model that continuously accredits all communications within the IoT ecosystem. Nonetheless, there are challenges associated with the implementation of such technologies into the IoT security systems, such as resource constraints, scaling, interoperability, and energy consumption. As an illustration, AI and blockchain demand significant computing capabilities, which might be impractical given the limited resources of IoT gadgets. Differences in protocols between various devices also add to the problem of interoperability. Additionally, the aspect of energy usage, particularly the reliance on batteries to power IoT devices, is a significant concern. To fully utilize AI, blockchain, and edge computing for IoT security, it is necessary to develop lightweight protocols that reduce computational load, enhance interoperability, and create more energy-efficient security systems. Although the paper is an excellent discussion of the theoretical advantages and issues of integrating these technologies, it does not offer any practical case studies or empirical data. As we progress, we should pay more attention to the practical implementation of Zero-Trust IoT security, particularly in such fields as smart cities, healthcare, and industrial IoT. With the emergence of IoT networks across various industries, integrating AI, blockchain, and edge computing with Zero-Trust concepts will significantly enhance the security, integrity, and scalability of IoT systems. Addressing these issues and focusing on viable applications, we can make the IoT ecosystems remain safe, responsive, and sustainable in our more interconnected world.

Acknowledgement: Not applicable.

Funding Statement: The researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025).

Author Contributions: Conceptualization, Inam Ullah Khan, Zeeshan Ali Haider, Fida Muhammad Khan; formal analysis, Inam Ullah Khan, Zeeshan Ali Haider; funding acquisition, Fahad Alturise; investigation, Zeeshan Ali Haider; methodology, Fida Muhammad Khan, Zeeshan Ali Haider; project administration, Fida Muhammad Khan; resources, Zeeshan Ali Haider; software, Fida Muhammad Khan; validation, Inam Ullah Khan, Zeeshan Ali Haider, Fida Muhammad Khan; visualization, Inam Ullah Khan Khan, Fida Muhammad Khan; writing—original draft, Inam Ullah Khan, Zeeshan Ali Haider; writing—reviewing and editing, Fida Muhammad Khan, Fahad Alturise, Fida Muhammad Khan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

Abbreviation	**Description**
AI	Artificial Intelligence
IoT	Internet of Things
ML	Machine Learning
IDS	Intrusion Detection Systems
PoS	Proof of Stake
SRHR	Sexual and Reproductive Health Rights
MEC	Mobile Edge Computing
RFID	Radio Frequency Identification
ITS	Intelligent Transportation Systems
DLT	Distributed Ledger Technology
ZERO-TRUST-ARCHITECTURE(ZTA)	Zero-Trust Architecture
DL	Deep Learning

PD	Proportional-Derivative
IAM	Identity and Access Management
ZKP	Zero-Knowledge Proofs
UPS	Uninterruptible Power Supply
GPS	Global Positioning System
VANETs	Vehicular *Ad Hoc* Networks

References

1. Falayi A, Wang Q, Liao W, Yu W. Survey of distributed and decentralized IoT securities: approaches using deep learning and blockchain technology. Fut Internet. 2023;15(5):178. doi:10.3390/fi15050178.
2. Rahman M, Saifullah A. Transparent and tamper-proof event ordering in the Internet of Things platforms. IEEE Internet Things J. 2023;10(6):5335–48. doi:10.1109/JIOT.2022.3222450.
3. Yang J, Wen J, Jiang B, Wang H. Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Netw. 2020;34(4):62–7. doi:10.1109/MNET.011.1900374.
4. Zhang K, Leng S, He Y, Maharjan S, Zhang Y. Mobile edge computing and networking for green and low-latency Internet of Things. IEEE Commun Mag. 2018;56(5):39–45. doi:10.1109/MCOM.2018.1700882.
5. Nathali Silva B, Khan M, Han K. Big data analytics embedded smart city architecture for performance enhancement through real-time data processing and decision-making. Wirel Commun Mob Comput. 2017;2017(1):9429676. doi:10.1155/2017/9429676.
6. He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: challenges and future trends. Wirel Commun Mob Comput. 2022;2022(1):6476274. doi:10.1155/2022/6476274.
7. Daah C, Qureshi A, Awan I, Konur S. Enhancing zero trust models in the financial industry through blockchain integration: a proposed framework. Electronics. 2024;13(5):865. doi:10.3390/electronics13050865.
8. Tesfaye A, Kebede Z. Real-time anomaly detection in IoT networks using hybrid AI models. Asian Am Res Lett J. 2024;1(3).
9. Alzoubi MM. Investigating the synergy of Blockchain and AI: enhancing security, efficiency, and transparency. J Cyber Secur Technol. 2025;9(3):227–55. doi:10.1080/23742917.2024.2374594.
10. Ruzbahani AM. AI-protected blockchain-based IoT environments: harnessing the future of network security and privacy. arXiv:2405.13847. 2024.
11. Kherraf N, Alameddine HA, Sharafeddine S, Assi CM, Ghrayeb A. Optimized provisioning of edge computing resources with heterogeneous workload in IoT networks. IEEE Trans Netw Serv Manag. 2019;16(2):459–74. doi:10.1109/TNSM.2019.2894955.
12. Li X, Liu Y, Ji H, Zhang H, Leung VCM. Optimizing resources allocation for fog computing-based Internet of Things networks. IEEE Access. 2019;7:64907–22. doi:10.1109/ACCESS.2019.2917557.
13. Khan D, Jung LT, Hashmani MA. Systematic literature review of challenges in blockchain scalability. Appl Sci. 2021;11(20):9372. doi:10.3390/app11209372.
14. Davis P, Coffey S, Beshaj L, Bastian ND. Emerging technologies for data security in zero trust environments. Cyber Def Rev. 2024;9(2):49–72.
15. Fei W, Ohno H, Sampalli S. A systematic review of IoT security: research potential, challenges, and future directions. ACM Comput Surv. 2023;56(5):1–40. doi:10.1145/3625094.
16. Raza H. Proactive cyber defense with AI: enhancing risk assessment and threat detection in cybersecurity ecosystems; 2021 [cited 2025 Jan 1]. Available from: https://www.researchgate.net/publication/384323201.
17. Rizvi M. Enhancing cybersecurity: the power of artificial intelligence in threat detection and prevention. Int J Adv Eng Res Sci. 2023;10(5):55–60. doi:10.22161/ijaers.105.8.
18. Das A, Adhikari N. Future-proofing IoT security: the impact of artificial intelligence. In: The intersection of 6G, AI/machine learning, and embedded systems. Boca Raton, FL, USA: CRC Press; 2025. p. 369–90.
19. Otoum Y, Gottimukkala N, Kumar N, Nayak A. Machine learning in metaverse security: current solutions and future challenges. ACM Comput Surv. 2024;56(8):1–36. doi:10.1145/3654663.

20. Albogami NN. Intelligent deep federated learning model for enhancing security in Internet of Things enabled edge computing environment. Sci Rep. 2025;15(1):4041. doi:10.1038/s41598-025-88163-5.
21. Schmitt M. Securing the digital world: protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. J Ind Inf Integr. 2023;36(1):100520. doi:10.1016/j.jii.2023.100520.
22. Bhushan B, Sinha P, Sagayam KM, Andrew J. Untangling blockchain technology: a survey on state of the art, security threats, privacy services, applications and future research directions. Comput Electr Eng. 2021;90(9):106897. doi:10.1016/j.compeleceng.2020.106897.
23. Gangwani P, Joshi S, Upadhyay H, Lagos L. IoT device identity management and blockchain for security and data integrity. Int J Comput Appl. 2023;184(42):49–55. doi:10.5120/ijca2023922529.
24. Zhang Z, Feng J, Pei Q, Wang L, Ma L. Integration of communication and computing in blockchain-enabled multi-access edge computing systems. China Commun. 2021;18(12):297–314. doi:10.23919/JCC.2021.12.019.
25. Xue H, Chen D, Zhang N, Dai HN, Yu K. Integration of blockchain and edge computing in Internet of Things: a survey. Future Gener Comput Syst. 2023;144(1):307–26. doi:10.1016/j.future.2022.10.029.
26. Kuchuk H, Malokhvii E. Integration of IoT with cloud, fog, and edge computing: a review. Adv Inf Syst. 2024;8(2):65–78. doi:10.20998/2522-9052.2024.2.08.
27. Sodiya EO, Umoga UJ, Obaigbena A, Jacks BS, Ugwuanyi ED, Daraojimba AI, et al. Current state and prospects of edge computing within the Internet of Things (IoT) ecosystem. Int J Sci Res Arch. 2024;11(1):1863–73. doi:10.30574/ijsra.2024.11.1.0287.
28. Souza C, Falcão M, Balieiro A, Alves E, Taleb T. Dynamic resource allocation for URLLC and eMBB in MEC-NFV 5G networks. Comput Netw. 2025;260(3):111127. doi:10.1016/j.comnet.2025.111127.
29. Filho WLR. The role of zero trust architecture in modern cybersecurity: integration with IAM and emerging technologies. Braz J Develop. 2025;11(1):e76836. doi:10.34117/bjdv11n1-060.
30. Gambo ML, Almulhem A. Zero trust architecture: a systematic literature review. arXiv:2503.11659. 2025.
31. Hassan YG, Collins A, Babatunde GO, Alabi AA, Mustapha SD. Blockchain and zero-trust identity management system for smart cities and IoT networks. Int J Multidiscip Res Growth Eval. 2023;4(1):704–9. doi:10.54660/.ijmrge.2023.4.1.704-709.
32. Chawda Y, Parmar M. Toward intelligent data access control: a dual-layered zero trust and blockchain-based data access model. Sci Pract Cyber Secur J. 2023;9(1):1–9.
33. Raghu N, Kannanugo N, Trupti VN, Ojashwini RN, Kiran B, Deepthi M. Real-time fraud detection in cryptocurrencies: leveraging AI and blockchain. In: Applications of blockchain and artificial intelligence in finance and governance. Boca Raton, FL, USA: CRC Press; 2025. p. 28–66.
34. Bello HO, Idemudia C, Iyelolu TV. Integrating machine learning and blockchain: conceptual frameworks for real-time fraud detection and prevention. World J Adv Res Rev. 2024;23(1):56–68. doi:10.30574/wjarr.2024.23.1.1985.
35. Khan BUI, Goh KW, Khan AR, Zuhairi MF, Chaimanee M. Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. Processes. 2024;12(9):1825. doi:10.3390/pr12091825.
36. Li Y, Shen J, Ji S, Lai YH. Blockchain-based data integrity verification scheme in AIoT cloud-edge computing environment. IEEE Trans Eng Manag. 2024;71(2014):12556–65. doi:10.1109/TEM.2023.3262678.
37. Reddy RRP. Enhancing endpoint security through collaborative zero-trust integration: a multi-agent approach. Int J Comput Trends Technol. 2024;72(8):86–90. doi:10.14445/22312803/ijctt-v72i8p112.
38. Tiwari S, Sarma W, Srivastava A. Integrating artificial intelligence with zero trust architecture: enhancing adaptive security in modern cyber threat landscape. Int J Res Anal Rev. 2022;9:712–28.
39. Chandan A, Potdar V, John M. Systematic literature review of blockchain technology's technical challenges: a tertiary study. Information. 2024;15(8):475. doi:10.3390/info15080475.
40. Rahman Z, Yi X, Mehedi ST, Islam R, Kelarev A. Blockchain applicability for the Internet of Things: performance and scalability challenges and solutions. Electronics. 2022;11(9):1416. doi:10.3390/electronics11091416.
41. Kumar R, Sharma A. Edge AI: a review of machine learning models for resource-constrained devices. Artif Intell Mach Learn Rev. 2024;5(3):1–11.

42. Mahmoud MA, Gurunathan M, Ramli R, Babatunde KA, Faisal FH. Review and development of a scalable lightweight blockchain integrated model (LightBlock) for IoT applications. Electronics. 2023;12(4):1025. doi:10.3390/electronics12041025.

43. Özkan C, Şahin S. AI applications in real-time edge processing: leveraging artificial intelligence for enhanced efficiency, low-latency decision making, and scalability in distributed systems. Int J Mach Intell Smart Appl. 2024;14(8):1–19.

44. Lee E, Seo YD, Oh SR, Kim YG. A survey on standards for interoperability and security in the Internet of Things. IEEE Commun Surv Tutor. 2021;23(2):1020–47. doi:10.1109/COMST.2021.3067354.

45. Albouq SS, Sen AAA, Almashf N, Yamin M, Alshanqiti A, Bahbouh NM. A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access. 2022;10:36416–28. doi:10.1109/ACCESS.2022.3162219.

46. Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero trust architecture (ZTA): a comprehensive survey. IEEE Access. 2022;10(3):57143–79. doi:10.1109/ACCESS.2022.3174679.

47. Otoum Y. AI-based intrusion detection systems to secure Internet of Things (IoT) [dissertation]. Ottawa, ON, Canada: Université d'Ottawa/University of Ottawa; 2022.

48. Liu B, Yu XL, Chen S, Xu X, Zhu L. Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services (ICWS); 2017 Jun 25–30; Honolulu, HI, USA. p. 468–75. doi:10.1109/ICWS.2017.54.

49. Shen M, Liu H, Zhu L, Xu K, Yu H, Du X, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J Sel Areas Commun. 2020;38(5):942–54. doi:10.1109/JSAC.2020.2980916.

50. Rashid A, Siddique MJ. Smart contracts integration between blockchain and Internet of Things: opportunities and challenges. In: 2nd International Conference on Advancements in Computational Sciences (ICACS); 2019 Feb 18–20; Lahore, Pakistan. p. 1–9.

51. Tian Z, Shi W, Wang Y, Zhu C, Du X, Su S, et al. Real-time lateral movement detection based on evidence reasoning network for edge computing environment. IEEE Trans Ind Inform. 2019;15(7):4285–94. doi:10.1109/TII.2019.2907754.

52. Reusch N, Pop P. Scheduling real-time applications on edge computing platforms with remote attestation for security. In: 2021 IEEE/ACM Symposium on Edge Computing (SEC); 2021 Dec 14–17; San Jose, CA, USA. p. 403–8.

53. Khan IU, Khan ZA, Ahmad M, Khan AH, Muahmmad F, Imran A, et al. Machine learning techniques for permission-based malware detection in Android applications. In: 2023 9th International Conference on Information Technology Trends (ITT); 2023 May 24–25; Dubai, United Arab Emirates. p. 7–13. doi:10.1109/ITT59889.2023.10184260.

54. Alnahdi A, Toka L. A survey on integrating edge computing with AI and blockchain in maritime domain, aerial systems, IoT, and industry 4.0. IEEE Access. 2024;12:28684–709. doi:10.1109/access.2024.3465274.

55. Pereira F, Correia R, Pinho P, Lopes SI, Carvalho NB. Challenges in resource-constrained IoT devices: energy and communication as critical success factors for future IoT deployment. Sensors. 2020;20(22):6420. doi:10.3390/s20226420.

56. Wylde A. Zero trust: never trust, always verify. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA); 2021 Jun 14–18; Dublin, Ireland. p. 1–4. doi:10.1109/cybersa52016.2021.9478244.

57. Adat V, Gupta BB. Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommun Syst. 2018;67(3):423–41. doi:10.1007/s11235-017-0345-9.

58. Rathore S, Kwon BW, Park JH. BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network. J Netw Comput Appl. 2019;143(4):167–77. doi:10.1016/j.jnca.2019.06.019.

59. Khan FM, Rahman T, Zeb A, Ali Haider Z, Khan IU, Bilal H, et al. Vehicular network security through optimized deep learning model with feature selection techniques. IECE Trans Sens Commun Control. 2024;1(2):136–53. doi:10.62762/tscc.2024.626147.

60. Ameer S, Praharaj L, Sandhu R, Bhatt S, Gupta M. ZTA-IoT: a novel architecture for zero-trust in IoT systems and an ensuing usage control model. ACM Trans Priv Secur. 2024;27(3):1–36. doi:10.1145/3671147.

61. Arora S, Tewari A. Zero trust architecture in IAM with AI integration. Int J Sci Res Arch. 2023;8(2):737–45. doi:10.30574/ijsra.2023.8.2.0163.
62. Ayeswarya S, Norman J. A survey on different continuous authentication systems. Int J Biom. 2019;11(1):67–99. doi:10.1504/ijbm.2019.10016811.
63. Ghadge N. Use of blockchain technology to strengthen identity and access management (IAM). Int J Inf Technol. 2024;1(3):1–17.
64. Rahman S, Perumath N. Implementing zero trust management in IoT environment—challenges and solutions: scoping review [master's thesis]. Stockholm, Sweden: Stockholm University; 2025.
65. Nie S, Ren J, Wu R, Han P, Han Z, Wan W. Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. Sensors. 2025;25(2):550. doi:10.3390/s25020550.
66. Kim H, Shon T. Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. J Supercomput. 2022;78(11):13554–63. doi:10.1007/s11227-022-04408-4.
67. Ali Haider MH, Fayaz M, Zhang Y, Noureen H, Ali Haider Z, Khan FM, et al. Enhancing authentication security in Internet of vehicles: a blockchain-driven approach for trustworthy communication. ICCK Trans Adv Comput Syst. 2024;1(1):48–62. doi:10.62762/tacs.2024.835144.
68. Arifeen M, Petrovski A, Petrovski S. Automated microsegmentation for lateral movement prevention in industrial Internet of Things (IIoT). In: 2021 14th International Conference on Security of Information and Networks (SIN); 2021 Dec 15–17; Edinburgh, UK. p. 1–6. doi:10.1109/SIN54109.2021.9699232.
69. Thapa M. Mitigating threats in IoT network using device isolation [master's thesis]. Espoo, Finland: Aalto University; 2018.
70. Mesbah W. Malware containment via firewall placement in large scale wireless IoT networks. TechRxiv. 2024. doi:10.36227/techrxiv.172710236.67831507/v1.
71. Batool H, Masood A. Enterprise mobile device management requirements and features. In: IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); 2020 Jul 6–9; Toronto, ON, Canada. p. 109–14. doi:10.1109/INFOCOMWKSHPS50562.2020.9162763.
72. Wang D, Ming J, Chen T, Zhang X, Wang C. Cracking IoT device user account via brute-force attack to SMS authentication code. In: Proceedings of the First Workshop on Radical and Experiential Security; 2018 Jun 4; Incheon, Republic of Korea. p. 57–60. doi:10.1145/3203422.3203426.
73. Jing X, Liu Z, Li S, Qiao B, Tan G. A cloud-user behavior assessment based dynamic access control model. Int J Syst Assur Eng Manag. 2017;8(3):1966–75. doi:10.1007/s13198-015-0411-1.
74. Ozdayi MS, Kantarcioglu M, Malin B. Leveraging blockchain for immutable logging and querying across multiple sites. BMC Med Genomics. 2020;13(Suppl 7):82. doi:10.1186/s12920-020-0721-2.
75. Tian G, Wei J, Kutyłowski M, Susilo W, Huang X, Chen X. VRBC: a verifiable redactable blockchain with efficient query and integrity auditing. IEEE Trans Comput. 2023;72(7):1928–42. doi:10.1109/TC.2022.3230900.
76. Aanandaram V, Deepalakshmi P. Blockchain-based digital identity for secure authentication of IoT devices in 5G networks. In: Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS); 2024 Mar 14–16; Virudhunagar, India; 2024. p. 1–6. doi:10.1109/INCOS59338.2024.10527739.
77. Ofili BT, Erhabor EO, Obasuyi OT. Enhancing federal cloud security with AI: zero trust, threat intelligence and CISA compliance. World J Adv Res Rev. 2025;25(2):2377–400. doi:10.30574/wjarr.2025.25.2.0620.
78. He D, Chan S, Guizani M. Security in the Internet of Things supported by mobile edge computing. IEEE Commun Mag. 2018;56(8):56–61. doi:10.1109/MCOM.2018.1701132.
79. Rupanetti D, Kaabouch N. Combining edge computing-assisted Internet of Things security with artificial intelligence: applications, challenges, and opportunities. Appl Sci. 2024;14(16):7104. doi:10.3390/app14167104.
80. Oshiro DM. Zero trust architecture implementation for the marine corps tactical cloud [master's thesis]. Monterey, CA, USA: Naval Postgraduate School; 2023.
81. Khan IU, Zeb A, Rahman T, Khan FM, Ali Haider Z, Bilal H. ViTDroid and hybrid models for effective Android and IoT malware detection. ICCK Trans Adv Comput Syst. 2024;1(1):32–47. doi:10.62762/tacs.2024.521915.
82. Khan MJ. Zero trust architecture: redefining network security paradigms in the digital age. World J Adv Res Rev. 2023;19(3):105–16. doi:10.30574/wjarr.2023.19.3.1785.

83. Patel R, Müller K, Kvirkvelia G, Smith J, Wilson E. Zero trust security architecture raises the future paradigm in information systems. Inform Digit Insight J. 2024;1(1):24–34.
84. Williams P, Dutta IK, Daoud H, Bayoumi M. A survey on security in Internet of Things with a focus on the impact of emerging technologies. Internet Things. 2022;19(5):100564. doi:10.1016/j.iot.2022.100564.
85. Vivek Menon U, Babu Kumaravelu V, Vinoth Kumar C, Rammohan A, Chinnadurai S, Venkatesan R, et al. AI-powered IoT: a survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. IEEE Access. 2025;13(2):50296–339. doi:10.1109/ACCESS.2025.3551750.
86. Belgaum MR, Alansari Z, Musa S, Mansoor Alam M, Mazliham MS. Role of artificial intelligence in cloud computing, IoT and SDN: reliability and scalability issues. Int J Electr Comput Eng. 2021;11(5):4458. doi:10.11591/ijece.v11i5.pp4458-4470.
87. Misra S, Mukherjee A, Roy A, Saurabh N, Rahulamathavan Y, Rajarajan M. Blockchain at the edge: performance of resource-constrained IoT networks. IEEE Trans Parallel Distrib Syst. 2021;32(1):174–83. doi:10.1109/TPDS.2020.3013892.
88. Khan B, Khan K, Khan FM, Noureen H, Ali A, Shah M. Comparing fine-tuned RoBERTa with traditional machine learning models for stance detection in political tweets. ICCK Trans Adv Comput Syst. 2024;1(2):78–96. doi:10.62762/tacs.2024.928069.
89. Brudy F, Holz C, Rädle R, Wu CJ, Houben S, Klokmose CN, et al. Cross-device taxonomy: survey, opportunities and challenges of interactions spanning across multiple devices. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems; 2019 May 4–9; Glasgow, UK. p. 1–28. doi:10.1145/3290605.3300792.
90. Alasbali N, Azzuhri SRB, Salleh RB, Kiah MLM, Ahmad Shariffuddin AAAS, bin Nik Mohd Kamel NMI, et al. Rules of smart IoT networks within smart cities towards blockchain standardization. Mob Inf Syst. 2022;2022(1):9109300. doi:10.1155/2022/9109300.
91. Domínguez-Bolaño T, Barral V, Escudero CJ, García-Naya JA. An IoT system for a smart campus: challenges and solutions illustrated over several real-world use cases. Internet Things. 2024;25(10285):101099. doi:10.1016/j.iot.2024.101099.
92. Bello O, Zeadally S, Badra M. Network layer inter-operation of device-to-device communication technologies in Internet of Things (IoT). Ad Hoc Netw. 2017;57(3):52–62. doi:10.1016/j.adhoc.2016.06.010.
93. Baccour E, Mhaisen N, Abdellatif AA, Erbad A, Mohamed A, Hamdi M, et al. Pervasive AI for IoT applications: a survey on resource-efficient distributed artificial intelligence. IEEE Commun Surv Tutor. 2022;24(4):2366–418. doi:10.1109/COMST.2022.3200740.
94. Villegas-Ch W, Gutierrez R, Maldonado Navarro A, Mera-Navarrete A. Lightweight blockchain for authentication and authorization in resource-constrained IoT networks. IEEE Access. 2025;13(4):48047–67. doi:10.1109/ACCESS.2025.3551261.
95. Qin M, Chen L, Zhao N, Chen Y, Yu FR, Wei G. Power-constrained edge computing with maximum processing capacity for IoT networks. IEEE Internet Things J. 2019;6(3):4330–43. doi:10.1109/JIOT.2018.2875218.
96. Villegas-Ch W, García-Ortiz J, Sánchez-Viteri S. Toward intelligent monitoring in IoT: aI applications for real-time analysis and prediction. IEEE Access. 2024;12(4):40368–86. doi:10.1109/ACCESS.2024.3376707.
97. Qi J, Chen X, Jiang Y, Jiang J, Shen T, Zhao S, et al. Bidl: a high-throughput, low-latency permissioned blockchain framework for datacenter networks. In: Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles; 2021 Oct 26–29; Virtual. p. 18–34. doi:10.1145/3477132.3483574.
98. Sonmez C, Ozgovde A, Ersoy C. EdgeCloudSim: an environment for performance evaluation of edge computing systems. Trans Emerg Telecommun Technol. 2018;29(11):e3493. doi:10.1002/ett.3493.
99. Bommana SR, Veeramachaneni S, Ahmed SE, Srinivas MB. Addressing adversarial attacks in IoT using deep learning AI models. IEEE Access. 2025;13:50437–49. doi:10.1109/ACCESS.2025.3552529.
100. Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. Security and privacy in IoT using machine learning and blockchain: threats and countermeasures. ACM Comput Surv. 2020;53(6):1–37. doi:10.1145/3417987.
101. Ali S. Securing edge computing with AI: intelligent threat detection for decentralized systems; 2024 [cited 2025 Jan 1]. Available from: https://www.researchgate.net/publication/388525892.

102. Zawish M, Ashraf N, Ansari RI, Davy S. Energy-aware AI-driven framework for edge-computing-based IoT applications. IEEE Internet Things J. 2023;10(6):5013–23. doi:10.1109/JIOT.2022.3219202.

103. Zhao J, Qu X, Wu Y, Fowler M, Burke AF. Artificial intelligence-driven real-world battery diagnostics. Energy AI. 2024;18(6464):100419. doi:10.1016/j.egyai.2024.100419.

104. Bada AO, Damianou A, Angelopoulos CM, Katos V. Towards a green blockchain: a review of consensus mechanisms and their energy consumption. In: 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS); 2021 Jul 14–16; Pafos, Cyprus. p. 503–11. doi:10.1109/dcoss52077.2021.00083.

105. Silva P, Costan A, Antoniu G. Investigating edge vs. cloud computing trade-offs for stream processing. In: 2019 IEEE International Conference on Big Data (Big Data); 2019 Dec 9–12; Los Angeles, CA, USA. p. 469–74. doi:10.1109/BigData47090.2019.9006139.

106. Joshi H. Emerging technologies driving zero trust maturity across industries. IEEE Open J Comput Soc. 2025;6(2):25–36. doi:10.1109/OJCS.2024.3505056.

107. DeMedeiros K, Hendawi A, Alvarez M. A survey of AI-based anomaly detection in IoT and sensor networks. Sensors. 2023;23(3):1352. doi:10.3390/s23031352.

108. Adeniran IA, Efunniyi CP, Osundare OS, Abhulimen AO. Enhancing security and risk management with predictive analytics: a proactive approach. Int J Manag Entrep Res. 2024;6(8):32–40. doi:10.56781/ijsret.2024.4.1.0021.

109. Kinyua J, Awuah L. AI/ML in security orchestration, automation and response: future research directions. Intell Autom Soft Comput. 2021;28(2):527–45. doi:10.32604/iasc.2021.016240.

110. Ramírez-Gordillo T, Maciá-Lillo A, Pujol FA, García-D'Urso N, Azorín-López J, Mora H. Decentralized identity management for Internet of Things (IoT) devices using IOTA blockchain technology. Fut Internet. 2025;17(1):49. doi:10.3390/fi17010049.

111. Marchioro NG, Velegrakis Y, Anantharaj V, Foster I, Fiore SL. Trustworthy provenance for big data science: a modular architecture leveraging blockchain in federated settings. arXiv:2505.24675. 2025.

112. Amato F, Cozzolino G, Moscato F, Moscato V, Xhafa F. A model for verification and validation of law compliance of smart contracts in IoT environment. IEEE Trans Ind Inform. 2021;17(11):7752–9. doi:10.1109/TII.2021.3057595.

113. Huang Y, Lu Y, Wang F, Fan X, Liu J, Leung VCM. An edge computing framework for real-time monitoring in smart grid. In: 2018 IEEE International Conference on Industrial Internet (ICII); 2018 Oct 21–23; Seattle, WA, USA. p. 99–108. doi:10.1109/ICII.2018.00019.

114. Veeramachaneni V. Edge computing: architecture, applications, and future challenges in a decentralized era. Recent Trends Comput Graph Multimed Technol. 2025;7(1):8–23.

115. Al-Hasnawi A, Carr SM, Gupta A. Fog-based local and remote policy enforcement for preserving data privacy in the Internet of Things. Internet Things. 2019;7(5):100069. doi:10.1016/j.iot.2019.100069.

116. Rane N, Choudhary S, Rane J. Blockchain and artificial intelligence (AI) integration for revolutionizing security and transparency in finance. SSRN J. 2023;4644253. doi:10.2139/ssrn.4644253.

117. Alrubei SM, Ball E, Rigelsford JM. A secure blockchain platform for supporting AI-enabled IoT applications at the edge layer. IEEE Access. 2022;10(14):18583–95. doi:10.1109/ACCESS.2022.3151370.

118. Barach J. Towards zero trust security in SDN: a multi-layered defense strategy. In: Proceedings of the 26th International Conference on Distributed Computing and Networking; 2025 Jan 4–7; Hyderabad, India. p. 331–9. doi:10.1145/3700838.3703671.

119. Khalil U, Malik OA, Uddin M, Chen CL. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. Sensors. 2022;22(14):5168. doi:10.3390/s22145168.

120. Gowda D, Chaithra SM, Gujar SS, Firoz Shaikh S, Ingole BS, Sudhakar Reddy N. Scalable AI solutions for IoT-based healthcare systems using cloud platforms. In: 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); 2024 Oct 3–5; Kirtipur, Nepal. p. 156–62. doi:10.1109/I-SMAC61858.2024.10714810.

121. Oualhaj OA, Mohamed A, Guizani M, Erbad A. Blockchain based decentralized trust management framework. In: 2020 International Wireless Communications and Mobile Computing (IWCMC); 2020 Jun 15–19; Limassol, Cyprus. p. 2210–5. doi:10.1109/iwcmc48107.2020.9148247.

122. Kozik R, Choraś M, Ficco M, Palmieri F. A scalable distributed machine learning approach for attack detection in edge computing environments. J Parallel Distrib Comput. 2018;119(2):18–26. doi:10.1016/j.jpdc.2018.03.006.
123. Tanikonda A, Pandey BK, Peddinti SR, Katragadda SR. Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. J Sci Technol. 2022;3(1):196–217. doi:10.2139/ssrn.5102358.
124. Igonor OS, Amin MB, Garg S. The application of blockchain technology in the field of digital forensics: a literature review. Blockchains. 2025;3(1):5. doi:10.3390/blockchains3010005.
125. Abouaomar A, Cherkaoui S, Mlika Z, Kobbane A. Resource provisioning in edge computing for latency-sensitive applications. IEEE Internet Things J. 2021;8(14):11088–99. doi:10.1109/JIOT.2021.3052082.
126. Liu HI, Galindo M, Xie H, Wong LK, Shuai HH, Li YH, et al. Lightweight deep learning for resource-constrained environments: a survey. ACM Comput Surv. 2024;56(10):1–42. doi:10.1145/3657282.
127. Al Ghamdi MA. An optimized and secure energy-efficient blockchain-based framework in IoT. IEEE Access. 2022;10(3):133682–97. doi:10.1109/ACCESS.2022.3230985.
128. Elgendy IA, Zhang WZ, Zeng Y, He H, Tian YC, Yang Y. Efficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile IoT networks. IEEE Trans Netw Serv Manag. 2020;17(4):2410–22. doi:10.1109/TNSM.2020.3020249.
129. Otoum S, Kantarci B, Mouftah H. A comparative study of AI-based intrusion detection techniques in critical infrastructures. ACM Trans Internet Technol. 2021;21(4):1–22. doi:10.1145/3406093.
130. Kravitz DW. Transaction immutability and reputation traceability: blockchain as a platform for access controlled IoT and human interactivity. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST); 2017 Aug 28–30; Calgary, AB, Canada. p. 3–309. doi:10.1109/PST.2017.00012.
131. Tsigkanos C, Bersani MM, Frangoudis PA, Dustdar S. Edge-based runtime verification for the Internet of Things. IEEE Trans Serv Comput. 2022;15(5):2713–27. doi:10.1109/TSC.2021.3074956.
132. Babu CS. Adaptive AI for dynamic cybersecurity systems: enhancing protection in a rapidly evolving digital landscape. In: Principles and applications of adaptive artificial intelligence. New York, NY, USA: IGI Global; 2024. p. 52–72.
133. Jabbar R, Kharbeche M, Al-Khalifa K, Krichen M, Barkaoui K. Blockchain for the Internet of Vehicles: a decentralized IoT solution for vehicles communication using ethereum. Sensors. 2020;20(14):3928. doi:10.3390/s20143928.
134. Solozabal R, Sanchoyerto A, Atxutegi E, Blanco B, Fajardo JO, Liberal F. Exploitation of mobile edge computing in 5G distributed mission-critical push-to-talk service deployment. IEEE Access. 2018;6:37665–75. doi:10.1109/ACCESS.2018.2849200.
135. Alevizos L, Ta VT, Hashem Eiza M. Augmenting zero trust architecture to endpoints using blockchain: a state-of-the-art review. Secur Priv. 2022;5(1):e191. doi:10.1002/spy2.191.
136. Schneller L, Porter CN, Wakefield A. Implementing converged security risk management: drivers, barriers, and facilitators. Secur J. 2023;36(2):333–49. doi:10.1057/s41284-022-00341-6.
137. Manda JK. AI-powered threat intelligence platforms in telecom: leveraging AI for real-time threat detection and intelligence gathering in telecom network security operations. SSRN J. 2024;5003638. doi:10.2139/ssrn.5003638.
138. Orrù D, Pinna A, Tonelli R. Low-cost tamper-proof IoT devices to improve data origin verification and privacy in blockchain-based energy consumption records. CEUR Workshop Proc. 2024;3791:1–11.
139. Ghosh S, Mukherjee A, Ghosh SK, Buyya R. Mobi-IoST: mobility-aware cloud-fog-edge-IoT collaborative framework for time-critical applications. IEEE Trans Netw Sci Eng. 2020;7(4):2271–85. doi:10.1109/TNSE.2019.2941754.
140. Jouhari M, Saeed N, Alouini MS, Amhoud EM. A survey on scalable LoRaWAN for massive IoT: recent advances, potentials, and challenges. IEEE Commun Surv Tutor. 2023;25(3):1841–76. doi:10.1109/COMST.2023.3274934.
141. Canavese D, Mannella L, Regano L, Basile C. Security at the edge for resource-limited IoT devices. Sensors. 2024;24(2):590. doi:10.3390/s24020590.
142. Noura M, Atiquzzaman M, Gaedke M. Interoperability in Internet of Things: taxonomies and open challenges. Mob Netw Appl. 2019;24(3):796–809. doi:10.1007/s11036-018-1089-9.

143. Latif SA, Wen FBX, Iwendi C, Wang LF, Mohsin SM, Han Z, et al. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Comput Commun. 2022;181(6):274–83. doi:10.1016/j.comcom.2021.09.029.

144. Ismail S, Nouman M, Dawoud DW, Reza H. Towards a lightweight security framework using blockchain and machine learning. Blockchain Res Appl. 2024;5(1):100174. doi:10.1016/j.bcra.2023.100174.

145. Bröring A, Schmid S, Schindhelm CK, Khelil A, Käbisch S, Kramer D, et al. Enabling IoT ecosystems through platform interoperability. IEEE Softw. 2017;34(1):54–61. doi:10.1109/MS.2017.2.

146. Ressi D, Romanello R, Piazza C, Rossi S. AI-enhanced blockchain technology: a review of advancements and opportunities. J Netw Comput Appl. 2024;225(21):103858. doi:10.1016/j.jnca.2024.103858.

147. Santoso A, Surya Y. Maximizing decision efficiency with edge-based AI systems: advanced strategies for real-time processing, scalability, and autonomous intelligence in distributed environments. Q J Emerg Technol Innov. 2024;9(2):104–32.

148. Chaganti KC. Advancing AI-driven threat detection in IoT ecosystems: addressing scalability, resource constraints, and real-time adaptability. TechRxiv. 2024. doi:10.36227/techrxiv.173738307.73168902/v1.

149. Rane N, Choudhary S, Rane J. Leading-edge artificial intelligence (AI), machine learning (ML), blockchain, and Internet of Things (IoT) technologies for enhanced wastewater treatment systems. SSRN J. 2023;4641557. doi:10.2139/ssrn.4641557.

150. Knapp ED. Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Amsterdam, The Netherlands: Elsevier; 2024.