future internet

Review

A Survey on Cybersecurity in IoT

Elias Dritsas * and Maria Trigka

Industrial Systems Institute (ISI), Athena Research and Innovation Center, 26504 Patras, Greece; trigka@isi.gr
* Correspondence: dritsas@isi.gr

Abstract: The proliferation of the Internet of Things (IoT) has transformed the digital landscape, enabling a vast array of interconnected devices to communicate and share data seamlessly. However, the rapid expansion of IoT networks has also introduced significant cybersecurity challenges. This paper presents a comprehensive survey of cybersecurity in the IoT ecosystem, examining the current state of research, identifying critical security vulnerabilities, and exploring advanced strategies for mitigating threats. The survey covers various facets of IoT security, including device authentication, data integrity, privacy, network security, and the emerging role of artificial intelligence (AI) in bolstering cybersecurity defenses. By synthesizing existing research and highlighting ongoing challenges, this survey aims to provide a holistic understanding of IoT cybersecurity and to guide future research endeavors.

Keywords: Internet of Things; cybersecurity; network security; data privacy; blockchain security

check for updates

Academic Editors: Christos Tryfonopoulos and Nicholas Kolokotronis

Received: 25 August 2024
Revised: 6 January 2025
Accepted: 9 January 2025
Published: 11 January 2025

Citation: Dritsas, E.; Trigka, M. A Survey on Cybersecurity in IoT. *Future Internet* **2025**, *17*, 30. https://doi.org/10.3390/fi17010030

1. Introduction

The IoT has emerged as a transformative force in modern technology, driving innovation across various sectors by enabling seamless connectivity among a vast array of devices, sensors, and systems. From industrial automation to smart healthcare, IoT is reshaping industries by facilitating real-time data collection, analysis, and decision-making, leading to enhanced operational efficiency, reduced costs, and the creation of new business models. However, the very characteristics that make IoT so powerful—its distributed nature, the heterogeneity of devices, and pervasive connectivity—also introduce unprecedented cybersecurity challenges [1–3].

Unlike traditional information technology (IT) systems, IoT networks consist of diverse devices, ranging from powerful servers to tiny, resource-constrained sensors, all of which must operate harmoniously in often untrusted environments. This heterogeneity presents unique security challenges, as each device type may require different protection mechanisms. Moreover, many IoT devices are designed with minimal security features due to cost constraints or limited computational resources, making them susceptible to various cyber threats. The consequences of such vulnerabilities can be severe, ranging from the compromise of individual devices to large-scale disruptions in critical infrastructure systems, potentially leading to catastrophic outcomes in sectors such as healthcare, energy, and transportation [4–6].

Furthermore, the IoT ecosystem is characterized by its extensive use of wireless communication, which, while enabling flexibility and scalability, also exposes networks to a wider range of attack vectors. Wireless communication channels are inherently less secure than wired ones, making them more vulnerable to eavesdropping, man-in-the-middle attacks, and jamming. Additionally, the dynamic nature of IoT environments, where devices frequently join and leave the network, further complicates the implementation of traditional security protocols, which are often designed for static, well-defined network architectures [7–9].

Another critical aspect of IoT security is the data it generates and processes. IoT devices continuously collect vast amounts of data, much of which are sensitive or private. The protection of these data throughout its lifecycle—from collection and transmission to storage and processing—is paramount. However, ensuring data confidentiality, integrity, and availability in IoT systems is challenging due to the decentralized nature of data storage and the reliance on third-party cloud services for data processing. Moreover, IoT systems often involve multiple stakeholders, each with different security requirements and risk tolerances, complicating the development of unified security policies [10–12].

The rapid evolution of IoT technology has outpaced the development of comprehensive security frameworks, resulting in a landscape where security considerations are often an afterthought rather than a foundational design principle. This oversight has led to the proliferation of insecure devices and networks, which are now being exploited by attackers for various malicious purposes, including data theft, unauthorized surveillance, and the orchestration of large-scale distributed denial-of-service (DDoS) attacks [13–15].

In response to these challenges, the field of IoT cybersecurity has seen a surge in research efforts aimed at developing innovative solutions that address the unique security needs of IoT environments. These efforts include the design of lightweight cryptographic algorithms tailored for resource-constrained devices, the development of decentralized security models such as blockchain, and the application of AI and machine learning (ML) to enhance threat detection and response capabilities [16,17].

The present survey distinguishes itself by addressing the cybersecurity challenges in IoT through a more comprehensive and integrative approach compared to the surveys summarized in Table 1. Unlike prior works that focus narrowly on specific aspects such as blockchain, ML applications, or industry-specific IoT environments, this survey provides a broader scope by synthesizing diverse cybersecurity dimensions, including device authentication, data integrity, privacy, network security, and the role of AI in enhancing security. Furthermore, it delves into emerging technologies and methodologies, such as federated learning, post-quantum cryptography, and decentralized identity management systems, which are only briefly touched upon or overlooked in existing studies. By offering an extensive analysis of both technical and operational challenges, this work serves as an essential resource for developing scalable, adaptive, and future-proof IoT security solutions. In conclusion, this submission contributes to the field of IoT cybersecurity in several significant ways:

- It provides a comprehensive overview of the unique cybersecurity challenges specific to IoT environments.
- It examines advanced strategies for IoT device authentication, data integrity, and privacy protection.
- It analyzes the security implications of various IoT communication protocols and network architectures.
- It explores the application of AI and ML in enhancing IoT cybersecurity measures.
- It identifies key areas for future research to address ongoing and emerging IoT security challenges.

The remaining paper is illustrated in Figure 1 and structured as follows. Section 2 notes the importance of device authentication and identity management. Next, Section 3 analyzes the challenges of data integrity and privacy in the IoT. Section 4 refers to network security and communication protocols. Moreover, Section 5 outlines the integration of AI and ML into IoT security. Section 6 discusses challenges and future directions. Finally, Section 7 summarizes the findings of this study.

Table 1. Descriptive summary of related surveys on cybersecurity in IoT.

Survey	Description
[18]	Overview of techniques and elements to achieve cybersecurity in blockchain-based systems. Includes lessons learned from analyzing academic papers and industrial applications. Highlights gaps and research opportunities.
[19]	Examines IoT cybersecurity frameworks, emphasizing communication protocols, cybersecurity challenges, and intrusion detection systems (IDSs). Presents a validated IoT cybersecurity framework and discusses its role in protecting data and systems.
[20]	Investigates the application of ML in static analysis for IoT cybersecurity. Focuses on automating and intellectualizing the analysis of heterogeneous IoT systems and proposes an intelligent framework.
[21]	Explores learning-based methods for detecting cyberattacks in IoT systems. Discusses ML and deep learning (DL) approaches for various attacks, including DDoS, spoofing, and man-in-the-middle attacks.
[22]	Surveys classifications and mitigations of cyberattacks on IoT and industrial IoT devices, focusing on Industry 4.0. Highlights the integration of IoT with supervisory control and data acquisition systems in manufacturing industries and related vulnerabilities.
[23]	Discusses cybersecurity threats in IoT-enabled maritime industries, addressing risks in maritime operations, confidentiality, and integrity. Analyzes risk mitigation strategies and frameworks for safeguarding critical systems.
[24]	Notes cybersecurity certification schemes for IoT, analyzing challenges in developing frameworks that integrate risk assessment, security requirements, and governance. Provides insights into certification for emerging IoT scenarios.
[25]	Comprehensive survey of cybersecurity in IoT-based cloud computing, focusing on threats, cloud architecture, and the integration of AI and DL to enhance security. Covers challenges related to data, network, and application layers.

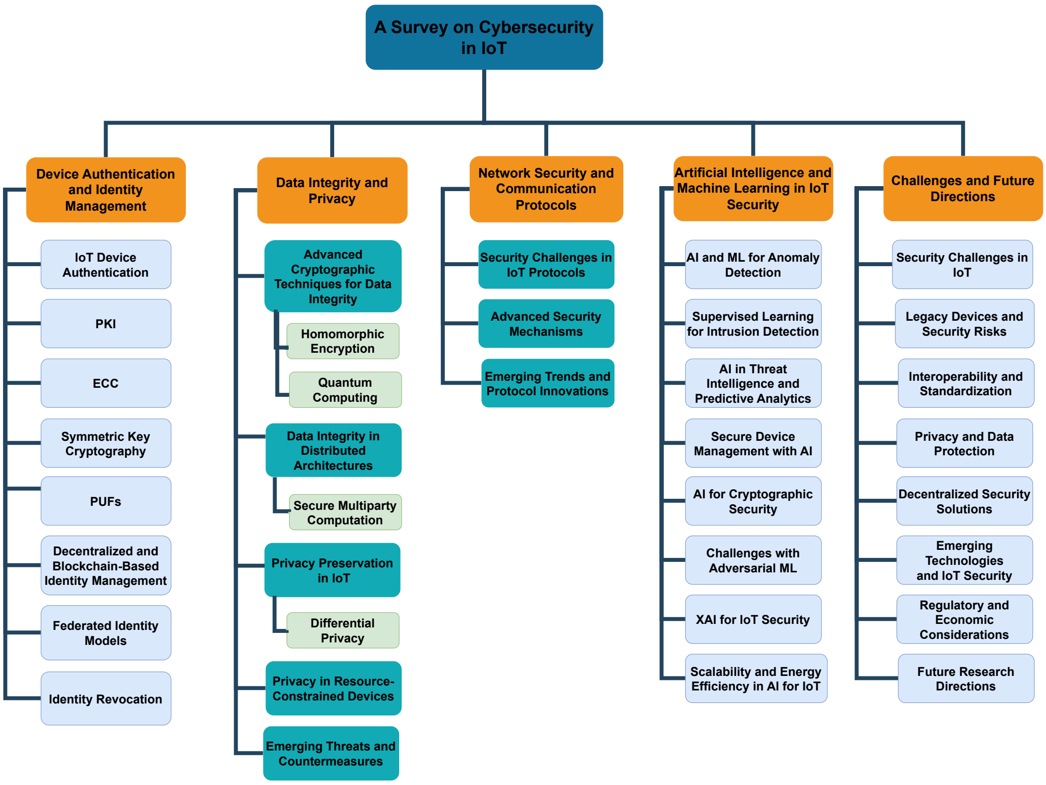
A Survey on Cybersecurity in IoT
Device Authentication and Identity Management
IoT Device Authentication
PKI
ECC
Symmetric Key Cryptography
PUFs
Decentralized and Blockchain-Based Identity Management
Federated Identity Models
Identity Revocation
Data Integrity and Privacy
Advanced Cryptographic Techniques for Data Integrity
Homomorphic Encryption
Quantum Computing
Data Integrity in Distributed Architectures
Secure Multiparty Computation
Privacy Preservation in IoT
Differential Privacy
Privacy in Resource-Constrained Devices
Emerging Threats and Countermeasures
Network Security and Communication Protocols
Security Challenges in IoT Protocols
Advanced Security Mechanisms
Emerging Trends and Protocol Innovations
Artificial Intelligence and Machine Learning in IoT Security
AI and ML for Anomaly Detection
Supervised Learning for Intrusion Detection
AI in Threat Intelligence and Predictive Analytics
Secure Device Management with AI
AI for Cryptographic Security
Challenges with Adversarial ML
XAI for IoT Security
Scalability and Energy Efficiency in AI for IoT
Challenges and Future Directions
Security Challenges in IoT
Legacy Devices and Security Risks
Interoperability and Standardization
Privacy and Data Protection
Decentralized Security Solutions
Emerging Technologies and IoT Security
Regulatory and Economic Considerations
Future Research Directions

Figure 1. Illustrative diagram of the survey's structure.

2. Device Authentication and Identity Management

Device authentication and identity management are critical components of the security architecture in the IoT ecosystem, serving as the first line of defense against unauthorized access and malicious activities [26]. Unlike traditional computing environments, IoT networks are characterized by a massive scale of heterogeneously connected devices, each with varying levels of computational power and security capabilities [27]. Diverse IoT scenarios impose varying requirements for authentication mechanisms. For instance, in healthcare IoT systems, device authentication must align with stringent privacy regulations like HIPAA to safeguard patient data. At the same time, industrial IoT environments demand real-time authentication to secure machinery and prevent unauthorized access. Similarly, smart city applications often require scalable identity management to handle dynamic additions and removals of devices such as connected traffic lights and environmental sensors [28–30].

One of the primary challenges in IoT device authentication is establishing trust in environments where devices are often deployed in untrusted or hostile settings [31]. Identity management in IoT extends beyond mere authentication to encompass the entire lifecycle of device identities, from provisioning and registration to revocation and decommissioning. One of the key challenges in IoT identity management is the dynamic nature of IoT environments, where devices frequently join and leave the network, often with little or no human intervention. This dynamic nature requires identity management systems that can operate autonomously, ensuring that devices are securely integrated into the network and that their identities can be managed without compromising security [32–36].

Traditional authentication mechanisms, such as Public Key Infrastructure (PKI), though widely used in conventional IT systems, are often impractical for IoT devices due to their resource-intensive nature [37–39]. IoT devices, particularly those with limited processing power and memory, cannot easily handle the computational overhead associated with PKI's key generation, encryption, and decryption processes. This limitation has spurred the development of alternative authentication methods specifically tailored to the constraints of IoT devices [40].

Elliptic Curve Cryptography (ECC) has emerged as a prominent solution for lightweight authentication in IoT [41,42]. ECC offers comparable security to traditional Rivest–Shamir–Adleman (RSA) encryption but with significantly smaller key sizes, leading to reduced computational and storage requirements [43]. The reduced key size translates into faster processing times and lower energy consumption, making ECC particularly well suited for IoT devices that operate on limited power sources [44]. However, the implementation of ECC in IoT environments requires the careful consideration of various factors such as key management, resistance to side-channel attacks, and the ability to scale across large networks [45].

In addition to ECC, symmetric key cryptography remains a popular choice for IoT authentication due to its efficiency in terms of both speed and energy consumption [46]. Protocols like the Advanced Encryption Standard (AES) are frequently employed for device authentication in IoT systems [47,48]. The AES, with key lengths of 128, 192, and 256 bits, is widely used for device authentication in IoT systems. A 128-bit key provides sufficient security against brute-force attacks while minimizing computational overhead, making it suitable for resource-constrained devices. Longer keys, such as 256-bit, offer enhanced security but increase processing requirements. The secure exchange of AES keys, often facilitated by the Diffie–Hellman or Elliptic Curve Diffie–Hellman protocols, can introduce vulnerabilities like susceptibility to man-in-the-middle attacks if not implemented correctly [49]. While AES ensures strong encryption and efficiency, its reliance on secure key management remains a limitation in large-scale IoT networks. However, the challenge with symmetric key cryptography lies in the secure distribution and management of keys, particularly in large-scale IoT deployments [50]. Secure key distribution protocols, such as the Diffie–Hellman key exchange, have been adapted for IoT but these still face challenges related to scalability and the potential for man-in-the-middle attacks during the key exchange process [51–53].

Beyond cryptographic techniques, physical unclonable functions (PUFs) have gained attention as a novel approach to device authentication in IoT [54,55]. PUFs exploit the inherent manufacturing variations in electronic circuits to generate unique, device-specific responses that can be used for authentication purposes. Since these responses are derived from the physical characteristics of the device, they are difficult to replicate or forge, providing a high level of security. PUF-based authentication is particularly appealing for IoT devices due to its low computational requirements and resistance to cloning attacks. PUFs generate unique responses based on inherent device variations, requiring minimal hardware operations like delay-based measurements. For example, ring oscillator PUFs consume a few hundred nanowatts of power and require only kilobytes of memory for challenge-response storage, making them suitable for resource-constrained IoT devices. These architectures are integrated into MCUs and FPGAs for lightweight authentication, with error-correction techniques ensuring reliability under environmental variations [56,57]. While PUF-based authentication is highly effective, deploying it at scale presents challenges, such as the need for standardized interfaces and protocols to integrate PUFs into diverse IoT ecosystems [58–60].

Decentralized identity management systems, leveraging blockchain and distributed ledger technologies (DLTs), have been proposed as a solution to the challenges of scalability and trust in IoT networks. By using blockchain, IoT devices can register their identities in a tamper-proof ledger that is distributed across the network. This approach provides several advantages, including the elimination of single points of failure and the ability to audit identity transactions transparently [61–63]. Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, can be utilized within blockchain-based identity systems to automate identity verification processes and enforce access control policies [64]. However, the integration of blockchain with IoT also raises issues related to the overhead of consensus mechanisms, the latency of blockchain transactions, and the energy consumption associated with maintaining a distributed ledger [65].

Another emerging trend in IoT identity management is the use of federated identity models, which allow IoT devices to share identity credentials across multiple domains or organizations. Federated identity management can simplify the process of integrating IoT devices into diverse and multi-stakeholder environments, such as smart cities or industrial IoT systems, by enabling devices to authenticate across different networks without needing to re-establish their identities. This model, however, requires robust trust frameworks and interoperability standards to ensure that identity information can be securely shared and managed across different domains [66–69].

Identity management also plays a crucial role in ensuring the secure decommissioning of IoT devices. When a device is retired or no longer trusted, its identity must be revoked to prevent it from being used as a vector for attacks. This process, known as identity revocation, must be carried out securely and efficiently to ensure that compromised or outdated devices do not remain a threat to the network [70]. Techniques such as certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP) have been adapted for IoT environments, but these solutions often face challenges related to the timely propagation of revocation information and the overhead of maintaining revocation infrastructure [71–74].

In summary, device authentication and identity management in IoT are complex, multifaceted challenges that require solutions tailored to the unique characteristics of

IoT environments. The development of lightweight, scalable, and secure authentication mechanisms is critical to ensuring the integrity and trustworthiness of IoT networks. As the IoT continues to evolve, the integration of emerging technologies such as PUFs, blockchain, and federated identity models will be essential in addressing the security challenges associated with the massive scale and heterogeneity of IoT devices [75–77]. A summary of the works that analyzed the aspects of device authentication and identity management in IoT is captured in Table 2.

Table 2. Summary of studies related to device authentication and identity management in IoT.

Topic	References	Summary
IoT Device Authentication	[26–36]	IoT device authentication and identity management are crucial for securing heterogeneous and dynamic IoT environments, addressing challenges such as trust, scalability, and compliance with specific requirements across diverse applications like healthcare, industrial, and smart city systems.
PKI	[37–40]	Focuses on the challenges and applications of PKI in IoT, including the computational overhead and the specific issues related to managing and distributing keys in IoT systems.
ECC	[41–45]	Examines ECC as an efficient cryptographic method for IoT devices, offering robust security with smaller key sizes that are suitable for devices with limited processing power.
Symmetric Key Cryptography	[46–53]	Discusses the use of symmetric key cryptography, particularly AES, for IoT authentication. It includes challenges related to secure key management, such as the adaptation of Diffie–Hellman key exchange, and addresses issues of scalability and security in large IoT networks.
PUFs	[54–60]	Covers PUFs as a hardware-based authentication method in IoT, leveraging unique physical characteristics of devices to provide secure and low-cost authentication solutions. These references discuss implementation challenges and potential applications in diverse IoT environments.
Decentralized and Blockchain-Based Identity Management	[61–65]	Discusses the role of blockchain and decentralized ledger technologies in managing IoT identities. These references highlight the potential of blockchain to provide secure, scalable, and tamper-proof identity management systems in IoT.
Federated Identity Models	[66–69]	Focuses on federated identity management in IoT, enabling devices to authenticate across multiple domains or networks without needing to re-establish their identities. The references discuss trust frameworks and the integration of federated identity systems in complex IoT environments.
Identity Revocation	[70–77]	These references address the processes for revoking the identities of IoT devices that are no longer trusted or operational. Methods like CRLs, OCSP, and blockchain-based revocation systems are discussed.

3. Data Integrity and Privacy

The challenges of data integrity and privacy in the IoT ecosystem are both profound and multifaceted, driven by the inherent characteristics of IoT networks, including heterogeneity, scale, and the frequent deployment of devices in untrusted or physically exposed environments. Ensuring data integrity within this context requires more than the application of conventional cryptographic techniques [78]; it demands a nuanced understanding of the specific threats and the development of solutions that are adaptable to the constraints and operational contexts of IoT devices [79].

3.1. Advanced Cryptographic Techniques for Data Integrity

Traditional methods such as hash functions [80–82], digital signatures [83–85], and message authentication codes (MACs) [86–88] are commonly utilized to ensure data integrity by verifying that data have not been altered. However, the resource constraints of IoT devices necessitate the adaptation of these techniques. Lightweight cryptographic algorithms like lightweight block ciphers (e.g., PRESENT, SPECK) and reduced-round hash functions have been specifically designed to operate within the limited computational capabilities of IoT devices [89–91]. Despite these adaptations, ensuring the integrity of data in transit and at rest remains challenging, particularly in environments where devices are exposed to physical tampering or where secure key management is problematic [92].

3.1.1. Homomorphic Encryption: Technical Depth and Mathematical Framework

Emerging research has also explored the use of homomorphic encryption, which is a cryptographic technique that allows computations to be carried out directly on encrypted data, producing results that, when decrypted, correspond to those obtained by performing the same operations on the plaintext. This property ensures that data remain confidential during computation, a critical requirement in secure data processing [93,94].

The mathematical foundation of homomorphic encryption can be described as follows. Let $\mathcal{E}$ be the encryption function, $\mathcal{D}$ the decryption function, and $\oplus$ and $\otimes$ the addition and multiplication operations, respectively. For a plaintext space $\mathcal{P}$ and ciphertext space $\mathcal{C}$, homomorphic encryption satisfies the following properties. For addition, the scheme ensures $\mathcal{E}(m_1) \oplus \mathcal{E}(m_2) = \mathcal{E}(m_1 + m_2)$, where $m_1, m_2 \in \mathcal{P}$. For multiplication, it guarantees $\mathcal{E}(m_1) \otimes \mathcal{E}(m_2) = \mathcal{E}(m_1 \cdot m_2)$. The decryption of the resulting ciphertext yields the corresponding operation performed on the plaintext, such that $\mathcal{D}(\mathcal{E}(m_1) \oplus \mathcal{E}(m_2)) = m_1 + m_2$ and $\mathcal{D}(\mathcal{E}(m_1) \otimes \mathcal{E}(m_2)) = m_1 \cdot m_2$.

Homomorphic encryption can be categorized into three main types based on the extent of operations it supports. Partially homomorphic encryption allows either addition or multiplication but not both. For example, RSA (Rivest–Shamir–Adleman) is a partially homomorphic encryption scheme supporting multiplication. In RSA, encryption is performed as $\mathcal{E}(m) = m^e \mod N$, where e is the public exponent and N is the modulus. For two plaintexts m_1 and m_2, the multiplicative homomorphic property ensures $\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) \mod N = (m_1 \cdot m_2)^e \mod N$, preserving the multiplication under encryption [95].

Somewhat homomorphic encryption extends partially homomorphic encryption by supporting a limited number of additions and multiplications. This approach is exemplified by schemes such as Brakerski–Gentry–Vaikuntanathan, which use polynomial rings and modular arithmetic to enable operations while controlling computational complexity [96].

Fully homomorphic encryption represents the most powerful form of homomorphic encryption, allowing an arbitrary number of additions and multiplications on ciphertexts. A foundational fully homomorphic encryption scheme, such as Gentry's construction, builds upon the learning-with-errors problem, a lattice-based cryptographic challenge believed to be resistant to quantum attacks. The key generation process involves selecting a secret key $\mathbf{s} \in \mathbb{Z}_q^n$, a public key matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, and a noise vector $\mathbf{e} \in \mathbb{Z}_q^m$. The ciphertext is formed as $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$.

Encryption in fully homomorphic encryption involves encoding the plaintext $m \in \{0, 1\}$ by adding it to the ciphertext modulus q scaled by $\lfloor q/2 \rfloor$. Thus, the ciphertext is expressed as $\mathcal{E}(m) = (\mathbf{A}, \mathbf{b} + m \cdot \lfloor q/2 \rfloor \mod q)$. Decryption is achieved by recovering m through modular arithmetic using the secret key $\mathbf{s}$. Specifically, the plaintext is obtained as $m = \lceil (\mathbf{b} - \mathbf{A}\mathbf{s}) / \lfloor q/2 \rfloor \rceil \mod 2$.

The evaluation of operations on ciphertexts is performed using modular arithmetic. The addition and multiplication of encrypted values increase the noise inherent in ciphertexts. Fully homomorphic encryption schemes address this by periodically reducing noise through bootstrapping, which involves refreshing ciphertexts to enable continued operations. Homomorphic encryption, particularly fully homomorphic encryption, represents a significant advancement in cryptographic techniques by enabling secure computation on encrypted data. Its mathematical rigor ensures the preservation of confidentiality throughout the data lifecycle, providing a robust foundation for privacy-preserving applications [97].

3.1.2. Quantum Computing and IoT Security

Quantum computing represents a transformative technological development, offering unparalleled computational capabilities while simultaneously posing significant threats to the security of classical cryptographic systems. In the context of IoT security, the emergence of quantum computing necessitates a reevaluation of cryptographic protocols to ensure long-term resilience against quantum attacks [98].

Classical cryptographic systems, such as RSA and elliptic curve cryptography, rely on the computational difficulty of problems like integer factorization and the discrete logarithm problem. Quantum algorithms, such as Shor's algorithm, efficiently solve these problems, rendering these cryptosystems vulnerable. For example, RSA encryption relies on the hardness of factoring a large composite modulus N, where $N = p \cdot q$ for two large primes p and q. Shor's algorithm can factor N in polynomial time, undermining the security of RSA-encrypted communications. To mitigate these risks, the field of post-quantum cryptography focuses on developing cryptographic protocols resistant to quantum attacks. These protocols are based on mathematical problems believed to remain intractable even for quantum computers, such as lattice-based cryptography, code-based cryptography, hash-based signatures, and multivariate polynomial problems [99].

Lattice-based cryptography is particularly promising due to its versatility and efficiency. One example is the learning-with-errors problem, which serves as the foundation for many lattice-based schemes. The learning-with-errors problem can be stated as follows. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a noise vector $\mathbf{e} \in \mathbb{Z}_q^m$, compute the vector $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$. The task of recovering $\mathbf{s}$ from $(\mathbf{A}, \mathbf{b})$ is computationally hard, even with quantum resources. This hardness forms the basis of several cryptographic primitives, including encryption schemes, key exchanges, and digital signatures [100].

Code-based cryptography leverages the hardness of decoding random linear codes. One notable example is the McEliece cryptosystem, which uses error-correcting codes to provide secure communication. Similarly, hash-based signatures, such as those based on Merkle trees, offer quantum-resistant authentication mechanisms by relying on the one-way nature of cryptographic hash functions [101].

Multivariate polynomial cryptography is another approach where the security relies on the difficulty of solving systems of multivariate quadratic equations over finite fields. Protocols based on this approach are efficient and suitable for resource-constrained environments, such as IoT devices. The adoption of post-quantum cryptographic protocols presents unique challenges for IoT systems. Many IoT devices are resource-constrained, with limited computational power, memory, and energy availability. Implementing quantum-resistant algorithms in such environments requires careful optimization to balance security and performance. Additionally, the transition to post-quantum cryptography involves ensuring compatibility with existing systems and standards, which adds complexity to the integration process [102].

3.2. Data Integrity in Distributed Architectures

IoT systems often rely on distributed architectures, such as edge computing, where data processing occurs at the edge of the network, closer to the data source. In such architectures, ensuring data integrity requires secure communication channels, resilient storage mechanisms, and robust synchronization protocols between edge devices and the central cloud [103,104]. Techniques such as secure multiparty computation (SMPC) and threshold cryptography have been explored to enable secure data aggregation and processing across distributed nodes, ensuring that even if some nodes are compromised, the overall integrity of the data is maintained [105–108].

Blockchain technology has also been proposed as a means to enhance data integrity in distributed IoT systems. By creating an immutable and distributed ledger of transactions, blockchain can ensure that data records are tamper-proof and verifiable by all participants in the network. However, the integration of blockchain into IoT presents significant challenges, particularly in terms of scalability and energy efficiency. The high computational cost and latency associated with consensus mechanisms like proof of work make blockchain less suited for real-time IoT applications, driving the need for alternative consensus algorithms, such as proof-of-stake or directed acyclic graphs (DAGs), which are more resource-efficient [109–114].

Secure Multiparty Computation and Threshold Cryptography

SMPC and threshold cryptography are advanced cryptographic techniques designed to enhance the security and privacy of distributed systems. These methods are particularly relevant in scenarios involving sensitive data processing across multiple entities, such as in IoT environments, where devices often interact within decentralized and untrusted networks. SMPC enables a group of parties to jointly compute a function over their inputs while keeping those inputs private. This ensures that no individual party learns the inputs of the others beyond what is revealed by the function's output. Formally, consider n parties, each with a private input x_i, and a function $f(x_1, x_2, \ldots, x_n)$ to be computed collaboratively. SMPC ensures that the parties compute the function correctly while preserving the privacy of x_i for all i.

The mathematical framework of SMPC typically relies on secret sharing schemes [115]. In Shamir's secret sharing, for instance, a secret s is divided into n shares $(s_1, s_2, \ldots, s_n)$ such that any subset of t or more shares can reconstruct the secret, while fewer than t shares reveal no information about s [116]. This is achieved using polynomial interpolation. The secret s is represented as the constant term of a randomly chosen polynomial $P(x)$ of degree $t-1$ over a finite field $\mathbb{F}_q$:

$$P(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1},$$

where $a_1, a_2, \ldots, a_{t-1}$ are random coefficients. Each party is given a share $s_i = P(x_i)$, where x_i is a unique identifier for that party.

The privacy and correctness of SMPC are ensured through protocols such as the GMW (Goldreich–Micali–Wigderson) and BGW (Ben–Or–Goldwasser–Wigderson) protocols. These protocols allow secure computation of any function represented as a Boolean or arithmetic circuit by ensuring that intermediate values during computation remain secret [117].

Threshold cryptography extends the principles of secret sharing to cryptographic operations, enabling secure key management and distributed trust [118]. In a (t, n)-threshold scheme, a private cryptographic key k is divided into n shares, such that any t or more shares can reconstruct k, but fewer than t shares reveal no information about the key. Threshold cryptography is particularly useful in distributed systems for tasks such as digital signing, decryption, and key generation. For example, in a threshold digital signature scheme, a group of parties collectively signs a message without reconstructing the private signing key. Let $H(m)$ represent the hash of a message m, and let the private key k be shared among n parties. A subset of t parties collaborates to produce partial signatures, which are then combined into a valid signature on m. Mathematically, threshold cryptography leverages techniques such as Lagrange interpolation for share reconstruction. Given t shares $(x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t)$, the secret k can be reconstructed as

$$k = \sum_{i=1}^{t} y_i \prod_{j \neq i} \frac{x_j}{x_j - x_i} \mod q,$$

where q is the modulus of the finite field.

3.3. Privacy Preservation in IoT

Privacy concerns in IoT extend beyond the mere protection of data during transmission and storage; they encompass the broader issue of preventing the unauthorized inference of sensitive information. IoT devices often generate vast amounts of data that, when aggregated and analyzed, can reveal patterns and insights about individuals or organizations. This has given rise to the concept of data minimization, where only a minimal amount of necessary data are collected and processed, thus reducing the risk of privacy breaches [119–121].

Techniques such as differential privacy have gained traction as a means to balance data utility with privacy. Differential privacy is a robust mathematical framework designed to protect individual privacy during data analysis. By introducing controlled noise into computations, differential privacy ensures that the inclusion or exclusion of a single data point has a negligible impact on the output, thereby safeguarding sensitive information about individuals [122–124].

Differential privacy is formally defined as follows. Let $\mathcal{M}$ be a randomized algorithm that operates on a dataset D, producing an output in a range $\mathcal{R}$. The algorithm $\mathcal{M}$ satisfies ϵ-differential privacy if, for all datasets D and D' differing in at most one element, and for all subsets $\mathcal{S} \subseteq \mathcal{R}$,

$$\Pr[\mathcal{M}(D) \in \mathcal{S}] \leq e^{\epsilon} \cdot \Pr[\mathcal{M}(D') \in \mathcal{S}],$$

where $\epsilon > 0$ is the privacy loss parameter. A smaller ϵ indicates stronger privacy guarantees.

This definition ensures that an observer cannot confidently determine whether any individual's data are included in the dataset based on the output of $\mathcal{M}$. The parameter ϵ controls the trade-off between privacy and utility: lower values of ϵ provide stronger privacy but may reduce the utility of the output.

Differential privacy is typically achieved by adding noise to the output of a computation. Two commonly used mechanisms are the Laplace Mechanism and the Gaussian Mechanism [125,126].

Laplace Mechanism:

For a function $f : D \to \mathbb{R}^k$, the Laplace Mechanism adds noise sampled from the Laplace distribution. If Δf is the global sensitivity of f, defined as

$$\Delta f = \max_{D,D'} \|f(D) - f(D')\|_1,$$

the mechanism outputs

$$\mathcal{M}(D) = f(D) + \text{Lap}(\Delta f / \epsilon),$$

where $\text{Lap}(b)$ denotes the Laplace distribution with scale parameter b.

Gaussian Mechanism:

The Gaussian Mechanism is suitable when privacy is measured using (ϵ, δ)-differential privacy, a relaxed version of the standard definition. It adds Gaussian noise with variance proportional to the global sensitivity:

$$\mathcal{M}(D) = f(D) + \mathcal{N}(0, \sigma^2), \sigma = \sqrt{2 \ln(1.25/\delta)} \cdot \Delta f / \epsilon.$$

In addition to differential privacy, the concept of federated learning has emerged as a promising approach to privacy-preserving ML in IoT. In federated learning, instead of sending raw data to a central server, IoT devices locally train ML models on their data and then send only the model updates to the central server. This approach significantly reduces the amount of sensitive data that need to be transmitted and stored centrally, thus enhancing privacy. However, federated learning introduces new challenges, such as ensuring the integrity and authenticity of the model updates and mitigating the risk of model inversion attacks, where adversaries attempt to reconstruct the original data from the model updates [127–129].

3.4. Privacy in Resource-Constrained Devices

The resource limitations of many IoT devices pose significant challenges for implementing robust privacy-preserving mechanisms. Traditional encryption methods, while effective, are often too resource-intensive for small, battery-powered devices [130]. To address this, lightweight encryption algorithms, such as the Advanced Encryption Standard (AES) in its truncated versions or custom lightweight block ciphers, have been developed to provide a balance between security and performance [131–134].

Moreover, the adoption of hardware-based security features, such as Trusted Execution Environments (TEEs) and PUFs, has been explored as a means to enhance privacy in resource-constrained IoT devices. TEEs provide a secure area within the device's processor that can execute code and store data in a manner that is isolated from the rest of the system, thereby protecting sensitive information even if the device is compromised [135–137]. PUFs, on the other hand, exploit the unique physical characteristics of semiconductor devices to generate unique cryptographic keys that cannot be replicated, thus providing a hardware-based root of trust [138–140].

3.5. Emerging Threats and Countermeasures

As the IoT continues to evolve, so do the threats to data integrity and privacy. One emerging threat is the use of AI by adversaries to carry out sophisticated attacks, such as data poisoning or model inversion, which can compromise both the integrity and privacy of IoT systems. Countering these threats requires a multi-faceted approach, combining traditional cybersecurity measures with advanced AI-based defenses, such as anomaly detection systems that can identify and mitigate suspicious activities in real-time [141–143].

In conclusion, ensuring data integrity and privacy in IoT systems is a complex and ongoing challenge that requires the continuous development and refinement of security mechanisms. As IoT continues to permeate every aspect of our lives, the importance of robust data integrity and privacy protection cannot be overstated. Thus, we should focus on developing scalable, efficient, and adaptable security solutions that can keep pace with the rapidly evolving IoT landscape, ensuring that the benefits of IoT can be realized without compromising security [144,145]. A summary of the works that analyzed the aspects of data integrity and privacy in IoT is shown in Table 3.

Table 3. A summary of studies related to data integrity and privacy in the IoT.

Topic	References	Summary
Advanced Cryptographic Techniques for Data Integrity	[79–102]	Discusses traditional and lightweight cryptographic techniques such as hash functions, digital signatures, and homomorphic encryption. Also covers post-quantum cryptography and its applicability to IoT data integrity.
Data Integrity in Distributed Architectures	[103–118]	Explores methods like SMPC, threshold cryptography, and blockchain technology for maintaining data integrity in distributed IoT systems, particularly in edge computing environments.
Privacy Preservation in IoT	[119–129]	Focuses on privacy-preserving techniques such as differential privacy and federated learning. Discusses the challenges of implementing these techniques in IoT, especially in scenarios with large-scale data analytics.
Privacy in Resource-Constrained Devices	[130–140]	Analyzes the implementation of privacy-preserving mechanisms in IoT devices with limited resources, including lightweight encryption algorithms and hardware-based security features like TEEs and PUFs.
Emerging Threats and Countermeasures	[141–145]	Identifies emerging threats to data integrity and privacy in IoT, such as AI-based attacks, and discusses potential countermeasures, including AI-driven security solutions and anomaly detection systems.

4. Network Security and Communication Protocols

The security of IoT networks is a complex and multifaceted challenge, deeply rooted in the diversity and heterogeneity of the communication protocols that facilitate interactions among IoT devices. These protocols, which govern the data exchange processes, are critical to ensuring the confidentiality, integrity, and availability of information transmitted across the IoT ecosystem. Given the limited resources of IoT devices, protocols are often designed with an emphasis on efficiency, which can result in trade-offs with security. This section delves into the intricacies of IoT network security, exploring the specific vulnerabilities associated with widely used communication protocols, advanced mitigation techniques, and emerging trends in protocol design and security [146–148].

4.1. Security Challenges in IoT Protocols

IoT communication protocols are essential for enabling seamless connectivity and data exchange in IoT ecosystems. However, their design for efficiency and resource-constrained environments often leads to significant security challenges. This section discusses the security issues associated with widely used protocols, including MQTT (Message Queuing Telemetry Transport) [149–151], CoAP (Constrained Application Protocol) [152–154], Zigbee [155–157], and additional protocols such as Bluetooth [158], Z-Wave [159], LoRaWAN [160], Thread [161], and Wi-Fi [162].

MQTT, which is widely used in industrial IoT and smart home applications, operates on a publish–subscribe model that, while efficient, is susceptible to several attack vectors, including man-in-the-middle (MitM) attacks [163], replay attacks [164], and unauthorized access due to its default lack of encryption [165]. Although TLS (Transport Layer Security) can be layered over MQTT to secure communication, the overhead introduced by TLS can be prohibitive for resource-constrained IoT devices [166].

CoAP, designed for use in lightweight M2M (machine-to-machine) communication, is another protocol that faces security issues due to its reliance on UDP (User Datagram Protocol), which inherently lacks the reliability and security features of TCP (Transmission Control Protocol) [167]. CoAP's use of DTLS (Datagram Transport Layer Security) to secure its communications adds a layer of protection, but challenges such as the proper implementation of DTLS in constrained environments and the potential for DoS attacks remain significant concerns [168,169].

Zigbee, commonly used in wireless sensor networks and smart home applications, operates on the IEEE 802.15.4 standard and uses AES-128 for encryption. Despite this, Zigbee networks have been shown to be vulnerable to attacks such as key extraction, traffic analysis, and device impersonation. The open nature of the Zigbee protocol stack, while beneficial for interoperability, also exposes it to a wide range of potential security threats [170–172].

Bluetooth, particularly Bluetooth Low Energy (BLE), is widely used in wearable devices and short-range IoT systems. Although BLE improves energy efficiency, it remains vulnerable to attacks like eavesdropping, replay attacks, and unauthorized device pairing. Enhanced authentication mechanisms and the adoption of Secure Simple Pairing (SSP) protocols can improve security in Bluetooth-based IoT applications [173,174].

Z-Wave, a low-power communication protocol often used in home automation systems, faces threats such as DoS attacks and encryption key compromise. Strengthening Z-Wave networks requires improved key management systems, regular firmware updates, and the integration of advanced encryption protocols [175,176].

LoRaWAN, a protocol for long-range, low-power IoT communication, is commonly used in smart agriculture, logistics, and urban infrastructure. It faces challenges like session key distribution vulnerabilities and replay attacks. Adopting end-to-end encryption and secure key provisioning methods can help secure LoRaWAN-based systems [177,178].

Thread, an IPv6-based low-power protocol for connected devices, offers strong security through its mesh networking capabilities. However, effective key management remains critical to preventing unauthorized network access and data breaches [179,180].

Wi-Fi, while ubiquitous in IoT applications, has its own vulnerabilities, such as susceptibility to key reinstallation attacks (e.g., KRACK) and weak password policies. Advanced security protocols like Wi-Fi Protected Access 3 (WPA3) provide enhanced encryption and authentication mechanisms, addressing many traditional Wi-Fi security issues [181,182].

4.2. Advanced Security Mechanisms

To address these vulnerabilities, several advanced security mechanisms have been developed and proposed. For MQTT, techniques such as payload encryption, token-based authentication, and the integration of zero-trust architectures are being explored to enhance security without significantly impacting performance. The concept of zero-trust, where every device is authenticated and authorized before it can communicate, is particularly relevant for IoT, where devices may be deployed in potentially hostile environments [183–185].

In CoAP, the use of object security, where security is applied directly to the data being transmitted rather than the transport layer, has been proposed as a means to improve security without the overhead associated with DTLS [186]. This approach, combined with the implementation of secure key management protocols such as OSCORE (Object Security for Constrained RESTful Environments), can mitigate many of the security risks inherent in CoAP-based systems [187,188].

Zigbee's security can be enhanced through the implementation of stronger key management practices and the use of frequency hopping techniques to make it more difficult for attackers to intercept and analyze communications. Additionally, ongoing research into the use of quantum-resistant cryptography for IoT networks promises to provide long-term security solutions that can withstand the advances in computational power expected in the coming years [189–191].

4.3. Emerging Trends and Protocol Innovations

As the IoT landscape continues to evolve, new communication protocols and security paradigms are emerging. One significant trend is the integration of Software-Defined Networking (SDN) with IoT, where SDN's centralized control model can provide greater visibility and control over network traffic, allowing for more dynamic and responsive security measures. By decoupling the control and data planes, SDN enables the real-time monitoring of network conditions and the application of security policies that can adapt to emerging threats [192–195].

Another emerging trend is the use of blockchain technology to enhance the security and integrity of IoT networks. Blockchain's decentralized and tamper-resistant nature makes it an attractive option for managing IoT device identities and securing communications. Protocols such as IOTA, designed specifically for IoT, leverage the Tangle architecture—a DAG that allows for scalable and secure transactions without the need for miners, which is resource-intensive. This approach is particularly suited for IoT environments, where resources are constrained and traditional blockchain solutions may be impractical [196–198].

Additionally, the development of protocol-agnostic security frameworks is gaining traction, where security measures are abstracted from the specific protocol and instead applied at a higher layer of the network stack. This allows for a more uniform application of security policies across heterogeneous networks, addressing one of the key challenges in IoT network security [199–201].

A summary of the above works that analyze network security and communication protocols is captured in Table 4.

Table 4. A list of topics and related studies dedicated to network security and communication protocols.

Topic	**References**	**Summary**
Communication Protocols Overview	[146–148]	Surveys and reviews on IoT communication protocols and their performance.
MQTT Protocol	[149–151]	Studies on the MQTT protocol, including use cases, security challenges, and implementations.
CoAP Protocol	[152–154]	Research on the CoAP protocol, focusing on securing communications and performance analysis.
Zigbee Protocol	[155–157]	Analysis of the Zigbee protocol, including its application in various networks and security aspects.
Bluetooth Protocol	[158,173,174]	Overview of Bluetooth vulnerabilities, such as eavesdropping, replay attacks, and pairing security issues.

Table 4. *Cont.*

Topic	References	Summary
Z-Wave Protocol	[159,175,176]	Security analysis of Z-Wave, including challenges like DoS attacks and encryption key compromise.
LoRaWAN Protocol	[160,177,178]	Examines LoRaWAN security challenges, such as session key vulnerabilities and replay attacks.
Thread Protocol	[161,179,180]	Studies on the Thread protocol, highlighting security through mesh networking and key management.
Wi-Fi Security Issues	[162,181,182]	Discusses Wi-Fi vulnerabilities such as KRACK attacks and advancements with WPA3 encryption.
MQTT Security Issues	[163–166]	Discussions on security challenges in MQTT, including attacks like MitM and DoS.
CoAP Security Enhancements	[167–169]	Enhancements to CoAP security, including DTLS vulnerabilities and protection methods.
Zigbee Security Vulnerabilities	[170–172]	Exploration of security vulnerabilities in Zigbee networks, such as key extraction and device impersonation.
Advanced MQTT Security Mechanisms	[183–185]	Proposed enhancements to MQTT security through payload encryption and zero-trust architecture.
Advanced CoAP Security Mechanisms	[186–188]	Improvement strategies for CoAP security, such as OSCORE for better key management.
Zigbee Quantum-Resistant Cryptography	[189–191]	Studies on the application of quantum-resistant cryptography in Zigbee networks.
SDN Integration with IoT	[192–195]	Research on integrating SDN with IoT for improved security.
Blockchain and IoT	[196–198]	Use of blockchain technology in IoT to enhance security and integrity.
Protocol-Agnostic Security	[199–201]	Development of security frameworks that are abstracted from specific communication protocols.

5. Artificial Intelligence and Machine Learning in IoT Security

The integration of AI and ML into IoT security represents a paradigm shift, offering both novel defense mechanisms and enhancing existing cybersecurity frameworks. In the context of IoT, AI and ML are not merely tools for automation but are fundamental in addressing the unique security challenges posed by the complexity, scale, and dynamic nature of IoT environments [202–204].

One of the most critical applications of AI in IoT security is anomaly detection [205]. Traditional security systems rely on predefined rules and signatures to identify threats [206]. However, IoT networks are characterized by high variability in device behavior, making it difficult to distinguish between normal and malicious activities using static rules. ML algorithms, particularly those employing unsupervised learning, can be trained to recognize patterns in network traffic and device behavior, enabling the detection of anomalies that may indicate security breaches [207]. Techniques such as clustering, autoencoders, and generative adversarial networks (GANs) are increasingly being employed to identify deviations from normal behavior, which can be indicative of a cyberattack [208–210].

Moreover, supervised learning models are being utilized to enhance IDS within IoT networks. By training on large datasets that include labeled instances of both normal and malicious activities, these models can classify incoming traffic in real time, improving the accuracy and speed of threat detection [211–213]. Ensemble methods, which combine the strengths of multiple learning algorithms, have shown particular promise in boosting detection rates while minimizing false positives. Furthermore, the deployment of federated learning techniques allows models to be trained across multiple IoT devices without the need for centralized data collection, preserving privacy while enhancing security [214–216].

AI and ML also play a crucial role in threat intelligence and predictive analytics within IoT security [217]. The vast amount of data generated by IoT devices can be leveraged to identify emerging threats and predict potential security incidents. Natural language processing (NLP) techniques are used to analyze unstructured data from threat reports, social media, and dark web forums, extracting actionable insights that can inform proactive defense strategies. Additionally, time-series forecasting models can be applied to predict the occurrence of security events based on historical data, enabling the development of predictive maintenance schedules and proactive security measures [218–221].

Another significant application is in the domain of secure device management. AI-driven solutions are being developed to automate the process of device enrollment, configuration, and firmware updates in IoT ecosystems. These systems can identify vulnerabilities in device firmware and initiate automated updates, reducing the window of exposure to potential exploits [222–225]. Furthermore, AI can enhance the security of device authentication processes by incorporating behavioral biometrics and continuous authentication mechanisms. These approaches analyze patterns in device usage and interactions, allowing for the dynamic assessment of trust and the detection of compromised devices [226–228].

In the context of cryptographic security, AI and ML are being employed to develop more resilient encryption schemes tailored to the resource constraints of IoT devices. For instance, AI-driven optimization techniques can be used to design lightweight cryptographic algorithms that balance security with computational efficiency [229–231]. Additionally, AI is being explored as a means to secure cryptographic keys through techniques such as quantum key distribution (QKD), where ML models are used to optimize key generation and distribution processes, enhancing the security of communication channels in IoT networks [232–234].

However, the integration of AI into IoT security is not without challenges. Adversarial ML is an emerging threat where attackers craft inputs specifically designed to deceive AI models. In the context of IoT, adversarial attacks can be particularly damaging, as they can lead to the misclassification of malicious activities as benign or vice versa. Research into robust AI models that can withstand such adversarial manipulations is critical. Techniques such as adversarial training, where models are trained on both legitimate and adversarial examples, are being explored to enhance the resilience of AI systems in IoT environments [235–240].

Additionally, the use of AI in IoT security raises concerns about the interpretability and transparency of ML models. In critical applications such as healthcare or industrial automation, it is essential not only to detect security breaches but also to understand the reasoning behind the AI's decisions. Explainable AI (XAI) is a burgeoning field that seeks to make ML models more transparent, allowing security analysts to comprehend the basis for a model's predictions and to trust its outputs in high-stakes scenarios [241–245].

The deployment of AI in IoT security also intersects with issues of scalability and energy efficiency. IoT networks can comprise millions of devices, each generating data that need to be processed in real time. Scaling AI solutions to handle this data deluge without overwhelming the computational resources of IoT devices is a significant challenge. Edge AI, where ML models are deployed directly on IoT devices or nearby edge servers, is emerging as a solution to this challenge. By processing data closer to the source, edge AI reduces latency and bandwidth usage while maintaining robust security measures. Research into low-power AI models, which can function within the strict energy constraints of IoT devices, is also gaining traction, with techniques such as model pruning and quantization being used to optimize the energy efficiency of AI algorithms [246–250]. The previously discussed works that describe the synergy of AI and ML for cybersecurity in IoT are listed in Table 5.

Table 5. A summary of studies related to AI and ML in IoT security.

Topic	References	Summary
AI and ML for Anomaly Detection	[202–210]	These references discuss the use of AI and ML techniques, especially unsupervised learning, to detect anomalies in IoT networks.
Supervised Learning for Intrusion Detection	[211–216]	Focuses on supervised learning models to enhance IDS in IoT environments.
AI in Threat Intelligence and Predictive Analytics	[217–221]	References cover AI and ML applications in threat intelligence and predictive analytics for IoT security.
Secure Device Management with AI	[222–228]	These studies explore AI-driven solutions for secure device management, including automated updates and continuous authentication.
AI for Cryptographic Security	[229–234]	Focus on AI applications in developing resilient cryptographic schemes and optimizing key distribution in IoT.
Challenges with Adversarial ML	[235–240]	Discusses the risks and countermeasures associated with adversarial machine learning in IoT security contexts.
XAI for IoT Security	[241–245]	References that delve into the importance of explainability in AI models used for IoT security.
Scalability and Energy Efficiency in AI for IoT	[246–250]	Covers research on scaling AI solutions and improving energy efficiency in IoT, including edge AI techniques.

6. Challenges and Future Directions

The field of IoT cybersecurity is confronted with an array of multifaceted challenges, which are exacerbated by the rapid and often haphazard deployment of IoT devices across diverse environments. These challenges are not only technical in nature but also span regulatory, economic, and operational domains, each with its own set of complexities that must be navigated to secure the IoT ecosystem effectively [251–253].

One of the most pressing challenges is the heterogeneity of IoT devices, which vary widely in terms of hardware capabilities, communication protocols, and security requirements. This diversity is particularly evident across application domains. Industrial IoT systems require real-time protection mechanisms to secure critical operational data and prevent downtime in predictive maintenance processes [254]. Wearable devices, used extensively in fitness and healthcare, demand advanced privacy mechanisms to safeguard sensitive personal data while respecting user consent [255]. Autonomous vehicles, meanwhile, require ultra-low-latency communication systems to ensure safe navigation and resilience against cyberattacks on sensor data or control systems [256]. These examples highlight the need for domain-specific security strategies that consider the unique operational and regulatory contexts of each IoT application [257–259].

Another significant challenge is the issue of legacy devices, which were not designed with security in mind and are often difficult or impossible to update. These devices represent a substantial portion of the current IoT landscape and pose serious security risks. The presence of these legacy systems creates a situation where new, secure devices must coexist with older, vulnerable ones, leading to a weakest-link problem in the network. Addressing this challenge requires innovative approaches such as retrofitting security mechanisms onto existing devices or developing gateway solutions that can act as a security intermediary between legacy devices and the broader network [260–262].

Interoperability among IoT devices and systems is another critical challenge, particularly in environments where devices from multiple vendors must work together seamlessly. The lack of standardized communication protocols and security frameworks can lead to significant vulnerabilities, as attackers may exploit gaps between different systems. Future research must focus on the development of robust interoperability standards that incorporate security as a foundational element. This includes not only technical standards but also agreements on governance and accountability mechanisms across different stakeholders, ensuring that security responsibilities are clearly defined and enforced [263–265].

Privacy concerns in IoT go beyond the mere protection of data; they encompass the need to provide users with control over their data and transparency about how it is used. The challenge lies in balancing the need for data collection, which is often essential for IoT functionality, with the need to respect user privacy. This is particularly complex in scenarios involving large-scale data aggregation and analysis, where the anonymization techniques may not be sufficient to prevent the re-identification of individuals. Advanced privacy-preserving techniques, such as secure multi-party computation and federated learning, are promising avenues for research, but their integration into IoT systems remains challenging due to resource constraints and the need for real-time processing [266–268].

The dynamic and often unpredictable nature of IoT environments also presents a significant challenge for security. Unlike traditional IT systems, IoT networks are highly distributed and decentralized, with devices frequently joining and leaving the network. This fluidity complicates the implementation of consistent security policies and makes it difficult to detect and respond to threats in real time. Traditional security monitoring tools are often inadequate for IoT environments, necessitating the development of new approaches that can handle the scale and dynamism of IoT networks. Techniques such as distributed ledger technology (DLT) and decentralized identity management systems hold promise in this regard, offering the potential to enhance the security and resilience of IoT networks by distributing trust and reducing single points of failure [269–271].

Emerging technologies such as 5G and edge computing are expected to further complicate the IoT security landscape. While these technologies offer significant performance improvements, they also introduce new attack vectors and exacerbate existing vulnerabilities. For instance, the shift towards edge computing, where data processing occurs closer to the source of data generation, reduces latency but also increases the attack surface by distributing processing across numerous, potentially insecure, edge devices. Securing these edge environments requires new approaches to threat detection and response, including the use of AI-driven security analytics that can operate in real time and adapt to evolving threats [272–275].

Furthermore, the regulatory environment surrounding IoT security is still in its nascent stages, with many regions lacking comprehensive legal frameworks to address the unique challenges posed by IoT devices. The absence of clear regulations and standards leads to a patchwork of security practices that vary widely across industries and geographies. There is a critical need for international cooperation in establishing regulatory standards that can provide a consistent baseline for IoT security while allowing for regional adaptations. This involves not only technical standards but also frameworks for data protection, privacy, and the ethical use of IoT technologies [276–279].

Economic factors also play a crucial role in shaping the IoT security landscape. The cost of implementing advanced security measures can be prohibitive for many organizations, particularly in sectors such as agriculture and small-scale manufacturing where margins are thin. This economic barrier often leads to security being deprioritized, resulting in vulnerable systems that are ripe for exploitation [280,281].

In conclusion, the challenges facing IoT cybersecurity are vast and varied, requiring a multidisciplinary approach that goes beyond technical solutions to encompass regulatory, economic, and operational considerations. Future research could explore cost-effective security solutions that do not compromise on protection, as well as innovative business models that incentivize investment in IoT security. Also, it should focus on developing adaptive, scalable, and cost-effective security solutions that can keep pace with the rapid evolution of IoT technologies. As the IoT continues to expand, the need for robust, integrated security measures will become increasingly critical, necessitating ongoing collaboration between industry, academia, and government to ensure the safety and resilience of the IoT ecosystem [282–287]. The list of key topics related to challenges of cybersecurity in IoT and future directions is summarized in Table 6.

Table 6. A summary of studies related to challenges and future directions of cybersecurity in the IoT.

Topic	References	Description
Security Challenges in IoT	[251–259]	IoT cybersecurity faces diverse challenges driven by device heterogeneity, regulatory constraints, and application-specific requirements such as real-time protection in IIoT, privacy in wearables, and ultra-low-latency in autonomous vehicles.
Legacy Devices and Security Risks	[260–262]	Focuses on the challenges posed by legacy IoT devices that were not designed with security in mind and potential solutions like retrofitting.
Interoperability and Standardization	[263–265]	Highlights the challenges related to interoperability among IoT devices and the need for standardized communication protocols and security frameworks.
Privacy and Data Protection	[266–268]	Addresses privacy concerns, emphasizing the need for advanced privacy-preserving techniques and secure data management in IoT.
Decentralized Security Solutions	[269–271]	Discusses decentralized approaches like blockchain and DLT for enhancing security in distributed IoT environments.
Emerging Technologies and IoT Security	[272–275]	Explores the impact of emerging technologies like 5G and edge computing on IoT security and the associated new attack vectors.
Regulatory and Economic Considerations	[276–281]	Examines the regulatory landscape and economic factors influencing IoT security, emphasizing the need for international cooperation and cost-effective solutions.
Future Research Directions	[282–287]	Suggests future research directions focusing on scalable security solutions, adaptive strategies, and enhancing stakeholder collaboration for IoT security.

7. Conclusions

The landscape of IoT cybersecurity is marked by both significant advancements and persistent challenges, reflecting the complexity and scale of IoT ecosystems. The diversity of IoT devices, coupled with their widespread deployment across critical sectors, necessitates a multifaceted approach to security that goes beyond traditional measures. The advancements in lightweight cryptographic techniques, privacy-preserving algorithms, and AI-driven anomaly detection represent important strides in securing IoT environments. However, these developments are not sufficient on their own to address the full spectrum of cybersecurity threats faced by IoT systems.

One of the critical insights from this survey is the need for holistic, end-to-end security frameworks that can be seamlessly integrated into the IoT lifecycle—from device manufacturing and deployment to ongoing operation and decommissioning. The lack of standardized security protocols and frameworks across different IoT ecosystems continues to be a significant barrier to achieving robust security. This fragmentation leads to inconsistent security postures across devices and networks, creating vulnerabilities that can be exploited by attackers. Future research must prioritize the development of interoperable and scalable security frameworks that can be adapted to the diverse range of IoT devices and applications.

Moreover, the rapid pace of technological innovation in IoT has outstripped the development of corresponding security measures. As IoT devices become more sophisticated and interconnected, the attack surface grows exponentially, making it increasingly difficult to secure these systems using conventional approaches. This necessitates a shift toward more proactive and adaptive security strategies. The integration of AI and ML in cybersecurity, while promising, also introduces new risks that must be carefully managed. For instance, adversarial attacks on AI models could undermine the effectiveness of these systems, leading to false positives or, worse, undetected breaches. This underscores the importance of developing resilient AI models that can withstand such attacks, as well as the need for continuous monitoring and updating of these models to keep pace with emerging threats.

Another crucial aspect highlighted in this survey is the need for enhanced collaboration between different stakeholders in the IoT ecosystem, including device manufacturers, network operators, service providers, and regulatory bodies. The complexity of IoT security challenges cannot be addressed by any single entity; rather, it requires coordinated efforts across the entire supply chain. This includes the establishment of industry-wide best practices, regulatory standards, and compliance frameworks that ensure a baseline level of security across all IoT devices and networks. The role of government and international regulatory bodies is particularly critical in setting these standards and ensuring their global adoption.

Looking forward, there is a pressing need to focus on the scalability of IoT security solutions. As the number of IoT devices continues to grow exponentially, security mechanisms must be capable of scaling accordingly. This includes not only the scalability of cryptographic and authentication mechanisms but also the ability to manage large-scale, distributed IoT networks securely. Techniques such as DLT, including blockchain, offer promising avenues for achieving decentralized and scalable security in IoT, but their integration into existing IoT infrastructures poses significant challenges that must be overcome.

Finally, the human factor remains a critical, yet often overlooked, component of IoT security. User awareness and education about IoT security risks, as well as the development of user-friendly security interfaces, are essential for ensuring that security measures are effectively implemented and maintained. As IoT devices increasingly permeate everyday life, the onus is on both manufacturers and users to prioritize security.

In conclusion, while the field of IoT cybersecurity has made considerable progress, it remains a dynamic and rapidly evolving area of research. The complexity of IoT ecosystems, combined with the ever-expanding threat landscape, requires continuous innovation in security approaches. By building on the current advancements and addressing the identified gaps, the research community can develop more robust and adaptive security solutions that are capable of protecting the next generation of IoT devices and networks. The future of IoT security lies in the ability to anticipate and counter emerging threats while ensuring that security solutions are scalable, interoperable, and user-centric.

Author Contributions: E.D. and M.T. conceived of the idea, designed and performed the experiments, analyzed the results, drafted the initial manuscript, and revised the final manuscript. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Villamil, S.; Hernández, C.; Tarazona, G. An overview of internet of things. *Telkomnika (Telecommun. Comput. Electron. Control)* **2020**, *18*, 2320–2327. [CrossRef]
2. Greengard, S. *The Internet of Things*; MIT Press: Cambridge, MA, USA, 2021.
3. Malhotra, P.; Singh, Y.; Anand, P.; Bangotra, D.K.; Singh, P.K.; Hong, W.C. Internet of things: Evolution, concerns and security challenges. *Sensors* **2021**, *21*, 1809. [CrossRef] [PubMed]
4. Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; Kashif Bashir, A. A survey of security and privacy issues in the Internet of Things from the layered context. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3935. [CrossRef]
5. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
6. Chanal, P.M.; Kakkasageri, M.S. Security and privacy in IoT: A survey. *Wirel. Pers. Commun.* **2020**, *115*, 1667–1693. [CrossRef]
7. Venu, D.N.; Arun Kumar, A.; Vaigandla, K.K. Review of internet of things (iot) for future generation wireless communications. *Int. J. Mod. Trends Sci. Technol.* **2022**, *8*, 01–08.
8. Gulati, K.; Boddu, R.S.K.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in Internet of Things (IoT). *Mater. Today Proc.* **2022**, *51*, 161–165. [CrossRef]
9. Celebi, H.B.; Pitarokoilis, A.; Skoglund, M. Wireless communication for the industrial IoT. In *Industrial IoT: Challenges, Design Principles, Applications, and Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 57–94.
10. Hajjaji, Y.; Boulila, W.; Farah, I.R.; Romdhani, I.; Hussain, A. Big data and IoT-based applications in smart environments: A systematic review. *Comput. Sci. Rev.* **2021**, *39*, 100318. [CrossRef]
11. Atiewi, S.; Al-Rahayfeh, A.; Almiani, M.; Yussof, S.; Alfandi, O.; Abugabah, A.; Jararweh, Y. Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. *IEEE Access* **2020**, *8*, 113498–113511. [CrossRef]
12. Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Gener. Comput. Syst.* **2022**, *131*, 209–226. [CrossRef]
13. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
14. Medhane, D.V.; Sangaiah, A.K.; Hossain, M.S.; Muhammad, G.; Wang, J. Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach. *IEEE Internet Things J.* **2020**, *7*, 6143–6149. [CrossRef]
15. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. *Sensors* **2022**, *22*, 1094. [CrossRef]
16. Kuzlu, M.; Fair, C.; Guler, O. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discov. Internet Things* **2021**, *1*, 7. [CrossRef]
17. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
18. Gimenez-Aguilar, M.; De Fuentes, J.M.; Gonzalez-Manzano, L.; Arroyo, D. Achieving cybersecurity in blockchain-based systems: A survey. *Future Gener. Comput. Syst.* **2021**, *124*, 91–118. [CrossRef]

19. Garrido, C.B.E.; Compte, S.S.; Roldan, L.R.; Malacara, A.A. Survey and testing of the IoT Cybersecurity Framework using intrusion detection systems. *Int. J. Comput. Networks Appl.* **2022**, *9*, 601–623.
20. Kotenko, I.; Izrailov, K.; Buinevich, M. Static analysis of information systems for IoT cyber security: A survey of machine learning approaches. *Sensors* **2022**, *22*, 1335. [CrossRef] [PubMed]
21. Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. *Electronics* **2022**, *11*, 1502. [CrossRef]
22. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 0406–0413.
23. Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y.B.; Nosheen, S. A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2677–2690. [CrossRef]
24. Matheu, S.N.; Hernandez-Ramos, J.L.; Skarmeta, A.F.; Baldini, G. A survey of cybersecurity certification for the internet of things. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 115. [CrossRef]
25. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics* **2021**, *11*, 16. [CrossRef]
26. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and identity management of IoHT devices: Achievements, challenges, and future directions. *Comput. Secur.* **2021**, *111*, 102491. [CrossRef]
27. Javed, A.; Malhi, A.; Kinnunen, T.; Främling, K. Scalable IoT platform for heterogeneous devices in smart environments. *IEEE Access* **2020**, *8*, 211973–211985. [CrossRef]
28. Tahir, M.; Sardaraz, M.; Muhammad, S.; Saud Khan, M. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
29. Alruwaili, O.; Tanveer, M.; Alotaibi, F.M.; Abdelfattah, W.; Armghan, A.; Alserhani, F.M. Securing the IoT-enabled smart healthcare system: A PUF-based resource-efficient authentication mechanism. *Heliyon* **2024**, *10*, e37577. [CrossRef]
30. Zhang, H.; Babar, M.; Tariq, M.U.; Jan, M.A.; Menon, V.G.; Li, X. SafeCity: Toward safe and secured data management design for IoT-enabled smart city planning. *IEEE Access* **2020**, *8*, 145256–145267. [CrossRef]
31. Alhandi, S.A.; Kamaludin, H.; Alduais, N.A.M. Trust evaluation model in IoT environment: a comprehensive survey. *IEEE Access* **2023**, *11*, 11165–11182. [CrossRef]
32. Rathee, T.; Singh, P. A systematic literature mapping on secure identity management using blockchain technology. *J. King Saud-Univ. Comput. Inf. Sci.* **2022**, *34*, 5782–5796. [CrossRef]
33. Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A lightweight blockchain-based IoT identity management approach. *Future Internet* **2021**, *13*, 24. [CrossRef]
34. Shobanadevi, A.; Tharewal, S.; Soni, M.; Kumar, D.D.; Khan, I.R.; Kumar, P. Novel identity management system using smart blockchain technology. *Int. J. Syst. Assur. Eng. Manag.* **2022**, *13*, 496–505. [CrossRef]
35. Alamri, B.; Crowley, K.; Richardson, I. Blockchain-based identity management systems in health IoT: A systematic review. *IEEE Access* **2022**, *10*, 59612–59629. [CrossRef]
36. Venkatraman, S.; Parvin, S. Developing an IoT identity management system using blockchain. *Systems* **2022**, *10*, 39. [CrossRef]
37. Mathur, S.; Arora, A. Internet of things (IoT) and PKI-based security architecture. In *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*; IGI Global: Hershey, PA, USA, 2020; pp. 25–46.
38. Danquah, P.; Kwabena-Adade, H. Public key infrastructure: an enhanced validation framework. *J. Inf. Secur.* **2020**, *11*, 241–260. [CrossRef]
39. Viriyasitavat, W.; Xu, L.D.; Sapsomboon, A.; Dhiman, G.; Hoonsopon, D. Building trust of Blockchain-based Internet-of-Thing services using public key infrastructure. *Enterp. Inf. Syst.* **2022**, *16*, 2037162. [CrossRef]
40. Höglund, J.; Lindemer, S.; Furuhed, M.; Raza, S. PKI4IoT: Towards public key infrastructure for the Internet of Things. *Comput. Secur.* **2020**, *89*, 101658. [CrossRef]
41. Gulen, U.; Baktir, S. Elliptic curve cryptography for wireless sensor networks using the number theoretic transform. *Sensors* **2020**, *20*, 1507. [CrossRef] [PubMed]
42. Ullah, S.; Zheng, J.; Din, N.; Hussain, M.T.; Ullah, F.; Yousaf, M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Comput. Sci. Rev.* **2023**, *47*, 100530. [CrossRef]
43. Hu, X.; Huang, H.; Zheng, X.; Liu, Y.; Xiong, X. Low-power reconfigurable architecture of elliptic curve cryptography for IoT. *IEICE Trans. Electron.* **2021**, *104*, 643–650. [CrossRef]
44. Adeniyi, A.E.; Jimoh, R.G.; Awotunde, J.B. A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. *Comput. Electr. Eng.* **2024**, *118*, 109330. [CrossRef]
45. Shaaban, M.A.; Alsharkawy, A.S.; AbouKreisha, M.T.; Razek, M.A. Efficient ECC-based authentication scheme for fog-based IoT environment. *arXiv* **2024**, arXiv:2408.02826. [CrossRef]

46. Sudhakaran, P. Energy efficient distributed lightweight authentication and encryption technique for IoT security. *Int. J. Commun. Syst.* **2022**, *35*, e4198. [CrossRef]
47. Sultan, I.; Mir, B.J.; Banday, M.T. Analysis and optimization of advanced encryption standard for the internet of things. In Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 27–28 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 571–575.
48. Salman, R.S.; Farhan, A.K.; Shakir, A. Lightweight modifications in the Advanced Encryption Standard (AES) for IoT applications: A comparative survey. In Proceedings of the 2022 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 15–17 March 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 325–330.
49. Tanksale, V. Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices. *Electronics* **2024**, *13*, 3631. [CrossRef]
50. Jerbi, W.; Guermazi, A.; Trabelsi, H. Crypto-ECC: a rapid secure protocol for large-scale wireless sensor networks deployed in internet of things. In Proceedings of the Theory and Applications of Dependable Computer Systems: Proceedings of the Fifteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, Brunów, Poland, 29 June–3 July 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 293–303.
51. Nashwan, S. Secure authentication scheme using Diffie–Hellman key agreement for smart IoT irrigation systems. *Electronics* **2022**, *11*, 188. [CrossRef]
52. Ali, S.; Humaria, A.; Ramzan, M.S.; Khan, I.; Saqlain, S.M.; Ghani, A.; Zakia, J.; Alzahrani, B.A. An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720925772. [CrossRef]
53. Muth, R.; Tschorsch, F. Smartdhx: Diffie–Hellman key exchange with smart contracts. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3–6 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 164–168.
54. Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comput. Netw.* **2020**, *183*, 107593. [CrossRef]
55. Yadav, A.; Kumar, S.; Singh, J. A review of physical unclonable functions (PUFs) and its applications in IoT environment. In *Ambient Communications and Computer Systems: Proceedings of RACCCS 2021, Ajmer, India, 20–21 August 2021*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 1–13.
56. Duan, S.; Sai, G. Protecting sram puf from bti aging-based cloning attack. In Proceedings of the 2022 35th SBC/SBMicro/IEEE/ACM Symposium on Integrated Circuits and Systems Design (SBCCI), Porto Alegre, Brazil, 22–26 August 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
57. Lounis, K.; Zulkernine, M. Lessons learned: Analysis of PUF-based authentication protocols for IoT. *Digit. Threat. Res. Pract.* **2023**, *4*, 1–33. [CrossRef]
58. Mostafa, A.; Lee, S.J.; Peker, Y.K. Physical unclonable function and hashing are all you need to mutually authenticate IoT devices. *Sensors* **2020**, *20*, 4361. [CrossRef] [PubMed]
59. Alkatheiri, M.S.; Sangi, A.R.; Anamalamudi, S. Physical unclonable function (PUF)-based security in Internet of Things (IoT): Key challenges and solutions. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 461–473.
60. Ning, H.; Farha, F.; Ullah, A.; Mao, L. Physical unclonable function: Architectures, applications and challenges for dependable security. *IET Circuits Devices Syst.* **2020**, *14*, 407–424. [CrossRef]
61. Gilani, K.; Bertin, E.; Hatin, J.; Crespi, N. A survey on blockchain-based identity management and decentralized privacy for personal data. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 97–101.
62. Alanzi, H.; Alkhatib, M. Towards improving privacy and security of identity management systems using blockchain technology: A systematic review. *Appl. Sci.* **2022**, *12*, 12415. [CrossRef]
63. Luecking, M.; Fries, C.; Lamberti, R.; Stork, W. Decentralized identity and trust management framework for Internet of Things. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–9.
64. Kemmoe, V.Y.; Stone, W.; Kim, J.; Kim, D.; Son, J. Recent advances in smart contracts: A technical overview and state of the art. *IEEE Access* **2020**, *8*, 117782–117801. [CrossRef]
65. Maitra, S.; Yanambaka, V.P.; Puthal, D.; Abdelgawad, A.; Yelamarthi, K. Integration of Internet of Things and blockchain toward portability and low-energy consumption. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4103. [CrossRef]
66. Gonçalves, C.; Sousa, B.; Vukovic, M.; Kusek, M. A federated authentication and authorization approach for IoT farming. *Internet Things* **2023**, *22*, 100785. [CrossRef]
67. Mahalle, P.N.; Railkar, P.N. *Identity Management for Internet of Things*; River Publishers: Aalborg, Denmark, 2022.

68. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Blockchain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731. [CrossRef]
69. Pöhn, D.; Hillmann, P. Reference service model for federated identity management. In Proceedings of the International Conference on Business Process Modeling, Development and Support, Melbourne, VIC, Australia, 28–29 June 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 196–211.
70. 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*, 49–55. [CrossRef]
71. Adja, Y.C.E.; Hammi, B.; Serhrouchni, A.; Zeadally, S. A blockchain-based certificate revocation management and status verification system. *Comput. Secur.* **2021**, *104*, 102209. [CrossRef]
72. Khodaei, M.; Papadimitratos, P. Scalable & resilient vehicle-centric certificate revocation list distribution in vehicular communication systems. *IEEE Trans. Mob. Comput.* **2020**, *20*, 2473–2489.
73. Huang, H.S.; Jiang, Z.Y.; Cheng, H.T.; Sun, H.M. Hybrid Online Certificate Status Protocol with Certificate Revocation List for Smart Grid Public Key Infrastructure. *arXiv* **2024**, arXiv:2401.10787.
74. Mahmmod, K.F.; Azeez, M.M.; Ismael, Z.H. Design an active verification mechanism for certificates revocation in OCSP for internet authentication. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 4208. [CrossRef]
75. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 100312. [CrossRef]
76. Sharma, A.; Pilli, E.S.; Mazumdar, A.P.; Gera, P. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. *Comput. Commun.* **2020**, *160*, 475–493. [CrossRef]
77. Rachit; Bhatt, S.; Ragiri, P.R. Security trends in Internet of Things: A survey. *SN Appl. Sci.* **2021**, *3*, 121. [CrossRef]
78. Dritsas, E.; Trigka, M.; Mylonas, P. A Survey on Privacy-Enhancing Techniques in the Era of Artificial Intelligence. In Proceedings of the Novel & Intelligent Digital Systems Conferences, Athens, Greece, 25–27 September 2024; Springer: Berlin/Heidelberg, Germany, 2024; pp. 385–392.
79. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors* **2021**, *21*, 3654. [CrossRef] [PubMed]
80. Anwar, M.R.; Apriani, D.; Adianita, I.R. Hash Algorithm In Verification Of Certificate Data Integrity And Security. *Aptisi Trans. Technopreneurship (ATT)* **2021**, *3*, 181–188. [CrossRef]
81. Fomichev, V.; Bobrovskiy, D.; Koreneva, A.; Nabiev, T.; Zadorozhny, D. Data integrity algorithm based on additive generators and hash function. *J. Comput. Virol. Hacking Tech.* **2022**, *18*, 31–41. [CrossRef]
82. Windarta, S.; Suryadi, S.; Ramli, K.; Pranggono, B.; Gunawan, T.S. Lightweight cryptographic hash functions: Design trends, comparative study, and future directions. *IEEE Access* **2022**, *10*, 82272–82294. [CrossRef]
83. Kavin, B.P.; Ganapathy, S. A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves. *Int. Arab J. Inf. Technol.* **2021**, *18*, 180–190.
84. Aggarwal, S.; Kumar, N. Digital signatures. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 95–107.
85. Lalem, F.; Laouid, A.; Kara, M.; Al-Khalidi, M.; Eleyan, A. A novel digital signature scheme for advanced asymmetric encryption techniques. *Appl. Sci.* **2023**, *13*, 5172. [CrossRef]
86. Megouache, L.; Zitouni, A.; Djoudi, M. Ensuring user authentication and data integrity in multi-cloud environment. *Hum. Centric Comput. Inf. Sci.* **2020**, *10*, 1–20. [CrossRef]
87. Garagad, V.G.; Iyer, N.C.; Wali, H.G. Data integrity: A security threat for internet of things and cyber-physical systems. In Proceedings of the 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2–4 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 244–249.
88. Li, H.; Kumar, V.; Park, J.M.; Yang, Y. Cumulative message authentication codes for resource-constrained IoT networks. *IEEE Internet Things J.* **2021**, *8*, 11847–11859. [CrossRef]
89. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access* **2021**, *9*, 28177–28193. [CrossRef]
90. Bhagat, V.; Kumar, S.; Gupta, S.K.; Chaube, M.K. Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7425. [CrossRef]
91. Sleem, L.; Couturier, R. Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. *Multimed. Tools Appl.* **2021**, *80*, 17067–17102. [CrossRef]
92. Yang, P.; Xiong, N.; Ren, J. Data security and privacy protection for cloud storage: A survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
93. Alharbi, A.; Zamzami, H.; Samkri, E. Survey on homomorphic encryption and address of new trend. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*. [CrossRef]

94. Yang, Z.; Hu, S.; Chen, K. FPGA-based hardware accelerator of homomorphic encryption for efficient federated learning. *arXiv* **2020**, arXiv:2007.10560.
95. Sihotang, H.T.; Efendi, S.; Zamzami, E.M.; Mawengkang, H. Design and implementation of Rivest Shamir Adleman's (RSA) cryptography algorithm in text file data security. *J. Phys. Conf. Ser.* **2020**, *1641*, 012042. [CrossRef]
96. Kumar, V.V.; Pabitha, P. Privacy-Preserving Brakerski-Gentry-Vaikuntanathan (BGV) Homomorphic Encryption for IoMT Data Security. In Proceedings of the 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chikkaballapur, India, 18–19 April 2024; IEEE: Piscataway, NJ, USA, 2024; Volume 1, pp. 1–6.
97. Marcolla, C.; Sucasas, V.; Manzano, M.; Bassoli, R.; Fitzek, F.H.; Aaraj, N. Survey on fully homomorphic encryption, theory, and applications. *Proc. IEEE* **2022**, *110*, 1572–1609. [CrossRef]
98. Bavdekar, R.; Chopde, E.J.; Bhatia, A.; Tiwari, K.; Daniel, S.J. Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. *arXiv* **2022**, arXiv:2202.02826.
99. Cho, C.H.; Chen, C.Y.; Chen, K.C.; Huang, T.W.; Hsu, M.C.; Cao, N.P.; Zeng, B.; Tan, S.G.; Chang, C.R. Quantum computation: Algorithms and applications. *Chin. J. Phys.* **2021**, *72*, 248–269. [CrossRef]
100. Bandara, H.; Herath, Y.; Weerasundara, T.; Alawatugoda, J. On advances of lattice-based cryptographic schemes and their implementations. *Cryptography* **2022**, *6*, 56. [CrossRef]
101. Balamurugan, C.; Singh, K.; Ganesan, G.; Rajarajan, M. Post-quantum and code-based cryptography—Some prospective research directions. *Cryptography* **2021**, *5*, 38. [CrossRef]
102. Kuang, R.; Barbeau, M. Indistinguishability and non-deterministic encryption of the quantum safe multivariate polynomial public key cryptographic system. In Proceedings of the 2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Virtual, 12–17 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
103. Welsh, T.; Benkhelifa, E. On resilience in cloud computing: A survey of techniques across the cloud domain. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 59. [CrossRef]
104. Hamdan, S.; Ayyash, M.; Almajali, S. Edge-computing architectures for internet of things applications: A survey. *Sensors* **2020**, *20*, 6441. [CrossRef] [PubMed]
105. Goyal, H.; Saha, S. Multi-party computation in iot for privacy-preservation. In Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), Bologna, Italy, 10–13 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1280–1281.
106. Sahinbas, K.; Catak, F.O. Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems. In *Interpretable Cognitive Internet of Things for Healthcare*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 57–72.
107. Kurt, A.; Mercan, S.; Shlomovits, O.; Erdin, E.; Akkaya, K. Lngate: Powering iot with next generation lightning micro-payments using threshold cryptography. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Virtual, 28 June–2 July 2021; pp. 117–128.
108. Tan, L.; Yu, K.; Yang, C.; Bashir, A.K. A blockchain-based Shamir's threshold cryptography for data protection in industrial internet of things of smart city. In Proceedings of the 1st Workshop on Artificial Intelligence and Blockchain Technologies for Smart Cities with 6G, New Orleans, LA, USA, 25–29 October 2021; pp. 13–18.
109. Hsueh, C.W.; Chin, C.T. Toward Trusted IoT by General Proof-of-Work. *Sensors* **2022**, *23*, 15. [CrossRef] [PubMed]
110. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Karizno, S.R. Slpow: Secure and low latency proof of work protocol for blockchain in green iot networks. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5.
111. Mišić, J.; Mišić, V.B.; Chang, X. Design of proof-of-stake PBFT algorithm for IoT environments. *IEEE Trans. Veh. Technol.* **2022**, *72*, 2497–2510. [CrossRef]
112. Singhal, D.; Ahuja, L.; Seth, A. POSMETER: Proof-of-stake blockchain for enhanced smart meter data security. *Int. J. Inf. Technol.* **2024**, *16*, 1171–1184. [CrossRef]
113. Li, Y.; Cao, B.; Peng, M.; Zhang, L.; Zhang, L.; Feng, D.; Yu, J. Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis. *IEEE/ACM Trans. Netw.* **2020**, *28*, 1643–1656. [CrossRef]
114. Bhandary, M.; Parmar, M.; Ambawade, D. A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 827–832.
115. Rahaman, M.; Arya, V.; Orozco, S.M.; Pappachan, P. Secure multi-party computation (SMPC) protocols and privacy. In *Innovations in Modern Cryptography*; IGI Global: Hershey, PA, USA, 2024; pp. 190–214.
116. Fu, X.; Xiong, L.; Li, F.; Yang, X.; Xiong, N. Blockchain-Based Efficiently Privacy-Preserving Federated Learning Framework Using Shamir Secret Sharing. *IEEE Trans. Consum. Electron.* **2024**. [CrossRef]
117. Linke, T.; Harth-Kitzerow, C. Optimizations for Secure Multiparty Computation Protocols. *Network* **2022**, *13–16.* [CrossRef]
118. Blackburn, S.R. Combinatorics and threshold cryptography. In *Combinatorial Designs and their Applications*; Routledge: London, UK, 2023; pp. 49–70.

119. Gheisari, M.; Javadpour, A.; Gao, J.; Abbasi, A.A.; Pham, Q.V.; Liu, Y. PPDMIT: A lightweight architecture for privacy-preserving data aggregation in the Internet of Things. *J. Ambient. Intell. Humaniz. Comput.* **2023**, *14*, 5211–5223. [CrossRef]
120. Liu, X.; Wang, X.; Yu, K.; Yang, X.; Ma, W.; Li, G.; Zhao, X. Secure data aggregation aided by privacy preserving in Internet of Things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 4858722. [CrossRef]
121. Tewari, A.; Gupta, B.B. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Gener. Comput. Syst.* **2020**, *108*, 909–920. [CrossRef]
122. Jiang, B.; Li, J.; Yue, G.; Song, H. Differential privacy for industrial internet of things: Opportunities, applications, and challenges. *IEEE Internet Things J.* **2021**, *8*, 10430–10451. [CrossRef]
123. Husnoo, M.A.; Anwar, A.; Chakrabortty, R.K.; Doss, R.; Ryan, M.J. Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. *IEEE Access* **2021**, *9*, 153276–153304. [CrossRef]
124. Zheng, Z.; Wang, T.; Bashir, A.K.; Alazab, M.; Mumtaz, S.; Wang, X. A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid. *IEEE Trans. Comput.* **2021**, *71*, 2915–2926. [CrossRef]
125. Kumar, G.S.; Premalatha, K.; Maheshwari, G.U.; Kanna, P.R.; Vijaya, G.; Nivaashini, M. Differential privacy scheme using Laplace Mechanism and statistical method computation in deep neural network for privacy preservation. *Eng. Appl. Artif. Intell.* **2024**, *128*, 107399. [CrossRef]
126. Dong, J.; Roth, A.; Su, W.J. Gaussian differential privacy. *J. R. Stat. Soc. Ser. B (Stat. Methodol.)* **2022**, *84*, 3–37. [CrossRef]
127. Zhao, Y.; Zhao, J.; Yang, M.; Wang, T.; Wang, N.; Lyu, L.; Niyato, D.; Lam, K.Y. Local differential privacy-based federated learning for internet of things. *IEEE Internet Things J.* **2020**, *8*, 8836–8853. [CrossRef]
128. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Poor, H.V. Federated learning for internet of things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1622–1658. [CrossRef]
129. Briggs, C.; Fan, Z.; Andras, P. A review of privacy-preserving federated learning for the Internet-of-Things. In *Federated Learning Systems. Studies in Computational Intelligence*; Springer: Cham, Switzerland, 2021; pp. 21–50.
130. Singh, S.; Sharma, P.K.; Moon, S.Y.; Park, J.H. Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *J. Ambient. Intell. Humaniz. Comput.* **2024**, *15*, 1625–1642. [CrossRef]
131. Teng, L.; Li, H.; Yin, S.; Sun, Y. A Modified Advanced Encryption Standard for Data Security. *Int. J. Netw. Secur.* **2020**, *22*, 112–117.
132. Muttaqin, K.; Rahmadoni, J. Analysis and design of file security system AES (advanced encryption standard) cryptography based. *J. Appl. Eng. Technol. Sci. (JAETS)* **2020**, *1*, 113–123. [CrossRef]
133. Nayancy; Dutta, S.; Chakraborty, S. A survey on implementation of lightweight block ciphers for resource constraints devices. *J. Discret. Math. Sci. Cryptogr.* **2022**, *25*, 1377–1398. [CrossRef]
134. Raza, A.R.; Mahmood, K.; Amjad, M.F.; Abbas, H.; Afzal, M. On the efficiency of software implementations of lightweight block ciphers from the perspective of programming languages. *Future Gener. Comput. Syst.* **2020**, *104*, 43–59. [CrossRef]
135. Geppert, T.; Deml, S.; Sturzenegger, D.; Ebert, N. Trusted execution environments: Applications and organizational challenges. *Front. Comput. Sci.* **2022**, *4*, 930741. [CrossRef]
136. Fan, Y.; Liu, S.; Tan, G.; Qiao, F. Fine-grained access control based on trusted execution environment. *Future Gener. Comput. Syst.* **2020**, *109*, 551–561. [CrossRef]
137. Zhang, Y.; Wang, Z.; Cao, J.; Hou, R.; Meng, D. ShuffleFL: Gradient-preserving federated learning using trusted execution environment. In Proceedings of the 18th ACM international Conference on Computing Frontiers, Virtual, 11–13 May 2021; pp. 161–168.
138. Gao, Y.; Al-Sarawi, S.F.; Abbott, D. Physical unclonable functions. *Nat. Electron.* **2020**, *3*, 81–91. [CrossRef]
139. Al-Meer, A.; Al-Kuwari, S. Physical unclonable functions (PUF) for IoT devices. *ACM Comput. Surv.* **2023**, *55*, 314. [CrossRef]
140. Cambou, B.; Philabaum, C.; Booher, D.; Telesca, D.A. Response-based cryptographic methods with ternary physical unclonable functions. In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), San Francisco, CA, USA, 14–15 March 2019*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 2, pp. 781–800.
141. Gong, X.; Chen, Y.; Yang, W.; Mei, G.; Wang, Q. InverseNet: Augmenting Model Extraction Attacks with Training Data Inversion. In Proceedings of the IJCAI, Montreal, QC, Canada, 19–27 August 2021; pp. 2439–2447.
142. Zhang, Y.; Jia, R.; Pei, H.; Wang, W.; Li, B.; Song, D. The secret revealer: Generative model-inversion attacks against deep neural networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 253–261.
143. Hong, S.; Chandrasekaran, V.; Kaya, Y.; Dumitraş, T.; Papernot, N. On the effectiveness of mitigating data poisoning attacks with gradient shaping. *arXiv* **2020**, arXiv:2002.11497.
144. Atlam, H.F.; Wills, G.B. IoT security, privacy, safety and ethics. In *Digital Twin Technologies and Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2020; pp.123–149.
145. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]

146. Bayılmış, C.; Ebleme, M.A.; Çavuşoğlu, Ü.; Küçük, K.; Sevin, A. A survey on communication protocols and performance evaluations for Internet of Things. *Digit. Commun. Netw.* **2022**, *8*, 1094–1104. [CrossRef]
147. Pai, G.N.; Pai, M.S.; Gowd, V.D.; Shruthi, M.; Naveen K, B. Internet of Things: A survey on devices, ecosystem, components and communication protocols. In Proceedings of the 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 5–7 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 611–616.
148. Gerodimos, A.; Maglaras, L.; Ferrag, M.A.; Ayres, N.; Kantzavelou, I. IoT: Communication protocols and security threats. *Internet Things Cyber Phys. Syst.* **2023**, *3*, 1–13. [CrossRef]
149. Yalçınkaya, F.; Aydilek, H.; Erten, M.Y.; İnanç, N. IoT based smart home testbed using MQTT communication protocol. *Int. J. Eng. Res. Dev.* **2020**, *12*, 317–324. [CrossRef]
150. Shanmugapriya, D.; Patel, A.; Srivastava, G.; Lin, J.C.W. MQTT protocol use cases in the Internet of Things. In Proceedings of the Big Data Analytics: 9th International Conference, BDA 2021, Virtual, 15–18 December 2021; Proceedings 9; Springer: Berlin/Heidelberg, Germany, 2021; pp. 146–162.
151. Chen, F.; Huo, Y.; Zhu, J.; Fan, D. A review on the study on MQTT security challenge. In Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud), Washington, DC, USA, 6–8 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 128–133.
152. Alhaidari, F.A.; Alqahtani, E.J. Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey. *J. Commun.* **2020**, *15*, 14–30. [CrossRef]
153. Bansal, S.; Kumar, D. A Reliable CoAP Protocol for IoT Communication. 2022. Available online: https://www.researchsquare.com/article/rs-1974849/v1 (accessed on 8 January 2025).
154. Azeez, H.H.; Abdullah, M.Z. Performance analysis of constrained application protocol (CoAP). *AIP Conf. Proc.* **2023**, *2591*, 030074.
155. Pereira, D.S.; De Morais, M.R.; Nascimento, L.B.; Alsina, P.J.; Santos, V.G.; Fernandes, D.H.; Silva, M.R. Zigbee protocol-based communication network for multi-unmanned aerial vehicle networks. *IEEE Access* **2020**, *8*, 57762–57771. [CrossRef]
156. Zohourian, A.; Dadkhah, S.; Neto, E.C.P.; Mahdikhani, H.; Danso, P.K.; Molyneaux, H.; Ghorbani, A.A. IoT Zigbee device security: A comprehensive review. *Internet Things* **2023**, *22*, 100791. [CrossRef]
157. Ding, S.; Liu, J.; Yue, M. The use of ZigBee wireless communication technology in industrial automation control. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 8317862. [CrossRef]
158. Ghori, M.R.; Wan, T.C.; Sodhy, G.C. Bluetooth low energy mesh networks: Survey of communication and security protocols. *Sensors* **2020**, *20*, 3590. [CrossRef] [PubMed]
159. Lilli, M.; Braghin, C.; Riccobene, E. Formal Proof of a Vulnerability in Z-Wave IoT Protocol. In Proceedings of the SECRYPT, Virtual, 6–8 July 2021; pp. 198–209.
160. Banti, K.; Karampelia, I.; Dimakis, T.; Boulogeorgos, A.A.A.; Kyriakidis, T.; Louta, M. LoRaWAN communication protocols: A comprehensive survey under an energy efficiency perspective. *Telecom* **2022**, *3*, 322–357. [CrossRef]
161. Dahyan, K.O.; Khattak, S.B.A.; Nasralla, M.M.; Esmail, M.A.; Iqbal, M. Enabling Smart Sensing Systems with Thread Protocol for IoT Connectivity and Cloud Integration. In Proceedings of the International Conference on Sustainability: Developments and Innovations, Riyadh, Saudi Arabia, 18–22 February 2024; Springer: Berlin/Heidelberg, Germany, 2024; pp. 127–134.
162. Tarish, H.A. Enhanced IoT Wi-Fi protocol standard's security using secure remote password. *Period. Eng. Nat. Sci. (PEN)* **2022**, *10*, 632–644. [CrossRef]
163. Wong, H.C. *Man-in-the-Middle Attacks on MQTT Based IoT Networks*; Missouri University of Science and Technology: Rolla, MO, USA, 2022.
164. Vaccari, I.; Aiello, M.; Cambiaso, E. SlowITe, a novel denial of service attack affecting MQTT. *Sensors* **2020**, *20*, 2932. [CrossRef] [PubMed]
165. Boppana, T.K.; Bagade, P. Security risks in MQTT-Based industrial IoT applications. In Proceedings of the 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Barcelona, Spain, 1–3 August 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
166. Shilpa, V.; Vidya, A.; Pattar, S. MQTT based secure transport layer communication for mutual authentication in IoT network. *Glob. Transitions Proc.* **2022**, *3*, 60–66.
167. Tsai, W.C.; Tsai, T.H.; Wang, T.J.; Chiang, M.L. Automatic key update mechanism for lightweight M2M communication and enhancement of iot security: A case study of CoAP using libcoap library. *Sensors* **2022**, *22*, 340. [CrossRef] [PubMed]
168. Sara, A.; Randa, J. Data protection in IoT using CoAP based on enhanced DTLS. *AIP Conf. Proc.* **2024**, *2729*, 040003.
169. Timiraos, M.; Michelena, Á.; Díaz-Longueira, A.; Jove, E.; Aveleira-Mata, J.; García-Rodiguez, I.; Bayón-Gutiérrez, M.; Alaiz-MoretÓn, H.; Calvo-Rolle, J.L. Categorization of CoAP DoS Attack Based on One-Class Boundary Methods. In Proceedings of the International Conference on Soft Computing Models in Industrial and Environmental Applications, Salamanca, Spain, 5–7 September 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 112–121.
170. Mishra, V.M.; Kumar, A.; Ompal. FPGA integrated IEEE 802.15. 4 ZigBee wireless sensor nodes performance for industrial plant monitoring and automation. *Nucl. Eng. Technol.* **2022**, *54*, 2444–2452.

171. Farha, F.; Ning, H.; Yang, S.; Xu, J.; Zhang, W.; Choo, K.-K.R. Timestamp scheme to mitigate replay attacks in secure ZigBee networks. *IEEE Trans. Mob. Comput.* **2020**, *21*, 342–351. [CrossRef]
172. Coboi, A.E.; Nguyen, V.; Nguyen, M.; Duy, N.; Tran, T. An Analysis of ZigBee Technologies for Data Routing in Wireless Sensor Networks. *ICSES Trans. Comput. Netw. Commun. (ITCNC)* **2021**.
173. Lacava, A.; Zottola, V.; Bonaldo, A.; Cuomo, F.; Basagni, S. Securing Bluetooth Low Energy networking: An overview of security procedures and threats. *Comput. Netw.* **2022**, *211*, 108953. [CrossRef]
174. Madugula, S.S.; Wei, R. Improvement of Passkey Entry Protocol for Secure Simple Pairing. In Proceedings of the 2023 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Jiangsu, China, 2–4 November 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 347–356.
175. Braghin, C.; Lilli, M.; Riccobene, E. A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study. *Comput. Secur.* **2023**, *127*, 103037. [CrossRef]
176. Nkuba, C.K.; Woo, S.; Lee, H.; Dietrich, S. ZMAD: Lightweight Model-Based Anomaly Detection for the Structured Z-Wave Protocol. *IEEE Access* **2023**, *11*, 60562–60577. [CrossRef]
177. Hessel, F.; Almon, L.; Hollick, M. LoRaWAN security: an evolvable survey on vulnerabilities, attacks and their systematic mitigation. *ACM Trans. Sens. Netw.* **2023**, *18*, 70. [CrossRef]
178. Gaffurini, M.; Flammini, A.; Ferrari, P.; Fernandes Carvalho, D.; Godoy, E.P.; Sisinni, E. End-to-End Emulation of LoRaWAN Architecture and Infrastructure in Complex Smart City Scenarios Exploiting Containers. *Sensors* **2024**, *24*, 2024. [CrossRef]
179. Akestoridis, D.G.; Sekar, V.; Tague, P. On the security of thread networks: Experimentation with openthread-enabled devices. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, TX, USA, 16–19 May 2022; pp. 233–244.
180. Darroudi, S.M.; Gomez, C. Experimental evaluation of 6blemesh: Ipv6-based ble mesh networks. *Sensors* **2020**, *20*, 4623. [CrossRef] [PubMed]
181. Baray, E.; Ojha, N.K. WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In Proceedings of the 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 8–10 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 23–30.
182. Kwon, S.; Choi, H.K. Evolution of Wi-Fi protected access: security challenges. *IEEE Consum. Electron. Mag.* **2020**, *10*, 74–81. [CrossRef]
183. Akshatha, P.; Dilip Kumar, S. Enhancing security mechanism of MQTT protocol using payload encryption. In Proceedings of the International Conference on Frontiers in Computing and Systems, Bara Phool, India, 19–21 December 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 199–208.
184. Michaelides, M.; Sengul, C.; Patras, P. An experimental evaluation of MQTT authentication and authorization in IoT. In Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization, New Orleans, LA, USA, 31 January–4 February 2022; pp. 69–76.
185. Sun, L.; Zhu, H. The Research on Security Technology of Earthquake Warning Information Release Based on Zero Trust MQTT Protocol. In Proceedings of the 2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS), Nanjing, China, 7–9 April 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 131–135.
186. Shah, V. Exploit DTLS Vulnerabilities & Provide a Novel approach to Protect DTLS in CoAP based IoT. *Int. J. Res. Appl. Sci. Eng. Technol.* **2020**, *8*, 216–221.
187. Gunnarsson, M.; Brorsson, J.; Palombini, F.; Seitz, L.; Tiloca, M. Evaluating the performance of the OSCORE security protocol in constrained IoT environments. *Internet Things* **2021**, *13*, 100333. [CrossRef]
188. Höglund, R.; Tiloca, M.; Bouget, S.; Raza, S. Key Update for the IoT Security Standard OSCORE. In Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 31 July–2 August 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 78–85.
189. Nguyen, C.V.; Coboi, A.E.; Bach, N.V.; Dang, A.; Le, T.; Nguyen, H.P.; Nguyen, M.T. ZigBee based data collection in wireless sensor networks. *Int. J. Inf. Commun. Technol.* **2021**, *10*, 211–224. [CrossRef]
190. Muñoz-Calderón, M.; Moh, M. Quantum-Resistant Authentication for Smart Grid: The Case for Using Merkle Trees. In *Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World*; IGI Global: Hershey, PA, USA, 2022; pp. 371–395.
191. Mattsson, J.P.; Smeets, B.; Thormarker, E. Quantum-resistant cryptography. *arXiv* **2021**, arXiv:2112.00399.
192. Ja'afreh, M.A.; Adhami, H.; Alchalabi, A.E.; Hoda, M.; El Saddik, A. Toward integrating software defined networks with the Internet of Things: A review. *Clust. Comput.* **2022**, *25*, 1619–1636. [CrossRef] [PubMed]
193. Mohammed, A.H.; Khaleefah, R.M.; Abdulateef, I.A.; Hussein, M.k. A review software defined networking for internet of things. In Proceedings of the 2020 International Congress on Human–Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 26–28 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
194. Al Hayajneh, A.; Bhuiyan, M.Z.A.; McAndrew, I. Improving internet of things (IoT) security with software-defined networking (SDN). *Computers* **2020**, *9*, 8. [CrossRef]

195. Bekri, W.; Jmal, R.; Chaari Fourati, L. Internet of things management based on software defined networking: a survey. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 385–410. [CrossRef]
196. Spathoulas, G.; Negka, L.; Pandey, P.; Katsikas, S. Can Blockchain Technology Enhance Security and Privacy in the Internet of Things? In *Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 199–228.
197. Alshaikhli, M.; Elfouly, T.; Elharrouss, O.; Mohamed, A.; Ottakath, N. Evolution of Internet of Things from blockchain to IOTA: A survey. *IEEE Access* **2021**, *10*, 844–866. [CrossRef]
198. Hellani, H.; Sliman, L.; Samhat, A.E.; Exposito, E. Tangle the blockchain: Towards connecting blockchain and DAG. In Proceedings of the 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, 27–29 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 63–68.
199. Tournier, J.; Lesueur, F.; Mouël, F.L.; Guyon, L.; Ben-Hassine, H. IoTMap: A protocol-agnostic multi-layer system to detect application patterns in IoT networks. In Proceedings of the 10th International Conference on the Internet of Things, Malmö, Sweden, 5–9 October 2020; pp. 1–8.
200. Morales, G.A.; Bienek-Parrish, A.; Jenkins, P.; Slavin, R. Protocol-agnostic IoT Device Classification on Encrypted Traffic Using Link-Level Flows. In Proceedings of the Cyber-Physical Systems and Internet of Things Week 2023, San Antonio, TX, USA, 9–12 May 2023; pp. 19–24.
201. Sahu, S.K.; Mohapatra, D.P.; Barik, D.R. An Exhaustive Survey of Privacy and Security Based on IoT Networks. In *IoT Applications, Security Threats, and Countermeasures*; CRC Press: Boca Raton, FL, USA, 2021; pp. 209–226.
202. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
203. Sarker, I.H.; Khan, A.I.; Abushark, Y.B.; Alsolami, F. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mob. Netw. Appl.* **2023**, *28*, 296–312. [CrossRef]
204. Wu, H.; Han, H.; Wang, X.; Sun, S. Research on artificial intelligence enhancing internet of things security: A survey. *IEEE Access* **2020**, *8*, 153826–153848. [CrossRef]
205. DeMedeiros, K.; Hendawi, A.; Alvarez, M. A survey of AI-based anomaly detection in IoT and sensor networks. *Sensors* **2023**, *23*, 1352. [CrossRef] [PubMed]
206. Díaz-Verdejo, J.; Muñoz-Calle, J.; Estepa Alonso, A.; Estepa Alonso, R.; Madinabeitia, G. On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. *Appl. Sci.* **2022**, *12*, 852. [CrossRef]
207. Adekunle, T.S.; Alabi, O.O.; Lawrence, M.O.; Adeleke, T.A.; Afolabi, O.S.; Ebong, G.N.; Egbedokun, G.O.; Bamisaye, T.A. An intrusion system for internet of things security breaches using machine learning techniques. In Proceedings of the Artificial Intelligence and Applications, Corfu, Greece, 27–30 June 2024, Vol. 2; pp. 188–194.
208. Ibor, A.E.; Oladeji, F.A.; Okunoye, O.B.; Ekabua, O.O. An Improved Cyberattack Prediction Technique With Intelligent Clustering And Deep Neural Network. *FUW Trends Sci. Technol. J.* **2020**, *5*, 15–22.
209. Flávio, M.; do Prado, C.B.; da Costa Carmo, L.F.R.; de Sá, A.O.; Ferrari, P.; Pasetti, M. Autoencoder-based Approach to Detect Stealth Cyberattacks in Battery Energy Storage Systems. In Proceedings of the 2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0 & IoT), Florence, Italy, 29–31 May 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 452–457.
210. Peppes, N.; Alexakis, T.; Demestichas, K.; Adamopoulou, E. A comparison study of generative adversarial network architectures for malicious cyber-attack data generation. *Appl. Sci.* **2023**, *13*, 7106. [CrossRef]
211. Abdallah, E.E.; Otoom, A.F.; Eleisah, W. Intrusion detection systems using supervised machine learning techniques: a survey. *Procedia Comput. Sci.* **2022**, *201*, 205–212. [CrossRef]
212. Baniasadi, S.; Rostami, O.; Martín, D.; Kaveh, M. A novel deep supervised learning-based approach for intrusion detection in IoT systems. *Sensors* **2022**, *22*, 4459. [CrossRef]
213. Mebawondu, J.O.; Alowolodu, O.D.; Mebawondu, J.O.; Adetunmbi, A.O. Network intrusion detection system using supervised learning paradigm. *Sci. Afr.* **2020**, *9*, e00497. [CrossRef]
214. Alotaibi, Y.; Ilyas, M. Ensemble-learning framework for intrusion detection to enhance internet of things' devices security. *Sensors* **2023**, *23*, 5568. [CrossRef] [PubMed]
215. Thakkar, A.; Lohiya, R. Attack classification of imbalanced intrusion data for IoT network using ensemble-learning-based deep neural network. *IEEE Internet Things J.* **2023**, *10*, 11888–11895. [CrossRef]
216. Alghanam, O.A.; Almobaideen, W.; Saadeh, M.; Adwan, O. An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning. *Expert Syst. Appl.* **2023**, *213*, 118745. [CrossRef]
217. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Ahmed, M.R.; Khan, R.T.; Kaiser, M.S.; Mahmud, M. Security threats and artificial intelligence based countermeasures for internet of things networks: A comprehensive survey. *IEEE Access* **2021**, *9*, 94668–94690. [CrossRef]
218. Georgescu, T.M. Natural language processing model for automatic analysis of cybersecurity-related documents. *Symmetry* **2020**, *12*, 354. [CrossRef]

219. Zhang, W.E.; Sheng, Q.Z.; Alhazmi, A.; Li, C. Adversarial attacks on deep-learning models in natural language processing: A survey. *ACM Trans. Intell. Syst. Technol. (TIST)* **2020**, *11*, 24. [CrossRef]
220. Wang, Y.; Wu, H.; Dong, J.; Liu, Y.; Long, M.; Wang, J. Deep Time Series Models: A Comprehensive Survey and Benchmark. *arXiv* **2024**, arXiv:2407.13278.
221. Liu, Z.; Zhu, Z.; Gao, J.; Xu, C. Forecast methods for time series data: a survey. *IEEE Access* **2021**, *9*, 91896–91912. [CrossRef]
222. Rangaraju, S. Secure by intelligence: Enhancing products with AI-driven security measures. *EPH—Int. J. Sci. Eng.* **2023**, *9*, 36–41. [CrossRef]
223. Keshta, I. AI-driven IoT for smart health care: Security and privacy issues. *Inform. Med. Unlocked* **2022**, *30*, 100903. [CrossRef]
224. Dhinakaran, D.; Sankar, S.; Selvaraj, D.; Raja, S.E. Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. *arXiv* **2024**, arXiv:2401.00794.
225. Rehan, H. AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *J. Artif. Intell. Gen. Sci. (JAIGS)* **2024**, *1*, 132–151. [CrossRef]
226. Abed, A.K.; Anupam, A. Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Secur. Priv.* **2023**, *6*, e285. [CrossRef]
227. Mayrhofer, R.; Sigg, S. Adversary models for mobile device authentication. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 198. [CrossRef]
228. Badhib, A.; Alshehri, S.; Cherif, A. A robust device-to-device continuous authentication protocol for the internet of things. *IEEE Access* **2021**, *9*, 124768–124792. [CrossRef]
229. Kumar, D.K.; Reddy, K.K.; Kathrine, G.J.W. Smart Grid Protection with AI and Cryptographic Security. In Proceedings of the 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 5–7 June 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 246–251.
230. Ishtaiwi, A.; Al Khaldy, M.A.; Al-Qerem, A.; Aldweesh, A.; Almomani, A. Artificial Intelligence in Cryptographic Evolution: Bridging the Future of Security. In *Innovations in Modern Cryptography*; IGI Global: Hershey, PA, USA, 2024; pp. 31–54.
231. Nitaj, A.; Rachidi, T. Applications of neural network-based AI in cryptography. *Cryptography* **2023**, *7*, 39. [CrossRef]
232. Okey, O.D.; Maidin, S.S.; Lopes Rosa, R.; Toor, W.T.; Carrillo Melgarejo, D.; Wuttisittikulkij, L.; Saadi, M.; Zegarra Rodríguez, D. Quantum key distribution protocol selector based on machine learning for next-generation networks. *Sustainability* **2022**, *14*, 15901. [CrossRef]
233. Radanliev, P. Artificial intelligence and quantum cryptography. *J. Anal. Sci. Technol.* **2024**, *15*, 4. [CrossRef]
234. Al-Mohammed, H.A.; Al-Ali, A.; Yaacoub, E.; Qidwai, U.; Abualsaud, K.; Rzewuski, S.; Flizikowski, A. Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios. *IEEE Access* **2021**, *9*, 136994–137004. [CrossRef]
235. Lin, J.; Dang, L.; Rahouti, M.; Xiong, K. Ml attack models: adversarial attacks and data poisoning attacks. *arXiv* **2021**, arXiv:2112.02797.
236. Pierazzi, F.; Pendlebury, F.; Cortellazzi, J.; Cavallaro, L. Intriguing properties of adversarial ml attacks in the problem space. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1332–1349.
237. Sadeghi, K.; Banerjee, A.; Gupta, S.K. A system-driven taxonomy of attacks and defenses in adversarial machine learning. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 450–467. [CrossRef] [PubMed]
238. Jmila, H.; Khedher, M.I. Adversarial machine learning for network intrusion detection: A comparative study. *Comput. Netw.* **2022**, *214*, 109073. [CrossRef]
239. Sarker, I.H. Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *Secur. Priv.* **2023**, *6*, e295. [CrossRef]
240. Hathaliya, J.J.; Tanwar, S.; Sharma, P. Adversarial learning techniques for security and privacy preservation: A comprehensive review. *Secur. Priv.* **2022**, *5*, e209. [CrossRef]
241. Zhang, Z.; Al Hamadi, H.; Damiani, E.; Yeun, C.Y.; Taher, F. Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access* **2022**, *10*, 93104–93139. [CrossRef]
242. Chamola, V.; Hassija, V.; Sulthana, A.R.; Ghosh, D.; Dhingra, D.; Sikdar, B. A review of trustworthy and explainable artificial intelligence (xai). *IEEE Access* **2023**, *11*, 78994–79015. [CrossRef]
243. Linardatos, P.; Papastefanopoulos, V.; Kotsiantis, S. Explainable ai: A review of machine learning interpretability methods. *Entropy* **2020**, *23*, 18. [CrossRef] [PubMed]
244. Tiwari, R. Explainable ai (xai) and its applications in building trust and understanding in ai decision making. *Int. J. Sci. Res. Eng. Manag* **2023**, *7*, 1–13. [CrossRef]
245. Spartalis, C.N.; Semertzidis, T.; Daras, P. Balancing XAI with Privacy and Security Considerations. In Proceedings of the European Symposium on Research in Computer Security, The Hague, The Netherlands, 25–29 September 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 111–124.

246. Rana, B.; Singh, Y.; Singh, P.K. A systematic survey on internet of things: Energy efficiency and interoperability perspective. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4166. [CrossRef]
247. Xu, Z.; Liu, W.; Huang, J.; Yang, C.; Lu, J.; Tan, H. Artificial intelligence for securing IoT services in edge computing: a survey. *Secur. Commun. Netw.* **2020**, *2020*, 8872586. [CrossRef]
248. Wang, C.; Yuan, Z.; Zhou, P.; Xu, Z.; Li, R.; Wu, D.O. The security and privacy of mobile edge computing: An artificial intelligence perspective. *IEEE Internet Things J.* **2023**, *10*, 22008–22032. [CrossRef]
249. Hussein, M.; Mohammed, Y.S.; Galal, A.I.; Abd-Elrahman, E.; Zorkany, M. Smart cognitive IoT devices using multi-layer perception neural network on limited microcontroller. *Sensors* **2022**, *22*, 5106. [CrossRef] [PubMed]
250. Zhu, S.; Ota, K.; Dong, M. Green AI for IIoT: Energy efficient intelligent edge computing for industrial internet of things. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 79–88. [CrossRef]
251. Jurcut, A.; Niculcea, T.; Ranaweera, P.; Le-Khac, N.A. Security considerations for Internet of Things: A survey. *SN Comput. Sci.* **2020**, *1*, 193. [CrossRef]
252. Ye, C.; Cao, W.; Chen, S. Security challenges of blockchain in Internet of things: Systematic literature review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4177. [CrossRef]
253. Nižetić, S.; Šolić, P.; Gonzalez-De, D.L.d.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef] [PubMed]
254. Mekala, S.H.; Baig, Z.; Anwar, A.; Zeadally, S. Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Comput. Commun.* **2023**, *208*, 294–320. [CrossRef]
255. Hora, A.; Kulkarni, P. Wearables and Cybersecurity: Navigating the Threat Landscape. In Proceedings of the 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 10–12 July 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 563–567.
256. Gómez-Olmos, J. IoT-enabled Edge Computing for Cybersecurity in Autonomous Vehicles-Challenges and Opportunities: Discusses challenges and opportunities in implementing IoT-enabled edge computing for cybersecurity in Avs. *J. Artif. Intell. Res. Appl.* **2023**, *3*, 1–16.
257. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of things: A general overview between architectures, protocols and applications. *Information* **2021**, *12*, 87. [CrossRef]
258. Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT security. *Comput. Sci. Rev.* **2022**, *44*, 100467. [CrossRef]
259. Singh, I.; Lee, S.W. Self-adaptive and secure mechanism for IoT based multimedia services: a survey. *Multimed. Tools Appl.* **2022**, *81*, 26685–26720. [CrossRef]
260. Carrillo-Mondéjar, J.; Turtiainen, H.; Costin, A.; Martínez, J.L.; Suarez-Tangil, G. Hale-iot: Hardening legacy internet of things devices by retrofitting defensive firmware modifications and implants. *IEEE Internet Things J.* **2022**, *10*, 8371–8394. [CrossRef]
261. Hurst, W.; Shone, N. Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation. In *Management and Engineering of Critical Infrastructures*; Elsevier: Amsterdam, The Netherlands, 2024; pp. 265–286.
262. Lins, F.A.A.; Vieira, M. Security requirements and solutions for iot gateways: A comprehensive study. *IEEE Internet Things J.* **2020**, *8*, 8667–8679. [CrossRef]
263. Albouq, S.S.; Abi Sen, A.A.; Almashf, N.; Yamin, M.; Alshanqiti, A.; Bahbouh, N.M. A survey of interoperability challenges and solutions for dealing with them in IoT environment. *IEEE Access* **2022**, *10*, 36416–36428. [CrossRef]
264. Rasheed, H. Consideration of Cloud-Web-Concepts for Standardization and Interoperability: A Comprehensive Review for Sustainable Enterprise Systems, AI, and IoT Integration. *J. Inf. Technol. Inform.* **2024**, *3*.
265. Sheron, P.F.; Sridhar, K.; Baskar, S.; Shakeel, P.M. A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3815. [CrossRef]
266. Lee, C.; Ahmed, G. Improving IoT privacy, data protection and security concerns. *Int. J. Technol. Innov. Manag. (IJTIM)* **2021**, *1*, 18–33. [CrossRef]
267. Hellani, H.; Sliman, L.; Samhat, A.E.; Exposito, E. On blockchain integration with supply chain: Overview on data transparency. *Logistics* **2021**, *5*, 46. [CrossRef]
268. Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Comput. Mater. Contin.* **2020**, *65*, 87–107. [CrossRef]
269. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
270. Vishwakarma, M.; Kesswani, N. DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT. *Decis. Anal. J.* **2022**, *5*, 100142. [CrossRef]

271. Panda, S.S.; Mohanta, B.K.; Dey, M.R.; Satapathy, U.; Jena, D. Distributed ledger technology for securing IoT. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; IEEE: Piscataway, NJ, USA, 2020, pp. 1–6.
272. Fonyi, S. Overview of 5G security and vulnerabilities. *Cyber Def. Rev.* **2020**, *5*, 117–134.
273. Bhat, S.A.; Sofi, I.B.; Chi, C.Y. Edge computing and its convergence with blockchain in 5G and beyond: Security, challenges, and opportunities. *IEEE Access* **2020**, *8*, 205340–205373. [CrossRef]
274. Zhao, Y.; Hu, N.; Zhao, Y.; Zhu, Z. A secure and flexible edge computing scheme for AI-driven industrial IoT. *Clust. Comput.* **2023**, *26*, 283–301. [CrossRef]
275. Sheeja, S.; Francis, E.G. Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review. *Eng. Appl. Sci. Res.* **2023**, *50*, 633–645.
276. Hadzovic, S.; Mrdovic, S.; Radonjic, M. A path towards an internet of things and artificial intelligence regulatory framework. *IEEE Commun. Mag.* **2023**, *61*, 90–96. [CrossRef]
277. Adestria, E.; Almubaroq, H.Z. Building International Cooperation in Utilizing the Internet of Things (Iot) for Defense: Towards Better Global Security. *Indones. J. Interdiscip. Res. Sci. Technol.* **2024**, *2*, 523–530. [CrossRef]
278. Gupta, R.; Gupta, I.; Singh, A.K.; Saxena, D.; Lee, C.N. An iot-centric data protection method for preserving security and privacy in cloud. *IEEE Syst. J.* **2022**, *17*, 2445–2454. [CrossRef]
279. Dhirani, L.L.; Mukhtiar, N.; Chowdhry, B.S.; Newe, T. Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors* **2023**, *23*, 1151. [CrossRef]
280. Abdulkareem, N.M. The Economic and Environmental Impact of Sustainable Enterprise Systems: Integrating Cloud, Web Technology, Attacks, AI, IoT, and Security. *J. Inf. Technol. Inform.* **2024**, 3.
281. Gopinath, V.; Rao, K.V.; Rao, S.K. A comprehensive analysis of IoT security towards providing a cost-effective solution: a layered approach. *Int. J. Inf. Technol.* **2023**, *15*, 3813–3826. [CrossRef]
282. Choo, K.K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Comput. Secur.* **2021**, *102*, 102136. [CrossRef]
283. Chiara, P.G. The IoT and the new EU cybersecurity regulatory landscape. *Int. Rev. Law, Comput. Technol.* **2022**, *36*, 118–137. [CrossRef]
284. Zikria, Y.B.; Ali, R.; Afzal, M.K.; Kim, S.W. Next-generation internet of things (iot): Opportunities, challenges, and solutions. *Sensors* **2021**, *21*, 1174. [CrossRef] [PubMed]
285. Alajlan, R.; Alhumam, N.; Frikha, M. Cybersecurity for blockchain-based IoT systems: a review. *Appl. Sci.* **2023**, *13*, 7432. [CrossRef]
286. Ding, S.; Tukker, A.; Ward, H. Opportunities and risks of internet of things (IoT) technologies for circular business models: A literature review. *J. Environ. Manag.* **2023**, *336*, 117662. [CrossRef] [PubMed]
287. Wessels, M.; van den Brink, P.; Verburgh, T.; Cadet, B.; van Ruijven, T. Understanding incentives for cybersecurity investments: Development and application of a typology. *Digit. Bus.* **2021**, *1*, 100014. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.