A Cross-Layer Secure and Energy-Efficient Framework for Internet of Things: A Comprehensive Survey

Rashid Mustafa , Nurul I. Sarkar * , Mahsa Mohaghegh , Shahbaz Pervez

Posted Date: 8 October 2024

doi: 10.20944/preprints202410.0518.v1

Keywords: Cross-layer Framework; Internet of Things; Secure IoT; General Data Protection Regulation; Energy Efficient

Article

A Cross-Layer Secure and Energy-Efficient Framework for Internet of Things: A Comprehensive Survey

Rashid Mustafa [1], Nurul I. Sarkar [1,*], Mahsa Mohaghegh [1] and Shahbaz Pervez [2]

[1] Department of Computer Science and Software Engineering, Auckland University of Technology, Auckland 1010, New Zealand
[2] Whitecliffe College, New Zealand
* Correspondence: nurul.sarkar@aut.ac.nz

Abstract: This survey delves into cross layer energy-efficient solutions and cutting-edge security measures for Internet of Things (IoT) networks. The conventional security techniques are considered inadequate, leading to the suggestion of AI-powered intrusion detection systems and novel strategies such as blockchain integration. In this paper, we provide a comprehensive review and analysis of secure and energy efficient cross-layer framework for IoT. We highlight the significance of developing IoT security for robust and sustainable connected systems. We discuss multi-layered security approaches and ways to enhance energy efficiency of resource-constrained devices in IoT networks. Finally, we identify open research issues and future research directions in the emerging field of cross-layer design for secure and energy efficient IoT networks. We expect this study will stimulate further research endeavors to build a secure and energy-efficient framework for next-generation IoT systems.

Keywords: cross-layer framework; internet of things; secure IoT; general data protection regulation; energy efficient

1. Introduction

The Internet of Things (IoT) has experienced exponential growth, bringing with it a new era of connectedness and altering our interactions with the surrounding environment. The IoT has an impact on a variety of industries, including healthcare, industrial applications, smart cities, and precision agriculture. But the development of networked devices has also presented several serious difficulties, the most important of which are related to the security and energy efficiency of these systems. We take inspiration for our journey to investigate and resolve these complex issues from an extensive analysis of recent studies conducted in the area. In this paper, we address the following research question: What is an IoT secure and energy efficient cross-layer framework that has been analysed and surveyed? The cross-layer framework for secure and energy-efficient IoT integration incorporates many security mechanisms at different IoT architecture layers while optimizing energy usage. It has been analysed and surveyed. This framework seeks to ensure effective resource use while addressing cybersecurity threats related to Internet of Things devices. It includes energy-efficient routing algorithms and communication protocols in addition to techniques like encryption, authentication, and intrusion detection at various IoT stack tiers. This framework offers a complete approach to IoT security and energy efficiency through thorough analysis and surveying, offering a strong foundation for building and managing IoT devices in a sustainable and secure manner. The availability and privacy of the network layer have become major concerns in recent years, leading to creative methods to prevent attacks and secure critical data [1]. An improved Intrusion Detection System (IDS) has been presented to address contemporary security and privacy challenges by utilising intelligent architectural frameworks. In the fight for IoT security, these intelligent solutions have emerged as a ray of hope, and our project is motivated by these innovative advancements. At the same time, we turn our attention to the physical-layer, also known as the perception-layer, where basic security protocols are essential [2]. The physical foundation of the environment is significantly shaped by the Internet of Things. (See Figure 2). The insights provided by this study regarding the significance of the physical layer are highly relevant to our research aims as we delve deeper into the nuances of IoT security. Additionally, we use a proactive approach, similar to the idea of ongoing active testing and monitoring of the IoT

 doi:10.20944/preprints202410.0518.v1

ecosystem, which is supported in [3]. Cities, businesses, and everyday life are all undergoing radical change as a result of the IoT exponential growth. But plenty of difficulties, such as network design complexity, privacy issues, energy efficiency problems, and security vulnerabilities, come along with this expansion of linked devices. This introduction gives a summary of recent research addressing cross-layer energy efficient framework with security measures in IoT.

1.1. Research Challenges

In this survey paper, we addressed the following research questions/challenges.

Question-01) What secure protocol can be developed to enhance the security aspect of the proposed IoT framework?

We tested and mitigated Man in the Middle (MitM), Eavesdropping, and data manipulation attacks and weaknesses of Application Layer by comparing real world data acquired by Contiki with the Cooja 2.7 Virtual IoT Simulator. Since technology has advanced, network segmentation and regular firmware updates are necessary in addition to establishing Transport Layer Security (TLS) with the COAP protocol, which is tested for robust security. virtual information. With this method, sensor behavior in controlled environments was simulated using the dedicated Contiki simulator. In particular, we looked at application, network, and sensor layer architecture in order to get insight into the accuracy and dependability of sensor networks. Our research clarifies the alignment or discrepancies between the two datasets by comparing real sensor data with simulated outcomes. This comparison study provides important insights for improving the security and dependability of sensor networks in a range of architectural contexts by illuminating how effectively these networks function in real-world situations.

Question-02) What energy-efficient protocol can be developed to enhance the energy efficiency aspect of the proposed IoT framework?

We looked into how sensors are used in relation to the Internet of Things as a whole and how smart buildings, smart homes, and smart cities are being developed. We evaluated and assessed the energy efficiency of the Contiki and Cooja 2.7 Virtual IoT Simulator when used with LEACH, RPL, and ContikiMAC protocols through real-world monitoring and simulated data creation. Because the results provide a thorough understanding of how these simulated networks function in application, network, and sensor layer architecture, they improve environmental surveillance, energy conservation, and overall building efficiency. Implications of this research go beyond improving living and working environments; it may also have an impact on the creation of IoT-driven technologies, offering concrete advantages for enhancing environmental sustainability and constructing energy efficiency in developing IoT networks. Energy consumption is minimized by RPL through the use of objective functions that can prioritize energy-efficient paths and by minimizing the number of transmissions needed for routing. Additionally reducing control message overhead and supporting other energy-saving techniques, with the help of clustering nodes into groups and rotating cluster heads on a regular basis to balance the energy burden, the hierarchical protocol LEACH seeks to lower energy usage. ContikiMAC is a duty-cycling MAC protocol. Nodes can sleep for extended periods of time and only wake up infrequently to monitor activity because to this feature. Compared to previous objective functions, our suggested approach, which is injected into the Contiki Operating System's core, guarantees a higher level of service quality. The findings shown that the new goal function can maintain a packet delivery ratio of more than 97% regardless of density, reduces the network's average power consumption by about 46%, and reduces latency and convergence times.

To make a suggested layered architecture more energy-efficient, various cross-layer routing protocols can be created. One strategy is to consider how layers interact and base routing choices on both network and physical layer characteristics. Using routing selection, recommended to choose the best routes that maintain network performance while consuming the least amount of energy possible. Utilizing reinforcement learning strategies to improve routing choices is another strategy. We may gain knowledge from the past to improve routing decisions in the future. This method can also consider

 doi:10.20944/preprints202410.0518.v1

other performance indicators, such as energy usage. In general, considering how layers interact while optimizing routing choices based on both network and physical layer characteristics is the key to creating an energy-efficient cross-layer routing protocol. By doing this, network performance can be preserved while energy consumption is decreased. Cross-Layer Framework refers to a system or set of protocols and strategies that operate across multiple layers of the IoT architecture. In traditional layered architectures, each layer operates somewhat independently, but in a cross-layer framework, there is communication and coordination between these layers to achieve specific goals. The primary objective of this framework is to conserve energy within the IoT system. Energy efficiency is crucial because many IoT devices, especially sensors, often operate on battery power. By optimizing energy usage, the devices can function for longer periods without frequent battery replacements or recharging. IoT systems are typically organized into layers, including the application layer (where data processing and user interaction occur), the network layer (which handles communication and data routing), and the sensor layer (where data is collected from the physical environment). The question focuses on improving energy efficiency across all these layers. So, in essence, the question is inquiring about the strategies, protocols, and mechanisms that can be employed to create a cross-layer framework capable of reducing energy consumption across the entire IoT system, from the application layer's data processing to the network layer's data transmission and the energy-hungry sensor layer's data collection. This framework should aim to optimize energy use without compromising the functionality and effectiveness of the IoT application. Complexity arises when integrating a cross-layer authentication system across various IoT networks and devices. Implementation problems include ensuring smooth compatibility and interoperability while upholding security standards throughout the many tiers of the IoT ecosystem.

1.2. Research Contribution

Highlighted below are this paper's primary contributions. Regarding secure and energy-efficient cross-layer frameworks for IoT networks, we conduct a critical analysis and survey of over 100 published research articles that we have chosen from academic journals and conference proceedings.

We categorize the current body of research on the cross-layer framework for Internet of Things that is both secure and energy-efficient according to its independent characteristics. To achieve this, we concentrate on an examination of the routing and multiple access protocols, network resource management, and energy efficiency of Internet of Things networks. A substantial amount of work has gone into the creation and implementation of the next-generation autonomous cross-layer framework that is secure and energy-efficient.

We list and talk about areas that need more research, such as the coverage of cross-layer secure and energy-efficient Internet of Things networks, IoT Layered Architecture, quality standards, industrial internet of things, mac routing, cross-layer energy-efficient framework, and energy-efficient lightweight protocols.

1.3. Summary of Existing Surveys

The fields of Internet of Things (IoT) and Cyber-Physical Systems (CPS) are explored in the studied literature, emphasizing the shortcomings of conventional security techniques in dealing with the dynamic issues in these areas. The research highlights the necessity for intelligent systems like AI-driven Intrusion Detection Systems (IDS) for continuous monitoring and adaptability to emerging threats, while traditional security relies on established protocols and perimeter defence. It also explores areas that are frequently missed by conventional approaches, such as multi-layer privacy, cross-layer strategies, and cutting-edge technologies like blockchain, to improve security. Furthermore, the literature presents approaches for risk identification and mitigation, broadening its scope to include cyber-physical systems. Environments related to Industry 4.0 are studied, emphasizing the necessity of thorough risk assessments at several levels. The paper also highlights the significance of strong security solutions for industrial networks and smart cities, including contemporary methods such as

 doi:10.20944/preprints202410.0518.v1

encrypted communication, machine learning-based threat detection, and authentication. The study also looks at issues with energy efficiency in Internet of Things networks and suggests solutions like better node location and routing. The literature emphasizes the need for energy-efficient [13] solutions to ensure the sustainability and dependability of IoT operations in our increasingly digitalized world, as well as the significance of developing IoT security technologies to address evolving threats and challenges efficiently. To defend against cyber-attacks, it also suggests next-generation cyber security designs and emphasizes the significance of industrial IoT security. The evaluation also touches on the deployment of remote monitoring and control systems in many industries, stressing the need for strong encryption and authentication methods. It also discusses issues surrounding smart city challenges and solutions, stressing the significance of data privacy protection via authentication and encryption techniques. Issues related to energy efficiency in Internet of Things devices and networks are also covered, and strategies for cross-layer optimization and energy-efficient routing are suggested as solutions. The literature analysis, in summary (See Table 1), offers a thorough overview of IoT security and highlights the necessity of developing security technologies to counteract changing risks and difficulties in the IoT environment.

1.4. Structure of this Paper

The structure and organization of the paper are shown in Figure 1. Section 1 covers the questions and challenges introduction. Additionally, the research contributions related to a cross-layer architecture that is both secure and energy-efficient are analyzed. Additionally, summary of existing survey, structure of this paper, cross-layer framework and IoT Network Design are provided. IoT security measures and energy effectiveness are covered in Section 2. The autonomous, secure, and energy-efficient cross-layer structure was also covered.Moreover, IoT layered architecture, trustworthy quality standards, industrial IIoT, MAC routing and energy-efficient cross-layer design were taken into consideration.

Section 3, "Key Strategies and Trends" identifies the following subjects as key strategies: Authentication and Encryption, Machine Learning for Threat Detection, Cross-Layer Security Framework, and Energy-Efficient Routing-Optimization. Furthermore, the Integration of Artificial Intelligence, Cognitive Radio for Spectrum Efficiency, Renewable Energy Integration, Holistic Security Approaches, and Cross-Layer Optimization are Emerging Trends. Open Research Areas and Challenges are identified in Section 4, along with a description of the challenges in EE and the secure cross-layer framework. The paper's main conclusions and future contributions are outlined in Section 5's Conclusion (Figure 1)

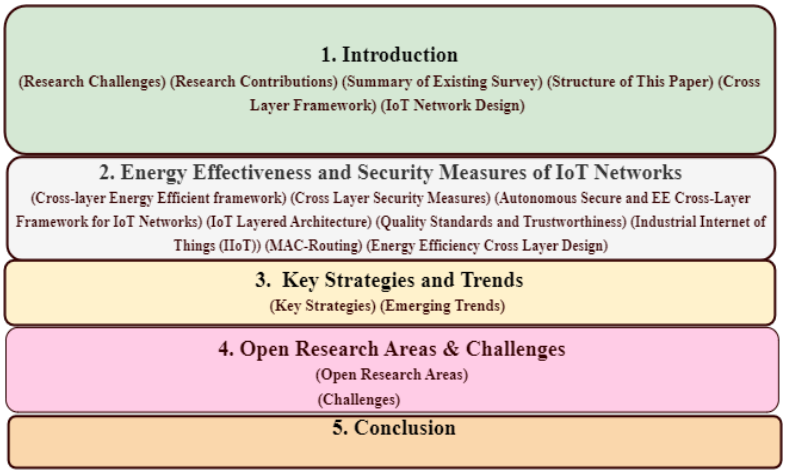

Figure 1. Main Structure Of Survey Paper.

 doi:10.20944/preprints202410.0518.v1

Table 1. Summary of Existing Relevant Survey.

Key Ideas	Survey Scope	Cross-Layer Inspired?	Challenges	References
LPWANs like LoRaWAN in IoT: Challenges and Cross-Layer Optimization, Cognitive Radio, EE Multi-Channel Cross-Layer MAC Framework	6G, LoRaWAN in IoT, CSMA Protocols, 6G Communication, EE in IoT Networks, CSMA Protocols	Yes	Protocol optimization, data rate, duty cycle, Massive connectivity Requirement, Energy Constraint	[4]
Cyber-physical systems: Testing platforms and vulnerability modelling, Combining Exposure Indicators and Predictive Analytics, Internal Assessment and Evaluation, H2020 ECHO Project Implementation,	Cyber-physical systems, Exposure Indicators and Predictive Analytics, Privacy-Preserving Evaluation, Cybersecurity Information Sharing	No	Data security, vulnerability modelling, Gaps Between Exposure Indicators and Predictive Analytics, Sensitive Information Protection, Trust and Transparency Among Stakeholders	[5]
Social Internet of Things (SIoT) Security, CPS in Industry, Hybrid Risk Identification Methodology, Four-Step Risk Identification Process,	SIoT security, Risk Identification in Industry, CPS Interactions, Risk Management Standards and Frameworks	Yes	Security, energy efficiency, graph-powered learning, Comprehensive Risk Identification, Complexity of CPS Interconnections, Redundancy of Risks	[6]
IoT Security Challenges and Solutions, Flying Ad Hoc Networks Challenges, Energy-Aware Routing Scheme, Path Selection Metrics, Performance Evaluation	IoT security challenges, Routing Algorithms in FANETs, Virtual Relay Tunnel (VRT) Concept, Comparison of Routing Schemes	No	Security vulnerabilities, cryptographic protocols, Dynamic Topology and High Mobility, Energy Restrictions, Efficient Path Selection	[7]
Smart City Concept, Smart City Security and Privacy: Suggested Solutions Using Blockchain and Encryption, Blockchain for Security	Adaptive cybersecurity, IoT and Cloud-based Security Issues, Data Privacy and Security Solutions, Smart City Data Management	No	Real-world network packet collection, machine learning, Resource Optimization vs. Security, Decentralized and Distributed Structure, Implementing Blockchain	[8]
Comprehensive Overview of IoT Security, Rapid Growth of IoT, IoT Security Concerns, Case Study on Camera-based IoT, Importance of Privacy and Stakeholder Roles	IoT security overview, IoT Overview and Security, Threat Analysis for Smart Camera Systems (SCS), IoT Security and Privacy	No	IoT development, security solutions, Complexity of IoT Security, Vulnerabilities in IoT Applications, Stakeholder Responsibility	[9]
NOMA-based-MIoT Communication System, 5G Technology in MIoT, NOMA-based Heterogeneous Communication System, Energy Efficiency (EE) Optimization, Iterative Approach for Optimization	MIoT Networks, MIoT communication, Energy Efficiency in MIoT, Optimization Techniques, Handling uncertain channel state Information	Yes	Energy efficiency, spectrum consumption, Complexity of Optimization, Inadequate Channel State Information, Balancing Constraints, Quality of Service	[10]
Energy-efficient Routing for Smart Dust Head Networks, Challenges with Movable Smart Dust Basestation, Flooding Approach, EE Routing Mechanism, Fuzzy Clustering and Optimization	Smart Dust energy-efficient routing, Movable BS Positioning, Routing Architectures, Optimization Techniques	No	Energy-efficient routing, network performance, High Power Usage, Network Stability, Efficient Routing	[11]
Cognitive Radio Technology for Energy-efficient IoT, IoT and Spectrum Demand, Cognitive Radio (CR) Technology, Efficient Communication Protocols, Cross-Layer Design Proposal	CR Technology for IoT, Cross-Layer Optimization, Simulation and Performance Evaluation	Yes	Spectrum optimization, Spectrum Utilization, Energy Efficiency, Network Adaptation	[12]

 doi:10.20944/preprints202410.0518.v1

1.5. Cross Layer Framework

The application layer, network layer, and sensor layer are the three basic layers that make up the Internet of Things Network Architecture. Energy-efficient and security-related components are shown at each layer. Security features like authentication and encryption are part of the Application Layer, along with energy-efficient application protocols like Message Queueing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP). The Network Layer incorporates machine learning-based security solutions like Intrusion Detection Systems and middleware security frameworks. This Layer also encompasses cross-layer security frameworks and energy-efficient routing algorithms, such as those designed for Low Power and Lossy Networks (See Figure 2). The Sensor Layer addresses IoT device security with device-level encryption and authentication, along with energy-efficient hardware design considerations. This hierarchical diagram provides a structured overview of how various components contribute to ensuring both security and energy efficiency within IoT networks, as indicated by the literature.

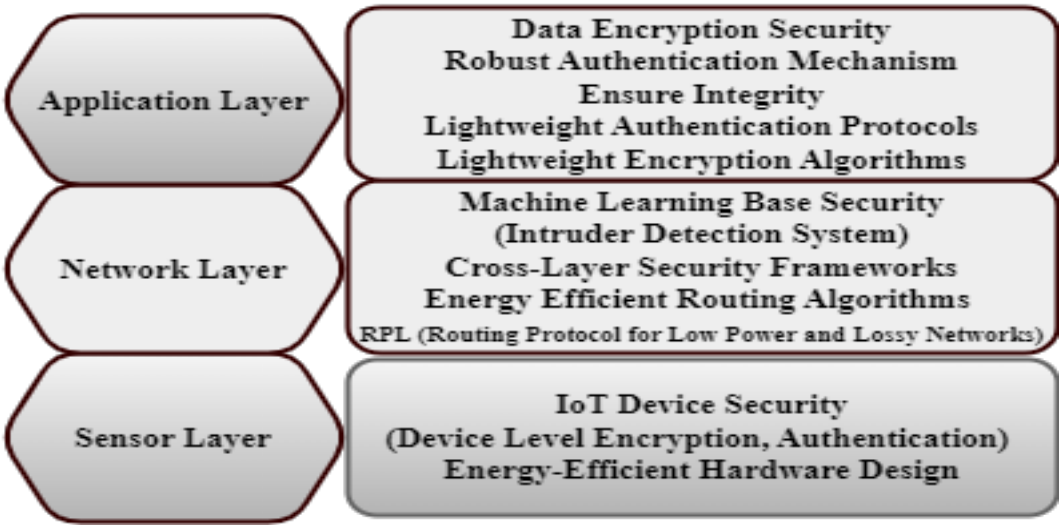

Figure 2. An overview of IoT Cross-Layer Framework.

1.6. IoT Network Design

Moreover, the performance and scalability of Internet of Things systems are significantly influenced by network design. Cross-layer optimization, in which several network stack layers are coordinated to achieve optimal resource allocation, traffic management, and quality of service, has been emphasized in recent research as being important. Researchers want to address the dynamic nature of IoT environments and accommodate a wide range of applications with different requirements by taking a comprehensive approach to network design [14]. In conclusion, the integration of AI-based analysis, the significance of network design considerations, the search of energy-effective solutions, and the importance of security and privacy safeguards are all highlighted in recent literature on IoT development. Researchers hope to solve these major issues to fully realize the promise of IoT technology and open the door to a more intelligent, sustainable, and networked future.

2. Energy Effectiveness and Security Measures of IoT Networks

2.1. Cross-Layer Energy Efficient Framework

Energy efficiency is a crucial consideration for Internet of Things installations, especially because IoT devices are resource-constrained and rely heavily depends on battery power and necessitates energy efficiency to preserve battery life. According to the literature review, routing algorithms, optimization techniques, and energy-efficient protocols are crucial elements of long-term, sustainable Internet of things networks. In security implementations, low-power authentication protocols and

 doi:10.20944/preprints202410.0518.v1

lightweight cryptographic algorithms are suggested to reduce computational overhead and energy consumption. In addition, energy-conscious routing plans and optimization techniques maximize the use of network resources, extending the life of Internet of Things devices and lowering their total energy usage (See Figure 3). A collection of low-power, long-range wireless technologies known as LPWAN are intended to support Internet of Things applications that need to be connected over wide geographic areas. Long Range Wide Area Network, or LoRaWAN,is a popular LPWAN technology that offers low data rates and low power consumption long-range communication. It operates in unlicensed frequency bands. Sigfox: Another LPWAN technology that offers long-range, low-power communication for Internet of Things devices, Sigfox uses ultra-narrowband modulation and operates in licensed spectrum. Low-power, wide-area connectivity for IoT devices is made possible by cellular-based LPWAN technologies like LTE-M and NB-IoT (Narrowband IoT), which take advantage of the current cellular infrastructure.

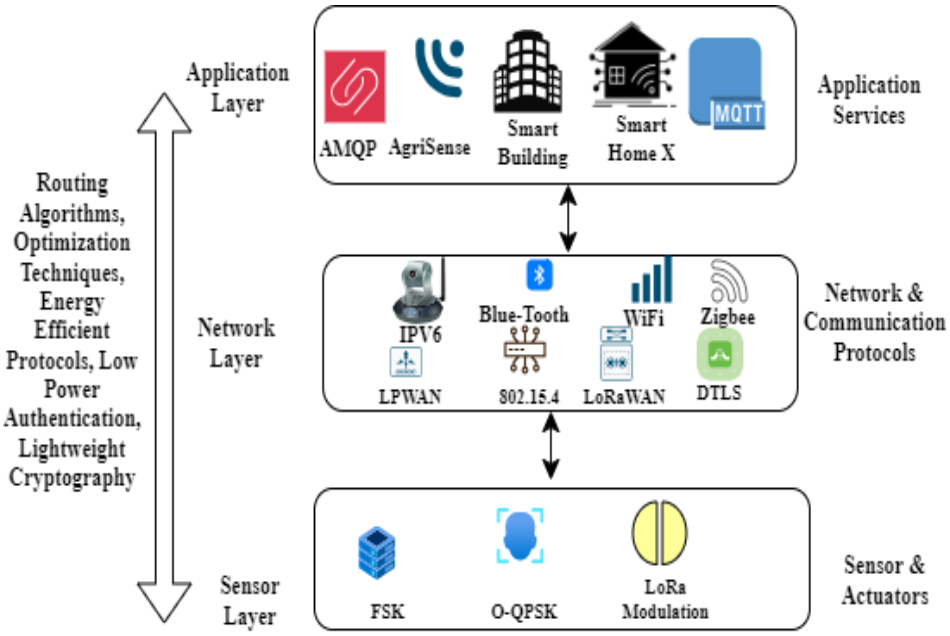

Figure 3. Energy efficient Next-Gen Energy Efficient Architecture.

The main ideas and takeaways from the survey papers are included into this combined introduction of energy effective cross layer IoT networks, which offers a thorough synopsis of the goals and focus of the research (See Table 2 below).

2.2. Cross Layer Security Measures

Numerous security issues, such as flaws in sensor hardware, cloud computing platforms, and network communication protocols, are highlighted in the literature analysis as being present in IoT ecosystems. Several cybersecurity techniques [15], including intrusion detection systems, authentication procedures, and encryption, are suggested as solutions to these problems. To effectively counteract complex cyber threats, cross-layer security strategies that integrate network, application, and physical layer defences are recommended. The resilience of IoT systems against new cyber-attacks is also improved by developments in AI and machine learning, which make it possible to detect and respond to threats with greater sophistication (See Figure 4). For the application layer, it is advised to use Constrained Application Protocol (COAP), Message Queuing Telemetry Transport (MQTT), and Hypertext Transfer Protocol Secure (HTTPS). Recommendations for network layer security include Media Access Control Security (MACsec), IEEE 802.1X, Virtual Private Network (VPN), and Internet Protocol Security (IPsec). Environmental protection, training, physical security policies, secure enclosures, and physical temperature resistance are advised for the sensor layer.

 doi:10.20944/preprints202410.0518.v1

Table 2. Summary of Literature Review on Energy Efficient Cross-Layer Contributions.

Key Contributions	Performance Evaluation Methods	Limitations	References
Enhanced LoRaWAN for IoT applications,Cross-Layer Optimization Overview, Classification of Techniques, Identification of Issues and Challenges, Performance Overview	State-of-the-Art Summary, Cross-Layer Optimisation of LoRaWAN, Overview of Challenges of LoRaWAN	Lack of empirical validation, Lack of Summary, Protocol Stack Restrictions, Optimization Gaps	[16]
Designed energy-efficient MAC solution for NB-IoT, Energy-Efficient MAC Layer Solution, Optimization Framework, Cross-Layer Approach, Probabilistic Sleep Scheduling	MINLP optimization; Lyapunov optimization, Distributed sleep scheduling, Simulation Results, High Traffic Load Testing	Reliance on simulation, Resource Constraints, Traffic Model Assumptions, Scalability	[17]
Integrated energy-efficient OF into RPL routing, Introduction of ELITE, New Routing Metric, Cross-Layer Integration, Path Selection Improvement	Energy-efficient cross-layer OF integration, RPL protocol, Comparison with Existing OFs, Simulation Results	Limited evaluation in diverse IoT environments, potential complexity in implementation, MAC Layer Dependency, Metric Specificity, Generalizability	[18]
Enhance HCN energy efficiency with NOMA, Focus on Energy Efficiency, Optimization Problem Formulation, Introduction of Quantum-inspired political optimizer(QPO) Algorithm	Hybrid resource allocation optimization, Simulation Results(Evaluation of the QPO algorithm's performance)	Reliance on simulated comparisons, potential challenges in real-world deployment, Non-Convex Problem Complexity, Algorithm Specific	[19]
Optimized routing for energy efficiency in FANETs, Virtual relay tunnel based on a suggested energy-conscious routing strategy (ECRS), Incorporation of Multiple Metrics, Path Correlation Metric (enhance route selection)	Energy-aware routing with virtual relay tunnel, comparison against existing methods, Comparative Analysis, Simulation Studies	Limited real-world validation; potential trade-offs between efficiency and longevity, Specificity to FANETs, Complexity in Path Selection, Comparative Scope	[20]
Investigated energy management in edge computing, Energy-Efficient Secure Data Transmission, Multi-Scale Grasshopper Optimization, Robust Multi-Cascaded CNN (RMC-CNN), Dynamic Honey Pot Encryption Algorithm	Cross-layer energy optimization, Comparison with Existing Techniques, Encryption and Decryption Time Analysis,	Lack of empirical validation; potential complexity in cross-layer management, Specific Dataset Focus, Complexity of Encryption and Detection Mechanisms, Scalability and Real-Time Constraints	[21]
Developed energy-efficient MAC for CR-enabled 6G-IoT, Joint Adaptation of Physical and MAC Layer Parameters, Per-Bit Energy Efficiency Maximization	Multi-channel MAC design, Numerical Results	Reliance on simulations; potential challenges in real-world deployment, Specific to Non-Persistent CSMA, Simulation-Based Evaluation, Design Constraints in 6G-IoT, Design Constraints in 6G-IoT	[4]
Integrated energy-efficient protocols into IoT, Cross-Layer Energy Architecture Model, Focus on Green and Renewable Energy, Mathematical Modeling	Utilization of MQTT, CoAP, Zigbee, Wi-Fi for energy efficiency; support for various IoT applications, Mathematical Analysis, Power Savings Estimation,	Lack of empirical validation, Limited Exploration of Practical Implementation, Focus on Theoretical Framework, Scalability and Applicability	[22]
Investigated energy efficiency, Thorough Review of IoT for EE, Identification of Common Design Factors, Future Research Directions	Examination of hardware, software for energy management, use of historical data for forecasting, Review and Analysis, Identification of Patterns	Lack of real-world validation, Lack of Original Empirical Data, Application-Specific Variables, Focus on Heating Systems	[23]

 doi:10.20944/preprints202410.0518.v1

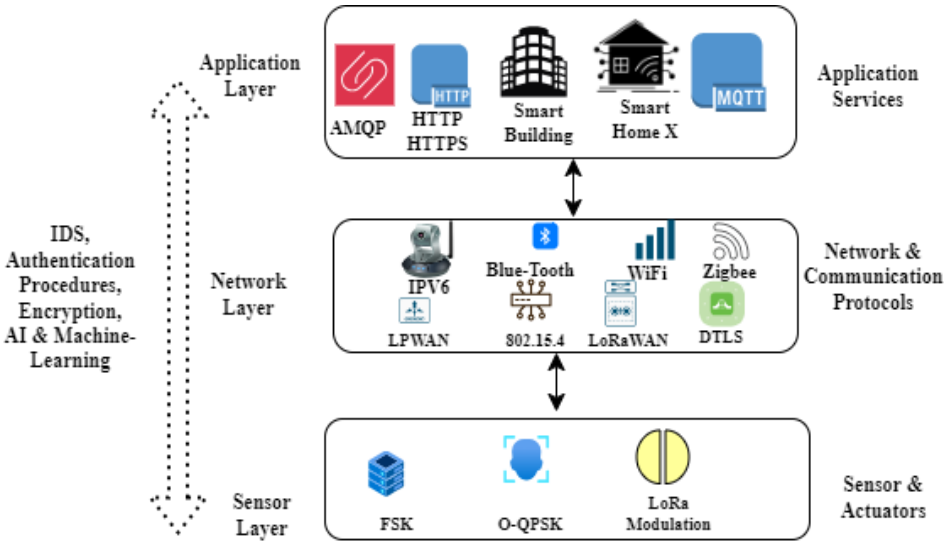

Figure 4. Cross-Layer Security Measures.

The main ideas and takeaways from the survey papers are included into this combined introduction of a secure cross layer IoT networks, which offers a thorough synopsis of the goals and focus of the research (See Table 3 below).

2.3. Autonomous Secure and Energy Efficient Cross-Layer Framework for IoT Networks

Given the growing sophistication of cyber-attacks, the examined literature emphasizes the urgent necessity for strong security measures in IoT systems. To overcome these obstacles, autonomous characteristics must be integrated into a cross-layer framework. The main independent characteristics that can be included in such a framework are as follows:

(a) **Security Management and AI Integration in IoT** Utilizing agentless SIEM modules, such as the Wazuh module, enhances IoT network security by analysing device traffic and creating alerts for anomalies without requiring endpoint software. This approach successfully protects industrial control systems in Industry 4.0 settings, as demonstrated using the SWaT dataset [24]. The integration of IoT with AI enables continuous data collection and opens new commercial opportunities through intelligent decision-making. Businesses can leverage AI to analyse IoT data with minimal human intervention, enhancing competitiveness [25]. Implementing federated learning models combined with host and network intrusion detection systems within fog computing environments significantly enhances DDoS attack detection and mitigation. This decentralized approach enhances security and lowers the possibility of single points of failure, achieving 89.753% detection accuracy [26]. utilizing machine learning techniques to identify denial-of-service attacks, such as support vector machines, random forests, and K nearest neighbours in IoT networks demonstrates strong detection capabilities, particularly in Information-Centric Networks (ICNs) [27].

(b) **Advanced Protocols and Network Integration** Utilizing PCC-RPL and SLF-RPL frameworks improves the security of the RPL protocol in IoT networks by reducing wormhole attacks. SLF-RPL shows better energy efficiency, lower packet loss, and higher attack detection rates compared to PCC-RPL [28]. Integrating Software-Defined Networking (SDN) with Recursive Internetwork Architecture (RINA) enhances IoT network security, flexibility, and scalability. This method facilitates seamless edge-to-cloud connectivity and network function data sharing while maintaining operational integrity [29]. Developing secure, lightweight authentication strategies for low-power IoT devices ensures data privacy and user authentication, which is crucial for applications like Industry 4.0, smart cities, and healthcare [30]. Utilizing learning automata and

 doi:10.20944/preprints202410.0518.v1

clustering, this protocol enhances network performance in UV networks by optimizing cluster node count, service class, and network topology.

(c) **IoT Integration in Smart Cities and Healthcare** Exploring the impact of network softwarization in the industrial sector, this study emphasizes how AI and IoT will play a part in mobile networks in the future., identifying gaps and suggesting areas for further research [31]. The integration of IoT, smart cities, and 5G technology enhances urban living by improving sustainability, efficiency, and responsiveness to citizen demands, transforming urban landscapes [32]. Proposing a Semantic IoT Middleware (SIM) for the healthcare sector addresses data interoperability, heterogeneity, and security using blockchain and AI for optimization and security enhancement [33]. Addressing data security and privacy in E-healthcare applications, this study integrates blockchain with NuCypher encryption to enhance resource use, resilience, and traceability [34].

(d) **IoT Security in Industrial and Environmental Applications** Integrating Raspberry Pi clusters with BME680 sensors in Kubernetes for environmental monitoring, coupled with OpenID Connect and HashiCorp Vault for dynamic secret management, reduces vulnerabilities and improves responsiveness in IoT installations by 40% and 30%, respectively [35]. The LEMARS model combines heuristic-driven techniques and Feistel architecture to provide a lightweight encryption solution for secure satellite photography, demonstrating higher attack resilience and quality metrics [36]. Systematizing existing research on enhancing IoT resilience, this study proposes a taxonomy and classification of resilience mechanisms to address practical concerns in building reliable systems [37]. Examining static, dynamic, symbolic, and hybrid analysis techniques for finding vulnerabilities in embedded firmware, this overview suggests taxonomies and evaluates these approaches for future research [38].

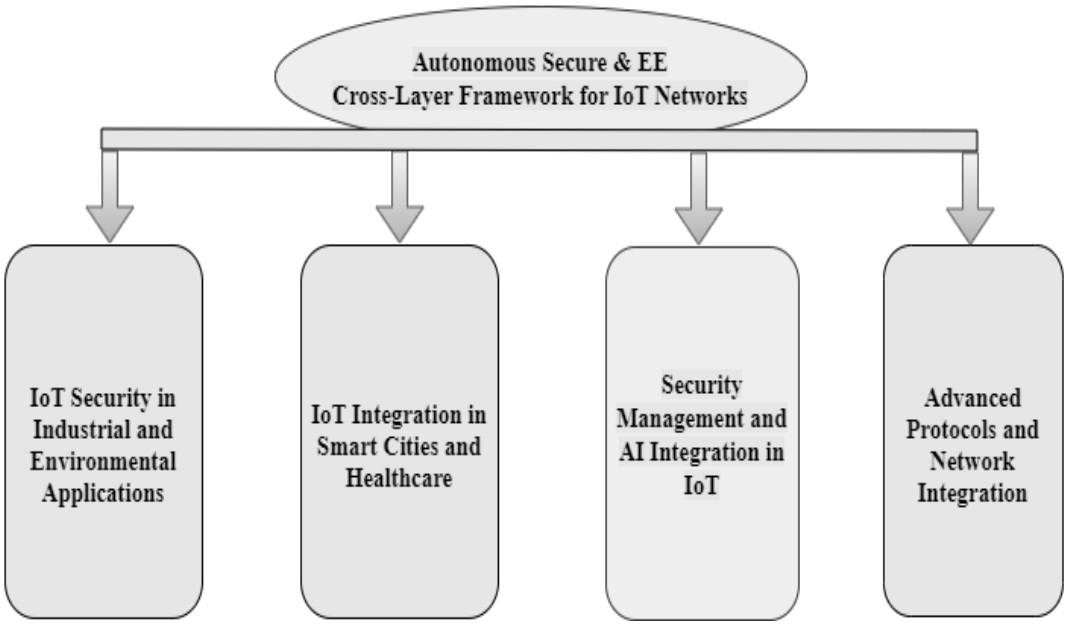

Figure 5. Autonomous Secure and EE Cross-Layer Framework for IoT Network.

 doi:10.20944/preprints202410.0518.v1

Table 3. Summary of literature review on Security measures.

Key Contributions	Limitations	Security Measures?	References
Cross-layer security and privacy were designed, Integration of IoT technologies with AI for security, Adoption of blockchain for decentralized coordination, Multidisciplinary approaches to ensure IoT security	Application layer security has not been explored, Resource constraints, Privacy concerns, Security issues, Lack of training data, Centralized architecture limitations	AI-based real-time data analysis, Blockchain for secure resource and data sharing, Addressing IoT and WSNs security threats dynamically	[39]
Presented various IoT framework tiers,Development of model to mitigate DDoS attacks in local networks, Utilization of Host Intrusion Detection Systems, Integration of Network Intrusion Detection System with federated learning	Think about tiered communication alone, Privacy concerns in decentralized IoT infrastructure, Potential for increased complexity in federated training/detection, Possible challenges in real-time and precise attack detection	Use of HIDS and NIDS for comprehensive attack identification, Federated learning data analysis/anomaly detection, Distributed architecture to prevent volumetric attack traffic, Near-real-time detection in fog Computing	[40]
Systematic literature review (SLR) on AI methods for IoT cybersecurity, investigation of machine learning and deep learning methods for IoT security, Finding popular techniques for high accuracy detection, such as random forests (RF) and support vector machines (SVM)	Framework for detecting intrusions at the network layer, Lacks a cross-layer strategy, Existing security and privacy challenges despite AI advancements, Need for intelligent architectural frameworks for better intrusion detection	Artificial intelligence (AI) techniques are utilized to secure Internet of Things devices. applying AI methods to identify cybersecurity threats, intelligent intrusion detection systems (IDS) with frameworks based on AI, Examination of AI techniques based on attack categories	[1]
At the most basic level of security, perception, the physical layer, and the wireless network layer were considered, Proposal of a global perspective security framework for PIoT, Focus on security issues in the perception layer of PIoT, Development of security policies and countermeasures for PIoT, Application of research results in real-world projects	Complexity of securing a large, complex cyber-physical network like PIoT, Potential challenges in implementing the proposed security framework across all layers, Complexity of securing a large, complex cyber-physical network like PIoT, Potential challenges in implementing the proposed security framework across all layers	The deployment of the autonomous safety system. security audits, residual information protection, intrusion prevention, and data backup, systems, Security framework spanning from perception layer to application layer, Specific security policies and countermeasures for addressing PIoT security issues	[2]
Discussion of existing vulnerabilities and attacks in the IoT ecosystem, Testing secure framework for IoT applications, Framework evaluates IoT applications from the initial phase	Complexity of securing IoT applications,Potential challenges in implementing comprehensive monitoring and security testing.	Monitoring and security testing framework and evaluate IoT applications, Focus on addressing security issues from the early stages of IoT application development	[3]
Examination of communication standards (ITU-T), Discussion of 4-levels of IoT security gateways, Overview of testing methods for IoT devices	Potential complexity in securing diverse communication standards, Challenges in applying uniform security measures across different levels	Identification of 4-levels of security in IoT systems, Application of security testing methods to evaluate IoT components and systems	[41]
Review of IoT threats, security requirements, challenges, Proposal of a novel paradigm combining IoT architecture with SDN, Discussion on SDN-based IoT deployment models	Challenges in unifying all IoT stakeholders on a single platform, Potential hurdles in implementing SDN-based security solutions across diverse IoT environments	Introduction of SDN-based IoT security solutions, Comprehensive overview of software-defined security (SDSec), Emphasis on network-based security solutions for the IoT paradigm	[42]
Analysis of IoT's impact across various domains, Discussion of Service Oriented Architecture model, Divided into application network and perception layers, Examination of IoT security attacks during COVID-19	Numerous privacy concerns in rapidly developing IoT environments, Increased security attacks on IoT devices, especially during the COVID-19	Security and privacy challenges in IoT based on SOA layers, Identification of different technologies used for communication in each IoT layer, Overview of attacks targeting specific SOA layers and IoT devices	[15]

 doi:10.20944/preprints202410.0518.v1

2.4. IoT Layered Architecture

Traditional security measures are often based on established principles and practices. In contrast, the above-mentioned research explores cutting-edge security measures for the rapidly evolving domains of IoT and Cyber-Physical Systems (CPS). Traditional security typically relies on known protocols and methods, whereas the research advocates for intelligent systems like AI-driven Intrusion Detection Systems (IDS) to monitor network integrity. While traditional security often focuses on perimeter defense and known vulnerabilities, the research emphasizes continuous monitoring and testing to adapt to emerging threats effectively. Moreover, traditional security may not be well-equipped to address the energy efficiency challenges of IoT networks, which the research explores extensively, offering strategies like optimized node placement and routing. The research also delves into multi-layer privacy, cross-layer techniques, and innovative technologies like blockchain to enhance security, areas that may not be covered comprehensively by traditional security measures. Furthermore, the research emphasizes the importance of deep learning and application-level security, as well as addressing specific challenges within IoT applications, healthcare, energy management, and efficient routing. It also investigates emerging standards, the role of software-defined security, location privacy in sensor networks, and cutting-edge research on Tactile Internet and 5G networks, which are areas less explored in traditional security approaches. A framework for threat detection of a real industrial network is presented using big data architecture and predictive analytics tools [5]. By obscuring sensitive data and private information, this framework was used to close gaps (See Figure 6), evaluate services and products on an internal level, and share results. Under the H2020 ECHO Project, a cutting-edge technological platform was created that will be used to exchange and assess cybersecurity data and foster greater trust among various stakeholders.

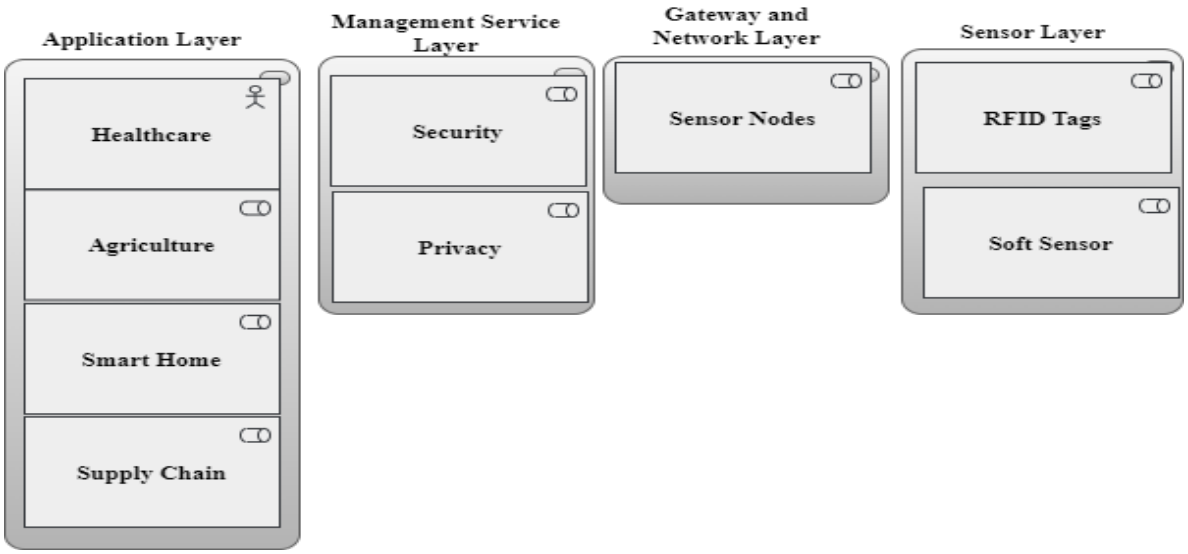

Figure 6. IoT Layered Architecture [5].

The review delves into LPWANs like LoRaWAN in IoT, highlighting their appeal for long-range, energy-efficient connectivity. Despite LoRaWAN's strengths, challenges persist, including protocol optimization, low data rates, and duty cycle restrictions. To tackle these, the paper proposes cross-layer optimization, allowing flexibility across protocol layers [16]. It identifies challenges and evaluates cross-layer optimization's performance in enhancing LoRaWAN for IoT applications.

While privilege escalation and malware infiltrations are security issues, the Internet of Things improves real-time communication. In order to safeguard IoT networks, this study suggests using an agentless Wazuh security information and event management (SIEM) module [24]. The IoT makes it possible to gather data continuously, and when it integrates with AI, it opens up new commercial options for more intelligent decision-making [25]. To be competitive, businesses need to leverage AI

 doi:10.20944/preprints202410.0518.v1

developments to analyse IoT data effectively with the least amount of human intervention. Due to its security flaws, the Internet of Things is vulnerable to DDoS attacks, which can seriously harm its finances [26]. In order to detect and mitigate DDoS attacks in corporate networks, This study uses infrastructure from Information-Centric Networks (ICNs) to address the problem of denial-of-service (DoS) assaults in Internet of Things networks. It suggests using machine learning (ML) to identify denial-of-service (DoS) assaults by contrasting different ML algorithms that perform better, such as support vector machine, random forest, and K nearest neighbour (KNN) [27]. Using the parental change control routing protocol for low power and lossy network (PCC-RPL) and subjective logical framework routing protocol for low power and lossy network (SLF-RPL) frameworks to reduce wormhole attacks, this study improves the security of the RPL protocol in Internet of Things networks [28]. In Contiki OS-based simulations with malicious nodes, subjective logic frame RPL surpasses PCC-RPL in terms of energy efficiency, packet loss, and attack detection. This study presents an integrated architecture that combines SDN with RINA to improve the security, flexibility, and scalability of Internet of Things networks [29]. This work focuses on hardware configuration and strong security benchmarks, integrating Raspberry Pi clusters and BME680 sensors in Kubernetes for sophisticated environmental monitoring [35]. By implementing OpenID Connect and HashiCorp Vault for dynamic secret management and authentication, it achieves 40% fewer vulnerabilities and 30% better responsiveness in Internet of Things installations. Secure device-to-device communication is required due to the growing need for IoT devices in applications such as Industry 4.0, smart cities, and healthcare. Considering the importance of IoT in daily life, data privacy and user authentication must be guaranteed [30]. In this research, a secure, lightweight authentication strategy for low-power IoT devices is proposed, and existing authentication strategies are reviewed. The influence of network softwarization on the industrial sector is the main subject of this survey, which examines the function of AI and IoT in future mobile networks [31]. The ways in which these technologies work in concert to improve a city's sustainability, efficiency, and ability to respond to the demands of its citizens are examined in this book [32]. These technologies are a transformative force that are changing urban landscapes. This study looks at the security void in IoT development and finds that business plans and configurations are not secure enough. In order to improve confidentiality, integrity, and availability while allowing for future developments, it suggests a dynamic security approach using strong IoT security architecture [33]. This survey proposed modern solutions like authentication, encrypted communication, and blockchain technology. It introduces novel approaches to threat detection in industrial networks and highlights data security challenges arising from the proliferation of IoT and smart devices. While traditional security approaches are fundamental, the research provides an in-depth, future-oriented exploration of security, and privacy in the dynamic landscape of IoT.

2.5. Quality Standards and Trustworthiness

Most of the discussion focused on the growth of IoT devices as well as cyber threats to sensor devices [43]. In addition, the cloud layer, application layer, and physical layer were all investigated. Vulnerabilities and attacks were examined, and cross-layer security was explained. A middleware security approach in the cloud and network, as well as a machine-learning algorithm for attack detection and prevention, are proposed. Cyber physical systems are made up of intelligent devices that are linked to computer systems and have many cyber vulnerabilities when connected to networks [6]. Many risk identification methodologies are considered, but none consider the interaction of cyber-physical devices. In the industry 4.0 environment, a gap in the literature has been identified. A four-step hybrid methodology is presented. In the first step, ISO 31000, PMBOK, and a risk model are used to identify risk. In the second step, a bottom-up HAZOP strategy is proposed. This physical layer-to-application layer risk analysis is performed. In the third step, the NIST strategy employed a top-down approach. In this step, the physical layer and lower layers of the cyber-physical system were considered. Finally, all risks are combined and analysed to reduce cyber-physical risk redundancy. The paper emphasizes how the Internet of Things (IoT) can be used for ubiquitous access and real-time

 doi:10.20944/preprints202410.0518.v1

analysis, which will enable the integration of IoT systems with social networks to create Social IoT (SIoT) [14]. Even though SIoT has advantages such improved data trustworthiness and network navigability, there are serious security issues that need to be resolved. Cross-layer security designs, striking a balance between security and energy efficiency, and utilizing graph-powered learning strategies from social networks are some of the suggested answers. This emphasizes how important it is to have strong security protocols and cutting-edge technology in place to protect SIoT ecosystems. The literature study discusses the security issues surrounding the Internet of Things, focusing on how vulnerable networked objects that exchange data over public networks are. It examines new cryptographic protocol standards created to protect Internet of Things communications and assesses how well they work in different application scenarios [44]. It also draws attention to current issues with cryptographic protocols, which is important for improving security in upcoming Internet of Things applications.

Experts in cybersecurity must constantly contend with emerging threats that take advantage of flaws in software. To fully realize the potential of IoT, knowledge sharing is essential in building collective resilience against security and privacy challenges associated to IoT [34]. This research highlights the necessity for strong IoT-Cyber Security deployment strategies in smart cities by identifying challenges and weaknesses in industries like healthcare and transportation (See Figure 7 below).

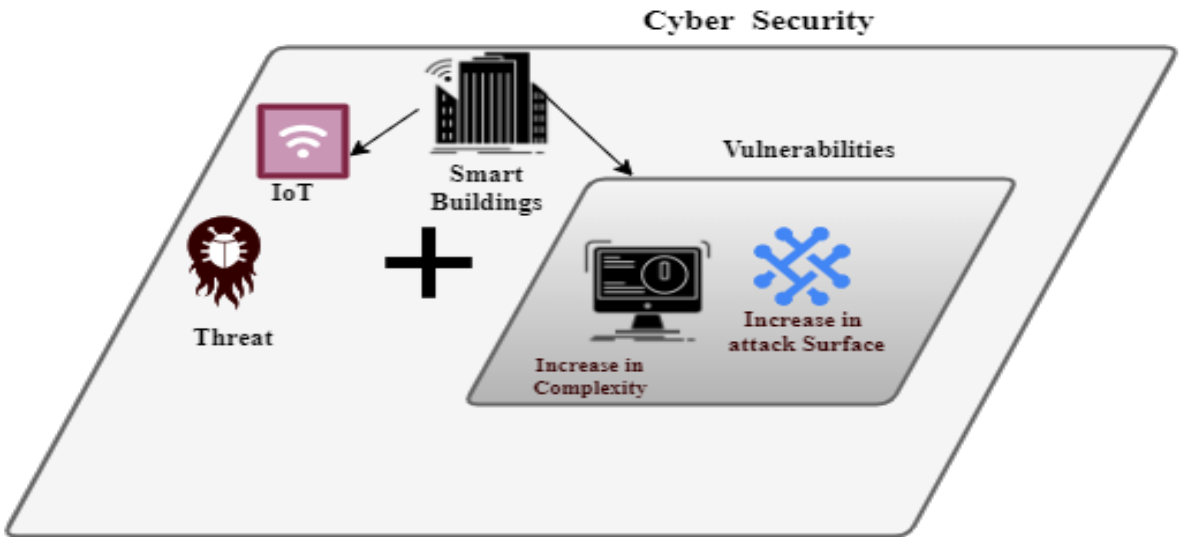

Figure 7. Main parameters of infrastructure risk in smart cities [34].

By integrating IoT, Blockchain, and artificial intelligence (AI), agricultural concerns such as water scarcity and seed quality can be tackled, potentially leading to future supremacy [45]. This study emphasizes seed quality and water management while utilizing blockchain and IoT for effective agricultural field monitoring. The Blockchain network improves communication reliability and performance evaluation in prototype design by securing data, promoting community trust, and supporting commercial solutions. In many industries with growing demand, communication technology are essential [36]. The LEMARS model combines heuristic-driven techniques and Feistel architecture to provide a lightweight encryption and attack-resistant steganography solution for safe satellite photography. Skill Optimization is used to cluster nodes, and Deep Q-Learning is used to compute trust [46]. The technique outperforms conventional protocols in simulations in detecting routing assaults such as Black Hole and Gray Hole. With the use of a blockchain-based control mechanism that combines software-defined network. This research tackles congestion in VANETs [47]. In simulations, the suggested approach, which targets connected cars and smart cities, achieves 82% and 98% dependability and efficiency while increasing throughput, packet delivery ratio, energy efficiency, and latency and routing overhead reduction. IoT ecosystems need resilient operability since they are integrated

 doi:10.20944/preprints202410.0518.v1

into critical infrastructures and are growing larger and more complex. This work systematizes existing research on enhancing IoT resilience and analyses state-of-the-art methods [37]. It also proposes a taxonomy and classification of resilience mechanisms. The Metaverse, made possible by technologies like 5G/6G, XR, and AI, promises immersive experiences but presents serious privacy, security, and trust issues [48]. In order to emphasize the risks connected with AI, this paper examines these problems in AI-XR applications, offers a taxonomy of viable fixes, and provides a case study focused on the metaverse. Unexplored study areas are noted for future investigation. This survey looks at edge-based Internet of Things architectures, highlighting the difficulties with decentralized trust management, which is important for safe services, dependable data, and user privacy [49]. Reviewing trust criteria, examining blockchain as a trust solution, and examining the performance characteristics of trusted edge IoT systems, The accuracy of trust recommendation models in the Social Internet of Things (SIoT) is evaluated in this survey, which also highlights the context-dependent aspects affecting the models' performance [50]. In order to better understand research gaps and future prospects for enhancing trust recommendations in SIoT, it suggests a taxonomy that classifies these models according to input attributes and design using the PRISMA approach. Embedded systems are essential in the Internet of Things age, yet they frequently have security flaws because of old or repurposed software [51]. This overview examines the most recent approaches to employing static, dynamic, symbolic, and hybrid analysis techniques to find vulnerabilities in embedded firmware. With billions of devices connected, the Internet of Things (IoT) presents significant privacy and security problems, such as handling data and behavioural profiling [38]. This review places these issues in the context of the Internet of Things' tiered architecture. The paper presents key management, authentication, and encryption techniques that are lightweight and designed for the Internet of Things (IoT) [52]. They guarantee increased security while using the fewest resources possible to maintain the sustainability of the system. Due to resource limitations and ad hoc topologies, standard cryptography is insufficient for securing the rapidly growing Internet of Things (IoT) [53]. In response, the cross-layer intrusion detection system IoT-Sentry is presented, which can identify five different types of attacks without requiring additional overhead. To improve attack detection, an innovative cross-layer dataset is also created and ensemble learning is used. IoT-Sentry, using Cooja IoT simulator analysis, achieves an astounding average accuracy of 99% for four out of five attacks, demonstrating a groundbreaking attempt to protect standardized IoT networks from various threats.

2.6. Industrial Internet of Things (IIoT)

For the industrial Internet of things (IIoT) to collect monitoring data across industries, wireless sensor networks (WSNs) are essential [54]. Sensitive sensor data security presents difficulties in the resource-constrained IIoT environment, though. In order to enable trustworthy communication amongst linked IoT items, the study surveys IoT authentication strategies that have been put out in the literature [55]. By offering a thorough review and comparison of different methods, together with evaluation models and security analysis, the study seeks to support researchers and encourage more research and development in the area of IoT authentication. The study suggests BF-IoT, a secure communication framework, in response to security issues with Bluetooth Low Energy (BLE)-based IoT networks [56]. In order to prevent spoofing, BF-IoT keeps an eye on device lifecycles and uses special network-flow features for authentication. Continuous device identity authentication is ensured both before and during session establishment by its two-phase defense system. Tests using commercially available IoT devices show that BF-IoT can reliably authenticate devices via sniffing transmission characteristics. The Internet of Things (IoT) makes it easier to integrate disparate systems, which is essential for smart city applications like traffic and water management [57]. Due to resource limitations, ensuring device authenticity for precise decision-making is difficult. The Industrial Internet of Things (IIoT), crucial for Industry 4.0, grapples with managing real-time manufacturing data amid evolving Internet and telecommunication standards [58]. 5G technology (See Figure 8), while aiding data transmission efficiency, introduces security vulnerabilities in IIoT device authentication. To mitigate

 doi:10.20944/preprints202410.0518.v1

this, the article proposes a secure cross-layer authentication framework using quantum walk on circles. This system employs random hash coding on multidomain physical-layer resources for secure device identifier encoding.

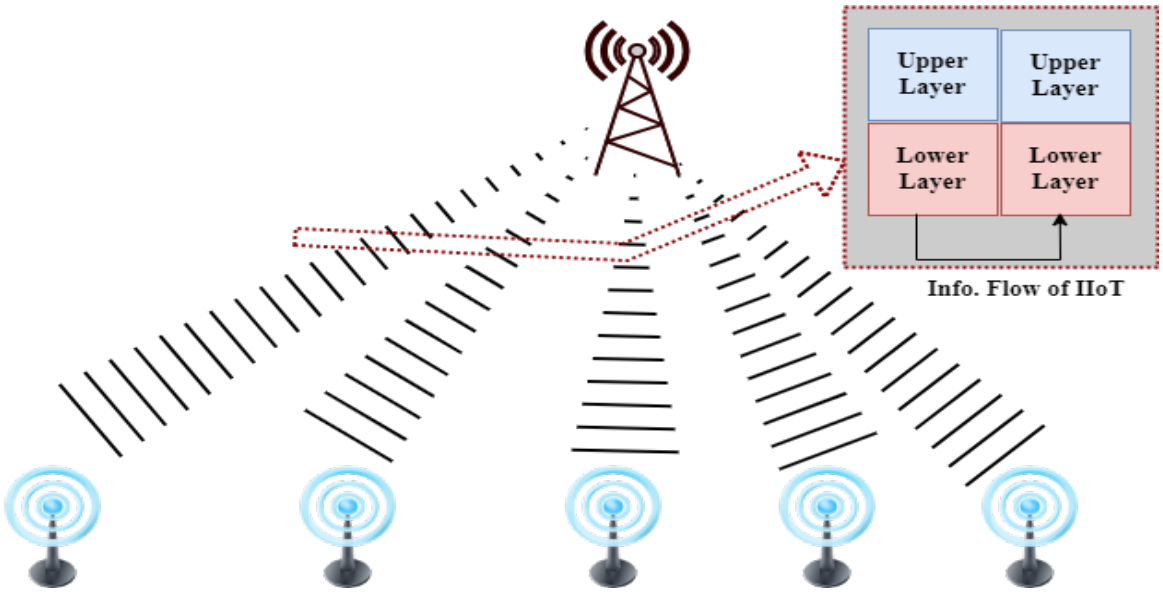

Figure 8. Illustration of 5G enabled IIoT in Industry 4.0 [59].

With the development of the Internet of Things (IoT), which connects everything and everyone, security and privacy have become increasingly important [60]. To reduce security risks in this diverse Internet of things context, authentication is essential. The review emphasizes the rapid evolution of IIoT in Industry 4.0 and the need for robust security solutions, particularly concerning 5G technology and device authentication vulnerabilities [58]. To address this, a cross-layer authentication framework based on quantum walk on circles is proposed. This framework ensures secure device identification, minimizes decoding errors, and provides high-level security against classical and quantum computers. It achieves ultra-high security and privacy protection with low latency, mitigating potential attacks effectively. The study proposes an innovative cybersecurity approach utilizing a Honeynet architecture to collect real-world network packets and identify attacks. The web-based IDS-AC allows user self-update and performance improvement. Scaling techniques and classifier optimization, particularly Gradient Boosting Classifier, show promise [61]. Future work aims to expand the dataset for comprehensive attack pattern coverage. This literature review systematically examines IoT security research, addressing vulnerabilities, challenges, technologies, and future prospects [62]. Surveying 171 recent publications, it offers a comprehensive overview of IoT development, limitations, and security solutions. The article discusses IoT architecture, common attacks, and mitigation strategies and providing a valuable resource for advancing IoT security technologies and strategies. This paper suggests a tiered IIoT and industrial control system architecture that optimizes resource allocation and specifies security procedures [63]. The utilization of deception attack simulation and water flow control system modelling for validation highlights the importance of aligning network and security structures for improved security. Interoperable connectivity, which is essential in E-healthcare for real-time patient data management, improves system configuration with IIoT [64]. Blockchain-based P2P networks and improved Wireless Sensor Network (WSN) lifecycle management maximize resource use [65], resilience, and traceability while tackling scalability and security issues in E-healthcare applications. Decentralized blockchain technology reduces the security threats that smart IoT devices in 5G-enabled networks confront [66]. By using clustered communication and local authentication, a multi-level blockchain security architecture is put forth to improve the security and simplicity of Internet of Things networks. When deployed on Hyperledger Fabric, the model guarantees the legitimacy and effective-

 doi:10.20944/preprints202410.0518.v1

ness of the network. IIoT networks with fog computing are used in smart cities to transfer workloads from resource-constrained sensor nodes, which are susceptible to malicious assaults that could impede task completion. Through the identification of malicious nodes and the efficient use of computational resources to ensure timely job completion, the Trust-based Efficient Execution of Offloaded IIoT Trusted tasks (EEOIT) improves fog nodes [67]. Cost, talent, and standardization constraints are the main reasons behind the delayed adoption of IoT in agriculture [68]. This review examines IIoT security and digital forensics, highlighting achievements, challenges, and future directions for cybersecurity [69]. Guidance for researchers and practitioners is outlined to address evolving threats in IIoT ecosystems. Industry 4.0, which emphasizes service-oriented computing for software infrastructure, uses ICT adoption to change production [70]. This paper outlines the function of microservices architecture and points up areas for further research as well as problems. SCADA systems integrate IoT and IIoT for enhanced industrial process control and monitoring [71]. This review explores opportunities and challenges in integrating IIoT with existing SCADA systems. Strong cybersecurity measures are required due to Industry 4.0's cyber physical production systems (CPPS) vulnerabilities in SCADA systems [71]. In order to reduce risks, this study suggests a multilayered structure that includes anomaly detection, encryption, access controls, micro-segmentation, and upgrades for legacy systems. In order to provide secure remote access for the collaborative demands of IIoT infrastructure, this article suggests a multi-level authorization architecture that allows for fine-grained access control, scalability, and maintainability [72]. It is implemented using open-source technology and secures the IIoT's edge and network domains. It has been verified in aircraft situations. This study examines WSNs for Internet of Things security [59]. It examines several attack vectors, approaches for mitigating them, dataset kinds, instruments, and performance metrics across contributions. It highlights the functions of deep learning and machine learning models, providing guidance for future IDS design paths that can effectively secure IoT networks. Computing, energy, and network management are among the issues brought forth by the growing use of IoT network technology in sensitive applications such as healthcare [73]. Based on comparative analysis, it is clear that ESPINA is superior to current protocols, which makes it a prime contender to fulfil 6G wireless communications standards.

2.7. MAC-Routing

In the context of IoT-driven smart city applications like e-healthcare, ensuring robust security, privacy preservation, and network longevity in Wireless Sensor Networks (WSNs) is crucial, especially during pandemics. To address these challenges, this paper [74] proposes the Cross-Layer and Cryptography-based Secure Routing (CLCSR) protocol. The increasing number of IoT devices in businesses increases security vulnerabilities, which are exacerbated by limitations such as computing capacity and energy resources. The difficulty of protecting IoT from assaults is becoming more and more pressing, especially for mobile devices that need secure data routing methods. In order to provide optimal routing decisions, this work presents a secure cross-layer protocol that makes use of MAC layer parameters [75]. Deploying IoT devices presents issues in the context of Industry 4.0, mostly because low-cost devices are not as capable of providing robust security solutions. In order to solve this, the paper presents a hierarchical authentication and key agreement mechanism that is both lightweight and effective, specifically designed for Internet of Things environments [76]. The paper proposes an energy-aware routing scheme (EARVRT) [7]. Utilizing a virtual relay tunnel (VRT) and considering route energy, hop counts, and path correlation, However, network longevity slightly decreases compared to one existing method. Future research aims to enhance routing with machine learning and develop intelligent virtual relay tunnels for dynamic adaptation to network conditions. Because of the rapid growth of IoT, modern industries are implementing remote monitoring and control of various IoT devices. In this paper [77], next generation cyber security architecture (NCSA) is proposed, as well as industry IoT, for detecting cyber threats [43] and vulnerabilities. A cyber defence authentication mechanism is used to prevent security attacks while a network session is established. A network-wide cryptographically encrypted identity token defence mechanism is established and

 doi:10.20944/preprints202410.0518.v1

verified by a virtual gateway system. The proposed NCSA lowers operational management costs while increasing industrial security. While the population of rural areas is declining, the population of cities and the entire world is growing quickly. Lack of resources and limited sources are both issues that arise [8]. As a result, the need for smart cities increases. Information technology and communication are combined in this idea. Data security is a major concern because of the exponential growth of IoT and new smart devices as well as the expansion of the internet [9]. The internet now has a new meaning thanks to IoT, and managing security is getting harder. There are two sections to this paper. IoT introduction, building blocks, enabling strategies, and security system requirements are covered in the first section. In the second section, examine the camera-based case study and assess its security attributes. By taking advantage of the camera system to spoofing attack that can completely control Smart Camera System (ScS). Following an investigation, it is possible to secure systems and address security issues. Protect customer privacy and begin with IoT security. For the purposes of using IoT devices, different stakeholders play different roles in preserving information security and privacy goals. The interaction between processors and sensor layers grows as the healthcare internet of things grows [78]. The use of artificial intelligence in healthcare and the internet of things is rapidly expanding these days. Tactile Internet and the Internet of Nano Things are also recent developments. Discuss emerging technologies as well as how to improve service quality. Using learning automata (LA) and clustering, this work presents an improved TDMA MAC protocol for UV networks with a focus on cluster node count, service class, and network topology [79]. The suggested protocol exhibits better network performance when compared to conventional TDMA and clustering systems, proving its usefulness for multi-node UV networking. Grid-based routing techniques for wireless sensor networks are covered in detail in this article, with an emphasis on energy efficiency [80]. A comparison analysis and a timeline are presented. With regard to grid topology and energy management in sensor networks, the survey provides insights into design difficulties, challenges, and methodology. This paper introduces a location-aware device-to-server authentication for IoT, enhancing device authenticity using MAC addresses, AES encryption, and MaskIDs generated by a Trusted Authority (TA). It emphasizes the importance of device proximity to servers for authentication, addressing security concerns like man-in-the-middle attacks [81](See Figure 9). Through analytical and real-world simulations, the proposed method demonstrates superior performance in communication, storage, and processing overheads compared to existing approaches in IoT authentication.

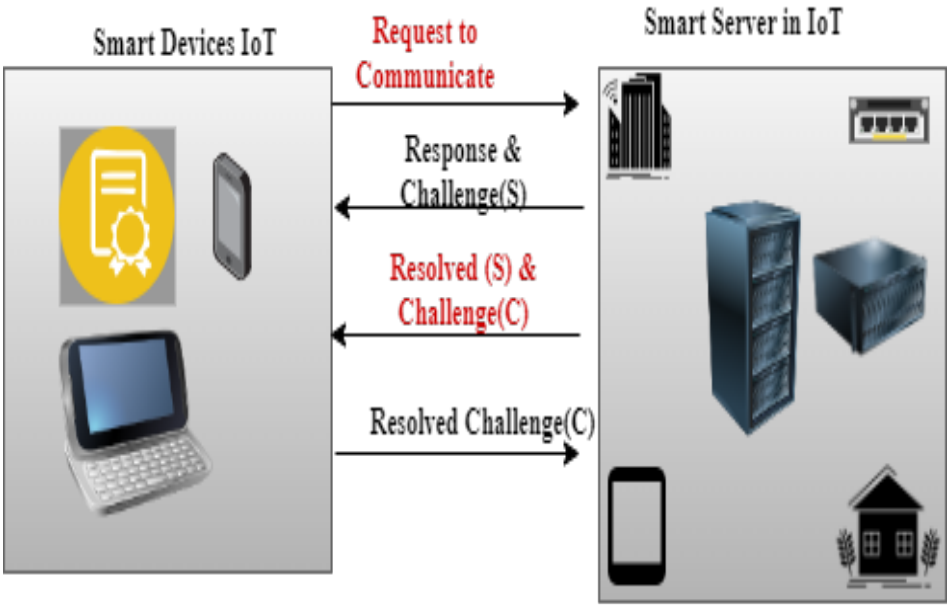

Figure 9. Generalized Device to Sever Authentication in IoT [81].

 doi:10.20944/preprints202410.0518.v1

With the support of IEEE 802.15.4-2015 and IEEE 802.15.6-2012 standards, low-power biomedical sensors are used in wireless body area sensor networks (WBASNs), which are becoming more and more recognized for their potential in patient monitoring [82]. In-depth analysis of current developments in medium access control (MAC) and routing protocols addresses outstanding issues, challenges, and application needs, offering guidance for future work. The results of this research are especially pertinent to the sixth generation (6G) networks that are predicted to improve quality of service (QoS) and connectivity for a wide range of sensor-based Internet of Things devices. Although the Wireless Medium Access Control (WMAC) protocol guarantees safe data transmission and intrusion detection, clever attackers can circumvent the MAC restrictions that are in place now. In order to secure sensor nodes, the Wireless Interleaved Honeypot-Framing Model (WIHFM) is suggested [83]. This model creates durable security standards and optimum Wireless Sensor Network (WSN) channels. WIHFM introduces honeypot frame traps to improve security 10% over existing methods like Secure Zebra MAC and block chain assisted secure routing mechanism (BASR). It does this by isolating distributed attacks creatively and managing the network dynamically. This paper examines distributed MAC protocols in Internet of Things (IoT) and wireless sensor networks (WSN), with an emphasis on cooperative optimization methods and game theory to improve network efficiency [84]. Key results include significant energy savings and delay reduction through hybrid distributed MAC and cross-layer techniques, as well as an improvement in spatial reuse of 3%–29% and an 8% increase in throughput. Methods such as optimum cuckoo search and stochastic methods, along with game theory optimization, demonstrate promising gains in attack detection, resource allocation, and overall network efficiency. The goal of Automotive Ethernet (AE), the industry's transition to Ethernet technology, is to increase in-vehicle communication bandwidth for driver-assistance and autonomous systems. But as vehicle connection grows, cybersecurity worries grow, leading to a thorough analysis of AE's security impact in comparison to protocols like the Controller Area Network [85]. In order to solve industry-specific constraints like low latency, the study concludes that more specialized AE solutions are required, setting a foundation for future improvements. The report outlines important security concerns, mitigation measures, and regulatory mappings. In order to improve security in underwater sensor networks (UWSNs), a secure data aggregation and authentication (SDAA) protocol designed specifically for underwater vehicular wireless networks (UVWSNs) is proposed in this study [86]. The cluster-based network architecture used by the SDAA protocol improves data communication security and energy efficiency by providing secure cluster head authentication and detecting malicious node attacks. When the SDAA protocol is used in UVWSNs for ship and vehicle monitoring, it shows better network latency and energy efficiency than the current secure MAC techniques. Because of malicious nodes, securing IoT communication networks and node safety is difficult [49]. SDN is used in the suggested Trust Evaluation based Secure Multi-path Routing (TESM) solution, which includes modules for anomaly handling, multi-path routing with reinforcement learning, and security verification. Based on simulations, TESM is able to localize threats and secure data transmission with just minor increases in latency (12.4%) and throughput loss (5.46%). Although VANETs increase traffic flow and driving safety, their lack of central control makes them susceptible to both internal and external attacks. Black Hole, Gray Hole, and DoS attacks are among the risks that the TDMA-aware Routing Protocol for Multi-hop communication in Vehicular networks must contend with [63]. A trust-based architecture is put out as a countermeasure, in which nodes build trust through packet forwarding and channel access behaviour. Simulations show how this model greatly lessens the effect of attacks on the network's functionality.

 doi:10.20944/preprints202410.0518.v1

2.8. Energy Efficiency Cross Layer Design

Coal mines can communicate data in real time by integrating smart sensing devices over the Mine Internet of Things (MIoT) [10]. Reliable communication is ensured by fifth generation (5G) technology. Energy effectiveness (EE) is increased by optimizing device access and spectrum consumption in a NOMA-based MIoT communication system. Iterative methods tackle issues such as insufficient channel state information, maximizing power allocation, and assigning subchannels while considering cross-layer limitations and quality of service demands. Traditional methods result in high power usage and network breakdowns, motivating the development of energy-efficient routing mechanisms. In the Smart Dust Head (SDH) environment, the latest BS location is disseminated to nodes, enabling optimization through algorithms like Enhanced Oppositional Grey Wolf Optimization (EOGWO) for enhanced network performance [11]. This paper provides a structured overview of the relationship between Artificial Intelligence and Variable Renewable Energy (VRE) through Deep Learning (DL) applications [87]. After that, it evaluates DL-based solutions and their suitability while emphasizing important architectures. The study identifies ten DL-based strategies that facilitate VRE integration in power systems. The paper tackles energy-efficient data collection in remote IoT surveillance by designing a Medium Access Control (MAC) layer uplink solution following the Narrowband IoT (NB-IoT) scheduled access scheme. It optimizes energy consumption per uplink frame using Mixed Integer Non-Linear Programming (MINLP), and introduces a distributed sleep scheduling scheme to enhance delay and energy conservation [17]. Simulation results demonstrate its superiority over existing solutions in terms of delay, buffer length, and energy consumption under high traffic load. The paper addresses energy consumption in IoT devices by proposing ELITE, an energy-efficient cross-layer objective function (OF) integrated into the RPL routing protocol [18]. Unlike existing OF, ELITE introduces the strobe per packet ratio (SPR) metric at the MAC layer, considering transmission operations' impact on energy consumption. By selecting paths with fewer strobe transmissions, ELITE reduces average strobes per packet by up to 25% and improves energy consumption by up to 39% The review addresses the energy consumption challenges in wireless networks, particularly focusing on energy-efficient heterogeneous cellular networks (HCNs) [19]. The paper formulates a hybrid joint resource allocation (HJRA) optimization problem and proposes a quantum-inspired political optimizer (QPO) algorithm to address the non-convex nature of the problem, showing superiority in total system EE through synchronous allocation of backhaul bandwidth, sub-channels, and power. The review addresses water scarcity in metropolitan areas and the need for intelligent water distribution systems, emphasizing IoT-Based monitoring to manage distribution challenges [88]. In smart city IoT-integrated water distribution systems, it addresses effective delay and energy offloading mechanisms and suggests communication network topologies that are customized to water network design parameters and land cover patterns. Through a case study in Kochi, India, it models delay and energy in IoT-based systems, discusses node categorization algorithms, and identifies optimal fog node placement, achieving up to 40% energy efficiency improvement. The paper addresses challenges in Flying Ad Hoc Networks (FANETs), emphasizing the importance of routing algorithms due to dynamic topology and energy constraints [7]. It introduces energy-aware routing scheme based on a virtual relay tunnel (EARVRT), an Energy-Aware Routing scheme utilizing a Virtual Relay Tunnel (VRT) to manage relay nodes, considering metrics like route energy, hop counts, and path correlation. Evaluation against existing methods demonstrates EARVRT's superiority in delay, network longevity, energy consumption, and packet delivery rate. The literature encompasses the surge in wireless devices, emphasizing their energy consumption concerns and prompting research into energy-efficient solutions [89]. It delves into diverse topics such as computation offloading, CoAP protocols, task scheduling algorithms, and device-to-device communication enhancements, aiming to optimize energy efficiency across various wireless applications. The literature examines IoT's connectivity and sustainability challenges due to the surge in connected devices, advocating for Cognitive Radio (CR) technology as a solution [12]. It proposes a cross-layer design optimizing modulation order and backoff probability to minimize energy consumption while meeting IoT delay requirements, PR channel availability, and user activities,

 doi:10.20944/preprints202410.0518.v1

demonstrating substantial energy reduction and delay satisfaction compared to single-layer approaches. The literature review addresses concerns about energy shortages due to global warming and climate change, focusing on home energy management [42]. The literature review discusses the Security concerns in the Social Internet of Things (SIoT), emphasizing the need to balance security with energy efficiency [14]. It suggests employing cross-layer architectures and leveraging graph-powered learning, effective in social networks, to strengthen SIoT security. Additionally, it outlines a study agenda for future research aimed at enhancing SIoT security. Examining the essential elements of low-power, long-range IoT connectivity, this literature study compares LoRaWAN with NB-IoT. NB-IoT is resistant to payload length effects, which is advantageous for buffered applications, according to in-field measurements. On the other hand, LoRaWAN is well-suited for longer IoT device lifetimes because to its remarkable energy efficiency, which requires 10 times less energy for similar payload delivery. Enhancing service quality, consistency, and cost management are the main goals of recent developments in IoT-enabled Wireless Sensor Networks (IWSN) [90]. A hybrid Artificial Neural Network (ANN) Simulated Annealing classifier and optimization based on MapDiminution are used to create an energy-efficient clustering and quick intrusion detection system that addresses security and energy concerns. This method lowers energy usage while achieving a high 97.57% detection accuracy. This work investigates the effective hardware implementation of feedforward artificial neural networks (ANNs) with time-multiplexed MAC blocks by recycling computational resources using approximation adders and multipliers, hence requiring less space and energy [91]. The optimal degree of approximation for hardware correctness is suggested using an algorithm. Comparing experiments with accurate hardware, MNIST and SVHN is a real-world datasets for developing machine learning algorithm databases demonstrate reductions of up to 50% energy and 10% area with negligible loss in accuracy. Energy-efficient wireless sensor networks (WSNs) are crucial for data collecting, as evidenced by the Internet of Things' exponential expansion [92]. In this study, an energy-efficient cluster-based Lightweight On Demand Ad hoc Distance Vector Routing Protocol–Next Generation (LOADng) is developed in response to the energy limitations of smart devices. By using LOADng for routing, a seagull optimization method for optimal cluster head selection, and k-means clustering for cluster formation, the technique minimizes power consumption and maximizes network life in comparison to other options. In order to address issues with resource allocation that is energy-efficient, this literature emphasizes the significance of IoT in the technological, social, and economic spheres [93](See Figure 10 below). A new technique for forest optimization is developed in order to minimize energy consumption and delays in resource distribution, while traditional methods did not account for this factor. MATLAB simulation results show that this method performs better than generic algorithm (GA), particle swarm optimization (PSO), and distance-based algorithms, with important practical applications and increased efficiency in IoT resource management.

 doi:10.20944/preprints202410.0518.v1

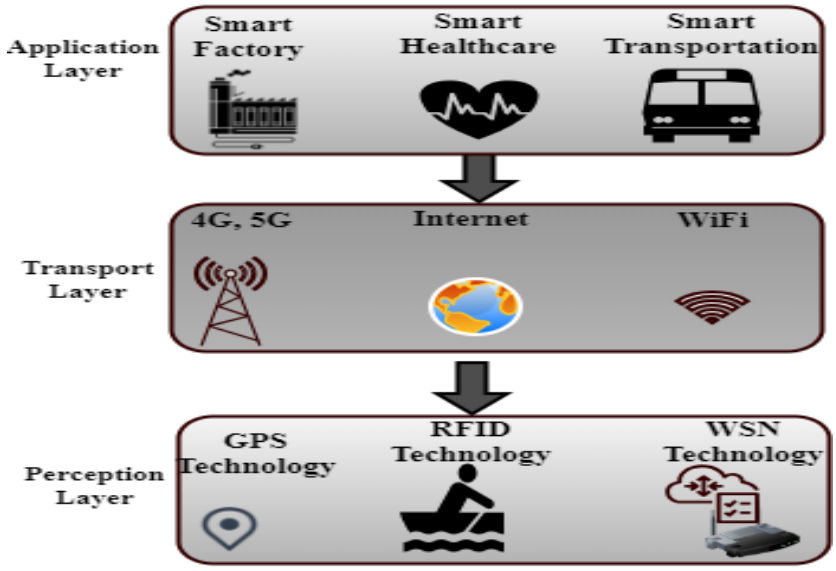

Figure 10. General Model of Proposed Energy Efficient Architecture [93].

In order to facilitate coordinated integration in IoT environments, this research suggests a hierarchical ensemble TinyML scheme that allows individual IoT parts to make decisions that affect the entire system [94]. The two-layered TinyML-based edge computing solution was applied in a smart agriculture use case, showing advantages including decreased energy usage, response times, and wireless transmissions while improving data security and privacy. The assessment demonstrates how well the plan works to produce intelligent, context-aware applications. The swift expansion of IoT in the healthcare sector permits the acquisition of patient data in real-time, while it presents difficulties in managing copious redundant data [95]. An Energy-Efficient Fuzzy Data Aggregation System (EE-FDAS) that reduces energy consumption by reducing typical sensor readings to a single digit is presented in the study as a solution to this problem. Based on NS-2.35 simulations, EE-FDAS outperforms other approaches in terms of aggregation efficiency and energy consumption. This study proposes a clustering technique and Q-learning for work offloading to UAVs, integrating UAVs with IoT to address memory and data processing problems [96]. The suggested approach performs better in terms of data transfer and energy efficiency than the current approaches, especially in emergency situations. The usage of IoT in a smart city for energy-efficient building control is covered in this study, which also suggests a flexible, hierarchical architecture that integrates online services, people, and devices [97]. The suggested model seeks to improve overall Smart Building operations and maximize intelligent energy regulation. In the ever-expanding landscape of edge computing, the surge in energy demand poses a critical challenge that demands meticulous management for the advancement of this technology. As edge computing evolves, there is a pressing need to delve into cross-layer architecture, exploring ways to scale energy output while optimizing overall performance [21]. Envisioned as a game-changer in communication, 6G systems are set to revolutionize wireless connectivity for IoT networks [4]. CR technology emerges as a solution for spectrum support, but adapting existing protocols to the energy constraints of 6G IoT devices poses challenges. Energy-efficient protocols like MQTT, CoAP, Zigbee for sensors, and Wi-Fi for networks are integrated into next-generation IoT architecture [22]. The literature on IoT traces the development of low-power sensors and actuators, promoting RPL-based protocols and lightweight routing strategies [13]. the Internet of Things is reviewed in The literature, with a focus on energy efficiency and data dependability. To enhance energy usage, CLEERDTS integrates node location data, optimizes transmit power at the MAC layer, and chooses transmission modes at the physical layer [98]. The security issues of cyber-physical systems, especially smart grids, where Internet of Things devices are susceptible to intrusions, are discussed in this study [99]. The power and computational limitations of IoT are addressed in this

 doi:10.20944/preprints202410.0518.v1

study by introducing EasyChain, a lightweight blockchain with Proof-of-Authentication (PoAh) for IoE networks [100].It is implemented in Python and tested on a single-board computer. This paper introduces cluster-based scheduling and routing in geographic routing protocol (CSRGR), a dynamic cluster-based duty cycle scheduling for efficient data transmission in resource-constrained WSNs using geographic routing [101]. Lightweight blockchain assisted intruder detection system (LB-IDS) employs Lightweight blockchain multifactor authentication for node authentication and multi objective strawberry optimization (MOSO) for optimal route selection, followed by deep-Q learning (DQL) based IDS for packet classification and Blockchain for trust updates [102]. This paper introduces LB-IDS, integrating Blockchain for enhanced security in MANETs. Lightweight blockchain assisted intruder detection system (LB-IDS) employs Lightweight blockchain multifactor authentication for node authentication and multi objective strawberry optimization (MOSO) for optimal route selection, followed by deep-Q learning (DQL) based IDS for packet classification and Blockchain for trust updates [102]. In order to preserve privacy while aggregating data in low-power Internet of Things devices, this study presents LiPI [103], a lightweight PPDA method that does away with complicated cryptography and outside dependencies. The focus of this work is on the suitability of lightweight cryptography protocols for Internet of Things security while dealing with devices that have limited resources [104]. It addresses the crucial requirement for effective authentication, privacy, data integrity, and control in Internet of Things networks by comparing the performance of the PRESENT block cipher to alternative lightweight algorithms.Concerns have been raised about the energy efficiency of computing devices and technologies relevant to low-power residential and commercial buildings [23]. A lightweight symmetric cryptographic algorithm is presented in this paper [105]. The reviewed paper proposes an energy-efficient multi-channel MAC framework with a tailored CSMA protocol for CR-enabled 6G-IoT networks. Through joint adaptation of physical and MAC layer parameters, the framework aims to boost IoT network energy efficiency significantly. Numerical results demonstrate up to a 50% improvement compared to a single-channel design, offering a promising solution for 6G-IoT networks' massive-connectivity demands. The surging (WSN-IoT) stands for Wireless Sensor Network on the Internet of Things. addresses demographic aging and job challenges but faces security threats with its resource-limited devices. Despite its critical role, research on WSN-IoT security is limited [65]. This review zooms in on security challenges, spotlighting a Contiki OS implementation of RPL's mechanisms. It critically analyses issues, explores machine learning for management, addresses the architecture, difficulties, network attacks, and goals of the Internet of Things in Low Power Networks (IoT-LPN).

 doi:10.20944/preprints202410.0518.v1

Table 4. Summary of related IoT Cyber Security Surveys.

Survey Scope	IoT Security	Security-Measure Implemented	Limitations	References
IoT Security Research,Focuses on the deployment of IoT technology in industrial automation, Next Generation Cyber Security Architecture (NCSA) for the Industrial IoT	NCSA Implementation, Automated Cyber-Defense	Vulnerabilities, attacks, cross-layer security, Real-time Protection, Identity Token Mechanism	Limited consideration of interaction of cyber-physical devices,Specific Focus on IIoT, No Detailed Performance Evaluation, Potential Integration Challenges	[77]
In-depth analysis of the IIoT ecosystem focusing on security and digital forensics, Overview of the state-of-the-art in IIoT security and digital forensics, Highlighting key achievements, Challenges	Examination of the structural and dynamic complexity of IIoT, Exploration of vulnerabilities introduced by the continuous integration of IIoT	Analysis of cutting-edge security mechanisms deployed in IIoT ecosystems to protect processes,Survey of digital forensics literature related to IIoT, Focusing on techniques and tools to mitigate security breaches	NCSA proposed for real-time threat detection,Complexity and Integration, Evolving Threat Landscape, Need for Future Research	[69]
Cyber-physical system risk identification, Analysis of risk identification in Industry (CPS), Examination of methodologies for identifying risks across physical, Interconnection layers in CPS	Focus on the security vulnerabilities and cyber-attacks associated with interconnected devices and equipment in Industry CPS	Proposed a new hybrid methodology for risk identification in Industry, Integrating existing frameworks and standards such as ISO 31000, PMBOK, HAZOP, and NIST, Developed a four-step process that includes identifying risks from various sources	Lack of consideration for interaction of cyber-physical devices, Incompleteness of Existing Methodologies	[6]
Threat detection in industrial networks, Exploration of a framework combining using AI tools, Focus on threat detection within real industrial IoT sensor networks	Addresses the challenge of detecting threats IIoT networks while maintaining privacy and security	Big data architecture, predictive analytics	Limited to real industrial network, AI-based predictive analytics, Securely sharing results, Application of the framework as part of the H2020 ECHO project	[5]
Cross-layer authentication framework, Focuses on addressing security challenges in IIoT of 5G technology, Explores the security implications of bypassing upper authentication protocols and supporting small data transmission during initial access in IIoT systems	Highlights the vulnerabilities in IIoT due to the use of 5G, Emphasizes the need for secure cross-layer authentication frameworks to address these vulnerabilities	Device authentication vulnerabilities, 5G technology, Proposes a secure cross-layer authentication framework, Utilizes a quantum walk-based privacy-preserving, Derives the space of one-time keys for encryption	Proposal addresses security vulnerabilities, Complexity, Scalability, Performance Overhead	[58]
Adaptive Cybersecurity system, Cybersecurity for networked devices using virtual environment services	Addresses increased risks due to widespread device connectivity	Real-world network packet collection, Machine learning, Honeynet architecture, Adaptive Cybersecurity (AC) system	Performance improvements needed, dataset expansion planned, Data dependency, Scalability challenges	[61]

 doi:10.20944/preprints202410.0518.v1

3. Key Strategies and Trends

3.1. Key Strategies

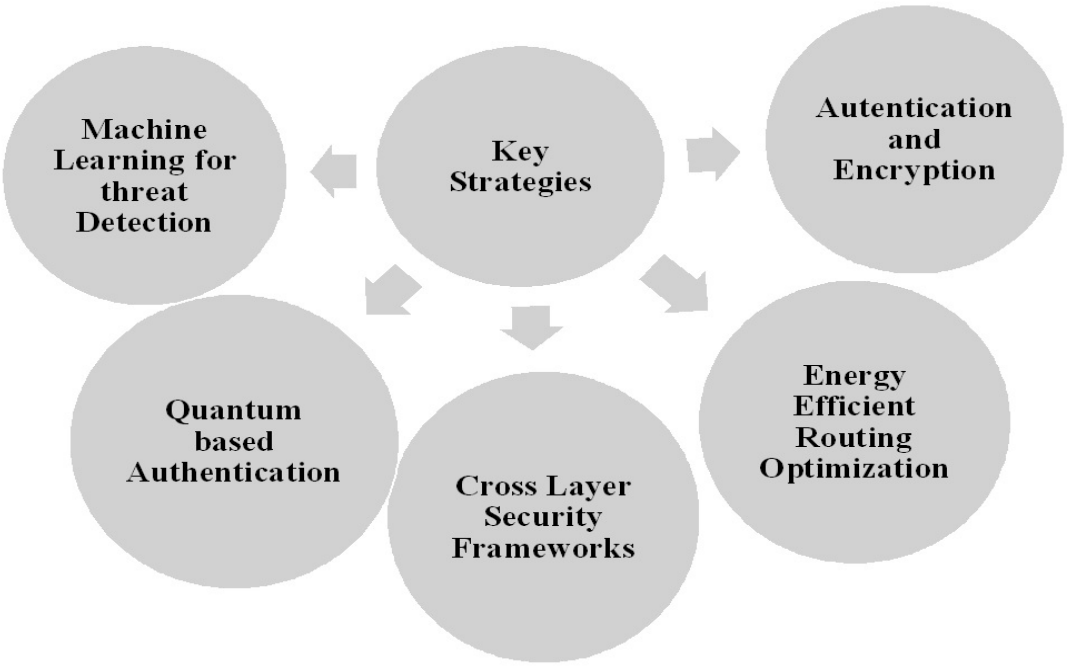

Figure 11. Key Strategies Of Survey Paper.

(a) **Authentication and Encryption:** As the number of IoT devices continues to grow rapidly, ensuring robust authentication and encryption mechanisms becomes imperative to protect sensitive data and maintain privacy [9,62]. Authentication mechanisms such as cryptographic protocols and identity management systems help verify the identities of devices and users, while encryption techniques such as symmetric and asymmetric encryption ensure secure communication channels. Additionally, blockchain technology is being explored to provide tamper-proof and decentralized solutions for data integrity and transaction security in IoT environments.

(b) **Machine Learning for Threat Detection:** With the increasing sophistication of cyber threats targeting IoT systems, machine learning algorithms are being leveraged for threat detection and prevention [61]. These algorithms analyze vast amounts of data generated by IoT devices to identify patterns indicative of malicious activities or anomalies. By continuously learning from new data, machine learning models can adapt and improve their accuracy in detecting and mitigating security threats, thereby enhancing the resilience of IoT networks.

(c) **Cross-Layer Security Frameworks:** Cyber-physical systems (CPS) present unique security challenges due to their interconnected nature and reliance -on both physical and digital components [6]. To address these challenges, hybrid security frameworks integrating established risk management methodologies such as ISO standards with domain-specific risk models are being developed. These frameworks facilitate comprehensive risk identification and management across multiple layers of CPS architectures, from the physical layer to the application layer. By considering interactions between different layers, organizations can better assess and mitigate security vulnerabilities in their IoT deployments.

(d) **Quantum-based Authentication:** With the advent of Industry IoT (IIoT) and the proliferation of 5G technology, traditional authentication mechanisms face new challenges related to device authentication vulnerabilities [58]. To address these challenges, cross-layer authentication frameworks based on quantum walk on circles are proposed. These frameworks utilize quantum

 doi:10.20944/preprints202410.0518.v1

principles to ensure secure device identification and authentication, thereby mitigating the risks associated with compromised authentication credentials and unauthorized access to IIoT networks.

(e) **Energy-Efficient Routing and Optimization** Energy efficiency is a critical concern in IoT deployments, particularly in resource-constrained environments [7,17,18,21]. Strategies such as energy-efficient routing schemes and cross-layer optimization techniques aim to minimize energy consumption while maximizing network performance and reliability. These approaches leverage techniques such as virtual relay tunnels, mixed-integer nonlinear programming (MINLP), and optimized transmission modes to optimize energy usage at both the MAC and physical layers of IoT networks. Additionally, the integration of renewable energy sources with IoT architectures further enhances energy efficiency and sustainability, reducing reliance on traditional power sources and minimizing environmental impact.

3.2. *Emerging Trends*

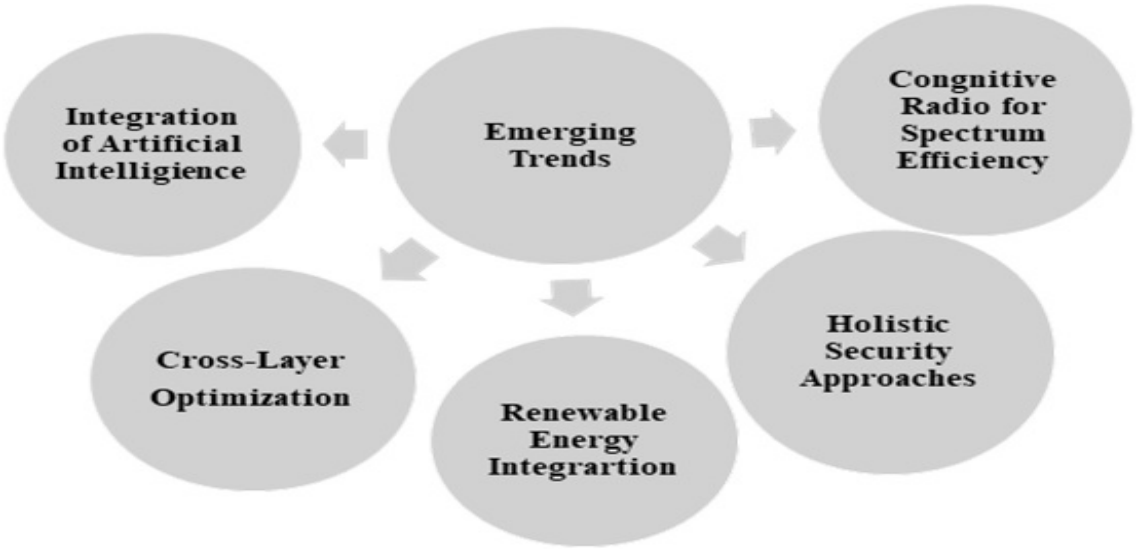

Figure 12. Emerging Trends of Survey Paper.

(a) **Integration of Artificial Intelligence:** The integration of artificial intelligence (AI) and machine learning algorithms is emerging as a trend to enhance IoT security and efficiency [61,87]. These technologies enable predictive analytics for threat detection and optimization of energy consumption in IoT systems. By analyzing large datasets generated by IoT devices, AI algorithms can identify patterns and anomalies indicative of security threats, enabling proactive mitigation strategies. Additionally, AI-based solutions facilitate the integration of variable renewable energy sources into power systems, improving forecasting accuracy and grid management.

(b) **Cognitive Radio for Spectrum Efficiency:** With the advent of 6G IoT networks, cognitive radio (CR) technology is proposed to optimize spectrum usage and energy efficiency [4]. Multi-channel MAC frameworks tailored for CR-enabled networks aim to improve IoT network performance and connectivity by dynamically allocating spectrum resources based on network conditions and user requirements. These frameworks enhance spectrum efficiency while minimizing interference and energy consumption, thereby enabling reliable and scalable communication in dense IoT deployments.

(c) **Renewable Energy Integration** The integration of renewable energy sources with IoT architectures is gaining traction for enhancing energy efficiency and sustainability [87]. Deep learning applications facilitate the integration of variable renewable energy sources into power systems, improving forecasting accuracy and grid management. By leveraging AI-based solutions, organi-

 doi:10.20944/preprints202410.0518.v1

zations can optimize energy usage and minimize reliance on traditional power sources, thereby reducing operational costs and environmental impact.

(d) **Holistic Security Approaches:** As IoT ecosystems become increasingly complex, holistic security approaches are being advocated to mitigate evolving cyber threats [9] [62]. These approaches encompass robust authentication mechanisms, encryption protocols, and proactive threat detection strategies to safeguard against unauthorized access, data breaches, and other security risks. By adopting comprehensive security measures, organizations can ensure the confidentiality, integrity, and availability of their IoT deployments, thereby enhancing trust and compliance with regulatory requirements.

(e) **Cross-Layer Optimization:** Cross-layer optimization techniques are being explored to improve energy efficiency and performance in IoT networks [21]. By jointly optimizing parameters across different protocol layers, such as the physical and MAC layers, organizations can minimize energy consumption while meeting the diverse requirements of IoT applications. These approaches enable dynamic adaptation to changing network conditions and user demands, enhancing reliability and scalability in IoT deployments. These findings highlight the necessity of comprehensive approaches to cyber-physical systems and IoT security, including improved cybersecurity architectures, all-encompassing security measures, and creative solutions that make use of cutting-edge technology like machine learning and quantum cryptography (See Table 5 for Key strategies and Trends).

 doi:10.20944/preprints202410.0518.v1

Table 5. Key Strategies and Trends.

Main Contributions	Trends	Application Area	Reference
Big Data Architecture, Predictive Analytics, Threat detection, Obscuring sensitive data, Evaluation framework	Enhances trust among stakeholders, Closes security gaps	Industrial networks	[5]
Cross-layer Optimization, LoRaWAN, Flexibility across protocol layers, Energy-efficient	Optimizes protocol, Enhances performance	IoT applications, LPWANs	[16]
Hybrid Methodology, Risk Identification, ISO 31000, PMBOK, HAZOP, NIST strategies	Reduces risk redundancy, Comprehensive analysis	Cyber-Physical Systems (CPS)	[6]
Social IoT (SIoT), Cross-layer Security, Data trustworthiness, Graph-powered learning strategies	Enhances network navigability, Balance energy efficiency	SIoT ecosystems	[14]
Lightweight Encryption, Key Management, Random key encryption, Information-theoretic security	Efficient and secure, Suitable for resource-limited IoT	IoT, Cyber-Physical Systems (CPS)	[52]
Cross-layer Intrusion Detection, Ensemble Learning, IoT-Sentry, Cooja IoT simulator analysis	High detection accuracy, Minimal overhead	Standardized IoT networks	[53]
IoT Authentication Strategies, Categorization by hierarchy, centralization, distribution	Comprehensive review, Encourages further research	IoT authentication	[55]
Lightweight Mutual Authentication, Smart city applications, Performance optimization	Balances security and efficiency, Outperforms existing protocols	Smart cities, Traffic and water management	[57]
Cross-layer Authentication, Quantum Walk, Device identifier encoding, Privacy-preserving protocol	High security and privacy, Low latency	IIoT, 5G networks	[58]
Honeynet Architecture, Machine Learning, Real-world attack detection, Web-based IDS-AC	Effective attack warnings, User self-update	Industrial networks, Cybersecurity	[61]
Survey of IoT Security Research, Vulnerabilities, Mitigation strategies, Future directions	Comprehensive overview, Guides future research	IoT development, Security solutions	[62]
ESPINA Protocol, IoT network technologies in delay, Improved security with keys-renewal strategy, Reduces computational cost	Energy optimization, 6G wireless connectivity, Superior to current protocols, Effective for 6G standards,6G wireless communications, Energy-efficient and secure protocols	Healthcare IoT, Embedded systems, Security-sensitive applications	[73]
CLCSR Protocol, Attack detection, Secure clustering, Lightweight cryptography	Enhances network performance, Privacy preservation	E-healthcare, Smart cities	[74]
Hierarchical Authentication, Key Agreement, Physically unclonable functions, Elliptic curve cryptography	Efficient and secure, Resistant to common attacks	Industry 4.0, IoT environments	[76]

 doi:10.20944/preprints202410.0518.v1

4. Open Research Problems and Challenges

4.1. Open Research Issues

i **DDOS:** It is still very difficult to create strong security measures to keep malware infiltrations, DDoS attacks, and privilege escalation out of IoT networks. For greater application and efficacy, existing solutions such as the agentless Wazuh SIEM module offer a good foundation, but they still require improvement [24].

ii **Routing Protocols:**It is crucial to create safe routing protocols for Internet of Things networks in order to thwart assaults like denial-of-service and wormhole attacks. Additional optimization is required for attack detection and energy efficiency in frameworks such as parental change control routing protocol for low power and lossy and subjective logical framework routing protocol for low power and lossy network [28].

iii **Blockchain Technology:** It is a viable way to improve IoT security and data integrity, particularly in the agricultural and healthcare industries [33].

iv **Semantic IoT Middleware:** It's crucial to create energy-efficient Internet of Things architectures that can handle a lot of devices without using a lot of power. Measures in this direction include the Semantic IoT Middleware and the hierarchical ensemble TinyML [94].

v **Robustness and Resilience:**It is essential to increase the robustness and resilience of IoT systems to withstand different kinds of cyberattacks and operational failures. More work needs to be done on taxonomies and classifications of resilience mechanisms [72].

4.2. Open Research Challenges

i **Host intruder Detection(HIDS):** HIDS system and network intruder detection system integration with federated learning to build decentralized, robust security solutions in fog computing environments [26].

ii **Integration of IoT & AI:**Ensuring the smooth integration of IoT and AI to manage analytics and real-time data processing. Addressing security and privacy concerns with data while keeping performance high [32].

iii **RPL Protocol:**Improving the RPL protocol in order to reduce packet loss, increase attack detection rates, and boost energy efficiency [28]. Customizing secure routing protocols to different Internet of Things contexts ensures scalability and compatibility.

iv **Blockchain Solution:**Putting into practice blockchain solutions that are lightweight and don't put an undue strain on IoT device resources [100]. Ensuring blockchain's compatibility with current IoT platforms to enable smooth integration.

v **Data Governance:**Strong frameworks for data governance that strike a compromise between the requirement for data accessibility and privacy [68].

vi **Encryption & Authentication:** Efficient encryption and secure authentication systems that work with low-power Internet of Things devices [81].

5. Conclusion

A cross-layer energy-efficient framework with security measures for Internet of Things (IoT) is surveyed. We have discussed and categorized cross-layer framework for IoT that is both secure and energy-efficient based on key parameters, such as routing and multiple access protocols, energy efficiency, and network resources. We also discussed the development of next-generation cross-layer framework that is secure and energy-efficient. The findings have shown that the importance of intelligent intrusion detection systems, multi-layered security framework, cross-layer techniques, and the adoption of advanced technologies like blockchain, artificial intelligence, and lightweight cryptography to safeguard IoT systems. Energy efficiency emerges as a paramount concern, with strategies ranging from energy-efficient network architectures to battery-saving cryptographic solutions. The safeguarding smart city ecosystems are explored, which digs into contemporary cybersecurity strategies designed for industrial networks in addition to discussing the need for secure data processing and transfer. In this research we focused on energy-efficient IoT network solutions.

 doi:10.20944/preprints202410.0518.v1

Future multidisciplinary approaches that tackle cybersecurity from both a technological and human perspective should be given priority in research on cyber-physical systems and IoT security. To combat quantum attackers, this entails creating sophisticated threat detection systems that make use of machine learning in addition to quantum-safe cryptography. The key areas of effort should be cross-domain security solutions, physical security improvements, and technologies that protect privacy with a focus on standardization, interoperability, and sustainability. The development of more secure, and trustworthy IoT ecosystems is suggested as future research work.

References

1. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review, 2022. doi:10.3390/electronics11020198.
2. Zhang, Y.; Zou, W.; Chen, X.; Yang, C.; Cao, J. The security for power internet of things: Framework, policies, and countermeasures. Proceedings - 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2014. Institute of Electrical and Electronics Engineers Inc., 2014, pp. 139–142. doi:10.1109/CyberC.2014.32.
3. SăLndescu, C.; Grigorescu, O.; Rughiniş, R.; Deaconescu, R.; Călin, M. Why IoT security is failing. the Need of a Test Driven Security Approach. Proceedings - 17th RoEduNet IEEE International Conference: Networking in Education and Research, RoEduNet 2018, 2018. doi:10.1109/ROEDUNET.2018.8514135.
4. Bani Irshaid, M.; Bany Salameh, H.; Jararweh, Y. Intelligent multichannel cross-layer framework for enhanced energy-efficiency in 6G-IoT wireless networks. *Sustainable Energy Technologies and Assessments* **2023**, *57*, 103211. doi:10.1016/j.seta.2023.103211.
5. Ruggiero, B. Combining exposure indicators and predictive analytics for threats detection in real industrial IoT sensor networks **2020**. pp. 423–428.
6. Santos, M.F.O.; Melo, W.S.; Machado, R. Cyber-Physical Risks identification on Industry 4.0: A Methodology Proposal. *2022 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2022 - Proceedings* **2022**, pp. 300–305. doi:10.1109/MetroInd4.0IoT54413.2022.9831576.
7. Hosseinzadeh, M.; Ali, S.; Mohammed, A.H.; Lansky, J.; Mildeova, S.; Yousefpoor, M.S.; Yousefpoor, E.; Hassan Ahmed, O.; Rahmani, A.M.; Mehmood, A. An energy-aware routing scheme based on a virtual relay tunnel in flying ad hoc networks. *Alexandria Engineering Journal* **2024**. doi:10.1016/j.aej.2024.02.006.
8. Karaturk, E. Security Concepts in Smart Cities **2020**.
9. Elkhouly, S.M.E.; Ahmed, Y.; Yehia, E.A. The Cyber Security Vulnerabilities in the Internet of Things : A Case Study. *Cf* **2020**, *18*, 97–111.
10. Arumugam, K.; Rajesha, N.; Prasad, M.; Shanmugasundaram, N.; Rao, D.S.; Suneela, B. Spectrum Sensing Framework and Energy-Efficient Resource Allocation for Cognition Enhancement Network. *2023 International Conference on Computer Communication and Informatics, ICCCI 2023* **2023**, pp. 1–5. doi:10.1109/ICCCI56745.2023.10128172.
11. Rajesh, D.; Rajanna, G.S. Energy aware data harvesting strategy based on optimal node selection for extended network lifecycle in smart dust. *Journal of Intelligent and Fuzzy Systems* **2023**, *44*, 939–949. doi:10.3233/JIFS-221719.
12. Salameh, H.A.; Bani Irshaid, M.; Al Ajlouni, A.; Aloqaily, M. Energy-efficient cross-layer spectrum sharing in CR green IoT networks. *IEEE Transactions on Green Communications and Networking* **2021**, *5*, 1091–1100. doi:10.1109/TGCN.2021.3076695.
13. Ambika, K.; Malliga, S. Secure hyper intelligence in routing protocol with low-power (RPL) Networks in IoT. *Advances in Engineering Software* **2022**, *173*, 103247. doi:10.1016/j.advengsoft.2022.103247.
14. Wu, Y.; Huo, Y. Cross-layer secure transmission schemes for social internet of things: Overview, opportunities and challenges. *Neurocomputing* **2022**, *500*, 703–711. doi:10.1016/j.neucom.2021.07.105.
15. Debnath, D.; Chettri, S.K.; Dutta, A.K. Security and Privacy Issues in Internet of Things. *Lecture Notes in Networks and Systems* **2022**, *314*, 65–74. doi:10.1007/978-981-16-5655-2_7.
16. Chaguile, C.C.; Alipio, M.; Bures, M. A Classification of Cross-Layer Optimization Approaches in LoRaWAN for Internet of Things. *International Conference on Ubiquitous and Future Networks, ICUFN* **2023**, *2023-July*, 259–264. doi:10.1109/ICUFN57995.2023.10199434.

17. Bhattacharjee, D.; Acharya, T.; Chakravarty, S. Energy efficient data gathering in IoT networks with heterogeneous traffic for remote area surveillance applications: A cross layer approach. *IEEE Transactions on Green Communications and Networking* **2021**, *5*, 1165–1178. doi:10.1109/TGCN.2021.3092765.
18. Safaei, B.; Monazzah, A.M.H.; Ejlali, A. ELITE: An Elaborated Cross-Layer RPL Objective Function to Achieve Energy Efficiency in Internet-of-Things Devices. *IEEE Internet of Things Journal* **2021**, *8*, 1169–1182. doi:10.1109/JIOT.2020.3011968.
19. Ma, J.; Gao, H.; Guo, L.; Li, H. Energy-efficient joint resource allocation for heterogeneous cellular networks with wireless backhauls. *AEU - International Journal of Electronics and Communications* **2024**, *176*, 155170. doi:10.1016/j.aeue.2024.155170.
20. Hosseinzadeh, M.; Ali, S.; Hussein, A.; Lansky, J. An energy-aware routing scheme based on a virtual relay tunnel in flying ad hoc networks. *Alexandria Engineering Journal* **2024**. doi:10.1016/j.aej.2024.02.006.
21. Uddin, R.S.; Manifa, N.Z.; Chakma, L.; Islam, M.M. Cross-Layer Architecture for Energy Optimization of Edge Computing. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* **2023**, *491 LNICST*, 687–701. doi:10.1007/978-3-031-34622-4_54.
22. Sakthidasan Sankaran, K.; Kim, B.H. Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. *Sustainable Energy Technologies and Assessments* **2023**, *56*, 102983. doi:10.1016/j.seta.2022.102983.
23. Yaici, W.; Krishnamurthy, K.; Entchev, E.; Longo, M. Survey of Internet of Things (IoT) Infrastructures for Building Energy Systems. *GIoTS 2020 - Global Internet of Things Summit, Proceedings* **2020**. doi:10.1109/GIOTS49054.2020.9119669.
24. Zahid, H.; Hina, S.; Hayat, M.F.; Shah, G.A. Agentless Approach for Security Information and Event Management in Industrial IoT. *Electronics (Switzerland)* **2023**, *12*. doi:10.3390/electronics12081831.
25. Bhushan, B.; Sangaiah, A.K.; Nguyen, T.N. *AI Models for Blockchain-Based Intelligent Networks in IoT Systems*; Vol. 6, 2023. doi:10.1007/978-3-031-31952-5.
26. de Caldas Filho, F.L.; Soares, S.C.M.; Oroski, E.; de Oliveira Albuquerque, R.; da Mata, R.Z.A.; de Mendonça, F.L.L.; de Sousa Júnior, R.T. Botnet Detection and Mitigation Model for IoT Networks Using Federated Learning. *Sensors* **2023**, *23*, 1–35. doi:10.3390/s23146305.
27. Bukhowah, R.; Aljughaiman, A.; Rahman, M.M. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. *Electronics (Switzerland)* **2024**, *13*. doi:10.3390/electronics13061031.
28. Javed, S.; Sajid, A.; Kiren, T.; Khan, I.U.; Dewi, C.; Cauteruccio, F.; Christanto, H.J. A Subjective Logical Framework-Based Trust Model for Wormhole Attack Detection and Mitigation in Low-Power and Lossy (RPL) IoT-Networks. *Information (Switzerland)* **2023**, *14*. doi:10.3390/info14090478.
29. Sarabia-Jácome, D.; Giménez-Antón, S.; Liatifis, A.; Grasa, E.; Catalán, M.; Pliatsios, D. Progressive Adoption of RINA in IoT Networks: Enhancing Scalability and Network Management via SDN Integration. *Applied Sciences (Switzerland)* **2024**, *14*. doi:10.3390/app14062300.
30. Saurabh.; Sharma, C.; Khan, S.; Mahajan, S.; Alsagri, H.S.; Almjally, A.; Alabduallah, B.I.; Ansari, A.A. Lightweight Security for IoT. *Journal of Intelligent and Fuzzy Systems* **2023**, *45*, 5423–5439. doi:10.3233/JIFS-232388.
31. Rojas, E.; Carrascal, D.; Lopez-Pajares, D.; Alvarez-Horcajo, J.; Carral, J.A.; Arco, J.M.; Martinez-Yelmo, I. A Survey on AI-Empowered Softwarized Industrial IoT Networks. *Electronics (Switzerland)* **2024**, *13*. doi:10.3390/electronics13101979.
32. Singh, S.K.; Tanwar, S.; Jadeja, R.; Singh, S.; Polkowski, Z. *Secure and intelligent IoT-enabled smart cities*; Vol. i, 2024; pp. 1–453. doi:10.4018/979-8-3693-2373-1.
33. Elkhodr, M.; Khan, S.; Gide, E. A Novel Semantic IoT Middleware for Secure Data Management: Blockchain and AI-Driven Context Awareness. *Future Internet* **2024**, *16*, 1–31. doi:10.3390/fi16010022.
34. Almagrabi, A.O. Challenges and vulnerability evaluation of smart cities in IoT device based on cybersecurity mechanism. *Expert Systems* **2023**, *40*, 1–16. doi:10.1111/exsy.13113.
35. Donca, I.C.; Stan, O.P.; Misaros, M.; Stan, A.; Miclea, L. Comprehensive Security for IoT Devices with Kubernetes and Raspberry Pi Cluster. *Electronics (Switzerland)* **2024**, *13*, 1–22. doi:10.3390/electronics13091613.
36. Madhu, D.; Vasuhi, S. Lightweight Encryption Assisted Man-in-The-Middle Attack-Resilient Steganography Model for Secure Satellite Imagery Services: LEMARS. *Journal of Intelligent and Fuzzy Systems* **2023**, *45*, 2847–2869. doi:10.3233/JIFS-223329.

37. Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. *ACM Computing Surveys* **2022**, *54*. doi:10.1145/3462513.
38. Magara, T.; Zhou, Y. Internet of Things (IoT) of Smart Homes: Privacy and Security. *Journal of Electrical and Computer Engineering* **2024**, *2024*. doi:10.1155/2024/7716956.
39. Wang, A.; Mohaisen, A.; Chen, S. XLF: A cross-layer framework to secure the internet of things (IoT). *Proceedings - International Conference on Distributed Computing Systems* **2019**, *2019-July*, 1830–1839. doi:10.1109/ICDCS.2019.00181.
40. Tandon, A.; Srivastava, P. Location based secure energy efficient cross layer routing protocols for IOT enabling technologies. *International Journal of Innovative Technology and Exploring Engineering* **2019**, *8*, 368–374.
41. Lazarev, A. MODERN METHODS OF TESTING AND INFORMATION SECURITY PROBLEMS IN IoT. *Bulletin of TUIT: Management and Communication Technologies* **2021**. doi:10.51348/tuitmct424.
42. Iqbal, W.; Abbas, H.; Daneshmand, M.; Rauf, B.; Bangash, Y.A. An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet of Things Journal* **2020**, *7*, 10250–10276. doi:10.1109/JIOT.2020.2997651.
43. Ozalp, A.N.; Albayrak, Z.; Cakmak, M.; Ozdogan, E. Layer-based examination of cyber-attacks in IoT. *HORA 2022 - 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings* **2022**. doi:10.1109/HORA55278.2022.9800047.
44. Zeadally, S.; Das, A.K.; Sklavos, N. Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things (Netherlands)* **2021**, *14*, 100075. doi:10.1016/j.iot.2019.100075.
45. Zeng, H.; Dhiman, G.; Sharma, A.; Sharma, A.; Tselykh, A. An IoT and Blockchain-based approach for the smart water management system in agriculture. *Expert Systems* **2023**, *40*, 1–14. doi:10.1111/exsy.12892.
46. Arulselvan, G.; Rajaram, A. Hybrid trust-based secure routing protocol for detection of routing attacks in environment monitoring over MANETs. *Journal of Intelligent and Fuzzy Systems* **2023**, *45*, 6575–6590. doi:10.3233/JIFS-231905.
47. Shukla, P.; Patel, R.; Varma, S. A novel of congestion control architecture using edge computing and trustworthy blockchain system. *Journal of Intelligent and Fuzzy Systems* **2023**, *44*, 6303–6326. doi:10.3233/JIFS-223073.
48. Qayyum, A.; Butt, M.A.; Ali, H.; Usman, M.; Halabi, O.; Al-Fuqaha, A.; Abbasi, Q.H.; Imran, M.A.; Qadir, J. Secure and Trustworthy Artificial Intelligence-extended Reality (AI-XR) for Metaverses. *ACM Computing Surveys* **2024**, *56*, 1–38, [2210.13289]. doi:10.1145/3614426.
49. Xiao, J.; Chang, C.; Ma, Y.; Yang, C.; Yuan, L. Secure multi-path routing for Internet of Things based on trust evaluation. *Mathematical Biosciences and Engineering* **2024**, *21*, 3335–3363. doi:10.3934/mbe.2024148.
50. Becherer, M.; Hussain, O.K.; Zhang, Y.; Den Hartog, F.; Chang, E. On Trust Recommendations in the Social Internet of Things - A Survey. *ACM Computing Surveys* **2024**, *56*. doi:10.1145/3645100.
51. Qasem, A.; Shirani, P.; Debbabi, M.; Wang, L.; Lebel, B.; Agba, B.L. Automatic Vulnerability Detection in Embedded Devices and Firmware: Survey and Layered Taxonomies. *ACM Computing Surveys* **2021**, *54*. doi:10.1145/3432893.
52. Wu, X.W.; Yang, E.H.; Wang, J. Lightweight security protocols for the Internet of Things. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC* **2017**, *2017-Octob*, 1–7. doi:10.1109/PIMRC.2017.8292779.
53. Kamaldeep.; Malik, M.; Dutta, M.; Granjal, J. IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things. *IEEE Sensors Journal* **2021**, *21*, 28066–28076. doi:10.1109/JSEN.2021.3124886.
54. Li, X.; Niu, J.; Bhuiyan, M.Z.A.; Wu, F.; Karuppiah, M.; Kumari, S. A robust ECC-Based provable secure authentication protocol with privacy preserving for industrial internet of things. *IEEE Transactions on Industrial Informatics* **2018**, *14*, 3599–3609. doi:10.1109/TII.2017.2773666.
55. Saadeh, M.; Sleit, A.; Qatawneh, M.; Almobaideen, W. Authentication techniques for the internet of things: A survey. *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016* **2016**, pp. 28–34. doi:10.1109/CCC.2016.22.
56. Gu, T.; Mohapatra, P. BF-IoT: Securing the IoT networks via fingerprinting-based device authentication. *Proceedings - 15th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2018* **2018**, pp. 254–262. doi:10.1109/MASS.2018.00047.
57. Li, N.; Liu, D. for IoT and Its Applications **2017**. *2*, 359–370.

58. Xu, D.; Yu, K.; Ritcey, J.A. Cross-Layer Device Authentication With Quantum Encryption for 5G Enabled IIoT in Industry 4.0. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 6368–6378. doi:10.1109/TII.2021.3130163.
59. Pamarthi, S.; Narmadha, R. Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems* **2022**, *10*, 482–506. doi:10.1108/IJIUS-05-2021-0028.
60. Salman, O.; Abdallah, S.; Elhajj, I.H.; Chehab, A.; Kayssi, A. Identity-based authentication scheme for the Internet of Things. *Proceedings - IEEE Symposium on Computers and Communications* **2016**, *2016-Augus*, 1109–1111. doi:10.1109/ISCC.2016.7543884.
61. Nguyen, K.V.; Nguyen, H.T.; Le, T.Q.; Truong, Q.N.M. Abnormal network packets identification using header information collected from Honeywall architecture. *Journal of Information and Telecommunication* **2023**, *7*, 437–461. doi:10.1080/24751839.2023.2215135.
62. Fei, W.; Ohno, H.; Sampalli, S. A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions. *ACM Computing Surveys* **2024**, *56*, 1–40. doi:10.1145/3625094.
63. Baccari, S.; Hadded, M.; Touali, H.; Muhlethaler, P. A Secure Trust-aware Cross-layer Routing Protocol for Vehicular Ad hoc Networks. *Journal of Cyber Security and Mobility* **2021**, *10*, 377–402. doi:10.13052/jcsm2245-1439.1023.
64. Khan, A.A.; Bourouis, S.; Kamruzzaman, M.M.; Hadjouni, M.; Shaikh, Z.A.; Laghari, A.A.; Elmannai, H.; Dhahbi, S. Data Security in Healthcare Industrial Internet of Things With Blockchain. *IEEE Sensors Journal* **2023**, *23*, 25144–25151. doi:10.1109/JSEN.2023.3273851.
65. Hussain, M.Z.; Hanapi, Z.M. Efficient Secure Routing Mechanisms for the Low-Powered IoT Network: A Literature Review. *Electronics (Switzerland)* **2023**, *12*. doi:10.3390/electronics12030482.
66. Alhusayni, A.; Thayananthan, V.; Albeshri, A.; Alghamdi, S. Decentralized Multi-Layered Architecture to Strengthen the Security in the Internet of Things Environment Using Blockchain Technology. *Electronics (Switzerland)* **2023**, *12*. doi:10.3390/electronics12204314.
67. Alvi, A.N.; Ali, B.; Saleh, M.S.; Alkhathami, M.; Alsadie, D.; Alghamdi, B. Secure Computing for Fog-Enabled Industrial IoT. *Sensors* **2024**, *24*, 1–21. doi:10.3390/s24072098.
68. Bulut, C.; Wu, P.F. More than two decades of research on IoT in agriculture: a systematic literature review. *Internet Research* **2023**. doi:10.1108/INTR-07-2022-0559.
69. Kebande, V.R.; Awad, A.I. Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions. *ACM Computing Surveys* **2024**, *56*. doi:10.1145/3635030.
70. Siqueira, F.; Davis, J.G. Service Computing for Industry 4.0: State of the Art, Challenges, and Research Opportunities. *ACM Computing Surveys* **2022**, *54*. doi:10.1145/3478680.
71. Nechibvute, A.; Mafukidze, H.D. Integration of SCADA and Industrial IoT: Opportunities and Challenges. *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)* **2024**, *41*, 312–325. doi:10.1080/02564602.2023.2246426.
72. Federici, F.; Martintoni, D.; Senni, V. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics (Switzerland)* **2023**, *12*. doi:10.3390/electronics12030566.
73. Bomgni, A.B.; Mdemaya, G.B.; Ali, H.M.; Zanfack, D.G.; Zohim, E.G. ESPINA: efficient and secured protocol for emerging IoT network applications. *Cluster Computing* **2023**, *26*, 85–98. doi:10.1007/s10586-021-03493-z.
74. Kore, A.; Patil, S. Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. *Wireless Networks* **2022**, *28*, 287–301. doi:10.1007/s11276-021-02850-5.
75. Kalyani, G.; Chaudhari, S. Cross Layer Security MAC Aware Routing Protocol for IoT Networks. *Wireless Personal Communications* **2022**, *123*, 935–957. doi:10.1007/s11277-021-09163-y.
76. Garg, S.; Kaur, K.; Kaddoum, G.; Choo, K.K.R. Toward Secure and Provable Authentication for Internet of Things: Realizing Industry 4.0. *IEEE Internet of Things Journal* **2020**, *7*, 4598–4606. doi:10.1109/JIOT.2019.2942271.
77. Vijayakumaran, C.; Muthusenthil, B.; Manickavasagam, B. A reliable next generation cyber security architecture for industrial internet of things environment. *International Journal of Electrical and Computer Engineering* **2020**, *10*, 387–395. doi:10.11591/ijece.v10i1.pp387-395.
78. Qadri, Y.A.; Nauman, A.; Zikria, Y.B.; Vasilakos, A.V.; Kim, S.W. The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Communications Surveys and Tutorials* **2020**, *22*, 1121–1167. doi:10.1109/COMST.2020.2973314.

79. Li, C.; Xu, Z.; Wang, J.; Zhao, J.; He, B.; Wang, L.; Li, J. Enhanced Clustering MAC Protocol Based on Learning Automata for UV Networks. *Photonics* **2024**, *11*. doi:10.3390/photonics11040340.
80. Jain, S.; Verma, R.K. A Taxonomy and Survey on Grid-Based Routing Protocols Designed for Wireless Sensor Networks. *ACM Computing Surveys* **2024**, *56*, 1–41. doi:10.1145/3653315.
81. Al-Otaibi, S.; Khan, R.; Ali, H.; Khan, A.A.; Saeed, A.; Ali, J. A Hybrid and Lightweight Device-to-Server Authentication Technique for the Internet of Things. *Computers, Materials and Continua* **2024**, *78*, 3805–3823. doi:10.32604/cmc.2024.049017.
82. Akbar, M.S.; Hussain, Z.; Sheng, M.; Shankaran, R. Wireless Body Area Sensor Networks: Survey of MAC and Routing Protocols for Patient Monitoring under IEEE 802.15.4 and IEEE 802.15.6. *Sensors* **2022**, *22*. doi:10.3390/s22218279.
83. Soundararajan, R.; Maheswar, R.; Muthuramalingam, A.; Hossain, E.; Lloret, J. Interleaved Honeypot-Framing Model with Secure MAC Policies for Wireless Sensor Networks. *Sensors* **2022**, *22*. doi:10.3390/s22208046.
84. Subramanyam, R.; Jancy, Y.A.; Nagabushanam, P. Cooperative optimization techniques in distributed MAC protocols – a survey. *International Journal of Pervasive Computing and Communications* **2024**, *20*, 285–307. doi:10.1108/IJPCC-07-2022-0256.
85. De Vincenzi, M.; Costantino, G.; Matteucci, I.; Fenzl, F.; Plappert, C.; Rieke, R.; Zelle, D. A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet. *ACM Computing Surveys* **2024**, *56*. doi:10.1145/3637059.
86. Erskine, S.K.; Chi, H.; Elleithy, A. SDAA: Secure Data Aggregation and Authentication Using Multiple Sinks in Cluster-Based Underwater Vehicular Wireless Sensor Network. *Sensors* **2023**, *23*. doi:10.3390/s23115270.
87. Klaiber, J.; Van Dinther, C. Deep Learning for Variable Renewable Energy: A Systematic Review. *ACM Computing Surveys* **2023**, *56*. doi:10.1145/3586006.
88. Velayudhan, N.K.; S, A.; Devidas, A.R.; Ramesh, M.V. Delay and Energy Efficient Offloading Strategies for an IoT Integrated Water Distribution System in Smart Cities. *Smart Cities* **2024**, *7*, 179–207. doi:10.3390/smartcities7010008.
89. Maheswar, R.; Kathirvelu, M.; Mohanasundaram, K. Energy Efficiency in Wireless Networks. *Energies* **2024**, *17*, 1–14. doi:10.3390/en17020417.
90. Nathiya, N.; Rajan, C.; Geetha, K. An energy-efficient cluster routing for internet of things-enabled wireless sensor network using mapdiminution-based training-discovering optimization algorithm. *Sadhana - Academy Proceedings in Engineering Sciences* **2024**, *49*. doi:10.1007/s12046-023-02371-1.
91. Esmali Nojehdeh, M.; Altun, M. Energy-Efficient Hardware Implementation of Fully Connected Artificial Neural Networks Using Approximate Arithmetic Blocks. *Circuits, Systems, and Signal Processing* **2023**, *42*, 5428–5452. doi:10.1007/s00034-023-02363-w.
92. Sharma, D.; Jain, S.; Maik, V. Energy Efficient Clustering and Optimized LOADng Protocol for IoT. *Intelligent Automation and Soft Computing* **2022**, *34*, 357–370. doi:10.32604/iasc.2022.025637.
93. Wu, M.; Zhang, F.; Rui, X. An energy-aware approach for resources allocating in the internet of things using a forest optimization algorithm. *Circuit World* **2023**, *49*, 269–280. doi:10.1108/CW-02-2020-0017.
94. Sanchez-Iborra, R.; Zoubir, A.; Hamdouchi, A.; Idri, A.; Skarmeta, A. Intelligent and Efficient IoT Through the Cooperation of TinyML and Edge Computing. *Informatica (Netherlands)* **2023**, *34*, 147–168. doi:10.15388/22-INFOR505.
95. Khan, M.N.U.; Cao, W.; Tang, Z.; Ullah, A.; Pan, W. Energy-Efficient De-Duplication Mechanism for Healthcare Data Aggregation in IoT. *Future Internet* **2024**, *16*, 1–21. doi:10.3390/fi16020066.
96. Komala, C.R.; Velmurugan, V.; Maheswari, K.; Deena, S.; Kavitha, M.; Rajaram, A. Multi-UAV computing enabling efficient clustering-based IoT for energy reduction and data transmission. *Journal of Intelligent and Fuzzy Systems* **2023**, *45*, 1717–1730. doi:10.3233/JIFS-231242.
97. Ahmed, A.S.; Kurnaz, S.; Hamdi, M.M.; Khaleel, A.M.; Khaleel, A.M.; Seno, M.E. Study for Buildings with IoT System for Energy Management. *ISMSIT 2022 - 6th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings* **2022**, pp. 53–57. doi:10.1109/ISMSIT56059.2022.9932729.
98. Panchal, M.; Upadhyay, R.; Vyavahare, P.D. Cross-Layer based Energy Efficient Reliable Data Transmission System for IoT Networks. *Proceedings - 2022 IEEE 11th International Conference on Communication Systems and Network Technologies, CSNT 2022* **2022**, pp. 527–532. doi:10.1109/CSNT54456.2022.9787600.

99. Singhal, S.; Tripathi, S. Data-driven Secure Authentication for Smart Grid IoT Networks. *Proceedings of CONECCT 2023 - 9th International Conference on Electronics, Computing and Communication Technologies* **2023**, pp. 1–6. doi:10.1109/CONECCT57959.2023.10234815.
100. Bapatla, A.K.; Puthal, D.; Mohanty, S.P.; Yanambaka, V.P.; Kougianos, E. EasyChain: an IoT-friendly blockchain for robust and energy-efficient authentication. *Frontiers in Blockchain* **2023**, *6*, 1–19. doi:10.3389/fbloc.2023.1194883.
101. Sridhar, M.; Pankajavalli, P.B. Energy - Efficient routing and scheduling using clustering in geographic routing protocol. *Journal of Intelligent and Fuzzy Systems* **2023**, *44*, 951–961. doi:10.3233/JIFS-220966.
102. Sugumaran, V.R.; Rajaram, A. Lightweight blockchain-assisted intrusion detection system in energy efficient MANETs. *Journal of Intelligent and Fuzzy Systems* **2023**, *45*, 4261–4276. doi:10.3233/JIFS-231340.
103. Goyal, H.; Kodali, K.; Saha, S. LiPI: Lightweight Privacy-Preserving Data Aggregation in IoT **2022**. [2207.12197]. doi:10.1109/TrustCom60117.2023.00226.
104. Murtaza, G.; Iqbal, F.; Altaf, A.; Rasheed, A. Techniques for Resource-Efficient, Lightweight Cryptography in IoT Devices for Smart Environment. *Proceedings - 2023 6th International Conference of Women in Data Science at Prince Sultan University, WiDS-PSU 2023* **2023**, pp. 223–228. doi:10.1109/WiDS-PSU57071.2023.00053.
105. Kousalya, R.; Sathish Kumar, G.A. A Survey of Light-Weight Cryptographic Algorithm for Information Security and Hardware Efficiency in Resource Constrained Devices. *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019* **2019**. doi:10.1109/ViTECoN.2019.8899376.