Hindawi
Journal of Electrical and Computer Engineering
Volume 2024, Article ID 7716956, 17 pages
https://doi.org/10.1155/2024/7716956

Review Article

Internet of Things (IoT) of Smart Homes: Privacy and Security

Tinashe Magara[1] **and Yousheng Zhou**[1,2]

[1] *College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2] *School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Correspondence should be addressed to Yousheng Zhou; zhouys@cqupt.edu.cn

Received 2 December 2023; Revised 21 March 2024; Accepted 29 March 2024; Published 8 April 2024

Academic Editor: Neng Ye

The Internet of Things (IoT) constitutes a sophisticated network that interconnects devices, optimizing functionality across various domains of human activity. Recent literature projections anticipate a significant increase, with estimates exceeding 50 billion connected devices by 2025. Despite its transformative potential, the IoT landscape confronts formidable privacy and security challenges, encompassing intricate issues such as data acquisition, anonymization, retention, sharing practices, and behavioural profiling. Effectively addressing these challenges mandates the development of scalable solutions, innovative management strategies, and adaptable policy frameworks. In this paper, we conduct an exhaustive examination of major IoT applications, alongside associated privacy and security concerns. We systematically categorize prevalent privacy, security, and interoperability issues within the context of the IoT layered architecture. The review highlights current research initiatives focused on developing energy-efficient devices, optimizing microprocessors, and fostering interdisciplinary collaborations to address the challenges in the IoT landscape. To efficaciously manage risks in this dynamic landscape, stakeholders must implement comprehensive strategies that span stringent data protection legislation, extensive user education initiatives, and the deployment of robust authorization and authentication frameworks. This paper aims to empower industry leaders, policymakers, and researchers by providing actionable solutions, not just insights, to navigate the complexities of the IoT landscape effectively. Future research initiatives should prioritize the fortification of security measures for large-scale IoT deployments, the formulation of user-centric privacy solutions, and the standardization of interoperability protocols. By establishing a robust foundational framework, our paper endeavours to spearhead the discourse on IoT applications, privacy paradigms, and security frameworks, paving the way towards a resilient and interconnected future.

1. Introduction

The Internet of Things (IoT) is a revolutionary idea that refers to a vast network of interconnected physical devices, vehicles, appliances, and various objects that are embedded with sensors, software, and other technologies that allow them to collect and exchange data via the Internet or other communication networks. These devices can be everyday objects like smartphones, wearable fitness trackers, home appliances, industrial machines, and even vehicles [1]. The key components of IoT are the embedded sensors and actuators that allow these devices to sense and interact with their environment. These sensors gather data from the surroundings, such as temperature, humidity, motion, and so on. The collected data is then processed by the device's software, which can make real-time decisions or send the data to a centralized server or cloud for further analysis and storage.

The main goal of IoT is to create a seamless and intelligent network where physical objects can communicate with each other and with humans, leading to more efficient and automated processes, improved decision-making, and an enhanced user experience [2]. By leveraging IoT, businesses and industries can optimise their operations, enhance productivity, and develop new innovative services and products [3]. However, with the increasing adoption of IoT, concerns regarding data privacy, security, and standardization have also emerged [4, 5]. As billions of devices get connected [6], it becomes crucial to ensure robust privacy and security measures are in place to protect sensitive information and prevent potential cyberattacks. The IoT has the potential to revolutionize various aspects of our lives, bringing forth a new era of interconnectedness and technological advancements. As technology continues to evolve, IoT is expected to play a central role in shaping the future of industry, infrastructure, and everyday living. We outline the following contributions in our paper:

(i) This paper provides a comprehensive review covering IoT applications, security issues, privacy concerns, and solutions across various domains.

(ii) We highlight the primary applications of IoT and associated privacy and security concerns within the IoT domain, along with proposed countermeasures found in existing literature.

(iii) We propose a threat taxonomy for IoT applications, privacy, and security.

(iv) Finally, we discuss open research directions relevant to the areas highlighted in this survey.

The rest of the paper is structured as follows. In Section 2, we introduce the multifaceted applications of IoT. In Section 3, highlights IoT security challenges, Section 4, highlights IoT privacy concerns, Section 5, proffers IoT security solutions and IoT interoperability. Finally, Section 6 summarises the research findings and concludes with a discussion on future trends.

2. IoT Applications

In recent years, a few surveys have been conducted to highlight research advancements across various domains. In the following subsections, we categorize existing survey works based on IoT-related objectives. In the following subsections, we categorize the existing survey works on the basis of IoT-related objectives. The way we connect to the world around us is being completely transformed by the Internet of Things (IoT). IoT applications are transforming businesses, improving our lives by connecting everyday objects to the Internet, and enabling them to interact [7].

The IoT is fostering innovation across every sector, from smart homes that provide convenience and energy efficiency to industrial settings that optimise operations through predictive maintenance [8]. The application of IoT for remote patient monitoring helps the medical field, and precision farming increases crop yields in agriculture [9]. Public safety is improved as traffic management becomes more effective in smart cities [10]. The potential of the Internet of Things is limitless as it develops, holding up the promise of a day when connection and data-driven insights will redefine what is possible in our increasingly networked world [11]. Based on the literature synthesis, Figure 1 and Table 1 provide a detailed summary of the multifaceted applications of IoT.

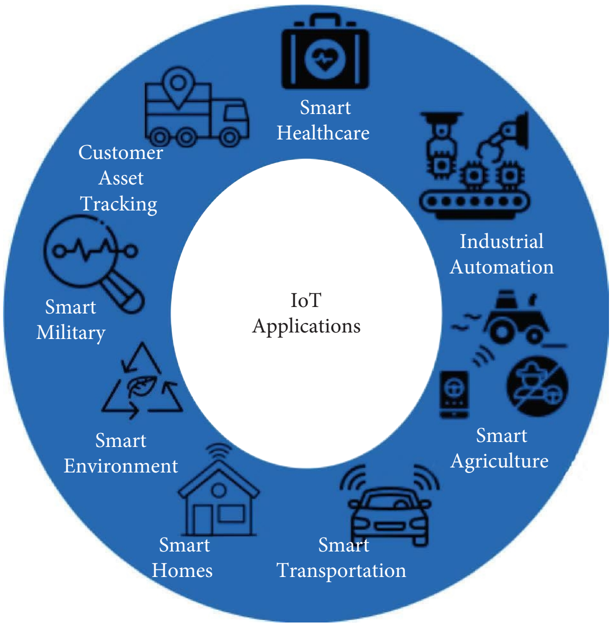

Figure 1: IoT applications.

2.1. Smart Healthcare. Smart healthcare is a game-changing method that uses cutting-edge technologies to improve the quality, efficiency, and accessibility of healthcare services [18]. It includes a wide range of applications aimed at improving patient care, streamlining healthcare processes, and empowering individuals to take control of their health [19]. Smart healthcare is changing the face of healthcare by improving patient experiences, lowering costs, and eventually leading to improved health outcomes for individuals and communities [20, 21]. It provides the potential for a future healthcare system that is more efficient and effective. Table 2 outlines recent research areas and major visions in IoT applications for smart healthcare.

2.2. Smart Transportation. Smart transportation uses innovative technologies and data-driven solutions to improve transportation systems' efficiency, safety, and sustainability [28]. It comprises a wide range of applications aimed at improving mobility, reducing congestion, and reducing environmental impact. Smart mobility is transforming how people and products move, providing answers to urban congestion, environmental concerns, and inefficiencies in transit. It has the potential to make future transit systems more sustainable, accessible, and safe [29]. Table 3 provides a summary of the applications of IoT in the domain of smart transportation and logistics.

2.3. Smart Agriculture. Smart agriculture, also known as precision agriculture, uses modern technology and data-driven solutions to optimise farming, practises, boost agricultural output, and encourage sustainable resource management [36]. Smart agriculture is revolutionising traditional agricultural practises by leveraging the power of technology and data analytics. It has the potential to enhance

Table 1: IoT applications.

Author	Survey	Objective
[12]	IoT application, a survey	The main objective includes the overview of current research trends, key technologies, and applications of IoT, along with the potential for complete automation in the future
[13]	IoT for industrial application: Survey	The main objective include the opportunities IoT provides for industrial systems, the development of modern IoT applications, and a proposed system for monitoring and decision-making in industrial applications using IoT
[14]	A survey of IoT applications in blockchain systems	The main objective includes an overview of key components of IoT blockchain and popular applications, a comparison of consensus protocols for IoT blockchains, and an analysis of traffic models for P2P and blockchain systems
[15]	Internet of things applications: A systematic review	The main findings include categorizing and analysing current research techniques on IoT applications approaches across various domains, presenting a technical taxonomy for IoT applications, and comparing IoT applications based on technical features while discussing achievements, disadvantages, weaknesses, and future research challenges
[16]	A survey on emerging IoT applications	The main objective of the paper includes the description of IoT as an emerging technology connecting devices for effective communication, the components of IoT like sensors and cloud for data processing, and the role of microcomputers in collecting and processing sensor data before sending it to the cloud for analysis and access through mobile applications
[17]	Internet of things and its applications: A comprehensive survey	The study showcases the varied selection of articles across different IoT focus areas, summarises key challenges in various application domains, and suggests the potential for business growth with an efficient network design

Table 2: Smart healthcare applications of IoT.

Author	Smart healthcare IoT
[22]	Proposed the concept of smart healthcare, which uses new information technologies to make healthcare more efficient, convenient, and personalized. It also discusses the existing problems with smart healthcare and the prospects of smart healthcare
[23]	The proposed system is superior in performance and is highly effective in delivering healthcare services during workouts. This research presents an intelligent healthcare framework based on IoT technology to provide ubiquitous healthcare to a person during his/her workout sessions
[24]	They suggested a deep learning model that outperforms state-of-the-art algorithms in terms of accuracy. A cognitive healthcare framework is developed that employs IoT-cloud technology and deep learning for intelligent decision-making
[25]	They suggested a smart Saskatchewan healthcare system based on IoT technology in four areas: Business analytics and cloud services, cancer care services, emergency services, and operational services
[26]	A four-layered architecture for monitoring and predicting infection in urine allows people to check their health daily and anticipate urinary infection so that preventive actions may be implemented early on. A four-layered architecture for monitoring and forecasting UI in urine was proposed
[27]	Adoption and use of IoT/WSN technologies to supplement existing treatment choices in order to give healthcare solutions are advocated. To demonstrate and promote the functioning IoT-based solution for cancer care services, we provided a number of frameworks and architectures

Table 3: Smart transportation applications of IoT.

Author	Smart transportation IoT
[30]	Proposed a smart transportation system that reduces the risk of accidents. IoT technology enables a smart transportation system that reduces the risk of accidents, improves safety, increases capacity, reduces fuel consumption, and enhances overall comfort and performance for drivers
[31]	Proposed in smart-sensor prototype that can create an O/D matrix for several BRT routes. Its smart sensor prototype can detect bluetooth signals from devices used by people travelling by BRT systems
[32]	The internet of things and blockchain technology are becoming a reality in smart transportation. A layered framework, BCTLF, has been proposed to integrate IoT and blockchain for smart logistics and transportation
[33]	A smart information system has been developed in which travellers receive notice of their present position, the upcoming location of the bus, and the crowd level within the bus. The suggested system emphasises how intelligent transportation system (ITS) may decrease obstacles to public transportation use and have a favourable influence on bus travel
[34]	The suggested architecture's simulation output is projected to provide a strategic guide for strategic security management of urban smart transportation. A smart transport security system can be proposed using a geospatial modelling technique. An experimental research was carried out in Beijing, China, to simulate the suggested design, which may serve as a strategic guide for urban smart transport strategic security management
[35]	The internet of things may be created by combining bus scheduling, bus presence detection, and passenger payment efficiency via a booking seat system. The usage of IoT has mostly focused on safety in order to avert road accidents

food output, minimise waste, and encourage environmental stewardship while assuring agricultural sustainability for future generations. Table 4 summarises the applications of IoT as applied in the domain of smart agriculture.

2.4. Smart Military. Smart military, also known as contemporary warfare or defence technology, is the integration of new technologies to improve the capabilities, effectiveness, and efficiency of armed forces. These technologies are intended to strengthen national security, safeguard soldiers, and give a strategic edge in a variety of operational areas [43]. Smart military technologies continue to advance, affecting the future of battle and defence. While these breakthroughs bring considerable benefits, ethical issues and international rules are critical to ensuring responsible and accountable usage in military operations. Table 5 summarises the applications of IoT as applied in the domain of smart military.

Table 4: Smart agriculture applications of IoT.

Author	Smart agriculture IoT
[37]	In the suggested concept, IoT sensor were employed. Crop management, resource management, cost efficiency, quality and quantity, crop monitoring, and field monitoring may all be improved by IoT
[38]	Smart agriculture is an automated and guided information technology used with the internet of things. They presented a remote monitoring system that enables quick access to agricultural facilities such as notifications via short messaging service (SMS) and guidance on weather patterns, crops, and so on
[39]	Sensors that can provide information about their agricultural areas are a new concept. Environmental conditions in agricultural areas may be monitored with IoT sensors. Temperature and humidity may be measured with a single CC3200 chip. The camera may be linked to the CC3200 in order to shoot photographs and send them through MMS to farmers' mobile phones over Wi-Fi
[40]	Farmers may use IoT-based systems to remotely monitor and regulate their crops, as well as gather and analyse data in real time. IoT-based solutions can also assist to cut farming costs, enhance crop yields, and improve agricultural product quality
[41]	The proposed technique minimises the network latency to a certain level. A scalable network architecture is proposed for monitoring and regulating agriculture and farms in rural regions. Reduced network latency to a certain extent. Cross-layer channel access and routing solutions for sensing and actuation
[42]	Smart agriculture takes advantage of IoT by storing data from numerous sensors in the cloud. IoT has emerged as a key 21st-century technology for agricultural management. Data for smart agriculture is being collected and stored using sensors and cloud computing. Smart agriculture has the ability to increase agricultural product quality and quantity

Table 5: Smart military applications of IoT.

Author	Smart military IoT
[44]	The study highlights the work done by the NATO IST-147 "military applications of internet of things" group, which investigates the possibility of using smart city IoT capabilities in military operations
[45]	They demonstrated how widely available IoT components could be integrated to create a secure and low-cost sensor system that could be utilised for a variety of military applications such as smart military base operations or logistic chain monitoring. They attempt to provide end-to-end security between a sensor gateway installed and a user
[46]	This research describes the history of IoT, as well as the technologies, framework and standardization process of IoT, as well as typical military applications of IoT, such as the battlefield troops presentation system, the battlefield resource guarantees integration system, and the simulation and verification system of tactics and operation schemes
[47]	Warfighters' lives are valuable, so we must do all possible to safeguard them. Military ammunition control is also a significant and necessary component of military operations. The research discusses and analyses several IoT applications and approaches for military missions. The research also explores the protocols and implementation approaches used and presented by people all around the world
[48]	The study outlines the work done by the NATO IST-147 "military applications of the internet of things" group to investigate the possibility of using civilian internet of things (IoT) software defined radio infrastructure as radio frequency sensors for military operations
[49]	Several difficult challenges and scenarios arise in defence. The research hybridization of IoTs with satellite networks can deliver exceptional outcomes that were before unattainable

2.5. Smart Homes. Smart homes use technology to improve their occupants' comfort, security, energy efficiency, and general level of living [50]. These developments strive to make daily chores easier and to provide consumers more control over many aspects of their living surroundings. Residents of smart homes enjoy greater control, energy savings, security, and convenience. Table 6 outlines IoT applications in the context of smart homes.

Table 6: Smart-homes applications of IoT.

Author	Smart homes IoT
[51]	This study found that IoT-based smart home technology can increase home security and energy efficiency. IoT can alleviate the difficulties that the elderly and handicapped encounter. Smart home technologies based on IoT have a bright future
[52]	The study found out that IoT is a growing Internet service with applications in industrial Wireless sensor network (WSN) and smart homes. In an IoT setting, smart homes may be utilised to automate home duties. There are challenges and issues with the IoT and smart home systems, but solutions may be discovered
[53]	According to the findings, IoT is a growing popularity among millennials for delivering smart home gadgets that can be operated remotely. Home automation and smart homes are the most visible IoT services, offering increased efficiency and comfort
[54]	This study emphasised how IoT technology is utilised in smart homes for security, privacy, personalisation, and physical environment control
[55]	The study found out that some potential solutions address the issues connected with smart home applications, such as adopting low-power consumption wireless technologies like Zigbee
[56]	According to the findings of this study, a low-cost home automation system has been built utilising IoT, allowing users to manage and monitor household appliances and electrical machinery via a website. This device may monitor a home's metering system, allowing customers and dealers to detect irregularities in the power distribution system. The planned system includes an online billing system

2.6. *Smart Industrial Automation.*

The integration of modern technology to improve manufacturing and industrial processes is referred to as smart industrial automation, often known as Industry 4.0 or the Industrial Internet of Things (IIoT) [57]. In a variety of industrial areas, these technologies increase efficiency, productivity, safety, and sustainability. Manufacturing and industrial processes are being transformed by smart industrial automation, which makes them more efficient, versatile, and sensitive to changing needs [58]. It is vital to the advancement of contemporary manufacturing and industrial enterprises. Table 7 summarises the applications of IoT as applied in the domain of smart industrial automation.

2.7. *Smart Environment.*

Smart environments are physical locations that have been improved with various technologies in order to increase efficiency, sustainability, safety, and the overall quality of life [65]. These smart environment applications have the ability to improve several parts of our life. These smart environment applications highlight how technology may be used to create more efficient, sustainable, and convenient living and working environments in a variety of disciplines. Table 8 summarises the applications of IoT as applied in the domain of smart environment.

2.8. *Surveillance.*

Smart surveillance is the application of new technologies such as artificial intelligence (AI), machine learning, and the Internet of Things (IoT) to improve traditional surveillance systems [72]. These technologies have a wide range of applications in security, safety, and monitoring [73]. Smart surveillance applications are constantly expanding as a result of breakthroughs in AI and IoT technology. While they provide several benefits in terms of security and safety, there are also worries regarding privacy and ethical consequences [74–76]. Table 9 summarises the applications of IoT as applied in the domain of surveillance.

2.9. *Customer Asset Tracking.*

Customer asset tracking, also known as customer equipment tracking, is the monitoring and management of assets or equipment held by a company but under the control of customers or clients. This is especially effective in increasing customer service efficiency and asset utilization in a variety of sectors [81–83]. Effective customer asset monitoring may help to streamline processes, decrease losses, improve customer happiness, and ultimately save money [84]. It is frequently accomplished by utilising technologies such as RFID (Radio-Frequency Identification), barcoding, GPS tracking, and asset management software. Table 10 summarises the applications of IoT as applied in the domain of customer asset tracking.

3. IoT Security Challenges

The rapid proliferation of Internet of Things (IoT) devices has brought numerous benefits, but it has also introduced significant security risks and vulnerabilities. Several studies and reports have highlighted the potential challenges associated with IoT security [90–92]. Figure 2 summarises the security challenges in IoT ecosystem.

According to Sikder one of the most major concerns about Internet of Things (IoT) devices is the threat of unauthorized access [93]. In addition, to Meneghello et al., if adversaries successfully infiltrate these devices, they will be able to exploit security flaws, perhaps exfiltrating sensitive data or coordinating device subversion [94]. Table 11 highlights the widespread security flaws intrinsic to the IoT ecosystem.

Table 7: Smart industrial automation applications of IoT.

Author	Smart industrial automation IoT
[59]	The study highlights that IoT and industrial automation encounter various issues, including data and service security, trust, data integrity, information privacy, scalability, interoperability, and automation domain constraints. The study combines the concepts of the raspberry pi industrial Workstation and industrial automation with IoT
[60]	In the industrial space, industrial automation plays a critical role in reducing time to market while maintaining good quality and productivity. This research describes the utilization of cloud and IoT capabilities to control devices and analyse the data generated by them
[61]	The study underscores that IoT systems may employ various processing and communication architectures, technologies, and design techniques
[62]	The paper proposes the integration of the internet of things (IoT) for the transformation of smart factories. The research highlights the connectivity of IoT and the distributed nature of intelligent devices. These devices, each exhibiting autonomous or semiautonomous behavior, enable higher production and better utilization of human resources by eliminating significant information gaps about real-time factory conditions. Coupled with innovative techniques like additive manufacturing, this approach facilitates the realization of an optimized advanced manufacturing floor and the vision of a lean, agile, and integrated factory of the future
[63]	The paper underlined that IoT is a crucial technology of the Fourth industrial revolution and offers a potential opportunity to establish influential services and applications for manufacturing. IoT enables smart machines to communicate with one another in order to share data and information, which is required for complex systems to make real-time choices. IoT has a favourable influence on sustainable development, particularly in terms of manufacturing dimensions
[64]	By analysing industrial IoT technology and its implementation in manufacturing workshops, this study proposes a reference design and building route for smart factories. A manufacturing workshop industrial IoT solution is provided, incorporating important technologies such as WSN and RFID. The system proves effective in monitoring production line data, as evidenced by the performance analysis in terms of real-time and quality

These vulnerabilities underscore the pressing need for a comprehensive and proactive approach to securing IoT ecosystems, encompassing robust authentication, encryption, firmware maintenance, interface security, patch management, credential management, physical protection, user education, and privacy preservation. Addressing these issues is paramount in mitigating the ever-evolving threats that IoT devices face. With the emergence of AI and the benefits it offers, it is susceptible to numerous challenges. Current AI security challenges include adversarial attacks, privacy concerns, bias, model security vulnerabilities, reliability issues, explainability gaps, data poisoning, and scalability challenges. Interdisciplinary efforts are needed to enhance robustness, transparency, and regulatory compliance while mitigating risks to privacy, fairness, and intellectual property. We have synthesized the literature and proposed a threat taxonomy for IoT applications, privacy, and security in Table 12.

4. Privacy Concerns in IoT

The massive amount of data collected by IoT devices raises significant privacy concerns as it involves the gathering of personal information, behavioural patterns, and sensitive data from individuals. Figure 3 shows some of the key privacy issues and challenges associated with IoT data collection:

Privacy problems in IoT are intertwined with a web of authorization issues, anonymization quandaries, data retention complexity, data sharing quandaries, and profiling paradoxes [105]. As we navigate through this perilous terrain, it becomes clear that privacy is more than just a legislative concern; it is inextricably linked to the underlying fabric of IoT functioning. To address these challenges, a multifaceted solution incorporating technology, legislation, user education, authorization, and security frameworks is required. Drawing from the literature provided, we propose privacy and security challenges for each IoT layer in Table 13.

5. IoT Security Solutions

Existing security measures and protocols for protecting IoT devices and networks have evolved to address the unique challenges posed by the wide-scale deployment of IoT devices [106–108]. Figure 4 summaries the proposed IoT solutions.

According to the literature, IoT privacy and security solutions are being suggested from a range of viewpoints, including unique concepts and technologies [109, 110]. They

Table 8: Smart environment applications of IoT.

Author	Smart environment IoT
[66]	By analysing industrial IoT technology and its implementation in manufacturing workshops, this study proposes a reference design and building route for smart factories. A manufacturing workshop industrial IoTs solution is provided, incorporating important technologies such as WSN and RFID. The system proves effective in monitoring production line data, as evidenced by the performance analysis in terms of real-time and quality
[67]	According to the findings of this study, the internet of things is considered a critical component in the development of smart environments. The internet of things is considered a critical component in the development of smart environments
[68]	According to this study, the internet of things and smart environments are radically changing the way organisations operate and how individuals interact with the physical world. The ability to communicate such intelligence to other machines, particularly those local and those providing cloud-based deep learning and AI capabilities, has enormous promise for enhancing people's lives in a variety of ways
[69]	The internet of things (IoT) is identified as the primary facilitator of smart environments in this study, including smart cities, building automation, smart transportation, smart grids, and healthcare. The internet of things permits the global networking of billions of small smart things. The internet of things (IoT) may be used to increase the efficiency and efficacy of smart environments
[70]	The term "smart environment" is defined as a technology that provides numerous facilities and solutions for many environmental application difficulties in this study. IoT technology has the ability to give benefits that contribute to the prospect of establishing a green planet and a sustainable lifestyle. IoT enables environmental sensors to communicate with other devices, such as smart phones, through bluetooth or Wi-Fi in order to provide massive volumes of data to the network
[71]	According to the findings, the internet of things is a technological revolution that symbolises the future of computers and communications. IoT offers various potential monitoring uses, such as recognising, automating, monitoring, and controlling items

Table 9: Surveillance.

Author	Surveillance
[77]	The paper presents a security surveillance system in buildings based on IoT using raspberry pi, with features like remote door locking, intruder detection, and alerting the owner. Additional features include rain sensing windows and automatic light control for energy efficiency. The main objective is to implement wireless home automation features and home security
[78]	They proposed a system that exhibits superior performance in resource efficiency, agility, and scalability compared to traditional IoT surveillance systems and state-of-the-art approaches
[79]	The paper focuses on utilising IoT and computer vision for detecting faces in security applications, enhancing security systems by automating detection processes and sending notifications to users
[80]	Development of an IoT-based mobile smart home surveillance application aimed at enhancing security, privacy, and energy efficiency by controlling smart sensors and recording data for future insights

use a first-principle approach to redefine network security for IoT in their study [111]. They address three primary concerns:

(i) The need for scalable alternatives to traditional perimeter defence, as IoT networks necessitate more adaptive security procedures.

(ii) They propose new ways for managing security inside deployed IoT networks, recognising the unique problems of safeguarding a large number of linked devices.

(iii) They suggest new security policies that provide the essential generality to regulate IoT devices and networks across a wide range of use cases, recognising the need for flexibility in IoT security.

Table 14 summarises the recent proposed IoT security solutions.

5.1. IoT Interoperability. IoT interoperability refers to the ability of systems to seamlessly communicate and collaborate across various IoT devices and platforms. It is essential

Table 10: Customer asset tracking.

Author	Customer asset tracking
[85]	The main findings include the identification of IoT technologies' feasibility in asset management, highlighting research potential for smart factories, and recognising significant potential for IoT technologies in managing different asset groups
[86]	The proposed solution offers a lightweight approach without integrating blockchain into IoT devices, meeting the demand for specific features in IoT blockchain applications, and addressing security issues in existing centralized IoT solutions
[87]	The paper presents an asset management system utilising NFC and IoT technologies to track and update asset information, addressing issues of inaccurate asset recording. A low-cost IoT-based NFC reader/writer is introduced as a companion module
[88]	The paper emphasises the need for integrating diverse devices and data ingestion mechanisms into a unified platform for security and data segregation, the development of interoperable platforms to meet increasing demand, and the goal of providing a user-friendly interface for managing devices and data visualization
[89]	The paper focuses on developing innovative IoT devices for better management of asset infrastructure through on-demand tracking and monitoring of rental items using various wireless technologies. The proposed architecture aims to maximize connectivity distance, minimise energy consumption, and address rental asset management challenges while ensuring scalability and quality-of-service. A case study is presented to support the feasibility of the proposed solution in real-world rental management asset scenarios

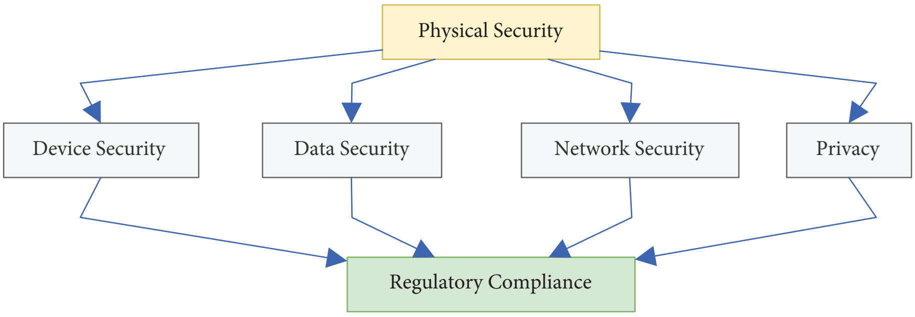

Figure 2: Summary of IoT security challenges.

Table 11: Summary of IoT security challenges.

Ref	Security weaknesses	Description
[95]	Inadequate authentication	A significant risk arises as a result of poor or inefficient authentication procedures, allowing unauthorized access to IoT devices
[96]	Poor encryption	Weak or non-existent encryption protocols can leave data transmissions susceptible to interception and compromise, jeopardising the secrecy of critical information
[97]	Vulnerable firmware	Outdated or inadequately patched firmware can be exploited, leaving devices susceptible to known vulnerabilities that may have been addressed in newer versions
[98]	Insecure interfaces	Interfaces and APIs that lack sufficient security safeguards can be used by malicious actors to influence device functionalities or undermine their integrity
[99]	Insufficient patching	Patch management practises that are irregular or poor may expose devices to known vulnerabilities for lengthy periods of time, raising the chance of exploitation
[100]	Default credentials	Manufacturers' use of default usernames and passwords makes it easier for unauthorized individuals to gain access, a significant security oversight
[101]	Lack of physical security	Insufficient safeguards against physical tampering, or an adversary can expose IoT devices to both direct physical attacks and unauthorized access, potentially leading to device compromise
[102]	Inadequate user education	End-users, often lacking awareness or understanding of IoT device security best practices, may inadvertently contribute to security breaches through misconfiguration or uninformed usage
[103]	Privacy concerns	Inadequate data protection and privacy measures may expose user data to unnecessary risks, raising concerns about unauthorized data collection and misuse
[104]	Denial of service (DoS)	IoT devices may be susceptible to DoS attacks, rendering them inoperative and disrupting critical services or functions

Table 12: Proposed threat taxonomy.

Threat	Description
Data privacy threats	(i) Unauthorized access (ii) Data breaches (iii) Data profiling
Device security threats	(i) Physical tampering (ii) Firmware vulnerabilities (iii) Default credentials
Network security threats	(i) Man-in-the-middle attacks (ii) Denial-of-service (DoS) attacks (iii) Network snooping
Supply chain threats	(i) Counterfeit devices (ii) Supply chain attacks (iii) Third-party risks
Interoperability and standards threats	(i) Protocol vulnerabilities (ii) Standards compliance (iii) Interoperability challenges
Data integrity threats	(i) Data manipulation (ii) Replay attacks (iii) Integrity verification
Physical security threats	(i) Location tracking (ii) Unauthorized control (iii) Physical destruction
Privacy violations	(i) Surveillance (ii) Data collection (iii) Profiling and discrimination

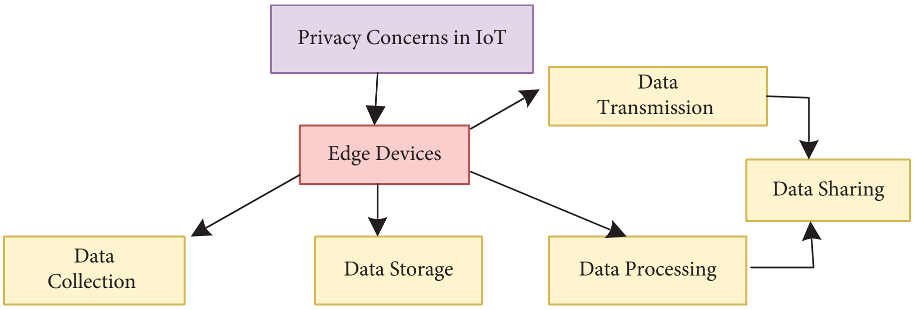

Figure 3: Summary of privacy concerns in IoT.

Table 13: Proposed IoT layers with privacy and security challenges.

IoT layer	Privacy challenges	Security challenge
Perception layer	(i) Unauthorized access (ii) Sensor spoofing	(i) Data collection (ii) User identification
Network layer	(i) Data leakage (ii) Traffic analysis	(i) Man-in-the-middle attacks (ii) Denial-of-service (DoS) attacks
Middleware layer	(i) Data aggregation (ii) Data retention	(i) Middleware vulnerabilities (ii) Insider threats
Application layer	(i) User profiling (ii) Third-party data sharing	(i) Insecure interfaces (ii) Application vulnerabilities
Business layer	(i) Data monetization (ii) Regulatory compliance	(i) Supply chain risks (ii) Insider threats

for the success and widespread adoption of the Internet of Things [112]. Abdelouahid et al. [113] proposed a universal meta-model for IoT interoperability, which is based on organizational concepts such as service, compilation, activity, and architectures. The framework provides a structured approach for understanding and resolving

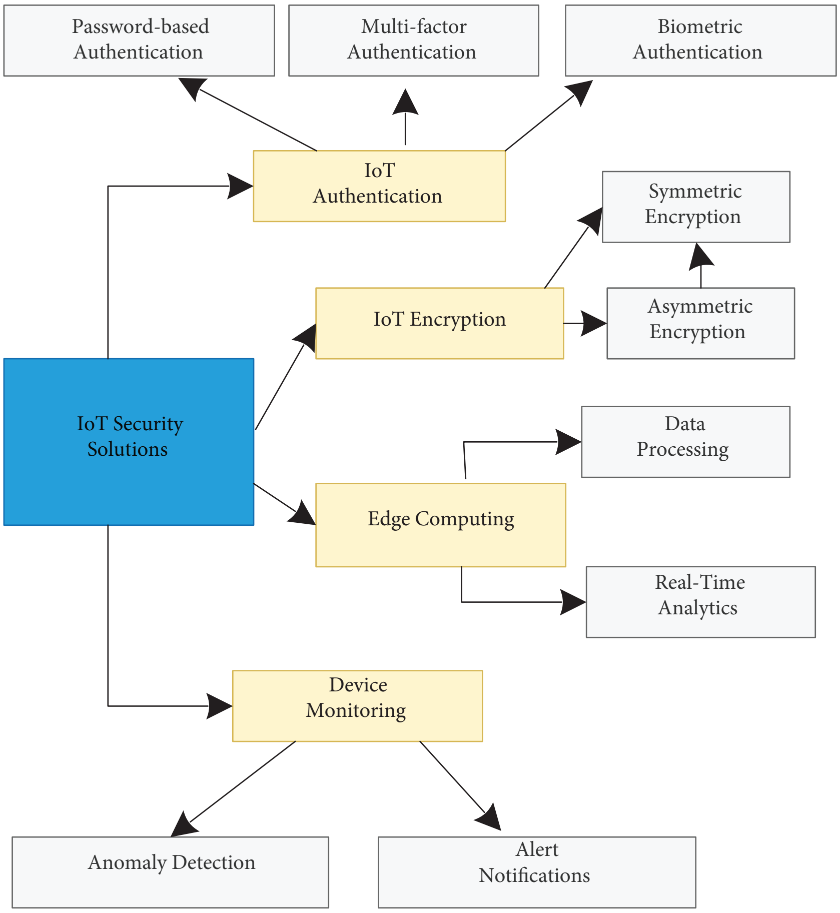

Figure 4: Proposed IoT security solutions.

Table 14: Proposed IoT security solutions.

Issues	Solution
Insecure communication protocols	(i) Encryption (ii) Secure protocols (iii) Message authentication
Vulnerabilities in IoT device firmware	(i) Regular firmware updates (ii) Secure boot (iii) Code signing
Weak authentication mechanisms	(i) Multi-factor authentication (MFA) (ii) Strong password policies (iii) Certificate-based authentication
Lack of secure device management	(i) Secure device provisioning (ii) Remote device monitoring and management (iii) Role-based access control (RBAC)
Insufficient data encryption	(i) Data encryption at rest (ii) Data encryption in transit (iii) Key management
Lack of device authentication	(i) Device identity management (ii) Mutual authentication (iii) Device certificates
Insider threats and unauthorized access	(i) Role-based access control (RBAC) (ii) Continuous monitoring (iii) User behaviour analytics (UBA)

Table 14: Continued.

Issues	Solution
Lack of secure software development practices	(i) Secure coding guidelines (ii) Code review and static analysis (iii) Security training and awareness
Data privacy concerns	(i) Data minimization (ii) Data anonymization (iii) Privacy impact assessments
Supply chain security risks	(i) Supply chain risk management (ii) Vendor security assessments (iii) Supplier security agreements

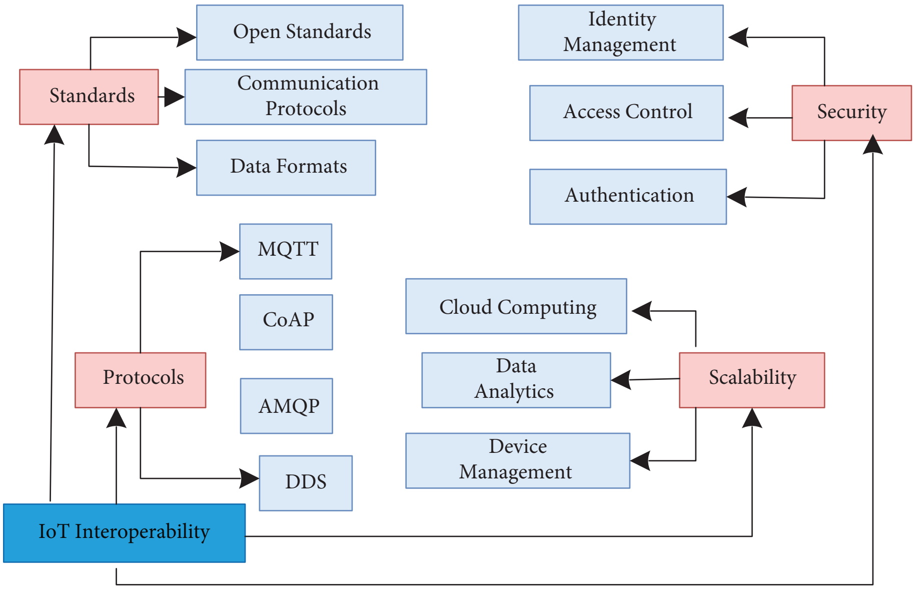

Figure 5: IoT interoperability ecosystem.

interoperability issues in different IoT contexts. Muppavarapu et al. [114] conducted an in-depth study on IoT interoperability, offering a comprehensive taxonomy and identifying unresolved challenges. The research provides valuable insights for both academics and practitioners, guiding efforts to navigate the complex landscape of IoT interoperability. As a result, achieving interoperability is presented with both challenges and significant benefits. It enables seamless communication, data exchange, and collaboration among diverse IoT ecosystems [115]. To ensure effective interoperability, efforts should focus on refining protocols, aligning with international standards, strengthening adherence to security protocols, and ensuring scalability. Recent advancements in IoT interoperability include the proposal of standardized protocols, adherence to international standards, meeting security requirements, and scalability. Additionally, there is a growing trend towards incorporating blockchain technology to enhance the security of IoT devices. Figure 5 provides a summary of the proposed IoT interoperability model, illustrating the various components and interactions involved. As the IoT ecosystem continues to evolve, these developments serve as guiding principles towards achieving a more connected and interoperable future.

6. Conclusion

In the landscape of Internet of Things (IoT) applications, privacy and security emerge as pivotal considerations. While IoT holds the potential to revolutionize businesses and enhance our daily lives, it also presents significant challenges that demand careful attention. Privacy and security, particularly concerning data collection, anonymization, retention, and sharing, stand out as pressing issues. The influx of data from IoT devices offers immense potential for insights and innovation, yet it also raises concerns about personal data privacy, behavioral surveillance, and data exploitation. Therefore, addressing these challenges is crucial to ensuring the responsible and ethical deployment of IoT technologies, fostering trust among users and stakeholders alike. By implementing robust privacy and security measures, fostering transparency, and adhering to regulatory frameworks, the potential of IoT can be realized while safeguarding individual privacy rights and mitigating associated risks. Such endeavors are essential to unlocking the full potential of IoT in driving positive societal impacts and economic growth, while also ensuring the protection of privacy and security in an increasingly interconnected world. The findings underscore the intrinsic relationship between privacy concerns and the operation of IoT. As the IoT becomes increasingly integrated into our daily lives and industries, maintaining a steadfast focus on privacy and security is imperative. The diverse concepts and approaches highlighted in this survey offer a glimpse of a potential path forward. Through a combination of technological advancements, regulatory frameworks, and user education initiatives, we can navigate the complexities of IoT while safeguarding individual privacy and security.

As we embark on the ongoing journey of the Internet of Things, these insights and innovations will undoubtedly shape the trajectory of our interconnected world. By addressing privacy and security challenges head-on, we can unlock the full potential of IoT and create a future that is both technologically advanced and ethically responsible.

6.1. Future Trends and Innovations. In light of the vast opportunities presented by IoT, future industry standards should incorporate AI and machine learning into IoT devices and platforms. This integration enables the analysis of massive datasets, the extraction of meaningful insights, and real-time decision-making, thereby fostering more intelligent and autonomous IoT applications. AI-powered predictive maintenance enhances device performance and efficiency, while edge analytics improves data processing at the network's edge, resulting in faster responsiveness and lower latency. Embracing edge computing in future designs reduces the need to transmit all data to centralized cloud servers due to its proximity to devices, leading to faster data processing, lower latency, and increased privacy and security, especially beneficial for real-time data analysis applications. Additionally, the integration of 5 G technology into these devices enhances their capabilities. To address security and privacy challenges, future research should focus on integrating blockchain technology, offering decentralized and tamper-proof data storage and validation, secure device identification, data integrity, and transparent transaction records.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 62272076).

References

[1] S. R. J. Ramson, S. Vishnu, and M. Shanmugam, "Applications of internet of things (iot)–an overview," in *Proceedings of the 5th international conference on devices, circuits and systems (ICDCS)*, pp. 92–95, IEEE, Coimbatore, India, March 2020.

[2] R. Salama, F. Al-Turjman, M. Aeri, and S. P. Yadav, "Internet of intelligent things (IoT)–An overview," in *Proceedings of the 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, pp. 801–805, Ghaziabad, India, April 2023.

[3] H. Pham, "Reducing the cost of implementing the advanced encryption standard as a quantum circuit," *IEEE Transactions on Quantum Engineering*, vol. 1, Article ID 2500112, 2020.

[4] A. K. R. Nadikattu, "IoT and the issue of data privacy," *International Journal of Innovations in Engineering Research and Technology*, vol. 5, no. 10, pp. 23–26, 2018.

[5] C. Lee and G. Ahmed, "Improving IoT privacy, data protection and security concerns," *International Journal of Technology, Innovation and Management (IJTIM)*, vol. 1, no. 1, pp. 18–33, 2021.

[6] S. Munirathinam, "Industry 4.0: industrial internet of things (IIOT)," *Advances in Computers*, vol. 117, no. 1, pp. 129–164, 2020.

[7] D. Singh, "Internet of things," *Factories of the Future: Technological Advancements in the Manufacturing Industry*, pp. 195–227, 2023.

[8] O. A. B. J. Vermesan, *Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution*, River Publishers, Denmark, Europe, 2017.

[9] E. F. I. Raj, "Precision farming in modern agriculture," *Smart Agriculture Automation Using Advanced Technologies: Data Analytics and Machine Learning*, Cloud Architecture, Automation and IoT, Singaporepp. 61–87, 2022.

[10] Z. Li and M. Shahidehpour, "Deployment of cybersecurity for managing traffic efficiency and safety in smart cities," *The Electricity Journal*, vol. 30, no. 4, pp. 52–61, 2017.

[11] W. Z. S. A. D. H. Qiao, S. Zhao, and H. Deng, "Multi-layer semantic middleware for cross-domain internet of things journal of physics: conference series," *Journal of Physics: Conference Series*, vol. 1993, no. 1, Article ID 012028, 2021.

[12] H. Devi Kotha and V. Mnssvkr Gupta, "IoT application: a survey," *International Journal of Engineering and Technology*, vol. 7, no. 2.7, pp. 891–896, 2018.

[13] S. Sonawane, "Survey on technologies, uses and challenges of IoT," *International Journal of Engineering Research*, no. 12, pp. 229–232, 2019.

[14] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–32, 2020.

[15] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: a systematic review," *Computer Networks*, vol. 148, pp. 241–261, 2019.

[16] V. D. Gunjal, "A survey on emerging IOT applications," *Journal of Electrical and Computer Engineering*, 2020.

[17] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and its applications: a comprehensive survey," *Symmetry*, vol. 12, no. 10, p. 1674, 2020.

[18] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: an overview," *Journal of Industrial Information Integration*, vol. 1, pp. 3–13, 2016.

[19] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017.

[20] J. Sanghavi, "Review of smart healthcare systems and applications for smart cities," in *Proceedings of the ICCCE 2019: Proceedings of the 2nd International Conference on Communications and Cyber Physical Engineering*, pp. 325–331, Singapore, August 2020.

[21] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and A. A. Abd El-Latif, "Edge enabled IoT system model for secure healthcare," *Measurement*, vol. 191, Article ID 110792, 2022.

[22] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," *Global Health Journal*, vol. 3, no. 3, pp. 62–65, 2019.

[23] M. Bhatia and S. K. Sood, "A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: a predictive healthcare perspective," *Computers in Industry*, vol. 92-93, pp. 50–66, 2017.

[24] S. U. M. S. H. G. M. M. A. M. A. R. Amin, M. S. Hossain, G. Muhammad, M. Alhussein, and M. A. Rahman, "Cognitive smart healthcare for pathology detection and monitoring," *IEEE Access*, vol. 7, pp. 10745–10753, 2019.

[25] A. S. L. M. E. Onasanya, S. Lakkis, and M. Elshakankiri, "Implementing IoT/WSN based smart Saskatchewan healthcare system," *Wireless Networks*, vol. 25, no. 7, pp. 3999–4020, 2019.

[26] M. S. K. S. K. S. Bhatia, S. Kaur, and S. K. Sood, "IoT-inspired smart toilet system for home-based urine infection prediction," *ACM Transactions on Computing for Healthcare*, vol. 1, no. 3, pp. 1–25, 2020.

[27] A. M. E. Onasanya and M. Elshakankiri, "Smart integrated IoT healthcare system for cancer care," *Wireless Networks*, vol. 27, no. 6, pp. 4297–4312, 2021.

[28] K. J. Bibri S.E, "The emerging data–driven Smart City and its innovative applied solutions for sustainability: the cases of London and Barcelona," *Energy Informatics*, vol. 3, pp. 1–42, 2020.

[29] A. Cheshmehzangi and S. M. Thomas, "Prioritizing accessible transit systems for sustainable urban development: understanding and evaluating the parameters of a transportation system in Mumbai," *Journal of Urban Planning and Development*, vol. 142, no. 4, Article ID 05016005, 2016.

[30] S. Mishra, "Exploring IoT-enabled smart transportation system," in *The IoT and the Next Revolutions Automating the World*, pp. 186–202, IGI Global, Hershey, PA, USA, 2019.

[31] L. F. Herrera-Quintero, J. C. Vega-Alfonso, K. B. A. Banse, and E. Carrillo Zambrano, "Smart ITS sensor for the transportation planning based on IoT approaches using serverless and microservices architecture," *IEEE Intelligent Transportation Systems Magazine*, vol. 10, no. 2, pp. 17–27, 2018.

[32] M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 58–62, 2020.

[33] R. S. R. G. D. B. Raju, "A smart information system for public transportation using IoT," *IJRTER*, vol. 3, pp. 222–230, 2017.

[34] J. Zhang, Y. Wang, S. Li, and S. Shi, "An architecture for IoT-enabled smart transportation security system: a geospatial approach," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6205–6213, 2021.

[35] H. A. Murad D.F, "IoT for development of smart public transportation system: a systematic literature review," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 18, pp. 3591–3604, 2018.

[36] T. Ayoub Shaikh, T. Rasool, and F. Rasheed Lone, "Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming," *Computers and Electronics in Agriculture*, vol. 198, Article ID 107119, 2022.

[37] S. S. K. S. Dagar R, "Smart farming–IoT in agriculture," in *Proceedings of the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 1052–1056, Coimbatore, India, July 2018.

[38] K. A. Patil and N. R. Kale, "A model for smart agriculture using IoT," in *Proceedings of the 2016 international conference on global trends in signal processing, information computing and communication (ICGTSPICC)*, pp. 543–545, Jalgaon, India, December 2016.

[39] S. R. Prathibha, A. Hongal, and M. P. Jyothi, "IoT based monitoring system in smart agriculture," in *Proceedings of the 2017 international conference on recent advances in electronics and communication technology (ICRAECT)*, pp. 81–84, Bangalore, India, March 2017.

[40] K. S. Arunlal, "Smart agriculture: IoT based precise and productive farming approach," *International Journal of advanced Research, Ideas and Innovations in Technology*, vol. 4, no. 6, pp. 771–775, 2018.

[41] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, 2018.

[42] R. D. Thakare, "A review on smart agriculture using IoT," in *Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES)*, pp. 500–502, Coimbatore, India, April 2021.

[43] C. Donghao, Z. Bohua, O. Chaomin, and C. Zhiyu, "Research on military internet of things technology application in the context of national security," in *Proceedings of the 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, pp. 992–998, Sanya, China, December 2021.

[44] F. T. Johnsen, "Application of IoT in military operations in a smart city," in *Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–8, Warsaw, Poland, May 2018.

[45] K. Wrona, A. de Castro, and B. Vasilache, "Data-centric security in military applications of commercial IoT technology," in *Proceedings of the IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 239–244, Reston, VA, USA, December 2016.

[46] W. Z. M. H. Z. Y. L. Q. Sun, "Key technologies and typical military application of IoT," *Internet Things Technol*, vol. 4, p. 33, 2012.

[47] R. S. Gotarane, "IoT practices in military applications," in *Proceedings of the 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 891–894, Tirunelveli, India, April 2019.

[48] J. G. H. D. P. V. S. N. Cohen, "Radio frequency IoT sensors in military operations in a smart city," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, pp. 763–767, Los Angeles, CA, USA, October 2018.

[49] J. A. S. A. S. K. A. S. Routray, "Military applications of satellite based IoT," in *Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 122–127, Tirunelveli, India, August 2020.

[50] V. Fabi, G. Spigliantini, and S. P. Corgnati, "Insights on smart home concept and occupants' interaction with

building controls," *Energy Procedia*, vol. 111, pp. 759–769, 2017.

[51] Z. Huang, "Analysis of IoT-based smart home applications," in *Proceedings of the IEEE International Conference on Computer Science, Artificial Intelligence and Electronic Engineering (CSAIEE)*, pp. 218–221, Charleston,, August 2021.

[52] P. G. J. A. G. S. Gaikwad, "A survey based on Smart Homes system using Internet-of-Things," in *Proceedings of the 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, pp. 0330–0335, Melmaruvathur, India, April 2015.

[53] B. N. Bansal N, "IoT applications in smart homes," *Designing Internet of Things Solutions with Microsoft Azure: A Survey of Secure and Smart Industrial Applications*, pp. 135–156, 2020.

[54] T. Kılıç and E. Bayır, "An investigation on Internet of Things technology (IoT) in smart houses," *Uluslararası Muhendislik Arastirma ve Gelistirme Dergisi*, vol. 9, no. 3, pp. 196–207, 2017.

[55] J. M. A. N. M. R. H. J. Bakhit, "Smart home applications based on internet of things: current scenario, issues and proposed solutions," in *Proceedings of the IEEE International RF and Microwave Conference (RFM)*, pp. 1–4, Kuala Lumpur, Malaysia, December 2022.

[56] A. S. S. K. Mahmud, "A smart home automation and metering system using internet of things (IoT)," in *Proceedings of the International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pp. 451–454, Dhaka, Bangladesh, January 2019.

[57] S. Munirathinam, "Industry 4.0: industrial internet of things (IIOT)," *Advances in Computers*, vol. 117, no. 1, pp. 129–164, 2020.

[58] H. N. M. R. O. B. P. A. P. C. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of industrial cyber-physical systems: a review," *ACM Computing Surveys*, vol. 54, no. 11s, pp. 1–35, 2022.

[59] A. D. Merchant, K. S. Himanshu, S. Ayush, Irfanuddin, and U. Hashmat, "Industrial automation using iot with raspberry pi," *International Journal of Computers and Applications*, vol. 168, no. 1, pp. 44–48, 2017.

[60] H. S. Raju, "Real-time remote monitoring and operation of industrial devices using IoT and cloud," in *Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 324–329, Greater Noida, India, December 2016.

[61] C. Maheswari, A. Ajeesh Babu Perinchery, E. Priyanka et al., "Review on online monitoring and control in industrial automation–an IoT perspective," *IOP Conference Series: Materials Science and Engineering*, vol. 1055, no. 1, Article ID 012034, 2021.

[62] V. G. P. M. Rong, "The internet of things (IoT) and transformation of the smart factory," in *Proceedings of the International Electronics Symposium (IES)*, pp. 399–402, Denpasar, Indonesia, September 2016.

[63] N. Santhosh, M. Srinivsan, and K. Ragupathy, "Internet of things (IoT) in smart manufacturing," *IOP Conference Series: Materials Science and Engineering*, vol. 764, no. 1, Article ID 012025, 2020.

[64] W. Chen, "Intelligent manufacturing production line data monitoring system for industrial internet of things," *Computer Communications*, vol. 151, pp. 31–41, 2020.

[65] W. W. E. C. T. S. C. D. D. S. Nixon, "Privacy, security, and trust issues in smart environments," in *Smart Environments: Technology, Protocols and Applications*, pp. 220–240, University of Strathclyde, Glasgow, Scotland, 2004.

[66] N. F. Raun, "Smart environment using internet of things (IOTS)-a review," in *Proceedings of the IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 1–6, Vancouver, BC, Canada, October 2016.

[67] C. Gomez, S. Chessa, A. Fleury, G. Roussos, and D. Preuveneers, "Internet of Things for enabling smart environments: a technology-centric perspective," *Journal of Ambient Intelligence and Smart Environments*, vol. 11, no. 1, pp. 23–43, 2019.

[68] S. S. Shahrestani, "The IoT and smart environments: an overview. Internet of things and smart environments: assistive technologies for disability," *Dementia, and Aging*, pp. 57–73, 2017.

[69] G. Ruggeri, V. Loscrí, M. Amadeo, and C. T. Calafate, "The internet of things for smart environments," *Future Internet*, vol. 12, no. 3, p. 51, 2020.

[70] M. E. Elmustafa, "Internet of things in smart environment: concept, applications, challenges, and future directions," *World Scientific News*, vol. 134, no. 1, pp. 1–51, 2019.

[71] P. R. Y. A. S. A. Thapliyal, "Internet of things for smart environment and integrated ecosystem," *International Journal of Engineering & Technology*, vol. 7, no. 3.12, pp. 1219–1221, 2018.

[72] G. S. G. H. D. M. P. S. Gunnemeda, "IOT based smart surveillance system," *International Journal for Advance Research and Development*, vol. 3, no. 2, pp. 166–171, 2018.

[73] S. K. S. A. P. P. Gulve, "Implementation of IoT-based smart video surveillance system," in *Computational Intelligence in Data Mining: Proceedings of the International Conference on CIDM*, pp. 771–780, Springer, Singapore, 2017.

[74] K. A. P. G. D. G. Lulla, "IoT based smart security and surveillance system," in *Proceedings of the International conference on emerging smart computing and informatics (ESCI)*, pp. 385–390, Pune, India, March 2021.

[75] G. D. McBride, "Design and construction of a hybrid edge-cloud smart surveillance system with object detection," in *Proceedings of the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pp. 642–647, Greater Noida, India, April 2021.

[76] P. K. Singh, "Smart security system using IOT," in *Proceedings of the International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 392–395, Bangalore, India, August 2020.

[77] V. M. J. V. Sanjay A, "Security surveillance and home automation system using IoT," *EAI Endorsed Transactions on Smart Cities*, vol. 5, no. 15, 2020.

[78] T. Sultana and K. A. Wahid, "IoT-guard: event-driven fog-based video surveillance system for real-time security management," *IEEE Access*, vol. 7, pp. 134881–134894, 2019.

[79] I. N. A. O. Aydin, "A new IoT combined face detection of people by using computer vision for security application," in *Proceedings of the 2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 1–6, Malatya, Turkey, September 2017.

[80] H. M. Erzİ, "IoT based mobile smart home surveillance application," in *Proceedings of the 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 1–5, Istanbul, Turkey, October 2020.

[81] C. Bhavitha, D. Yuvaraju, B. P. Kumar, D. Giribabu, and G. R. Krishna, "RF tracking system for assets using IOT,"

International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 4, pp. 1789–1793, 2022.

[82] A. Krishnan, "RFID-enabled IoT asset management system and machine learning integration," in *Proceedings of the 8th International Conference on Communication and Electronics Systems (ICCES)*, pp. 1239–1244, Coimbatore, India, June 2023.

[83] M. G. Kibria, "Tracking moving objects for intelligent iot service provisioning in web objects enabled iot environment," in *Proceedings of the International conference on information and communication technology convergence (ICTC)*, pp. 561–563, Jeju, Korea, October 2016.

[84] C. Ploder, *Customer Relationship Management Improvement Using IoT Data*, IoTBDS, Angers, France, 2021.

[85] S. K. Kinnunen, A. Ylä-Kujala, S. Marttonen-Arola, T. Kärri, and D. Baglee, "Internet of things in asset management: insights from industrial professionals and academia," *International Journal of Service Science, Management, Engineering, and Technology*, vol. 9, no. 2, pp. 104–119, 2018.

[86] L. Hang and D. H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.

[87] K. Saraubon, "Asset management system using NFC and IoT technologies," in *Proceedings of the 2019 3rd International Conference on Software and e-Business*, pp. 124–128, New York, NY, USA, May 2019.

[88] F. Lubrano, D. Sergi, F. Bertone, and O. Terzo, "Multinetwork technology cloud-based asset-tracking platform for IoT devices," in *Proceedings of the Complex, Intelligent and Software Intensive Systems: Proceedings of the 14th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2020)*, pp. 344–354, Heidelberg, Germany, June 2021.

[89] R. Khalid and W. Ejaz, "Internet of things-based on-demand rental asset tracking and monitoring system," in *Proceedings of the 2022 5th International Conference on Information and Computer Technologies (ICICT)*, pp. 84–89, New York, NY, USA, March 2022.

[90] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. Dang Hai, "Recent challenges, trends, and concerns related to IoT security: an evolutionary study," in *Proceedings of the International Conference on Advanced Communication Technology (ICACT)*, pp. 405–410, Chuncheon, Korea, March 2018.

[91] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, Article ID 100227, 2020.

[92] K. Fazal, "A systematic literature review on the security challenges of Internet of Things and their classification," *International Journal of Technology and Research*, vol. 5, no. 2, pp. 40–48, 2017.

[93] A. K. Sikder, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," 2018, https://arxiv.org/abs/1802.02041.

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

[95] B. Janes, H. Crawford, and T. Oconnor, "Never ending story: authentication and access control design flaws in shared IoT devices," in *Proceedings of the IEEE Security and Privacy Workshops (SPW)*, pp. 104–109, San Francisco, CA, USA, May 2020.

[96] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[97] M. Bettayeb, "Firmware update attacks and security for IoT devices: survey," in *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, pp. 1–6, New York, NY, USA, March 2019.

[98] C.-H. Yang and S. K. Choi, "System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats," *KSII Transactions on Internet & Information Systems*, vol. 12, no. 2, 2018.

[99] S. Liu, R. Kuhn, and H. Rossman, "Surviving insecure it: effective patch management," *IT professional*, vol. 11, no. 2, pp. 49–51, 2009.

[100] B. Knieriem, "An overview of the usage of default passwords," in *Digital Forensics and Cyber Crime 9th International Conference, Proceedings*, pp. 195–203, Springer, Heidelberg, Germany, 2017.

[101] R. Mozny, P. Ilgner, P. Dzurenda, and P. Cika, "Design of physical security for constrained end devices within the IoT ecosystem," in *Proceedings of the 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 85–89, Valencia, Spain, October 2022.

[102] J. M. Blythe, N. Sombatruang, and S. D. Johnson, "What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?" *Journal of Cybersecurity*, vol. 5, no. 1, p. 5, 2019.

[103] J. Linn, "Technology and Web user data privacy-A survey of risks and countermeasures," *IEEE Security and Privacy Magazine*, vol. 3, no. 1, pp. 52–58, 2005.

[104] E. Džaferović, A. Sokol, A. A. Almisreb, and S. Mohd Norzeli, "DoS and DDoS vulnerability of IoT: a review," *Sustainable Engineering and Innovation*, vol. 1, no. 1, pp. 43–48, 2019.

[105] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving iot environments: a survey," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 1032761, 15 pages, 2018.

[106] M. Memon, N. Saxena, A. Roy, and D. Shin, "Backscatter communications: inception of the battery-free era—a comprehensive survey," *Electronics*, vol. 8, no. 2, p. 129, 2019.

[107] S. Kadry, Y. Zhang, and S. Li, "Advanced microprocessor optimization methods for the Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. 4187, 2020.

[108] I. Dodig, D. Cafuta, T. Kramberger, and I. Cesar, "A novel software architecture solution with a focus on long-term IoT device security support," *Applied Sciences*, vol. 11, no. 11, p. 4955, 2021.

[109] A. Kamble and S. Bhutad, "Survey on internet of things (IoT) security issues & solutions," in *Proceedings of the 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 307–312, Coimbatore, India, January 2018.

[110] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: security and solutions survey," *Sensors*, vol. 22, no. 19, p. 7433, 2022.

[111] S. Seshan and Y. S. V. Agarwal, *TWC: Medium: Handling a Trillion Unfixable Flaws on Billions of Internet-Of-Things*, Carnegie, Victoria, Australia, 2016.

[112] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja, and K. Wasielewska, "Semantic interoperability in the Internet of Things: an overview from the INTER-IoT perspective,"

Journal of Network and Computer Applications, vol. 81, pp. 111–124, 2017.

[113] R. A. Abdelouahid, O. Debauche, and A. Marzak, “Internet of things: a new Interoperable IoT platform. Application to a smart building,” *Procedia Computer Science*, vol. 191, pp. 511–517, 2021.

[114] V. Muppavarapu, G. Ramesh, A. Gyrard, and M. Noura, “Knowledge extraction using semantic similarity of concepts from Web of Things knowledge bases,” *Data & Knowledge Engineering*, vol. 135, Article ID 101923, 2021.

[115] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in internet of things: taxonomies and open challenges,” *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019.