Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Authentication, access control and scalability models in Internet of Things Security–A review

M Kokila, Srinivasa Reddy K*

School of Computer Science and Engineering, VIT-AP University, Amaravathi. Andhra Pradesh, India

ARTICLE INFO

Keywords:
Internet of Things
Blockchain
Scalability
Data Security
Edge computing
Authentication schemes

ABSTRACT

The Internet of Things (IoT) leads to the next phase of human interaction with technology. With the help of the IoT, physical objects can be given the ability to generate, receive, and seamlessly trade data with one another. The IoT includes a wide variety of applications, each of which focuses on automating a specific task and works to give inanimate objects the ability to act independently of human intervention. The currently available and upcoming IoT applications hold a great deal of promise for enhancing the level of convenience, productivity, and automation enjoyed by users. High levels of security, privacy, authentication, and the ability to recover from attacks are required for the implementation of such a world in a manner that is constantly expanding. In this light, it is necessary to make the necessary adjustments to the architecture of IoT applications to accomplish end-to-end security in IoT environments. In this article, a comprehensive review of the security-related challenges and potential sources of danger posed by IoT applications is provided. Following a discussion of security concerns, a variety of new and established technologies that are focused on achieving a high degree of trust in the applications of the IoT are covered. Machine learning, fog computing, edge computing, and blockchain are just a few of the technologies that help the IoT provide greater security.

1. Introduction

The Internet of Things (IoT) is one of the disruptive technologies of the 21st century that has revolutionized every business dimension across the globe. The Internet has become an essential component in daily activities such as e-commerce, e-learning, e-conferences, etc. According to [1], the number of IoT devices deployed may exceed 21.3 billion by 2022. Intelligent interfaces connect IoT devices in order to collaborate, gather, communicate, and store data. Deploying IoT devices enhances business productivity by optimizing operational procedures and maximizing the utilization of available resources. IoT brings innovation in the way things are monitored and managed remotely with the help of real-time data acquired from the sensors. With the unrestrained volumes of data generated by billions of connected devices, storage, management, and security are arduous. Security aspects such as authentication, authorization, privacy, confidentiality, availability, and integrity form the basis for information exchange in a trusted environment. Authentication is the process of identifying the genuineness of an entity. The authorization process allows only authenticated users to access the resources. The protection of privacy prevents hackers from accessing the user's private information. Data confidentiality is an outcome of authentication and authorization. It prevents sensitive data from being reclaimed and exploited. A device's availability confirms that IoT devices and services are resilient to attacks and are accessible all the time. Data integrity is the process of providing a tamper-proof platform for information communication, exchange, and storage.

1.1. Motivation

The IoT needs to gain users' trust before it can be widely used in business. To earn the trust of its users, the IoT must guarantee the users' complete privacy and security. There is a very limited amount of published work that examines the security of the IoT, despite the fact that it is a very active research topic. On the other hand, the work is not current. Due to the fact that new threats in the IoT are discovered on a regular basis, we felt the need to conduct a comprehensive and up-to-date review of IoT security in order to provide researchers with direction regarding the efforts that are required in particular security areas. There is no discussion of support layer security in the IoT in any of the reviews that are currently available. Through the identification and discussion of a large number of support layer security issues in our paper, we were able to close the gap. The authentication and control of access are sig-

Peer review under responsibility of KeAi Communications Co., Ltd.

* Corresponding author.
E-mail addresses: kokila.23phd7047@vitap.ac.in (M. Kokila), srinivasareddy.k@vitap.ac.in (S. Reddy K).

https://doi.org/10.1016/j.csa.2024.100057
Received 4 February 2024; Received in revised form 20 March 2024; Accepted 10 April 2024
Available online 14 April 2024

nificant security challenges in the IoT, and a lot of work has been done in this area. We present an analysis of the most recent authentication and access control mechanisms in the IoT.

1.2. Contribution

Among all the applications of the IoT, healthcare applications are the most important. The IoT has played a vital role in the sharing of various medical resources, making it an essential factor in the field of medicine. Today, information is shared freely across different networks, making it easy for practitioners and institutions to work with the available resources and deliver on the medical needs of society. However, recent advancements in technology have developed smart and intelligent IoT devices connected to the Internet that continuously transmit data. So providing security and privacy to this data in IoT is a very challenging task, which is to be considered the highest priority for several current and future applications of IoT.

Security schemes in the IoT provide unauthorized access to information or other objects by protecting against alterations or destruction. Privacy schemes maintain the right to control the collected information for its usage and purpose. In this paper, we have surveyed major challenges such as confidentiality, integrity, authentication, and availability for IoT, briefly concerning remote health monitoring applications. In this survey, we present a systematic analysis of existing access control solutions for IoT that addresses the above issues in existing survey papers. Our goal is to identify open challenges in existing authorization and access control solutions to drive the research and development of more effective access control solutions for IoT. The main contributions to our survey are the following:

- Developing a Framework for Systematic and Comparative Analysis of Authorization, Access Control, and Scalability Solutions for IoT: This framework comprises a set of prerequisites that IoT authorization solutions should fulfill, along with defined criteria for their evaluation.
- A review of several recent authorization frameworks for IoT and their evaluation with respect to the requirements and criteria in the framework.
- Creating Guidelines for the Design of an Access Control Framework Tailored to the Specific Requirements and Constraints of prevalent IoT Applications.
- There are currently unresolved difficulties in authenticating IoT devices and implementing scalable access control solutions.

1.3. Survey method

In order to conduct our survey, we begin by presenting a comprehensive analysis of the key features of IoT systems and the technologies that support them. This analysis is based on an extensive review of existing literature and the latest advancements in the field of IoT. Our analysis has shown that cloud computing and edge computing are commonly utilized as fundamental technologies in the IoT to streamline the administration of devices and resources within IoT ecosystems. In order to achieve this objective, we examine the ways in which these computing paradigms have been modified for the IoT. Through the analysis of practical situations, we ascertain a collection of non-functional prerequisites for IoT systems.

Based on these outlined requirements, we distill specific criteria that authorization solutions for IoT must meet. These criteria encompass essential tasks within the access control process, spanning policy definition, administration, assessment, and implementation. To gauge the alignment of existing authorization frameworks with these identified requirements, we scrutinize the features of the IoT ecosystems in which these frameworks operate.

This examination involves a thorough analysis of IoT architecture styles, communication protocols, and data formats to grasp the inherent assumptions of the IoT environment. Particular attention is given to understanding the capabilities of nodes and their interconnections. Additionally, we delve into the characteristics of proposed authorization frameworks, encompassing the access control model, policy evaluation strategy, and deployment configuration.

In our critical assessment, we evaluate multiple contemporary authorization frameworks tailored for the IoT against the specified requirements and criteria. We also gauged the suitability of these solutions for typical IoT applications. Our literature review has yielded valuable insights, guiding us in identifying significant trends and pointing towards emerging research avenues in the realm of access control for the IoT.

Notably, our observations highlight a rising interest in crafting authorization frameworks explicitly designed for IoT systems. However, it is evident that many proposed frameworks aim to provide a one-size-fits-all solution to address authorization challenges in the IoT landscape. Our analysis underscores that diverse IoT applications exhibit unique requirements, emphasizing the absence of a universal solution capable of accommodating all scenarios. Therefore, the development of an IoT-tailored authorization framework should meticulously consider the distinctive requirements and limitations inherent to the specific IoT application under consideration.

The subsequent sections of the paper are organized as follows. In Section 2, we provide an introductory explanation of IoT. In Section 3, a summary of the technology that makes IoT possible follows this with respect to provide security. In Section 4, we analyze the fundamental functional and non-functional prerequisites for IoT systems authentication and contributions made in authentication systems in the literature. Finally, the Section 4 concluded with open research issues related to IoT device authentication. In Section 5, we outline the primary criteria that IoT access control and privacy frameworks must meet, and in Section 6, we assess the frameworks with respect to scalability issues and existing solutions with research gaps. We then provide a conclusion to the paper at Section 70, by highlighting unresolved matters and propose areas for future research.

2. Technology behind IoT

IoT is not a single technology but a blend of multiple technologies. Machine-to-Machine (M2M), Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), and Supervisory Control and Data Acquisition (SCADA) are the four technologies on which the IoT technology is based on big data analytics, cloud computing, and embedded systems, which are the technologies that enable building IoT applications. M2M technology, also known as the Internet of Devices, is used to capture events using a network connection and forward them to a central server. This server translates these events into meaningful information and uses it according to the specific applications. RFID, also known as the Internet of Objects, is a technology that uses simple, low-cost contactless disposable cards to store numbers and other attributes. These chips contain antennas, and using RFID readers, this data can be retrieved. WSN, also known as the Internet of Transducers, is used for sensing and collecting data from the environment where the devices are installed and then forwarding the acquired data to the central authorities. Computer systems monitor and regulate processes in industrial control systems using SCADA technology. SCADA uses Human Machine Interfaces (HCI), Programmable Logic Controllers (PLC), and Distributed Control Systems (DCS) to achieve this task.

With billions of devices installed across the globe, enormous amounts of data are generated. Storing and managing such a large volume of data is a tedious process. "Big data" is a technology that is designed to store, analyze, and manage large volumes and varieties of data that arrive at different velocities. Cloud computing is an emerging technology that provides applications and services to its users over the Internet. It provides resources for computing, networking, and storing resources on-demand as a metered service. Different services offered on the cloud computing platform include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Embedded sys-

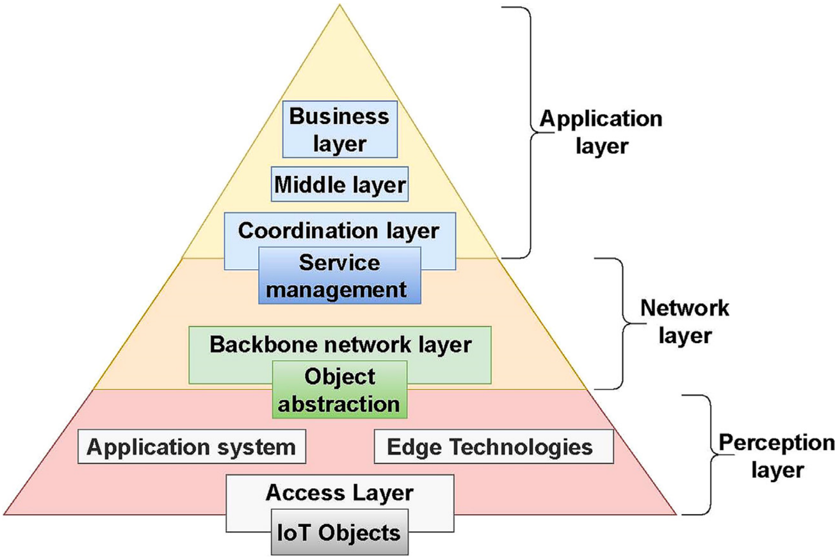

Fig. 1. IoT functional layers Architecture.

tems are smaller, hardware-based systems that are used to control larger systems. They use modules such as microprocessors/microcontrollers, memory modules, networking, digital signal processing, and graphical processors to accomplish different application-specific functions. Commercial-of-The-Shelf (COTS) modules are also used in some high-end applications where real-time processes are modeled with maximum precision and high operational accuracy. Network processors and Digital Signal Processors (DSPs) are also used in some domain-specific IoT applications.

2.1. IoT layered architecture

Numerous authors and researchers have proposed diverse IoT architectures, with a common focus on a three-layer architecture [2]. Typically, the fundamental structure of IoT can be categorized into three primary layers: the application layer, the network layer, and the perception layer, as illustrated in the Fig. 1 [2]. The research community acknowledges that [3] is the most recent and widely used IoT architecture, which starts with the presentation of the three-layered structure. Subsequently, we delve into an exploration of additional layers that extend this architecture into a five-layered model.

Perception layer: Within this layer, diverse devices establish connections, encompassing physical devices like sensors, Radio Frequency Identification (RFID), and Bluetooth, as well as virtual devices such as barcodes, Quick Response (QR) codes, and Global Positioning System (GPS). This layer's primary function involves the aggregation of data from end nodes and its subsequent transmission to the network layer. These devices within this layer are typically acknowledged as resource-constrained.

Network layer: This layer is responsible for gathering data transmitted by the end nodes of the perception layer and facilitating its transfer to the application layer. Its core duty lies in establishing connectivity with the devices integrated into the perception layer, employing various technologies such as 4 G and Wi-Fi. Additionally, it ensures the security of information received from the perception layer by implementing robust security mechanisms to safeguard against potential attacks.

Application layer: Within this layer, end-users engage with applications tailored to their specific requirements. Services are provided in accordance with the users' needs, allowing them to interact with technology based on the functionalities of the end nodes. In addition to the foundational 3-layer architecture, we also observe the emergence of intermediate architectures, culminating in a 5-layered IoT architecture as detailed in the reference [3]. These additional layers focus on data processing originating from the perception layer and on aspects of system management. The transition is illustrated in Fig. 1, depicting a sequence of critical elements in IoT architectural designs: identification, sensing, communication, computation, services, and semantics. It is evident that the initial step in IoT processes is device identification. Consequently, authenticating and verifying the devices within the perception layer hold significant importance in IoT applications.

2.2. IoT applications

The IoT enables machine-to-machine, human-to-human, and machine-to-human communication. Recent advancements in IoT systems have had a favorable influence on individuals' daily activities, ranging from information access to real-time service delivery. The IoT has altered how humans interact with technology, with far-reaching implications for daily living, industry, and society as a whole. Its importance rests in a number of crucial areas, including ubiquitous computing, smart automation, remote applications, and so on. The potential of the IoT to integrate smoothly into daily life, automate and improve decision-making processes, deliver customized experiences, and open up new avenues for innovation and sustainability is the primary reason for the relevance of the IoT in human engagement with technology. As IoT technology continues to advance, it is anticipated that its influence on human engagement with technology will become more profound. This highlights the significance of tackling the issues that accompany it in order to fully achieve the potential benefits that it offers.

IoT connects objects to the internet and to one another, allowing for hitherto inconceivable levels of interaction and data sharing. This pervasive connectivity enables seamless integration of technology into daily things, making human-technology interaction more intuitive and natural. IoT creates new chances for creative services and business models. For example, the capacity to monitor items in real-time leads to models such as "Product as a Service," in which firms charge based on consumption rather than selling the product itself. This transformation can result in more sustainable consumption patterns and new revenue sources for businesses. IoT devices are critical for environmental monitoring, including tracking pollution levels, water quality, and wildlife migrations. This information can help guide conservation activities and policies aimed at ensuring sustainability. Furthermore, IoT can improve resource utilization in enterprises and residences, thereby increasing energy efficiency and reducing waste.

The IoT is a technology that allows inanimate objects to act autonomously in order to improve efficiency, convenience, and quality of life. By integrating sensors, software, and other technologies, IoT enables these objects to gather and exchange data and perform tasks without human input. The technology also provides comprehensive environmental data collection and analysis for better decision-making. In agriculture, for example, IoT sensors can measure soil moisture, ambient temperature, and plant health to optimize watering and fertilization programs for greater resource efficiency and crop yields. IoT-capable machines can monitor their own operating state and anticipate potential issues, scheduling maintenance at optimal times to reduce downtime and extend equipment lifespan. IoT solutions can also automatically respond to risks and inconsistencies, improving safety and security. Security frameworks powered by the IoT can instantly alert authorities or take pre-set actions to address hazards. IoT devices can automate tedious and time-consuming tasks, improving quality of life. Automated home systems, voice-activated controls, and emergency alerting systems powered by IoT give elderly and disabled individuals more independence. Additionally, IoT can customize device functionalities to match user habits and preferences, providing a more personalized experience across entertainment, healthcare, and commerce.

The IoT can be utilized in many different aspects of life, both in the private and public sectors. With IoT, people can track lost pets, monitor their house's security system, and keep track of appliance maintenance schedules. Consumers can use IoT to make restaurant reservations, monitor their exercise progress and overall health, and receive coupons for stores they pass by. Businesses can use IoT to monitor supply chains, track customer spending habits, collect feedback, maintain inventory levels, and engage in predictive maintenance of their machines and devices. The IoT is also helpful in IT service management, which is an essential detail since IT departments are called upon to do more in a digital world with more reliance on wireless networks. Blockchain, a more efficient and secure method of transaction and data processing, is also a natural beneficiary of IoT technology. Thus, we can expect to see IoT and Blockchain working together more frequently in the future.

The digitalization of things has drastically increased over the past few years and has been made possible through cheap resources that are now available to everyone. IoT grew significantly during the COVID-19 pandemic, driven by the rising penetration of smart analytics and remote monitoring. There has also been a strong shift over the last decade from non-IoT devices to IoT devices. In fact, it is expected that 75% of all devices will be IoT by 2030. The IoT has been smoothly integrated into many aspects of our globalized economy and way of life, from interconnected consumer products such as appliances, security systems, and automobiles to big manufacturing applications such as those in agribusiness and power. As the number of connected devices grows, businesses must find the most effective ways of ensuring cybersecurity in a technology-driven world.

2.3. Need for security in IoT

The security of traditional systems remains a pervasive concern, with the ongoing reliance on traditional frameworks for development lacking specific standards. Technologies that continue to rely on these frameworks are particularly vulnerable to security threats. As the IoT market expands, safeguarding company data and intellectual property becomes increasingly critical. Ensuring the security of IoT devices requires developers to adhere to the following key services:. **Authentication:** The upcoming challenge for IoT revolves around authenticating IoT users, a task that has become more intricate with the introduction of new standards and self-configuring protocols, in contrast to the relatively simpler traditional approaches. Utilizing two-factor authentication, such as Google's two-step notification, offers some degree of control over applications, especially when utilizing the widely used mobile devices. The attributes that render smartphones effective authentication factors are the very characteristics that will empower devices like watches, wristbands, and thermostats to form opinions about our identity and assert that opinion. **Confidentiality:** The most recent technologies make messages susceptible to interception by outside parties in the IoT world. For instance, when a user accesses their homecare application from a public Wi-Fi network at a restaurant, live video content from their home becomes vulnerable to access by unauthorized third parties on the same network. Hence, ensuring confidentiality is paramount, and messages must remain concealed from intermediate entities. End-to-End (E2E) message secrecy emerges as a crucial requirement in the IoT landscape. Additionally, stored data, encompassing messages and personal information on IoT devices, must be safeguarded from unauthorized entities. **Data Integrity:** Remarkably, a significant portion of IoT research has directed its focus towards privacy, recognizing it as a crucial element in ensuring a secure IoT environment. Within any application, integrity stands out as a paramount component, surpassing even availability in importance. This emphasis is particularly critical in scenarios such as medical devices or a car's braking system, where a compromise in integrity could potentially result in severe consequences, even costing lives. Over the years, both Public Key Infrastructure (PKI) and Keyless Signature Infrastructure (KSI) have played pivotal roles in ensuring data security, each with its own distinct and complementary functions. PKI excels in authentication and facilitating secure communication over networks, while KSI serves as a robust solution for ensuring integrity. **Access Control:** In conventional systems, access controls are typically designed for closed systems, where all users are familiar entities within the system. Given the significant role that unidentified entities play in the IoT, the approach needs to take into account both open and closed systems. Access control involves three decision factors along with two decision properties.

2.4. Need for communication security

Implementing the security services mentioned in the previous section will help secure communication in the IoT, which is essential. The utilization of standardized security mechanisms enables the provision of communication security across various layers. Table 1 illustrates an IoT stack with standardized security solutions implemented at different layers.

Link Layer: The most recent state-of-the-art security solution for the IoT is IEEE 802.15.4′s link layer security. This link-layer security operates on a per-hop basis, ensuring that each node in the communication path is trusted. A single pre-shared key is employed to safeguard all communication within this framework. In the event of a compromise, where an attacker gains access to one device and a key, the impact is limited to a single hop or device. This per-hop security approach not only minimizes the extent of potential compromise but also allows for detection at an early stage. While link layer security has its limitations, its flexibility is noteworthy, enabling it to operate seamlessly with multiple protocols across different layers.

Network Layer: In the context of IoT, which is predominantly implemented over the internet, it relies on network IP Security (IPsec) provided at the network layer. IPsec delivers end-to-end security encompassing authentication, confidentiality, and integrity. Operating at the network layer, IPsec is compatible with various transport layer protocols, including TCP, UDP, HTTP, and CoAP. Through the use of the Encapsulated Security Payload (ESP) protocol, IPsec ensures the confidentiality and integrity of the IP payload. Simultaneously, the Authentication Header (AH) protocol guarantees the integrity of both the IP header and payload. Notably, IPsec has become mandatory in all IPv6 protocols, signifying that all IPv6-ready devices inherently possess default support for IPsec. Data Security: Ensuring the security of communication is paramount in IoT, yet many application developers overlook the importance of securing the data generated by IoT devices. A significant challenge arises from the small size of most IoT devices, which imposes constraints on implementing robust security measures due to limited resources. While various solutions exist, the diverse communication technologies employed in the IoT suggest that a single solution may not suffice to comprehensively secure every aspect.

Table 1
Comparative analysis of related works.

Ref.	Survey	Objective
Hameed et al. [23]	Comprehending the security needs and confronting challenges within the IoT	Security vulnerabilities are categorized, emphasizing challenges, current solutions, and areas of ongoing research.
Wang et al. [24]	Exploration of Blockchain Applications in the IoT	Advancements in Blockchain Data Structure and Consensus Protocols: Review of Relevant Research Works.
Sengupta et al. [8]	An In-Depth Analysis of Threats, Privacy Concerns, and Blockchain-Based Solutions for IoT and Industrial IoT	Classification of Attacks on IoT and Countermeasures; In-Depth Examination of Blockchain-Based Solutions for IoT and IIoT Applications.
Neshenko et al. [25]	A Comprehensive Examination of Vulnerabilities in IoT Systems	IoT taxonomy, effects and remediation with an initial investigation into Large-Scale exploitation
Meneghello et el. [13]	IoT: The Internet of Dangerous Things? A Survey of Practical Security Vulnerabilities in Real IoT Devices	Security measures taken by the IoT communication protocols that are used the most, as well as the vulnerabilities in those protocols.
Rafique et al. [15]	Enhancing IoT Services via Software-Defined Networking and Edge Computing: A Thorough Exploration	Utilizing SDN and Edge Computing for Resource-Constrained, Compute-Intensive Tasks.
Al-Garadi et al. [20]	Examination of Machine and Deep Learning Strategies for Augmenting Security in the IoT	Security Challenges in IoT and Resolutions Employing Machine Learning and Deep Learning.
Sharma et al. [12]	Ensuring Security, Privacy, and Trust in Smart Mobile-IoT (M-IoT): An In-Depth Survey	TComparative Analysis of Threats and Countermeasures in Existing Literature for Smart Mobile-IoT (M-IoT).
Fernandez et al. [26]	Transitioning from Pre-Quantum to Post-Quantum IoT Security: An Exploration of Quantum-Resistant Cryptosystems for the IoT	Contrasting Traditional and Quantum Security Vulnerabilities and Impacts: A Comparative Analysis.
Stoyanova et al. [11]	An Exploration of IoT Forensics: Challenges, Approaches, and Unresolved Issues - A Comprehensive Survey	Discussed present challenges and solution of IoT forensics.
Chettri et al. [10]	A Comprehensive Survey on IoT Toward 5 G Wireless Systems	5 G layers, the impact of 5 G on IoT, and an evaluation of 5 G low-power wide-area networks.
Friha et al. [27]	Revolutionizing Smart Agriculture through the IoT: An In-Depth Examination of Emerging Technologies - A Comprehensive Survey	Integration of Emerging Technologies such as SDN, NFV, and Blockchain in Applications Relevant to Smart Agriculture: A Comprehensive Exploration.
Sadawi et al. [28]	An In-Depth Review of Integrating Blockchain with IoT to Boost Performance and Overcome Challenges: A Comprehensive Survey	Addressing Challenges and Enhancing Resistance Against Attacks Through the Utilization of Blockchain Technology.
Song et al. [29]	Applications of the IoT in Smart Logistics: A Comprehensive Survey	The Application of IoT in Smart Logistics: A Comprehensive Exploration.
Khan et al. [7]	Exploration of Security and Privacy Concerns in Edge Computing-supported IoT: A Comprehensive Survey	Enhancing Data Processing Efficiency and Resilience against Attacks through Edge Computing.
Alwarafy [30]	Survey on Lightweight Cryptographic Protocols for Constrained IoT Devices	Discussed IoT architecture and lightweight cryptographic protocols.
Arora et al. [21]	Overview of Machine Learning-Based Security Solutions in Healthcare	An in depth analysis of implementing Healthcare Security Solutions through Machine Learning.
Barua et al. [6]	Exploring Security and Privacy Threats in Bluetooth Low Energy for IoT and Wearable Devices: An In-Depth Survey	Security Threats, Classification, and Remedial Approaches for Bluetooth-Based Attacks.
Gaurav et al. [22]	An In-Depth Review of Machine Learning Approaches for Detecting Malware in IoT-Centric Enterprise Information Systems	Utilizing Machine Learning for Malware Detection in IoT Networks: A Comprehensive Overview.
This Paper	Engaged in a Detailed Discussion on IoT Taxonomy, Impacts, and Countermeasures; Presented an Overview of Various IoT Applications;	Offered an Overview and Comparative Analysis of IoT and IoE Networks; Conducted an In-Depth Examination of authentication, access control and scalability issues in IoT security.

3. Security in IoT

The significant impact of the IoT on daily life has spurred extensive research efforts aimed at enhancing its benefits for humanity. Numerous researchers have undertaken surveys to elucidate the intricacies of the IoT ecosystem. While some studies have focused on providing an overview of the challenges confronting IoT, others have delved into the realm of security threats.

Several works, including [4–8], have reviewed security threats in IoT, addressing various types of attacks. For instance, [6] specifically highlighted security vulnerabilities in Bluetooth, shedding light on potential attacks leveraging these vulnerabilities within the IoT context. The challenges posed by IoT have been explored by researchers in works such as [4,9]. Additionally, [10] presented security guidelines, and the impact of 5 G on IoT systems.

The architectural aspects of IoT, including its layers, were the focal point of [11], while different protocols were discussed in various works like [12–14]. Diverse applications of IoT, exemplified by [8], emphasized the transformative impact of smart logistics in industries. Given the resource-constrained nature of IoT devices, there is a need for efficient and lightweight operations. This led to investigations into how edge computing, as illustrated in references [15,16], can facilitate the processing of IoT services such as smart agriculture and smart logistics.

Authentication frameworks can be conceptualized through centralized methods or decentralized mechanisms, with decentralized solutions leveraging blockchain technology gaining attention in the research community, as evident in various review papers like [17–19]. In the realm of smart mobile IoT architecture, diverse security mechanisms were expounded upon in [20]. Conversely, intrusion detection solutions based on machine learning were illustrated in [20–22]. Notably, our research distinguishes itself by providing a comprehensive review of IoT attacks, encompassing taxonomy, attack surfaces, security mechanisms, secure data communication methods, and more. Table 1 succinctly outlines the contributions of different review papers, highlighting the unique perspective our paper brings to the landscape compared to other survey papers.

3.1. IoT internal security architecture

Despite the significant and extensive applications of IoT, its deployment in mission-critical domains presents formidable challenges, with paramount concerns related to security and privacy. For instance, a successful security breach in a smart healthcare system could result in the loss of numerous patient lives and substantial financial repercussions. Similarly, in the context of intelligent transportation systems, a security breach could lead to both financial losses and human casualties. Securing IoT is an intricate and demanding field, necessitating further research efforts to effectively address these challenges. In this section, we delve into these security challenges at the layer level, providing an illustrated overview of IoT node security, as depicted in the accompanying Fig. 2.

Perceptual layer Security: Perceptual layer consists of resource constrained IoT devices i.e. Sensors, RFID tags, Bluetooth and Zigbee devices. These devices are more prone to cyber-attacks. As large amount

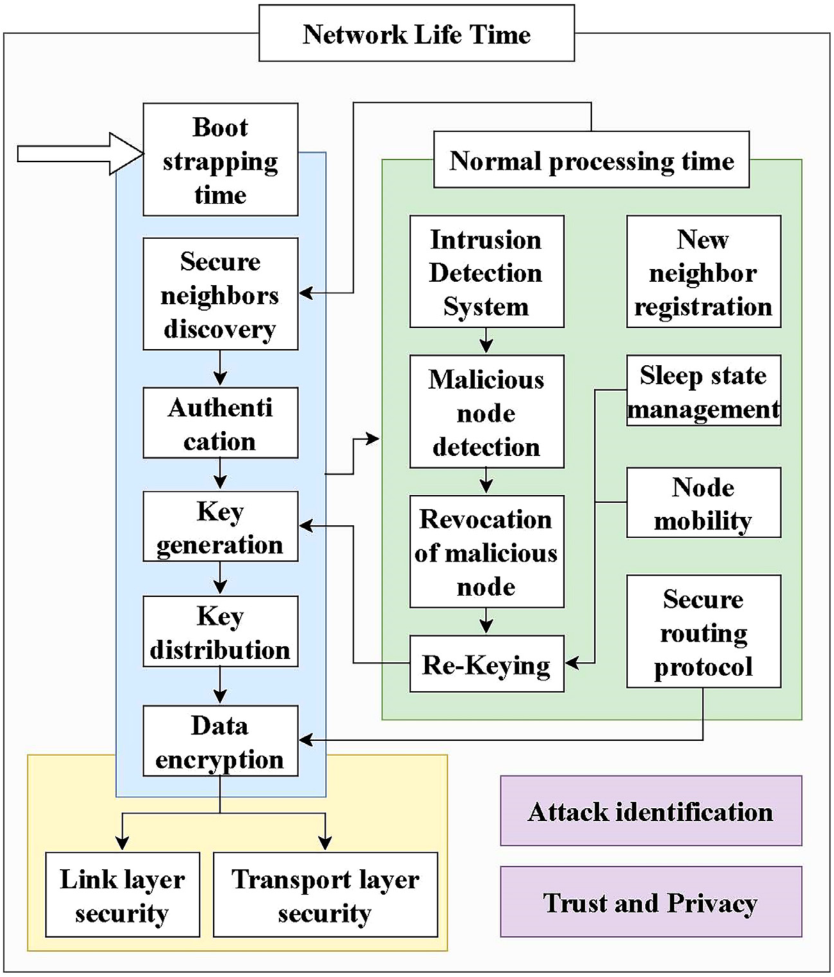

Fig. 2. IoT Internal Security Architecture.

Table 2
IoT Attacks in Perceptual layer Security.

Issue	Description
Node Tempering	In the event that an adversary is able to obtain physical access to sensor nodes, they will be able to replace the hardware or connect directly in order to either gain access or alter sensitive information [14]. It's possible that the sensitive information includes encryption keys or routing table routes.
Fake Node	Hackers can inject malicious data into IoT systems by creating a fake node, causing low-power devices to consume energy [31]. It also attacks as a man in the middle.
Side Channel Attack	Attackers exploit power, time, and electromagnetic radiation from sensor nodes to breach encryption [31].
Physical attack	IoT devices can be physically damaged by attackers for denial of service (DoS) attacks, especially in open and closed environments.
Code injection malice	An adversary gains illegal access to a system by physically compromising a node and inserting malicious code [32].
Sensor Data Security	Sensor data confidentiality is relatively low since adversaries can readily intercept the data. However, ensuring the integrity and authenticity of this data is of paramount importance.
Mass-Node authentication	Authentication problems are prevalent among numerous nodes within an IoT system [33]. The substantial volume of network communication required for authentication procedures can have adverse effects on system performance.

of IoT devices is physically deployed in open fields, it encounters many physical attacks, which are presented in Table 2. It is crucial to secure the IoT system from physical access by adversaries. Additionally, node authentication is necessary to prevent unauthorized system access. To ensure data integrity and confidentiality between nodes, lightweight cryptographic algorithms should be designed for secure transmission. Improving key management is a challenge in the IoT context.

Network Layer Security: Even though the core network has adequate security measures, there are some problems that still persist. The integrity and confidentiality of data may be compromised if traditional security flaws are not addressed. There are many different kinds of network attacks that are still affecting the network layer, such as eavesdropping attacks, denial of service attacks, man-in-the middle attacks, and virus invasions. The detailed IoT attacks in the network layer are presented in Table 3. While core network security is mature, harmful IoT security concerns such as denial of service and distributed denial of service must be addressed at this layer. Communication protocols must be mature to address routing attacks, congestion, and spoofing security issues.

Support Layer Security: The security of the support layer is not dependent on the security of other layers, and cloud computing security is an expansive field of security. The Cloud Security Alliance (CSA) is responsible for the establishment of many standard cloud security frameworks. In addition to this, the development of a mechanism for continuous cloud audit, such as the Security Content Automation Protocol (SCAP), and the provision of trusted results through Trusted com-

Table 3
IoT Attacks in Network layer security.

Issue	Description
Heterogeneity problem	The IoT perceptual layer encompasses a diverse range of technologies. Within this layer, the access network accommodates multiple access methods, creating a significant challenge in ensuring both security and interoperability [34].
Network Congestion	Network congestion can result from various factors, such as the substantial volume of sensor data and the communication overhead generated by numerous devices authenticating themselves, among other reasons [34]. This issue could potentially be addressed through the implementation of a practical device authentication mechanism and the utilization of efficient transport protocols.
RFIDs Interference	This type of attack, which targets the network layer, entails disrupting the radio frequency signals employed by RFIDs by introducing noise signals, ultimately leading to a denial of service [35].
Jamming	This type of attack bears similarities to radio frequency interference, as previously discussed in the context of RFIDs. In this attack, the malicious actor interferes with the radio frequency used by wireless sensor networks to disrupt their ability to offer services [36]. It represents another variation of a denial-of-service attack.
Sniffing Attack	This activity is commonly referred to as "sniffing" and involves the interception of wireless traffic in the vicinity of Wireless Sensor Networks (WSNs), RFIDs, or Bluetooth devices. Since the device layer in IoT primarily relies on wireless communication, attackers often initiate their attacks by first gathering information through the process of sniffing. Various specialized tools, such as packet sniffers, are employed for this purpose [37].
RFID Spoofing	In this attack, the intruder gains unauthorized access to the system by mimicking RFID signals and reading the RFID tag. Subsequently, they transmit counterfeit data while using the original RFID tag [4]
Route attacks	Attackers can alter routing information and distribute it in the network, causing loops, false routes, error messages, or traffic drop [38].
Sybil Attack	In Sybil attack, a single malicious node impersonates multiple nodes. This node can cause harm by distributing false routing information or disrupting the WSN election process [38].

puting (TCG) is being worked on. Because this layer hosts the data and applications used by IoT users, it is imperative that both be safeguarded against unauthorized access. At this layer of security, some of the concerns include the table [tab:tab3]. IoT users' data and applications are stored on cloud and fog nodes. Cloud security and privacy should not be compromised. The CSA has established numerous security standards, laws, and regulations for cloud security. Continuous monitoring of security standards is necessary, and IoT systems should only use clouds that meet CSA standards. Additionally, users need a simple online cloud audit mechanism to build trust with their vendors.

Application Layer Security: At the application layer, the various applications each have their own unique set of security requirements. There is currently no agreed-upon standard for the construction of IoT applications. On the other hand, one of the characteristics of the IoT application layer is the sharing of data. The sharing of data is fraught with difficulties regarding data privacy and access control. The table [tab:tab4] presents some of the more common concerns regarding application layer security. It is necessary to have a robust authentication and access control mechanism in order to deal with application layer security. In addition to these, it is essential to instruct users on the importance of using robust passwords. It is necessary to have powerful anti-virus software in order to protect against malware.

3.2. IoT security requirements

IoT offers a lot of benefits, but it also brings some challenges. These challenges include concerns over privacy, security vulnerabilities, and the digital divide. As IoT evolves, it is important to ensure that devices are secure, user privacy is respected, and technology is accessible to all. Since IoT devices collect, transmit, and process vast amounts of data, including sensitive personal information, it is crucial to secure these devices and their ecosystems. Implementing IoT applications requires essential security requirements such as end-to-end encryption, access control, privacy, authentication, resilience against attacks, data integrity, and availability, among others.

Implementing these requirements demands a holistic approach that encompasses not only the technological aspects but also the processes and people involved. Security, privacy, authentication, and resilience should be integral to the design and operation of IoT systems, following the principle of "security by design" to anticipate and mitigate risks from the outset. Hence, adjusting the architecture of IoT applications is necessary to address the unique security challenges posed by IoT environments, including the complexity of IoT ecosystems, diverse communication protocols, data privacy concerns, integration with legacy systems, the dynamic nature of IoT environments, and regulatory compliance requirements. By implementing end-to-end security measures, organizations can mitigate risks and protect sensitive data across the entire IoT ecosystem, from device to cloud.

To ensure the security of equipment, it is imperative to comprehend the fundamental security objectives. Traditional security principles, as encapsulated in the CIA triad, include confidentiality, integrity, and availability. Confidentiality entails defining rules that establish criteria for authorized entities with access to information. Integrity plays a crucial role in ensuring the delivery of trustworthy services by making sure that IoT devices only receive legitimate commands and data. Furthermore, availability ensures that IoT functionalities remain accessible to legitimate objects and users at all times and in all locations. In the realm of Information Assurance and Security (IAS-octave), a comprehensive framework, an expanded set of security goals are introduced to address the limitations of the CIA triad and provide a more encompassing approach to security. IAS-octave expands on the original OCTAVE framework by providing an expanded set of security goals. These goals are designed to address various aspects of information assurance and security within an organization. With respect to IoT security, these security requirements are defined as follows:

- End-to-End Encryption: Data transmitted between IoT devices and servers should be encrypted to prevent interception and unauthorized access.
- Access Control: Implement strong access controls to limit who can interact with the IoT system and under what conditions.
- Privacy: Users should be informed about what data is collected, how it is used, and who it is shared with, allowing for informed consent.
- Device Authentication: Securely authenticate devices before they join the network to prevent unauthorized devices from connecting.
- Intrusion Detection Systems (IDS): Monitor network traffic for signs of suspicious activity and potential security breaches.
- Data Integrity Protection: Implement mechanisms to ensure that data has not been tampered with during transmission or storage.

These security goals provide a framework for IoT to evaluate their current security posture, identify areas for improvement, and develop strategies and initiatives to enhance information assurance and security capabilities. By addressing these goals comprehensively, organizations can mitigate risks, protect critical assets, and maintain the confidentiality, integrity, and availability of their information and systems.

3.3. IoT vulnerabilities

IoT devices have become integral to delivering enhanced consumer experiences and are omnipresent in our surroundings. However, the pro-

Table 4
IoT Attacks in Support layer Security.

Issue	Description
Data Security	Maintaining data confidentiality and security in the cloud requires protection from breaches. This can be achieved through tools for detecting cloud data migration, preventing data loss, and monitoring file and database activity. Cloud data security can be achieved through data dispersion and fragmentation [9].
Portability, Interoperability	Interoperability and portability among cloud vendors are major issues today. Cloud migration can be challenging due to proprietary standards used by different vendors. This heterogeneity increases security risks [9].
Recovery and Continuity	Cloud vendors must maintain services during natural disasters such as floods, fires, and earthquakes. Business continuity clouds should be located in a location that is least affected by disasters. It should follow the quick response team approach. Clouds should have data backup plans [9].
Audit Cloud	The Cloud Security Alliance establishes standards for cloud vendors, requiring ongoing audits to ensure compliance and build user trust.
Tenant Safety	It is possible for several users' data to be kept on the same physical drive in the cloud or for data to be shared by tenants, who are users of IaaS. An adversary could steal tenant data due to the shared physical media.
Virtual Security	Virtualization processes can differ from provider to provider of cloud services. It is important to ensure that virtualization is secure. Some virtual machine communication may circumvent network security controls [9]. For there to be no problems with cloud auditing, virtual machine migration needs to be secure.

liferation of IoT devices has given rise toto an escalating threat landscape in terms of security. Hackers are exploiting the vast network of interconnected devices, potentially compromising sensitive data. In the absence of robust security measures, IoT devices are susceptible to data breaches. What makes this situation even more concerning is that IoT and cybercriminal activities often operate inconspicuously, beyond the scope of ordinary observation, posing a constant threat. Moreover, IoT devices are particularly vulnerable to attacks and security risks due to their inherent limitations, including their affordability, low power capabilities, limited computing resources, and the sheer heterogeneity and scale of the IoT network. The vulnerability of IoT devices is not solely attributed to technical factors but also extends to user behavior. These factors collectively contribute to the ongoing risks associated with these smart devices.

- Limited computing capabilities and hardware constraints: IoT devices are typically designed for specific applications with minimal processing power, leaving little room for robust security and data protection measures.
- Heterogeneous transmission technology: IoT devices communicate with various devices using diverse communication technologies, making it challenging to establish consistent protection measures and protocols.
- Vulnerable device components: Insecure or outdated fundamental components can leave millions of smart devices susceptible to harm.
- User security awareness: Many users lack sufficient knowledge about security, exposing IoT devices to potential risks and attack vectors. Additionally, the integration of third-party apps on IoT devices can introduce further vulnerabilities.
- Weak physical security: Unlike the secured data centers of internet services, many IoT components are physically accessible not only to users but also to individuals with malicious intent, increasing the risk of unauthorized access and tampering.

Security concerns in the realm of IoT can be categorized into two main types: software-level threats and hardware-level threats. Software-level attacks, such as hacking, information leakage, and illegal access, aim to disrupt system functionality and gather sensitive information like credit card details and passwords. Employing security measures like firewalls, keeping virus databases updated, and using the latest software versions can help mitigate software-based attacks.

However, the security landscape extends beyond software vulnerabilities, as hardware-level attacks also pose a significant risk. Ensuring complete hardware security requires the development of secure Integrated Circuits (ICs) or Systems on Chips (SoCs). This task has become increasingly complex due to the intricate nature of nanoscale design, the distributed fabrication of embedded Very Large Scale Integration (VLSI) chips, and the incorporation of third-party Intellectual Property (IP) cores. The insertion of a single malicious circuit during the fabrication process can compromise the entire system, and such intrusions may remain imperceptible to the original designers.

Defects within the components of a system can create vulnerabilities that broaden the attack surface. Adversaries often seek to exploit both the hardware and software of IoT systems to carry out malicious activities. According to a report by HP, approximately 50% of commercially available IoT devices exhibit significant security flaws. It is imperative to proactively address and respond to the vulnerabilities mentioned earlier, as they have the potential to expose sensitive information and compromise IoT systems.

Given the IoT network's susceptibility to various forms of attacks, conducting comprehensive security analysis and implementing foolproof security measures is a complex undertaking. However, the substantial volume of data generated within IoT environments also contributes to enhancing the overall security level of the system.

3.4. Thread model

Threat modeling facilitates the discovery of security flaws in computer systems and business processes. The thread model ensures that the system is not exposed to any potential vulnerabilities, which results in a heightened awareness of potential threats to system security [41]. IoT device networks are susceptible to newer security threats as a result of the challenges and issues that are associated with these networks. The requirements for security should be addressed at both the device level and the application level. The necessary precautions differ from one application to the next, as well as between domains.

IoT devices have a limited amount of resources, which means that they are easily exploitable and could potentially serve as an entry point to the network. Each device that is part of the network needs to be shielded so that there is less of a chance that there will be a breach in the network's data integrity. Because breaches in networks serving critical applications can endanger people's lives and cause financial harm, higher levels of security are required for those applications. Examples of such applications include healthcare and banking systems. In [42], the cyberattack known as BrickerBot targeted healthcare applications. Attackers were successful in compromising the medical device and destroying the memory and data it contained with the assistance of this middleware, which they used to initiate a brute force method of attack. Tables 4 and 5

The impact of security attacks on the data systems of the IoT can range from minor to severe damage. The summary of device-level vulnerabilities and possible threats is presented in Table 6 for a selection of domains, including healthcare, business, and smart cities. The exponential growth in the number of connected devices around the world presents a formidable obstacle for identity and access management. In order to construct a trusted operating environment in which untrusted

Table 5
IoT Attacks in Application layer Security.

Issue	Description
Data Authentication and Access	In applications with multiple users possessing different access privileges, it is essential to implement authentication and access control measures at the application layer [39].
Phishing attack	Adversaries employ infected emails or web links to illicitly obtain valid user credentials, thereby gaining unauthorized access [40].
Malicious Active X Scripts	An adversary has the capability to compromise the system by transmitting an Active X script to the IoT user over the internet, prompting the user to execute it [5].
Malware attack	Attackers can employ malware to pilfer data or disrupt applications through denial of service. Adversaries utilize threats like Trojan horses, worms, and viruses as means to exploit vulnerable systems [5].

Table 6
Comparison of different Vulnerabilities and Threads in IoT.

Application	Vulnerabilities	Threads
Routine Monitoring	Weak or no data encryption	Man-in-the-Middle Attacks, Cloning and Spoofing
Heart Monitoring	Weak or no data encryption, Lack of authentication mechanisms, Electrical/Radio Frequency interference	Device Manipulation, Incomprehension of data, Cloning and Spoofing
Radio Frequency Identification	Weak or no data encryption, Lack of authentication mechanisms	Reverse Engineering, No perfect forward secrecy, Cannot resist the desynchronization attack
Wireless Sensor Networks	Weak or no data encryption, Resource constrained nodes	Sink hole, Cloning and Spoofing and Wormhole
Access Control and Data Acquisition	Weak or no data encryption and Buffer overflows	DoS attacks and Information disclosure.
Smart Home	Communication channels that lack security and a lack of authentication procedures	Identity theft, Device manipulation and Location tracking
Smart Transportation	Insecure communication channels and Lack of authentication mechanisms	Remote compromising of vehicles and Location tracking
Smart Traffic Management	Weak or no data encryption, Insecure communication channels, Lack of authentication mechanisms	Cloning and spoofing, Hacking of remote traffic control unit.
Surveillance	Weak or no data encryption, Insecure communication channels	Device hack and Reconnaissance Analysis

IoT devices can communicate and share information over an unsecured channel, it is essential to establish mutual authentication between IoT devices and servers and other access points.

4. Authentication schemes

Authentication is one of the time-consuming tasks involved in determining the legitimacy of a remote user on a public network. Authentication is a critically important component in the overall security architecture of IoT applications. The different types of authentication mechanisms are broken down and categorized in Fig. 3. Authentication requirements shift between layers in a hierarchical structure. Authentication issues pertaining to key management, confidentiality, and integrity, as well as software for the middleware, are tackled in the application layer. The application layer has a number of problems, including identity theft disclosure, desynchronization attacks, and a lack of forward secrecy. Stolen passwords are another problem.

A four-way handshake method has been developed using a token-based approach to provide perfect forward secrecy (PFS) in RFID-based systems [43]. Using this interactive protocol, devices can be mutually authenticated for legitimate interactions. Due to the low-resource nature of IoT networks, complex authentication mechanisms cannot be employed. Authors in [44,45] developed a lightweight protocol that can resist collision attacks and DoS attacks. This method is computationally and communication-wise expensive but can withstand known security attacks. As presented in [46], the process of authenticating RFID tags can be made more complicated so that it can withstand attacks involving false nodes and other forms of impersonation. The authors in

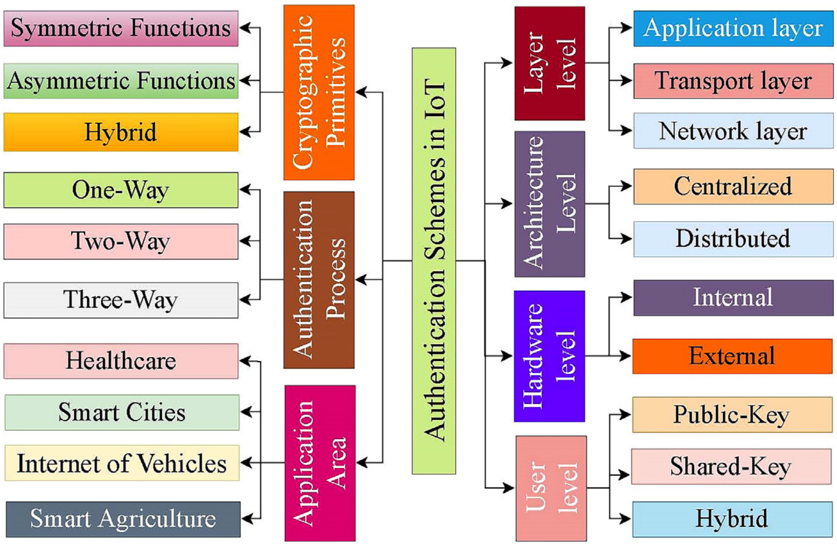

Fig. 3. IoT authentication mechanisms.

[47] found that using handshake methods, low-intensity authentication, and key agreement schemes were effective ways to accomplish efficient authentication and build trust in the system. To meet the demanding requirements of IoT applications, lightweight authentication protocols are currently in the process of being developed. Considering that these applications can process things and exchange information without the intervention of a human, authentication is becoming an increasingly important factor [48].

Recently developed cryptographic hash functions that are based on the Lightweight New Mersenne Number Transform (LNMNT) are ideal for providing security for IoT applications because of their lightweight nature. According to [49], these functions offer effective performance in terms of the amount of memory used, the amount of energy consumed, and the speed at which they are executed. The IoT and cloud computing platforms are combined to deliver more potent services, such as those referred to as Exchange to Exchange (E2E) and Smart to Smart (S2S) services. The number of security breaches, on the other hand, rises as a direct consequence of this integration, highlighting the ongoing requirement for a data delivery system that is both lightweight and effective. The authors in [50] found that this enabled better communication between a pair of IoT devices while also reducing the amount of power consumed and providing mutual authentication.

There is a need for augmentation methods due to the fact that high bitwidth cryptographic algorithms cannot be accommodated in IoT devices [51]. These methods involve the use of commercial processors that have high computational capabilities. Authentication mechanisms that are both effective and efficient are required for hierarchical IoT networks. In these networks, nodes must have the ability to directly access real-time data. In addition to passing all of the security validations, the model should be able to guarantee anonymity and incorporate a mechanism for automatically upgrading software [52]. At the physical layer, authentication from one device to another is nearly impossible due to the fact that compromised credentials, such as passwords, can make an attacker appear to be a legitimate user. [53] says that to stop these kinds of attacks, physical layer authentication schemes and standard cryptographic algorithms with low overhead must work together without any problems.

Existing encryption algorithms can be modified so that they are compatible with IoT devices that have limited resources. The authors in [54] found that even after algorithms such as AES were altered to work with the new hardware, they still maintained the same high level of security. The novel requirements of advanced IoT applications are beyond the capabilities of many of the existing security algorithms. According to [55], identity-based mutual authentication schemes that make use of puncturable pseudo-random functions can meet the requirements of mobile clients operating in an IoT environment.

Tampering with the device and installing replacement nodes are two examples of potential physical threats to physical IoT devices. The author in [56] suggests that multi-stage mutual authentication mechanisms should be implemented in order to prevent attacks of this nature. Increasing the level of internal and external hardware security within a network can help improve device authentication and ensure secure communication between the various entities that make up a network. Electronic circuits that are designed to function in only one direction are known as physical unclonable functions, or PUFs for short. It takes the same inputs but applies them at different time intervals, and as a result, it produces two distinct outputs. Because of this, it is difficult to "clone" them.

Yanambaka et al. [57] found that a robust authentication scheme that uses hybrid oscillator arbiter PUF can set up an authentication mechanism that is both more reliable and more quickly established. A PUF-based three-factor authentication system that uses biometrics, smart cards, and passwords is proposed by Liu et al. in [58]. This technique offers tamper resistance for IoT devices at a low cost and requires only a moderate amount of memory resources for computations. In [59], the authors present a proposal for a mutual authentication protocol that makes use of a hybrid arbiter and ring oscillator PUF. The session keys are generated and saved locally, either on the device or the server, when utilizing this method.

An adversary may create a proxy to imitate the device's behavior and gain unauthorized access to the network in this way. According to [60], resource-efficient PUFs are used in the modeling of the protocols that protect the integrity of IoT hardware and software. After going through a process of mutual authentication, the devices are then able to communicate with one another by using PUFs. When utilizing hardware-based security protocols, the vital metrics that need to be taken into consideration include the physical area of the PUF, the amount of energy that is consumed, and the rate at which keys are generated [61]. It is essential to have mechanisms in place to verify remote users in order to engage in trustworthy communication and data sharing. According to Zhao et al. in [62], PUFs can serve as a foundation for the identification of various types of devices.

In addition to this, the PUFs can serve as a source for the generation of cryptographic keys. The authors in [63] found that SRAM memories can be used to derive secret keys, which can then be used for encryption and decryption procedures. Standard algorithms, such as AES, can be utilized, along with the keys that are generated by PUFs, in order to encrypt the data. The challenge-response (CR) pairs that are used for enrollment and other purposes such as validation and verification have the potential to become access points for model-based attacks. Therefore, in order to ensure the safety of CR-pairs, the same encryption mechanisms can be utilized, as stated in [64].

In recent years, blockchain technology has garnered a lot of attention for its ability to provide a safe and reliable environment for the storage of data and the exchange of information. Through the utilization of digital contracts, the blockchain platform enables the safe transfer of data. These contracts are used to authenticate the users, which also provides role-based access control to the system. In some applications, like vehicular networks, broadcasting forged messages to attract user attention poses a threat to users' privacy as well as their ability to authenticate themselves. According to Khan et al. in [65], it is of the utmost importance in anonymous networks to both discover the true identities of participants and protect their privacy. A blockchain is used to store the data so that its veracity as well as its privacy can be preserved. As a result, this system offers a protected framework through the utilization of a distributed blockchain network.

The blockchain is entirely independent in that it does not involve any third parties in its operations. Before being allowed to share the data, the nodes and any other entities involved, therefore, have to carefully authenticate themselves. As mentioned in [66], effective methods of identity management and authentication are necessary in order to safeguard both the availability and integrity of data. In applications such as vehicular networks, traceability and the privacy of user data are both absolutely necessary. Pseudonyms and methods for tracing anonymous messages sent from malicious nodes are two of the techniques that are required in order to provide trusted communications in an environment where there is a lack of trust between vehicles and between vehicles and infrastructure. According to Zheng et al. in [67], blockchain technology may be able to provide assistance in meeting these essential requirements.

The medical and healthcare platforms are examples of domains that have made optimal use of the benefits and innovations offered by IoT networks, thereby realizing their full potential. The Internet of Medical Things (IoMT) refers to the collection of medical devices that are connected to the internet. These devices contain sensors that are interfaced to them in order to collect vital patient body parameters such as body temperature, heart rate, blood pressure, etc. Depending on the device, the sensors send their collected data via wired or wireless communication networks to a central server. The physicians can use this information to evaluate the performance of the remote patient as well as the patient's current state of recovery, and they can also prescribe additional medication. By utilizing encryption and the built-in tamper-proof architecture

Table 7
Comparison of different authentication schemes in IoT.

Ref.	Key Findings	Advantages	Disadvantages
[71]	The study suggests a mutual authentication and session key generation strategy for IoT applications.	The present study addresses IoT system issues such high computation and communication costs, lack of access level determination, and smart card theft susceptibility.	The scalability of the proposed solution with regard to managing a substantial quantity of IoT devices and services is not addressed in the study.
[72]	The suggested method zones the network and connects nodes using two keys inside and between zones.	The lightweight authentication operation for intra-zone communication reduces computational overhead and improves efficiency	The research does not discuss how network size, node density, or dynamics may affect approach performance and security.
[73]	The proposed method includes an authentication protocol to authenticate cluster heads before sending information, preventing malicious nodes in the network	Provides a regular structure for the transfer of information within the cluster and keys to secure the information exchanged in subsequent communications	The author does not Extend the proposed security method to other networks, including mobile networks.
[60]	The scheme utilizes temporary identities generated by the central server using a master key during the device registration process.	The paper introduces the concept of Physical Unclonable Functions (PUFs) and highlights their advantage in generating unpredictable outputs, which can contribute to the overall security of the scheme	The analysis of attack scenarios in the paper is limited to an informal discussion and does not include a formal security analysis or experimental validation
[74]	The smart cabin lighting system is designed with four features: automatic control of lighting devices around people, touch keypad control, app control, and data collection for analysis	Offers a cost-effective and energy-efficient ship cabin smart lighting system design.	Potential privacy concerns or considerations pertaining to the accumulation and analysis of data from the smart lighting system are not addressed in the paper.
[75]	The paper proposes a lightweight authentication and key agreement protocol for IoT-based smart healthcare systems, addressing the security concerns associated with IoT devices in healthcare.	Addresses the security concerns associated with IoT devices in healthcare, ensuring the confidentiality and integrity of patient data	The research makes no mention of real-world implementation or validation of the recommended methodology in an actual smart healthcare system, which may restrict the generalizability of the findings.
[76]	The paper discusses the impact of embedding watermarks on recognition accuracy in iris biometric authentication and highlights the need for comparative evaluations between watermarked and watermark-free systems	The proposed approach of embedding iris biometric watermarking offers high security, resistance to attacks, and non-intrusiveness, enhancing the overall security and robustness of authentication systems	The technology and methodology utilized to integrate iris biometric watermarking are not examined in the study.
[77]	This paper proposes a privacy-preserving Distributed Application (DA) that generates and maintains healthcare certificates using blockchain technology.	For security, the distributed application integrates blockchain with IoT-based medical devices. It also secures by specifying smart contract rules.	The technology and methodology utilized to integrate is highly computational overhead are not examined in the study.

that the blockchain "citexu2019healthchain" provides, a blockchain network enables the establishment of mutual authentication among users as well as data privacy.

Innovation and healthcare go hand in hand, with the former being applied to medical diagnosis and treatment. As mentioned in [68], because every procedure in the system is saved as an immutable record, users are unable to make any changes to them. The healthcare applications include things like tracking devices used by patients, billing insurance companies, and settling payments with pharmacies. Authentication and privacy protection mechanisms are necessities for any negotiations to take place between these entities. Another study [69] suggests that the transaction speed within the blockchain needs to be increased in order to ensure smooth and trouble-free transactions within the network. The data gathered from patients by healthcare applications may be stored on-chain or off-chain, depending on the provider's preference. The paper [70] recommends exercising caution whenever data from this storage is shared in order to protect the confidentiality of the data and stop unauthorized access. Further, some important solutions that address the authentication issues have been summarized in Table 7.

4.1. Open research dimensions in authentication

Comparing existing surveys and looking at the different authentication methods and tools that make them work shows a number of useful research directions in the area of IoT and its security. The drawbacks associated with the discussed authentication methods across different sections underscore the necessity for ongoing research efforts as IoT applications continue to diversify. Addressing these shortcomings, contingent on the specific application domains, will be a crucial task for future researchers. These identified limitations serve as a foundation for defining research problems that must be tackled to enhance the maturity and sustainability of IoT security in the future. These open research problems offer valuable guidance for algorithm developers, industry professionals, and academia. Building upon the discussions in the preceding sections, here we provide a consolidated list of directions for future research endeavors.

Architectural aspects: The review of research works underscores the prevalence of the three-layered architecture as the most widely adopted IoT framework. While other architectures are available, they have not received significant research attention thus far. The concept of a five-layered architecture emerges as a potential candidate for future IoT frameworks. Observations indicate that as IoT functionalities expand, designers introduce additional layers to accommodate various operations. These supplementary layers indeed provide finer granularity to the system. However, it is essential to have a comprehensive understanding of the underlying dependencies to define security requirements effectively and apply appropriate methods. Therefore, it becomes imperative to thoroughly grasp the merits and drawbacks of these architectural choices, enabling the association of well-defined functions with each layer to harness their architectural advantages optimally.

Security requirements: The authentication of both the sender and the data is a fundamental requirement for ensuring secure communication. In addition to this, employing an attestation process is essential to upholding both the integrity and authentication of the transmitted information. For instance, implementing remote attestation for IIoT-related patches and software updates is crucial. While several remote authentication methods are already in existence, there remains room for further advancements in this domain, particularly in the context of adopting decentralized frameworks.

Decentralization aspects: Authentication is typically established through the use of digital signatures, which rely on cryptographic keys. In conventional systems, the process of key generation is centralized and susceptible to potential failures. Researchers have already commenced investigations into distributed key generation processes, but further advancements are required to make them applicable in resource-constrained environments. Furthermore, in authentication schemes based on blockchain technology, achieving consensus poses a significant challenge. It is imperative to explore lightweight consensus mechanisms or alternatives like "proof of X" for such authentication methods.

Requirement of randomness: Reports from security protocol developers and NIST requirements have emphasized the need for the creation of robust random and pseudo-random number generators. In contemporary security protocols, the absence of reliable random numbers poses a significant challenge. Consequently, there is a demand for the development of simpler yet effective random number generators. Another facet of future research involves integrating these random numbers into security algorithms and analyzing their impact on the behavior of existing security protocols.

Authentication phase aspects: The survey provided a clear depiction of the infrequent use of authentication protocols with four to eight phases. Although these multi-phase structures were initially introduced with the aim of improving efficiency, they have encountered several drawbacks, which have hindered their adoption in the research domain. It is crucial to identify the underlying reasons for these challenges and to develop algorithms or functions that can help rejuvenate these phase structures. Moreover, it's important to acknowledge that an increased number of phases within a single operation, such as authentication, can potentially elevate complexity and resource consumption. This heightened complexity may, in turn, jeopardize the overall system's performance and lead to potential failures.

Authentication type aspects: Both IoTs and Wireless Sensor Networks (WSNs) have incorporated generic and standard security protocols to deliver authentication services. Industrial IoT (IIoT) and the Internet of Medical Things (IoMT) have also adopted this approach and have even ventured into developing customized authentication methods tailored to their specific domains. However, as devices become increasingly sophisticated and resource-constrained, the demand for security protocols has shifted from generic solutions to lightweight and even ultra-lightweight alternatives. In the future, security protocol designers should prioritize the development of robust algorithms that offer both lightweight and ultra-lightweight features. This is essential to meet the evolving needs of these diverse IoT domains while ensuring the security and efficiency of their operations.

Attack orientation: The survey conducted in this research work underscores the vulnerabilities of IoT systems to a range of security threats, including de-synchronization attacks, message modification attacks, cloning attacks, masquerading problems, node compromise issues, wormhole problems, and smart card vulnerabilities. Despite the recognition of these threats, research efforts to mitigate and address such attacks have not received substantial attention, leaving ample room for advancement in future research endeavors.

Password problem: The global challenge of passwords affects the security of IoT systems, as the trade-off between usability and security continues to impact their effectiveness. One-time passwords (OTPs) also fall within this spectrum, introducing additional concerns related to phishing when combined with shared secret practices. Consequently, IoTs are in search of a comprehensive authentication system that can effectively address these multifaceted problems.

Authentication requirements: Authentication protocols in IoT systems necessitate certain properties, namely backward secrecy and anonymity, to ensure robust authentication features. However, these two critical attributes have not received extensive research attention and require significant focus for enhancement. Furthermore, lightweight end-to-end authentication methods are highly favored in the context of IoT systems.

Authentication overhead: Creating an authentication protocol might seem straightforward, but crafting an efficient one is a challenging endeavor. An efficient authentication protocol should not introduce unnecessary overhead by exchanging an excessive number of messages. In the context of IoTs, this challenge is exacerbated as the number of devices increases, causing a significant rise in message exchanges. Furthermore, the message size should be kept to a minimum. Therefore, authentication protocol designers must strike a balance by utilizing a limited number of messages with efficient size constraints to enhance the productivity of the authentication system.

Post-quantum sustainability: The advancement of quantum computing poses a significant challenge to the sustainability of existing cryptosystems. To ensure the resilience of authentication protocols, designers must prioritize the development of quantum-resistant constructions for authentication keys or their derivatives.

Privacy-awareness: Privacy is an integral component of security, and even an authenticated entity can potentially compromise the privacy of data. Consequently, researchers should focus on designing an authentication mechanism that can effectively safeguard privacy. Moreover, it's essential to consider the interdependencies of various privacy parameters when developing authentication solutions.

Authorization integration: It is a common observation that legitimate users can be more susceptible to misusing the authorization process. Detecting such misuse can be challenging, especially when a user is authenticated but not properly authorized for a specific operation. Many authentication methods primarily focus on verifying the identity of nodes or users and often treat authorization as an assumed or separate module. Nevertheless, an optimal approach is to integrate an authentication mechanism that seamlessly incorporates authorization features, creating a coherent and unified process for both authentication and authorization.

Scalability: In the literature, it's a common trend to find authentication schemes claiming to be scalable. However, these claims often fall short of validation in real-world scenarios. Hence, it becomes imperative to establish a clear and substantiated correlation between these authentication schemes and scalability, backed by valid proofs and evidence.

Authentication as a service (AaaS): Authentication as a Service (AaaS) offers a range of authentication services, including multifactor authentication, single sign-on, and password management in the cloud. While cloud-based solutions provide these authentication services, they also inherit inherent security vulnerabilities that could lead to breaches. Therefore, there is a need to further develop efficient AaaS solutions that explicitly address and enhance cloud security. These aforementioned aspects of future research work play a pivotal role in ensuring the sustainable development of the IoT environment. They must be given significant attention to enhance the efficiency of IoT applications. Future researchers should actively consider these challenges and issues when working on IoT advancements, whether in the form of services or products.

Achieving robust authentication in IoT applications is crucial for verifying the identity of devices and users, ensuring that only authorized entities can access the network, data, and services. Implementing effective authentication mechanisms in IoT applications requires careful consideration of the specific requirements and constraints of the IoT ecosystem, including device capabilities, network architecture, and the sensitivity of the data being protected. A layered approach, combining multiple authentication methods, often provides the best defense against unauthorized access, ensuring that IoT systems remain secure and trustworthy. In conclusion, this survey suggests some important technologies and methods for strengthening authentication in IoT ecosystems.

Public Key Infrastructure (PKI) and Digital Certificates utilize a system of digital certificates, incorporating public and private keys, to authenticate devices securely within IoT environments. By verifying each other's trusted Certificate Authority (CA)-issued digital certificates, this system enables devices to mutually authenticate, facilitating secure communications. To further bolster security, Multi-Factor Authentication (MFA) demands two or more verification forms from different credential categories, such as knowledge (passwords), possession (security tokens or smart cards), and inherence (biometric verification like fingerprints or facial recognition). Additionally, OAuth and token-based authentication provide secure mechanisms for authorizing device access to services and resources without sharing passwords, using standards like

OAuth for access delegation and tokens (e.g., JSON Web Tokens, JWT) for managing sessions and information transmission securely.

In addition to these, two-step verification, which combines a password with another verification method like an SMS or app-generated code, adds an additional layer of security similar to MFA. For physical device security, Secure Elements (SEs) offer a tamper-resistant platform for securely hosting applications and their cryptographic data, enabling secure storage of digital keys and cryptographic operations on IoT devices. Similarly, Trusted Platform Modules (TPM) provide a secure cryptoprocessor that can securely store cryptographic keys used for authentication, ensuring these keys remain protected outside the TPM's environment. Together, these technologies form a comprehensive framework for enhancing the authentication and security of devices within the IoT, ensuring robust protection against unauthorized access and other security threats.

5. Access control and data privacy models

The IoT focuses primarily on facilitating the unbroken exchange of data across a variety of platforms. Security measures, including access control and data privacy, are managed at the local network level in IoT networks because these networks do not use standard architectures or protocols. Access control mechanisms are utilized in order to detect and prevent unauthorized access to the system's resources, which may include data, hardware, and software applications. These resources may include access to the system. Fig. 4 presents an overarching categorization of the various access control mechanisms.

The administrator of the network has the ability to set a limit on the number of users who have access to the network resources and to keep a list of authorized users thanks to access control mechanisms that are discretionary in nature. The list is kept up-to-date over the course of some time, and access is granted according to the privileges that are currently available. Only administrators and managers will be able to access the resources when mandatory access control mechanisms are in place, because access will be denied to any other users. The operations can only be performed by a select group of users, despite the fact that this access control mechanism is the most secure one. These days, the most common type of access control mechanism, particularly in applications based on the IoT, is the role-based model. Users have access to the resources they need based on the roles they play in their organizations, making role-based access control a more flexible form of access control.

There are a number of additional mechanisms that enable the modification of permissions in accordance with a predetermined set of rules, so rule-based access control mechanisms do not exist in a vacuum. There is a potential for data loss and disruption of service due to the inability of centralized access control mechanisms to scale to meet the demands of ever-growing IoT applications. In today's world, centralized mechanisms have taken on a significant role. The paper [78] describes the non-blockchain as a distributed access control mechanism that does not put its faith in centralized authorities having control over end users. Another research study [79] provides an illustration of one of these mechanisms by referring to organization-based distributed control access control.

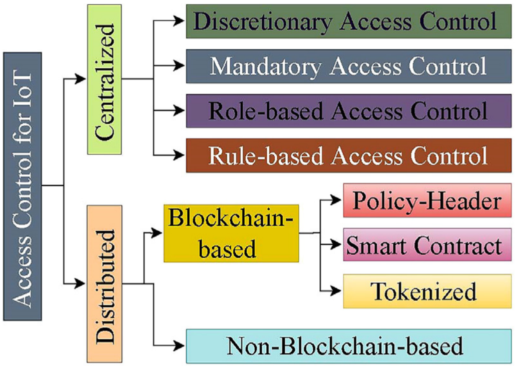

Fig. 4. IoT access control models.

Blockchain technology offers individualized solutions to a variety of security challenges, including access control. Access to the resources is granted on the basis of the information contained in the response's header regarding the access control mechanism, which, in the case of policy-header-based access control, is where the authorization information is stored. As was covered in the chapter before this one, smart contracts are composed of coded sets of agreements that, once satisfied, grant access to the resources. Token-based access control involves providing authorized users with tokens that contain particular validation rules and time stamps. These tokens are unique to each user. At the time of access, the system verifies the token, and only users who have tokens that are still valid are granted permission to access the resources.

Computing in the cloud is one of the key technologies that made it possible to build the IoT. The vast majority of the data generated by IoT applications is kept in the cloud, where user applications can connect to it in order to better serve the requirements of end users. The use of attribute-based signatures, also known as ABS schemes, can be beneficial for both controlling access and maintaining data privacy. The paper [58] reports that lightweight versions of these schemes are currently being developed for a wide variety of applications in order to accomplish the goals of unforgeability and anonymity. In certain applications, such as healthcare, it is absolutely necessary to validate the authenticity of the user. The data authenticators could be validated by using lightweight protocols that were deployed at the edges of the network in order to protect data privacy and prevent unauthorized access [80].

As a result of the fact that cloud services can be accessed through public networks like the internet, they are at risk of being subject to severe security breaches. Although the cloud offers blackbox security measures, it is possible that these safeguards are not suitable for all applications. Access control and privacy concerns for applications dealing with sensitive data, such as those dealing with healthcare and finances, have been addressed with the help of reputation-based mechanisms [81]. In an environment like this, trust plays a critical role, and the paper [82] proposes defining a set of parameters at various levels in order to perform periodic evaluations of the system.

Internet applications make extensive use of systems known as public key infrastructure (PKI), which are designed to protect the confidentiality of both data and communications. On the other hand, resource-constrained IoT networks are unable to make use of them because the PKI necessitates intensive computing and memory requirements. A recently developed lightweight compact certificate was designed to be suitable for IoT applications [83]. The work [84] explains that novel key derivation procedures that make use of fuzzy logic extractors and lightweight encryption algorithms can be combined together to simplify access control mechanisms and make them suitable for resource-limited networks. Techniques like division computation over encrypted data with privacy provisioning have become increasingly popular to serve the access control and privacy needs of the IoT networks [80].

Access control in a blockchain environment can be implemented in a variety of different ways. The utilization of smart contracts enables the provision of mechanisms for role-based access control. These contracts are deployed on blockchain platforms and written in the Solidity programming language. Each transaction that takes place within the network triggers the execution of a smart contract, and access to the network is granted only to authentic users who have passed validation. Every user has a role that is assigned to them, and the permissions they have are determined by that role [85,86]. All of the relations are mapped to the internal data structures using the coded rules that are contained within the smart contracts. According to [87], blockchain networks naturally incorporate security features such as the provenance of data and the confidentiality of transactions.

The introduction of blockchain technology and the increased level of security it provides have brought about revolutionary improvements

Table 8
Summary of researches in the area of access control and data privacy.

Ref.	Contributions	Advantages	Limitations
[92]	Access control solutions in a cloud computing environment are categorized by authors using various classifications. Furthermore, they provided a performance evaluation of various access control models.	It examine the relationships between models and technologies, application scenarios, and pros and cons. It also discuss emerging access control issues and cloud computing research directions.	The authors only dealt with the access control model as a standard. They didn't deal with the stages and nature of access control.
[93]	The authors suggested several access control categories, one of which is related to blockchain technology, notably smart contracts and transactions. Furthermore, they specified the precise application domain and blockchain platform used for each project.	It is an in depth discussion of blockchain taxonomy, application/use-cases, consensus mechanisms, prospective research, future directions, and related technologies. It also discusses the pros, cons, and opportunities of blockchain technology with IoT security.	The authors ignored access control criteria such as access control models, stages, and natures. Furthermore, the blockchain platform, hardware, and performance parameters are included in the implementation criteria.
[94]	The authors presented a classification system for authentication using blockchain technology: Access management based on smart contracts and on transactions.	This article explains IoT security and privacy with block chain. It also discussed how blockchain technology can improve IoT applications by providing security solutions.	The survey did not contain the comparison criteria for access control, as well as general factors like implementation and evaluation.
[95]	This literature review covers blockchain-based IoT access control, VANET, healthcare, and supply chain network privacy and security methods.	It evaluates methods for scalability, privacy, extensibility, accuracy, storage overhead, and computation overhead.	The authors failed to differentiate between blockchain technology requirements and access control criteria.
[96]	The authors presented a classification scheme for authentication that makes use of blockchain. Both transaction-based and smart-contract-based access controls are included in this classification system.	This paper covers device security, data collection and sharing, and industrial application. It also examine IIoT blockchain platform technical requirements.	The comparison was based solely on two criteria: implementation and security levels.
[97]	In order to implement access control in IoT systems utilizing blockchain technology, the authors defined particular characteristics of access control.	This paper examines the important aspects of blockchain for IoT access control include decentralized control, secure storage, and trustless information sharing, as well as their benefits and limitations.	Their focus was limited to specific access control criteria, namely attribute management and permission enforcement.

in a variety of industrial applications. In order to improve safety while continuing to take advantage of the innovative solutions offered by the IoT, many IIoT applications are being converted into blockchain-based applications [88]. Sharing electronic healthcare records, also known as EHRs, is one of the most significant challenges facing healthcare platforms [89]. Motes, which have a slow computational speed and a limited amount of memory, are used in body area networks (BANs). They are utilized to collect vital signs from the patient's body and convey this information to the central authorities in charge of the operation.

According to the paper [90], the use of specialized verification schemes and digital signatures is a viable option for achieving both access control and data security. For IoT networks with limited resources, it is possible to implement security mechanisms such as the outsourced calculation of rational numbers that protect users' privacy and allow for secure data sharing and access. Utilizing these strategies could prevent data from becoming accessible to unauthorized users [58]. According to [91], there are a large number of decentralized algorithms and other blockchain mechanisms that can be customized to fit the needs of IoT applications while maintaining the same level of data privacy and security. Table 8 provides a summary of some significant contributions made to the access control and privacy aspects of blockchain technology and the IoT.

5.1. Open research issues in access control

Access control has a rich history of research and development, with several access control models having been effectively implemented in real-world applications. However, as IoT technologies continue to evolve, different information resources are becoming deeply integrated for extensive use. The distinctive characteristics of IoT systems, including node heterogeneity, open environments, and the sharing of resources among multiple parties, introduce new requirements for access control models and mechanisms. Despite these challenges, many research endeavors have concentrated on introducing innovative models and mechanisms that enable fine-grained access control in IoT systems and their associated resources. Nevertheless, there remain numerous important issues and challenges that demand further attention and resolution.

Policy Conflict Caused by Different Authorizations: In this article, various access control models designed for IoT environments were introduced, including RBAC and ABAC. Several proposals related to RBAC have centered on integrating interpersonal relationships into access decision-making processes. However, these proposals frequently ignore the characteristics of multiparty resource sharing and assume that resources belong to a single entity. Conversely, numerous ABAC-related proposals have employed a straightforward approach to tackle this situation, requiring access to be authorized only when all users grant approval. Yet, this strategy can be overly restrictive for real-world applications, as it may limit resource availability. To address these challenges, more extensive efforts are necessary to concentrate on resolving policy conflicts arising from diverse authorizations. Such efforts can significantly enhance the automation of policy composition and conflict resolution, making access control in the IoT more adaptable and practical for real-world applications.

Policy Conflict Caused by Multiparty Relationships: The challenge of policy conflicts arises due to the distinctive characteristics of the IoT search environment. When integrating multiparty access control policies, the policies of different agents often include numerous constraints. For a given resource, different owners may impose varying constraints on its access. As a result, several access control decisions may emerge, each aligning with the requirements of individual users. However, these decisions can sometimes be mutually exclusive. The amalgamation of these constraints frequently leads to inconsistencies and conflicts. Hence, finding efficient and dynamic methods to swiftly select and adjust access control decisions for diverse users is a pressing issue that needs to be addressed. **Attribute-Permission Assignment Within Noise Data:**IoT search operates within a multidomain collaborative environment where different access control policies are utilized in distinct domains. To establish unified policy management, it is often necessary to convert other access control models into the attribute-based access control (ABAC) model. ABAC relies on attributes as its core components, and access control decisions are based on the set of attributes that the requester possesses. This characteristic makes ABAC particularly well-suited for the IoT search environment, as it effectively segregates policy management from access control decision-making.

The process of converting other policy types into ABAC entails creating high-quality attribute-permission correspondences, primarily based on role-permission and user-permission relationships. Notably, original user-permission relations may contain noise data, significantly impacting the accuracy of policy generation and introducing substantial security risks to access control systems. Addressing the assignment of attribute-permission relationships within noisy data represents a substantial research challenge in the realm of access control for IoT search. **Modeling and Evaluation of IoT Security Search:** It is imperative to maintain a balance between quality, security, and efficiency throughout the process of IoT search. The escalating growth of IoT has brought increased focus to its security. Over the past decades, modeling and simulation (MS) techniques have effectively addressed various complex security challenges. Given that IoT possesses a distinctive address and relies on standard communication protocols, MS methods and tools are well-suited for addressing IoT-related issues. Despite this, there has been limited exploration into the modeling and evaluation of IoT security searches.

Authentication and Anonymous Protection of Physical Devices in the IoT: Within industrial control security IoT, numerous authentication methods are developed to facilitate real-time communication between the cloud platform and sensing devices. However, often, these methods face a challenge in simultaneously ensuring both efficiency and security. Consequently, there is a need for increased emphasis on the technology related to device authentication and anonymity protection. This emphasis is crucial to guaranteeing the trustworthiness of data sources, preserving privacy, and maintaining data availability.

6. Scalability models

Scalability is the primary issue that arises with IoT networks. In order to keep the system in a state of equilibrium, the network will need to modify itself to accommodate the growing number of nodes and the volume of traffic. When connected to blockchain networks, IoT devices bring an exponential increase in the severity of this problem. Because each transaction needs to be validated before it is added to the block and then stored at every node in the network, blockchains are unable to accommodate the growing number of transactions generated by the IoT. According to the paper [98] some ineffective ways of increasing scalability include increasing the block size and reducing the amount of time spent on the consensus protocol. Researchers from all over the world have come up with a variety of solutions to address the scalability issues, and this section will discuss a few of those solutions.

LPWAN, which stands for low-power wide area networks, is one of the technologies that made it possible for the Internet to exist. Scalability is an issue that needs to be addressed in order to meet the demanding requirements of an increasing number of applications for the IoT. According to the paper [70], increasing scalability can be accomplished through the seamless integration of polynomial-based optimization techniques into these networks. Some of the obstacles that must be overcome in order to achieve scalability include interoperability, deployability, and the absence of standard communication protocols. The scalability of the system can be improved to some degree [99] by making it possible for edge devices to conform to the modular properties of the applications.

Scalability in the IoT can be attributed, in large part, to the fact that the majority of its applications are geared toward centralized cloud servers. The authors in [100] found that, as a consequence of this, blockchain-based decentralized applications exhibited superior scalability. Altering the data structures already present within the blockchain to better suit the needs of the application is yet another method for increasing the system's capacity to scale. The corresponding algorithms are developed in order to gain access to and process these structures, thereby reducing the amount of time necessary for the processing of the blocks contained within the blockchain. The paper [101] explains that the scalability of transactions can be improved in this way.

As IoT devices are incapable of executing complex consensus algorithms, direct integration of blockchain and IoT is not possible. Instead, a local loop network can serve as an interface between these two networks to facilitate communication. The authors in [102] found that the transaction rate could be increased by relieving blockchain of the additional burden of processing data from IoT devices. According to the paper "cite" tang2022coordinate, techniques like source look-up techniques and discovery techniques can reduce the communication overhead.

Security from beginning to end and scalable data sensing mechanisms are prerequisites for systems that have more stringent requirements for the collection of data, the flow of data from one entity to another, and the storage of data. According to the paper [103], a more effective strategy for accomplishing the goal of achieving the required level of scalability is to design infrastructures that are capable of being configured in order to collect and exchange data. According to the paper [104], algorithms that cut down on the amount of time needed for validation and consensus processes also make valuable contributions to improving scalability. In addition, scalability can be improved by utilizing scheduling and synchronization mechanisms [105]. These mechanisms give users greater access while simultaneously reducing the likelihood of collisions. According to the paper [106], the quality of the services that are offered to final users can be adjusted to better meet their Quality of Service (QoS) requirements.

Access control is vital for securing the vast network of devices in the IoT. In conclusion, this survey suggests some key technologies used to achieve robust access control in the IoT. Authentication serves as the critical layer that determines the identity of a user or device attempting to access a resource, employing mechanisms such as passwords, biometrics, and digital certificates to ensure security. Access Control Lists (ACLs) are utilized to define specific rules that either permit or restrict access to resources for particular users or devices; for instance, an ACL might enable a user to view but not modify sensor data. Role-Based Access Control (RBAC) takes a different approach by assigning permissions according to predefined roles, meaning a "maintenance technician" might have the authority to reboot devices but not to change their configurations. Attribute-Based Access Control (ABAC) provides an even finer level of control by evaluating attributes like location, time, or device type, potentially restricting thermostat access to authorized devices within the office network during work hours. The management of access control has traditionally been centralized, relying on a central server; however, distributed models offer an alternative by allowing devices to independently make access decisions based on established rules, thereby diminishing the dependency on a central authority and enhancing system resilience.

7. Conclusion and future directions

In this paper, the methods that are currently available in the literature are discussed, and this paper also presents the methods that are currently available. The subsequent step is an in-depth discussion of the numerous security risks and the importance of threat modeling. The subsequent topic is a discussion of the various IoT applications' necessary security precautions. It reviews the prior research on the numerous security issues and the solutions put forth by various researchers. The holes that were found while conducting this literature review served as inspiration for the current research work.

7.1. Research challenges

The billions of IoT devices deployed across the globe collect personal and sensitive data and exchange it with other networks using intelligent interfaces. Providing device authentication, authorization, data privacy, and security in such an un trusted environment is a challenge. Centralized trusted infrastructure cannot scale to the dynamic and ever intensifying traffic and, thus, leading to bottlenecks in the network. Distributed authentication can scale to the increasing demands of the IoT networks, but requires distributed trusted systems. The majority of the work in the IoT security domain focuses on embracing the security mechanisms of WSNs and conventional Internet-based applications. However, these mechanisms are far from being implemented in real-time scenarios due to the specific challenges of IoT, such as

Scalability With the number of IoT devices installed surpassing the total world human population, designing scalable architectures that cater to the demanding needs of the broad spectrum of IoT applications is the need of the hour.

Device Heterogeneity The IoT nodes operate on different hardware and operating system platforms and use different sets of protocols for communication and other purposes. The quality of service (QoS) requirements are also different for different services, or for the same set of services, there may be different modes of operation.

Interoperability, which allows a device to communicate and exchange information with other devices across various networks, emerges from the challenges posed by heterogeneity and the absence of standardized protocols and architectures within IoT networks. In the early stages of research focused on IoT security, a thorough literature review highlighted several notable deficiencies in current state-of-the-art approaches. Among these are the need for a lightweight mechanism that can facilitate secure communication and data sharing in IoT networks constrained by limited resources. Additionally, there is a crucial demand for improved access control and data privacy measures to protect sensitive information. Furthermore, the development of user and IoT device authentication methods is essential for establishing a trusted operating environment, underscoring the gaps that future research must address to enhance IoT security.

Resource Limited By design, most the IoT devices have low memory and low computational processing ability. They operate on battery power in harsh environments.

The distributed nature of the resources The resources in the IoT network are distributed to provide different functionalities, cooperation, and data classification based on applications.

7.2. Future directions

The integration of advanced technologies such as machine learning, fog computing, edge computing, and blockchain into IoT ecosystems significantly enhances their security. Each of these technologies addresses specific vulnerabilities and brings unique strengths to the security architecture of IoT networks. Machine Learning (ML) plays a pivotal role in IoT security, offering capabilities such as anomaly detection, adaptive threat response, and automated security. ML algorithms excel at processing extensive datasets generated by IoT devices, identifying patterns, and detecting anomalies, which are crucial for early breach detection and intervention. Over time, ML can adapt to new threats dynamically, offering superior threat detection and response compared to static measures. Moreover, ML automation reduces manual oversight, enhancing security efficiency and response speed.

Fog computing, operating closer to data sources, reduces latency in threat detection and response, mitigating risks faster. By processing data locally, fog computing minimizes the attack surface and follows a decentralized security model, enhancing resilience against attacks. Edge computing further strengthens IoT security by processing data at the source, reducing data transit risks, and enabling real-time security actions. It optimizes resources by empowering devices to autonomously analyze data, enhancing privacy and security. Blockchain technology reinforces security and trust within IoT ecosystems through its secure, immutable ledger, resistant to tampering and fraud. Its decentralized approach mitigates single points of failure, enhancing network resilience while enabling secure, transparent transactions between devices, essential for secure machine-to-machine interactions.

Funding

The authors did not receive financial support from any organization for the submitted work.

Availability of data and materials

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

M Kokila: Writing – original draft, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Srinivasa Reddy K:** Writing – review & editing, Visualization, Validation, Supervision, Software, Project administration, Investigation, Funding acquisition.

Acknowledgment

We acknowledge that the assistance provided by VIT-AP University on the aspect of getting subscribed journal and conference articles to complete the review.

References

[1] Z. Lv, R. Lou, J. Li, A.K. Singh, H. Song, Big data analytics for 6G-enabled massive internet of things, IEEe Internet. Things. J. 8 (7) (2021) 5350–5359.
[2] M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the IoT world: present and future challenges, IEEe Internet. Things. J. 5 (4) (2017) 2483–2495.
[3] V. Adat, B.B. Gupta, Security in internet of things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. 67 (2018) 423–441.
[4] C. Maniveena, R. Kalaiselvi, A survey on IoT security and privacy, AIP conference proceedings, AIP Publishing, 2023.
[5] S.A.H. Ali, J.V. Rani, Attack detection in IoT using machine learning—a survey, Intell. Cyber Phys. Syst. Internet of Things: ICoICI 2022 3 (2023) 211.
[6] A. Barua, M.A. Al Alamin, M.S. Hossain, E. Hossain, Security and privacy threats for bluetooth low energy in iot and wearable devices: a comprehensive survey, IEEE Open J. Commun. Soc. 3 (2022) 251–281.
[7] M.N. Khan, A. Rao, S. Camtepe, Lightweight cryptographic protocols for IoT-constrained devices: a survey, IEEe Internet. Things. J. 8 (6) (2020) 4132–4156.
[8] J. Sengupta, S. Ruj, S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, J. Netw. Comput. Appl. 149 (2020) 102481.
[9] F. Neves, R. Souza, J. Sousa, M. Bonfim, V. Garcia, Data privacy in the internet of things based on anonymization: a review, J. Comput. Secur. (Preprint) (2023) 1–31.
[10] L. Chettri, R. Bera, A comprehensive survey on internet of things (IoT) toward 5G wireless systems, IEEe Internet. Things. J. 7 (1) (2019) 16–32.
[11] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues, IEEE Commun. Surv. Tutorials 22 (2) (2020) 1191–1221.
[12] V. Sharma, I. You, K. Andersson, F. Palmieri, M.H. Rehmani, J. Lim, Security, privacy and trust for smart mobile-internet of things (m-IoT): a survey, IEEe Access. 8 (2020) 167123–167163.
[13] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices, IEEe Internet. Things. J. 6 (5) (2019) 8182–8201.
[14] R.K. Shrivastava, et al., Securing internet of things devices against code tampering attacks using return oriented programming, Comput. Commun. 193 (2022) 38–46.
[15] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R.U. Rasool, W. Dou, Complementing IoT services through software defined networking and edge computing: a comprehensive survey, IEEE Commun. Surv. Tutorials 22 (3) (2020) 1761–1804.
[16] H. Xue, D. Chen, N. Zhang, H.N. Dai, K. Yu, Integration of blockchain and edge computing in internet of things: a survey, Future Gener. Comput. Syst. 144 (2023) 307–326.
[17] S. Mathur, A. Kalla, G. Gür, M.K. Bohra, M. Liyanage, A survey on role of blockchain for IoT: applications and technical aspects, Comput. Netw. 227 (2023) 109726.
[18] S. Abed, R. Jaffal, B.J. Mohd, A review on blockchain and iot integration from energy, security and hardware perspectives, Wirel. Pers. Commun. 129 (3) (2023) 2079–2122.
[19] S. Alam, et al., An overview of blockchain and IoT integration for secure and reliable health records monitoring, Sustainability. 15 (7) (2023) 5660.
[20] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for internet of things (IoT) security, IEEE Commun. Surv. Tutorials 22 (3) (2020) 1646–1685.

[21] P. Arora, B. Kaur, M.A. Teixeira, Machine learning-based security solutions for healthcare: an overview, in: Emerging Technologies for Computing, Communication and Smart Cities: Proceedings of ETCCS 2021, 2022, pp. 649–659.

[22] A. Gaurav, B.B. Gupta, P.K. Panigrahi, A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system, Enterp. Inf. Syst. 17 (3) (2023) 2023764.

[23] S. Hameed, F.I. Khan, B. Hameed, Understanding security requirements and challenges in internet of things (IoT): a review, J. Comput. Netw. Commun. 2019 (2019) 1–14.

[24] X. Wang, et al., Survey on blockchain for internet of things, Comput. Commun. 136 (2019) 10–29.

[25] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutorials 21 (3) (2019) 2702–2733.

[26] T.M. Fernández-Caramés, From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the internet of things, IEEe Internet. Things. J. 7 (7) (2019) 6457–6480.

[27] O. Friha, M.A. Ferrag, L. Shu, L. Maglaras, X. Wang, Internet of things for the future of smart agriculture: a comprehensive survey of emerging technologies, IEEE/CAA J. Automatica Sinica 8 (4) (2021) 718–752.

[28] A. Al Sadawi, M.S. Hassan, M. Ndiaye, A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges, IEEe Access. 9 (2021) 54478–54497.

[29] Y. Song, F.R. Yu, L. Zhou, X. Yang, Z. He, Applications of the internet of things (IoT) in smart logistics: a comprehensive survey, IEEe Internet. Things. J. 8 (6) (2020) 4250–4274.

[30] A. Alwarafy, K.A. Al-Thelaya, M. Abdallah, J. Schneider, M. Hamdi, A survey on security and privacy issues in edge-computing-assisted internet of things, IEEe Internet. Things. J. 8 (6) (2020) 4004–4022.

[31] P. Nayak, G. Swapna, Security issues in IoT applications using certificateless aggregate signcryption schemes: an overview, Internet of Things 21 (2023) 100641.

[32] Y.R. Siwakoti, M. Bhurtel, D.B. Rawat, A. Oest, R. Johnson, Advances in IoT security: vulnerabilities, enabled criminal services, attacks and countermeasures, IEEe Internet. Things. J. (2023).

[33] L. Fotia, F. Delicato, G. Fortino, Trust in edge-based internet of things architectures: state of the art and research challenges, ACM. Comput. Surv. 55 (9) (2023) 1–34.

[34] S.Z. Marshoodulla, G. Saha, An approach towards removal of data heterogeneity in SDN-based IoT framework, Internet of Things 22 (2023) 100763.

[35] J. Xiang, A. Zhao, G.Y. Tian, W. Woo, L. Liu, H. Li, Prospective RFID sensors for the IoT healthcare system, J. Sens. 2022 (2022).

[36] F. tu Zahra, Y.S. Bostanci, M. Soyturk, Real-time jamming detection in wireless IoT networks, IEEe Access. (2023).

[37] Z. Abukari, E.Y. Baagyere, M.M. Iddrisu, A new text encryption scheme suitable for combating sniffing attacks in IoT applications via non-supersingular elliptic curves over binary extension fields, Earthline J. Math. Sci. 13 (2) (2023) 451–472.

[38] S. Dogan-Tusha, S. Althunibat, M. Qaraqe, Doppler shift based sybil attack detection for mobile IoT networks, IEEe Internet. Things. J. (2023).

[39] Z. Chen, Y. Jiang, X. Song, L. Chen, A survey on zero-knowledge authentication for internet of things, Electronics. (Basel) 12 (5) (2023) 1145.

[40] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, J. Porras, Mitigation strategies against the phishing attacks: a systematic literature review, Comput. Secur. (2023) 103387.

[41] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures, IEEe Access. 7 (2019) 82721–82743.

[42] M. Shobana, S. Rathi, Iot malware: an analysis of iot device hijacking, Int. J. Scientif. Res. Comput. Sci. Comput. Eng. Inf. Technol. 3 (5) (2018) 2456–3307.

[43] M. Wazid, P. Bagga, A.K. Das, S. Shetty, J.J. Rodrigues, Y. Park, AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment, IEEe Internet. Things. J. 6 (5) (2019) 8804–8817.

[44] K. Mansoor, A. Ghani, S.A. Chaudhry, S. Shamshirband, S.A.K. Ghayyur, A. Mosavi, Securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography, Sensors 19 (21) (2019) 4752.

[45] S.K. Choi, J.S. Ko, J. Kwak, A study on IoT device authentication protocol for high speed and lightweight, in: 2019 international conference on platform technology and service (PlatCon), IEEE, 2019, pp. 1–5.

[46] F. Wang, G. Xu, G. Xu, A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map, IEEe Access. 7 (2019) 101596–101608.

[47] B. Narwal, A.K. Mohapatra, SALMAKA: secured, anonymity preserving and lightweight mutual authentication and key agreement scheme for WBAN, Int. J. Sensors Wirel. Commun. Control 11 (4) (2021) 374–384.

[48] S. Patranabis, et al., Lightweight design-for-security strategies for combined countermeasures against side channel and fault analysis in IoT applications, J. Hardw. Syst. Secur. 3 (2019) 103–131.

[49] N. Nabeel, M.H. Habaebi, M.R. Islam, Security analysis of LNMNT-lightweight crypto hash function for IoT, IEEe Access. 9 (2021) 165754–165765.

[50] M.A. Al Sibahee, et al., Lightweight secure message delivery for E2E S2S communication in the IoT-cloud system, IEEe Access. 8 (2020) 218331–218347.

[51] Y. Zhang, L. Xu, Q. Dong, J. Wang, D. Blaauw, D. Sylvester, Recryptor: a reconfigurable cryptographic cortex-M0 processor with in-memory and near-memory computing for IoT security, IEEe J. Solid-State Circuits. 53 (4) (2018) 995–1005.

[52] H.S. Trivedi, S.J. Patel, Design of secure authentication protocol for dynamic user addition in distributed internet-of-things, Comput. Netw. 178 (2020) 107335.

[53] P. Hao, X. Wang, W. Shen, A collaborative PHY-aided technique for end-to-end IoT device authentication, IEEe Access. 6 (2018) 42279–42293.

[54] J.N. Mamvong, G.L. Goteng, B. Zhou, Y. Gao, Efficient security algorithm for power-constrained IoT devices, IEEe Internet. Things. J. 8 (7) (2020) 5498–5509.

[55] M.A. Saleem, Z. Ghaffar, K. Mahmood, A.K. Das, J.J. Rodrigues, M.K. Khan, Provably secure authentication protocol for mobile clients in IoT environment using puncturable pseudorandom function, IEEe Internet. Things. J. 8 (22) (2021) 16613–16622.

[56] T. Alladi, V. Chamola, et al., HARCI: a two-way authentication protocol for three entity healthcare IoT networks, IEEE J. Sel. Areas Commun. 39 (2) (2020) 361–369.

[57] V.P. Yanambaka, S.P. Mohanty, E. Kougianos, D. Puthal, PMsec: physical unclonable function-based robust and lightweight authentication in the internet of medical things, IEEE Trans. Consumer Electron. 65 (3) (2019) 388–397.

[58] J. Liu, H. Tang, R. Sun, X. Du, M. Guizani, Lightweight and privacy-preserving medical services access for healthcare cloud, IEEe Access. 7 (2019) 106951–106961.

[59] H. Luo, T. Zou, C. Wu, D. Li, S. Li, C. Chu, Lightweight authentication protocol based on physical unclonable function, Comput. Mater. Contin. 72 (3) (2022) 5031–5040.

[60] S. Das, S. Namasudra, S. Deb, P.M. Ger, R.G. Crespo, Securing IoT-based smart healthcare systems by using advanced lightweight privacy-preserving authentication scheme, IEEe Internet. Things. J. (2023).

[61] S. Abdolinezhad, A. Sikora, A lightweight mutual authentication protocol based on physical unclonable functions, in: 2022 IEEE international symposium on hardware oriented security and trust (HOST), IEEE, 2022, pp. 161–164.

[62] B. Zhao, P. Zhao, P. Fan, ePUF: a lightweight double identity verification in IoT, Tsinghua Sci. Technol. 25 (5) (2020) 625–635.

[63] S. Chanda, A.K. Luhach, W. Alnumay, I. Sengupta, D.S. Roy, A lightweight device-level public key infrastructure with DRAM based physical unclonable function (PUF) for secure cyber physical systems, Comput. Commun. 190 (2022) 87–98.

[64] S. Banerjee, V. Odelu, A.K. Das, S. Chattopadhyay, J.J. Rodrigues, Y. Park, Physically secure lightweight anonymous user authentication protocol for internet of things using physically unclonable functions, IEEe Access. 7 (2019) 85627–85644.

[65] M.A. Khan, M.T. Quasim, N.S. Alghamdi, M.Y. Khan, A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data, IEEe Access. 8 (2020) 52018–52027.

[66] A. Rashid, A. Masood, A. ur R. Khan, Zone of trust: blockchain assisted IoT authentication to support cross-communication between bubbles of trusted IoTs, Cluster. Comput. 26 (1) (2023) 237–254.

[67] D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang, A traceable blockchain-based access authentication system with privacy preservation in VANETs, IEEe Access. 7 (2019) 117716–117726.

[68] L. Ge, B. Lv, N. Li, S. An, F.Y. Wang, A hypertension parallel healthcare system based on the ACP approach, IEEe J. Radio Freq. Identif. 6 (2022) 724–728.

[69] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Inf. Secur. Appl. 50 (2020) 102407.

[70] M.Z.U. Rahman, S. Surekha, K.P. Satamraju, S.S. Mirza, A. Lay-Ekuakille, A collateral sensor data sharing framework for decentralized healthcare systems, IEEe Sens. J. 21 (24) (2021) 27848–27857.

[71] A.G. Mirsaraei, A. Barati, H. Barati, A secure three-factor authentication scheme for IoT environments, J. Parallel. Distrib. Comput. 169 (2022) 87–105.

[72] P. Alimoradi, A. Barati, H. Barati, A hierarchical key management and authentication method for wireless sensor networks, Int. J. Commun. Syst. 35 (6) (2022) e5076.

[73] M. Ataei Nezhad, H. Barati, A. Barati, An authentication-based secure data aggregation method in internet of things, J. Grid. Comput. 20 (3) (2022) 29.

[74] Y.K. Huang, Design of a smart cabin lighting system based on internet of things, Cloud Comput. Data Sci. (2023) 112–121.

[75] S. Das, M.P. Singh, S. Namasudra, A lightweight authentication and key agreement protocol for IoT-based smart healthcare system, in: 2023 world conference on communication & computing (WCONF), IEEE, 2023, pp. 1–5.

[76] T. Taj, M. Sarkar, A survey on embedding iris biometric watermarking for user authentication, Cloud Comput. Data Sci. (2023) 203–211.

[77] P. Sharma, S. Namasudra, N. Chilamkurti, B.G. Kim, R.Gonzalez Crespo, Blockchain-based privacy preservation for IoT-enabled healthcare system, ACM. Trans. Sens. Netw. 19 (3) (2023) 1–17.

[78] S. Ravidas, A. Lekidis, F. Paci, N. Zannone, Access control in internet-of-things: a survey, Journal of Network and Computer Applications 144 (2019) 79–101.

[79] D.V. Medhane, A.K. Sangaiah, M.S. Hossain, G. Muhammad, J. Wang, Blockchain-enabled distributed security framework for next-generation IoT: an edge cloud and software-defined network-integrated approach, IEEe Internet. Things. J. 7 (7) (2020) 6143–6149.

[80] R. Ding, H. Zhong, J. Ma, X. Liu, J. Ning, Lightweight privacy-preserving identity-based verifiable IoT-based health storage system, IEEe Internet. Things. J. 6 (5) (2019) 8393–8405.

[81] F. Kong, Y. Zhou, B. Xia, L. Pan, L. Zhu, A security reputation model for IoT health data using s-AlexNet and dynamic game theory in cloud computing environment, IEEe Access. 7 (2019) 161822–161830.

[82] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, D. Chen, Enhancing cloud-based IoT security through trustworthy cloud service: an integration of security and reputation approach, IEEe Access. 7 (2019) 9368–9383.

[83] F. Marino, C. Moiso, M. Petracca, PKIoT: a public key infrastructure for the internet of things, Trans. Emerg. Telecommun. Technol. 30 (10) (2019) e3681.

[84] C. Adams, A privacy-preserving blockchain with fine-grained access control, Secur. Privacy 3 (2) (2020) e97.

[85] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, Y. Zhang, A smart-contract-based access control framework for cloud smart healthcare system, IEEe Internet. Things. J. 8 (7) (2020) 5914–5925.

[86] P. Kamboj, S. Khare, S. Pal, User authentication using blockchain based smart contract in role-based access control, Peer. Peer. Netw. Appl. 14 (5) (2021) 2961–2976.

[87] H. Huang, W. Kong, S. Zhou, Z. Zheng, S. Guo, A survey of state-of-the-art on blockchains: theories, modelings, and tools, ACM Comput. Surv. (CSUR) 54 (2) (2021) 1–42.

[88] J. Wan, J. Li, M. Imran, D. Li, et al., A blockchain-based solution for enhancing security and privacy in smart factory, IEEe Trans. Industr. Inform. 15 (6) (2019) 3652–3660.

[89] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure ehrs sharing of mobile cloud based e-health systems, IEEe Access. 7 (2019) 66792–66806.

[90] Y. Ren, Y. Leng, F. Zhu, J. Wang, H.J. Kim, Data storage mechanism based on blockchain with privacy protection in wireless body area network, Sensors 19 (10) (2019) 2395.

[91] T.A. Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, T. Alghamdi, A comparative analysis of blockchain architecture and its applications: problems and recommendations, IEEe Access. 7 (2019) 176838–176869.

[92] F. Cai, N. Zhu, J. He, P. Mu, W. Li, Y. Yu, Survey of access control models and technologies for cloud computing, Cluster. Comput. 22 (2019) 6111–6122.

[93] B. Shrimali, H.B. Patel, Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities, J. King Saud Univ.-Comput. Inf. Sci. 34 (9) (2022) 6793–6807.

[94] P. Bagga, A.K. Das, V. Chamola, M. Guizani, Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions, Telecommun. Syst. 81 (1) (2022) 125–173.

[95] P. Patil, M. Sangeetha, V. Bhaskar, Blockchain for IoT access control, security and privacy: a review, Wirel. Pers. Commun. 117 (2021) 1815–1834.

[96] R. Huo, et al., A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges, IEEE Commun. Surv. Tutorials 24 (1) (2022) 88–122.

[97] S. Pal, A. Dorri, R. Jurdak, Blockchain for IoT access control: recent trends and future research directions, J. Netw. Comput. Appl. 203 (2022) 103371.

[98] L. Zhou, L. Wang, Y. Sun, P. Lv, Beekeeper: a blockchain-based iot system with secure storage and homomorphic computation, IEEe Access. 6 (2018) 43472–43488.

[99] A. Javed, A. Malhi, T. Kinnunen, K. Främling, Scalable IoT platform for heterogeneous devices in smart environments, IEEe Access. 8 (2020) 211973–211985.

[100] W. Xiang, Z. Yuanyuan, Scalable access control scheme of internet of things based on blockchain, Procedia Comput. Sci. 198 (2022) 448–453.

[101] Y. Liu, K. Wang, K. Qian, M. Du, S. Guo, Tornado: enabling blockchain in heterogeneous internet of things through a space-structured approach, IEEe Internet. Things. J. 7 (2) (2019) 1273–1286.

[102] J.P. Mehare, A.K. Gaikwad, A comparative analysis of IoT-based blockchain frameworks for secure and scalable applications, Int. J. Intell. Syst. Appl. Eng. 11 (9s) (2023) 46–58.

[103] S. Kahveci, B. Alkan, A. Mus'ab H, B. Ahmad, R. Harrison, An end-to-end big data analytics platform for IoT-enabled smart factories: a case study of battery module assembly system for electric vehicles, J. Manuf. Syst. 63 (2022) 214–223.

[104] S. Biswas, K. Sharif, F. Li, S. Maharjan, S.P. Mohanty, Y. Wang, PoBT: a lightweight consensus algorithm for scalable IoT business blockchain, IEEe Internet. Things. J. 7 (3) (2019) 2343–2355.

[105] S. Lee, J. Lee, H.S. Park, J.K. Choi, A novel fair and scalable relay control scheme for internet of things in LoRa-based low-power wide-area networks, IEEe Internet. Things. J. 8 (7) (2020) 5985–6001.

[106] C. Qiu, H. Yao, F.R. Yu, C. Jiang, S. Guo, A service-oriented permissioned blockchain for the internet of things, IEEe Trans. Serv. Comput. 13 (2) (2019) 203–215.