REVIEW

Open Access

Dissecting zero trust: research landscape and its implementation in IoT

Chunwen Liu[1], Ru Tan[1,2], Yang Wu[3], Yun Feng[1], Ze Jin[1], Fangjiao Zhang[1], Yuling Liu[1,2] and Qixu Liu[1,2*]

Abstract

As a progressive security strategy, the zero trust model has attracted notable attention and importance within the realm of network security, especially in the context of the Internet of Things (IoT). This paper aims to evaluate the current research regarding zero trust and to highlight its practical applications in the IoT sphere through extensive bibliometric analysis. We also delve into the vulnerabilities of IoT and explore the potential role of zero trust security in mitigating these risks via a thorough review of relevant security schemes. Nevertheless, the challenges associated with implementing zero trust security are acknowledged. We provide a summary of these issues and suggest possible pathways for future research aimed at overcoming these challenges. Ultimately, this study aims to serve as a strategic analysis of the zero trust model, intending to empower scholars in the field to pursue deeper and more focused research in the future.

Keywords Zero trust, Research landscape, Bibliometrics method, Internet of things, Hot topics

Introduction

The widespread adoption of Internet of Things (IoT), cloud computing, and bring your own device has led to an expansion of current networks (Buck et al. 2021), with a rising number of terminals engaging in data transactions, information exchange, and resource utilization both within and across network perimeters (Xiaojian et al. 2021). This has resulted in increasingly blurred network boundaries and significant implications for cybersecurity (Da Rocha et al. 2021; Jabar and Mahinderjit Singh 2022). Traditional security methods, such as firewalls, VPNs, intrusion detection systems and intrusion prevention systems, typically divide networks into trusted internal networks and untrusted external ones (Teerakanok et al. 2021; Dhar and Bose 2021). However, this boundary security model relies on implicit trust, and is vulnerable to threats from external attackers or malicious insiders (Buck et al. 2021). In IoT scenarios, the issue becomes even more prominent due to the use of various devices like sensors, surveillance cameras, industrial equipment, and smart home appliances. These devices present notable disparities in terms of operating systems, software platforms, and types, often with restricted resources. Consequently, their deployment often lacks extensive multi-layered network and information system protection, exacerbating the challenge of guaranteeing device security, communication security, and data security within the IoT environment. As a result, traditional security measures become ineffective, highlighting the vital importance of device security and authentication, particularly in large-scale and dynamic IoT deployments (Misbahuddin et al. 2022). Considering this situation, the zero trust model has become a key solution for network security. It challenges the implicit trust assumption of the traditional boundary security model by strengthening security measures and mitigating potential risks related to compromised IoT devices' access and disruption of

*Correspondence:
Qixu Liu
liuqixu@iie.ac.cn
[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3] China Cybersecurity Review Technology and Certification Center, Beijing 100013, China

network resources through the adoption of agent-centric trust evaluation, continuous verification, and authentication mechanisms (Vanickis et al. 2018; Ge et al. 2023).

Zero trust security is based on the principle of "never trust, always verify" (Adahman et al. 2022), which means that no implicit trust is given to assets or user accounts just because of their physical or network location (Ameer et al. 2022). A zero trust architecture will not grant access to resources unless the user/device, asset, or workload is confirmed through a robust authentication and authorization process (Piya et al. 2021). This verification takes into account various factors and sources of information, such as access privileges (Omar et al. 2020), device information (Zhao et al. 2020), and user behavior (Fang et al. 2022), etc. Zero trust is also known as perimeterless security, as it shifts the focus from network devices to assets (Karabacak et al. 2022).

Currently, zero trust has evolved from a security concept to a crucial technology for network security and is gaining increasing recognition in governments, corporations, and academic institutions. The rapid development of the zero trust field has spurred numerous studies to explore the concept, key characteristics, technologies, research progress, and trends. For instance, Syed et al. (2022) delved into the role of authentication and access control in zero trust architectures, and thoroughly analyzed the current techniques for authentication and access control in various situations. Yan and Wang (2020) conducted a comprehensive survey of zero trust, including its components and key technologies, and demonstrated its application in various scenarios, highlighting its benefits such as big data capabilities, cloud networks, and IoT. Jabar and Mahinderjit Singh (2022) presented the concepts of zero trust and zero trust architecture as outlined based on National Institute of Standards and Technolog (NIST) Special Publication (SP) 800-207 and examined the difficulties, actions, and factors to consider when transitioning from a legacy architecture to a zero trust architecture. Buck et al. (2021) conducted a multivocal literature review, taking into account multiple perspectives, to assess the current state of knowledge about zero trust and to uncover potential avenues for future research.

The driving force behind this work is the requirement for a deeper understanding of zero trust using a range of computational tools, given the rapidly growing interest in this field. Furthermore, there has not been an in-depth exploration of the growth of publications, performance of leading players and their collaborations, understanding of underlying knowledge structures, identification of hot and emerging topics in the field of zero trust, and thorough analysis of zero trust in IoT. Therefore, the main objective of this paper is to enhance previous research by utilizing bibliometric methods and providing a comprehensive analysis of zero trust in IoT. To the best of our knowledge, this study is the first to conduct a bibliometric and scientometric analysis of publications related to zero trust. By employing this literature-based method, we aim to minimize researcher bias resulting from incomplete manual reading and reduce selective perception, leading to improved reading efficiency and more accurate research outcomes.

The key contributions of this paper are:

(i) We utilize bibliometric methods to gain a comprehensive understanding of the current state of research on zero trust. Our methodology encompasses three key steps. Firstly, we analyze the overall trend of research growth to determine the developmental stages of academic research in this field. Secondly, we use scientific indicators and collaborative partnerships to examine leading countries and obtain insights into the worldwide advancement of zero trust research. Finally, we extract keywords from relevant research papers and apply co-occurrence network analysis to identify present and emerging areas of interest, as well as potential future research directions.

(ii) We conduct a comprehensive analysis of the practical applications of zero trust in IoT. Initially, we investigate and summarize the security threats that are present in the IoT, analyzing the security challenges and potential attack vectors across different layers, such as the perception, network, and application layers. Next, we provide detailed outlines of zero trust solutions that can be employed to counter security vulnerabilities and attack techniques in each of these layers.

(iii) Based on the existing research foundation, we develop a mapping structure that encompasses threat locations, vulnerabilities, application scenarios, types of attack, zero trust solutions, and core technologies for each layer of IoT. In addition, we conduct an analysis of the challenges and obstacles associated with implementing zero trust security in IoT environments, and present potential directions for future research.

Conceptual background of zero trust

The concept of zero trust security originated with the work of the Jericho Forum, a security consortium, in 2003 (Al-Ruwaii and De moura 2021). However, the term "zero trust" was officially coined by Forrester in 2010 (Kindervag and Balaouras 2010) and has since matured, gaining widespread recognition in the industry (Xiao et al. 2022). In the zero trust model, trust is not given blindly to entities seeking access to network resources, even after undergoing initial authentication and authorization (Ramezanpour and Jagannath 2022). This approach, which prioritizes data and identity awareness, views trust points as potential weaknesses (Campbell 2020). The implementation of zero trust architecture through this method has proven to be a cost-efficient way of securing access to sensitive resources when compared to VPN (Adahman et al. 2022), and has been successful in preventing cyberattacks and the strategies used by cybercriminals (Al-Ruwaii and De moura 2021).

The subsequent sections present and examine the zero trust architecture and core technologies.

Zero trust architecture

The implementation of zero trust architecture may vary according to the specific requirements of an organization (Buck et al. 2021), but it typically includes five major components. These components, as depicted in Fig. 1, are subject, Policy Enforcement Point(PEP), Policy Administrator(PA), Policy Engine(PE) and resource (Teerakanok et al. 2021).

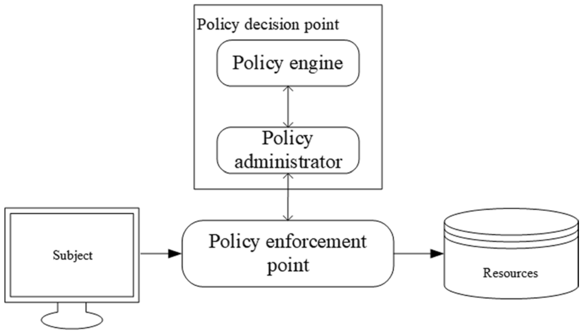

Fig. 1 Typical components of the logical structure of zero trust architecture

Subsequently, scholars began to expand on this logical architecture by incorporating concepts such as policy information points (PIP) and policy storage (Buck et al. 2021). Based on existing research (Teerakanok et al. 2021; Rose et al. 2020), the updated zero trust logic architecture and it key components are summarized in Fig. 2, which includes six major components: network participants, PEP, policy decision points (PDP), PIP, policy administration points (PAP), and resources.

As depicted in Fig. 2, the logical framework of zero trust security encompasses all interactions between network participants, including users, diverse devices, and applications, and the associated resources such as data, APIs, and apps. The PDP is comprised of the PE and PA components. The PE component is considered the “brain” of the zero trust architecture, where a crucial decision-making process known as the trust algorithm takes place (Jabar and Mahinderjit Singh 2022). It continuously evaluates the trustworthiness of network participants based on information from PIP and PAP, such as threat intelligence, behavioral data, network traffic, and access policies. The PA component continuously manages the authorization policies. The PEP is the actual implementation of these policies and facilitates communication between users/devices/Apps and requested resources (Buck et al. 2021).

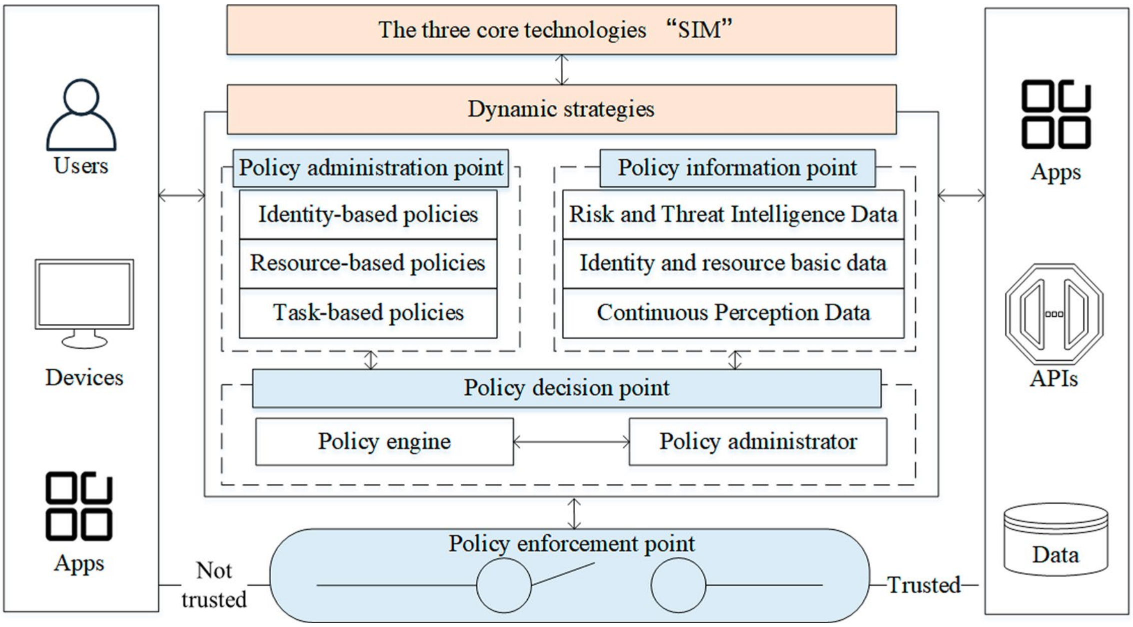

Fig. 2 The updated zero trust logic architecture and it key components

According to the access flow depicted in Fig. 1 and Fig. 2, the process begins with a network participant initiating a request for resource access to the PEP. Subsequently, the PEP forwards the request information to the PDP. Next, the PE component of the PDP evaluates the level of trust based on a combination of diverse and multiple sources of data. The PA component of the PDP then makes a decision on the authorization strategy based on the trust value that was previously evaluated by the PE. Once the access has been granted, the PDP will issue a command to the PEP to set up a secure communication channel for the access. The PDP will continuously evaluate the trust and make decisions on authorization policies, providing feedback to the PEP as necessary to maintain the security of the resources. The PEP will then carry out the appropriate actions in response to this feedback to ensure the security of the resources at all times.

The NIST has released the final version of its publication, "Special Publication (SP) 800-207, Zero Trust Architecture" (Rose et al. 2020). This document highlights the security concept of zero trust and introduces three technologies, known as "SIM", to implement this architecture. These technologies include Software Defined Perimeter (SDP), Identity and Access Management (IAM), and Micro-segmentation (MSG). The SDP addresses security concerns from south to north, IAM is considered a fundamental technology for identity management, and MSG aims to tackle security issues from east to west. These technologies establish dynamic and granular access control and data isolation mechanisms, achieving user and device identity verification and authorization to ensure network and data security. Therefore, the"SIM" technologies, which refer to the SDP, IAM, and MSG, are key to the zero trust logical architecture and indispensable in implementing zero trust security strategies.

Core technology of zero trust

Despite advancements in security technology, "SIM" technologies continue to be the foundation of the zero trust field. Here is a comprehensive overview of these technologies.

SDP is a new generation network security model based on the concept of zero trust proposed by CSA in 2013. Its unique solution is access control and resilience against network-based attacks (Kumar et al. 2019). The SDP creates a dynamic and detailed service access tunnel between visitors and resources, involving the SDP controller, the initiating host, and the accepting host (Wang et al. 2023). The SDP framework is shown in Fig. 3. SDP creates a virtual boundary through software and only allows access to authorized users and machines, effectively providing a "cloak of invisibility" for infrastructure and resources to prevent network attacks (Kumar et al. 2019; Moubayed et al. 2019). The SDP framework consists of five security control layers: Single Packet Authentication (SPA), Mutual Transport Layer Security (mTLS), Device Validation (DV), Dynamic Firewall (DF), and Application Binding (AppB) (Singh et al. 2020; Refaey et al. 2019), which together provide mutual device authentication and confidential communication, validate user authenticity, ensure only authorized devices can access network resources, establish encrypted tunnels to secure service access, and defend against various network-based attacks (Palmo et al. 2021), such as Denial of Service (DoS) attacks, man-in-the-middle (MITM) attacks, tampering attacks, and sniffing attacks.

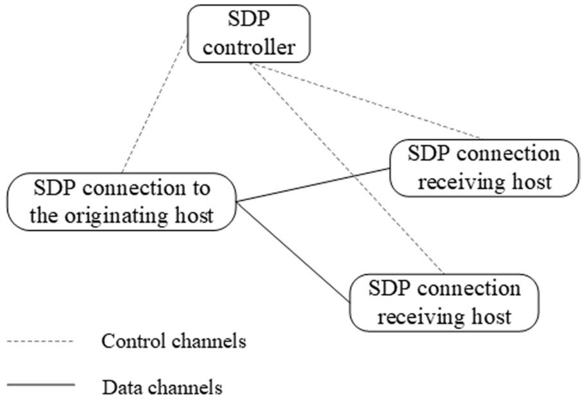
SDP controller
SDP connection to the originating host
SDP connection receiving host
SDP connection receiving host
Control channels
Data channels

Fig. 3 The SDP framework

IAM is a solution designed to manage access to resources (Nahar and Gill 2022), which encompasses both identity management and access management (Kunz et al. 2015). It aims to ensure that the right individuals have access to the right resources at the appropriate time and for the right reasons, within the proper access environment, by analyzing and managing crucial data, including identity, authority, environment, and activities (Sharma et al. 2015; Indu et al. 2018). Identity management and authentication are crucial steps in granting access to resources, and with the zero trust model, stronger forms of identity authentication like multi-factor authentication (Indu et al. 2018), enhanced biometric authentication (Darwish 2021), and continuous authentication techniques (Song et al. 2022) are needed. Authorization for accessing resources in a zero trust network follows the principle of minimum privilege, and granular access control based on trust labels is essential (Ali et al. 2021). Continuous monitoring and trust evaluation methods, including machine learning, can enhance the accuracy and effectiveness of access control decisions (Fang et al. 2022).

MSG is a relatively new security technique and a critical component of the zero trust security framework

(Basta et al. 2022). Traditional security measures primarily focus on defending the perimeter (Klein 2019), but once the protective boundary is breached, conventional firewall methods are unable to prevent indiscriminate access between internal traffic. MSG addresses this concern by dividing the network infrastructure into smaller (Syed et al. 2022), logically isolated segments, allowing for a more granular approach to access control based on user and device profiles (Vanickis et al. 2018). The architecture of MSG proposed by NIST is depicted in Fig. 4. It's an essential task for security professionals working with virtualization architecture in a multi-cloud or hybrid environment (Klein 2019).

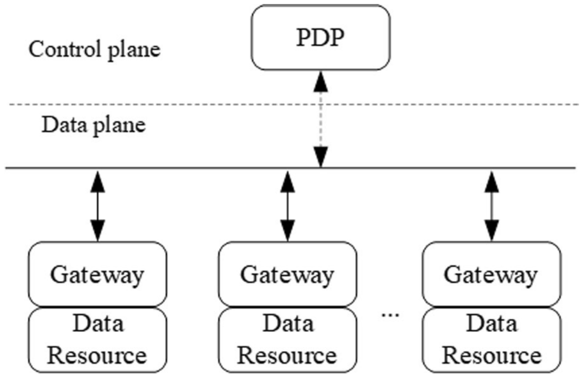

Fig. 4 The MSG framework

Data and research methods

In this bibliometric study, we utilize scientific papers as the data source and conduct a comprehensive analysis through a combination of statistical analysis, network analysis, and text mining to understand the research landscape of zero trust.

Data collection and processing

Web of Science (WoS) and Scopus are widely used databases for bibliometric analysis in the sciences, with WoS Core Collection being highly regarded for its quality and extensive coverage (Merigo et al. 2017; Chen et al. 2015). While Scopus is said to have a more European focus and includes more modern sources and conference proceedings (Chappin and Ligtvoet 2014). While Google Scholar offers a broader range of coverage, it does have limitations when it comes to advanced search capabilities for keywords, abstracts, and other fields. Additionally, the lack of bulk downloading functionality makes it challenging for bibliometric analysis. In our bibliometric analysis, we consider publications within the zero trust domain that are indexed in the WoS and Scopus databases, which encompass articles, conference papers, and book chapters, as the primary unit of analysis. However, for the analysis of "key research hotspots and future trends for zero trust" and "IoT threat and zero trust solutions", we manually searched and reviewed influential literature from Google Scholar as well to ensure a more comprehensive analysis.

To ensure the search for the most relevant results, we identify related terms that are used as synonyms for zero trust concept, as suggested by Buck et al. (Buck et al. 2021). We also incorporate three technologies and their corresponding synonyms that are suggested by NIST (Rose et al. 2020). The search string used is ("zero trust" OR "zero-trust" OR "software defined perimeter" OR "identity and access management" OR "micro segmentation" OR "micro-segmentation"). A search of titles, abstracts, and keywords conducted on September 14, 2023 yields 422 papers in WoS and 955 papers in Scopus, all published between 2010 and 2023.

To ensure the accuracy of the bibliometric analysis, we conduct noise reduction on the aforementioned data by removing duplicate records and deleting irrelevant literature. Subsequently, we identify and download 814 records that are the most relevant for bibliometric analysis. Scientific papers are used as they not only have the highest impact in the field of zero trust but also represent the latest research directions.

Bibliometric analysis

Bibliometric analysis is a commonly used tool for quantitatively analyzing publications in scientific and applied fields (Ellegaard and Wallin 2015). It employs quantitative analysis, correlation networks, and statistics to provide an informative overview of the bibliographic material in a specific area (Gao et al. 2021).

To gain insights into the global development of research on zero trust, we conduct a simple bibliometric analysis. Initially, we examine the annual volumes of scientific publications, cumulative publication amounts, and fit a curve to the latter to determine the growth trajectory of the research. We then conduct an in-depth analysis of leading countries to illustrate technology advantage and differences at the country/area level, utilizing scientometric indicators and network analysis. The analysis includes the following variables:

(a) Total Publications (*TP*)—the total number of publications of actors

(b) Total Citations (*TC*)—the number of total citations of actors

(c) Cumulative publication amounts (*CPA*)—cumulative number of *TP* with year

(d) Cited Publications (*CP*)—the number of cited publications

(e) International Collaboration ratio (*ICR*)—the percentage of the international collaboration publications

(f) *H*-index—*H* papers in the published papers have been cited at least H times

Knowledge structure analysis

To depict the topic landscape of zero trust, this study utilizes network analysis based on graph theory to map the relationships between keywords (Ji et al. 2018). By using high-frequency keywords and keyword co-occurrence network analysis, this study identifies current hotspots, emerging topics, and future research avenues. Natural language processing algorithms are employed to extract key terms from titles and abstracts of papers without keywords, which are then normalized and visualized through VOSviewer Clustering Workbench to reveal the underlying structure of complex networks.

Analysis of zero trust in IoT

The analysis of the zero trust knowledge structure has revealed that it is closely intertwined with various fields such as IoT, artificial intelligence (AI), blockchain, cloud computing, and big data. The IoT plays a particularly significant role in the zero trust network as it has the highest total link strength among all the keywords, excluding the IAM-related basic vocabulary (i.e. identity and access managements and authentication). Additionally, the recent trend of its appearance indicates that IoT is a research hotspot for zero trust and its research enthusiasm continues to grow. Therefore, this paper will delve deeper into zero trust in IoT, exploring its implications for securing network resources and identifying potential challenges and solutions.

The goal of IoT security is to protect IoT systems and devices from attacks and misuse. This involves evaluating and securing the IoT networks, devices, applications, and cloud services to ensure reliability, confidentiality, integrity, and availability. Due to the complexity of the IoT architecture and the diversity of business scenarios, conventional security boundaries are difficult to establish. Therefore, to ensure IoT security, it is necessary to focus on the architectural layers, threats and application scenarios of the IoT, and research how zero trust can ensure IoT security from which technologies and aspects. To this end, a framework for analysis is proposed as shown in the Fig. 5. An analysis of attack vectors is conducted at the three layers of IoT architecture (i.e. application layer, network layer, and perception layer) based on the scientific paper on zero trust in IoT, and corresponding zero trust solutions are summarized. The application layer mainly includes data security and access control, while the network layer comprises direct and indirect communication, and the perception layer encompasses sensors and devices.

Research landscape of zero trust

This section presents an overview of the research landscape regarding zero trust, divided into two parts: basic bibliometric analysis and knowledge structure analysis. The former aims to provide insight into the publication trends and characteristics of zero trust research; while

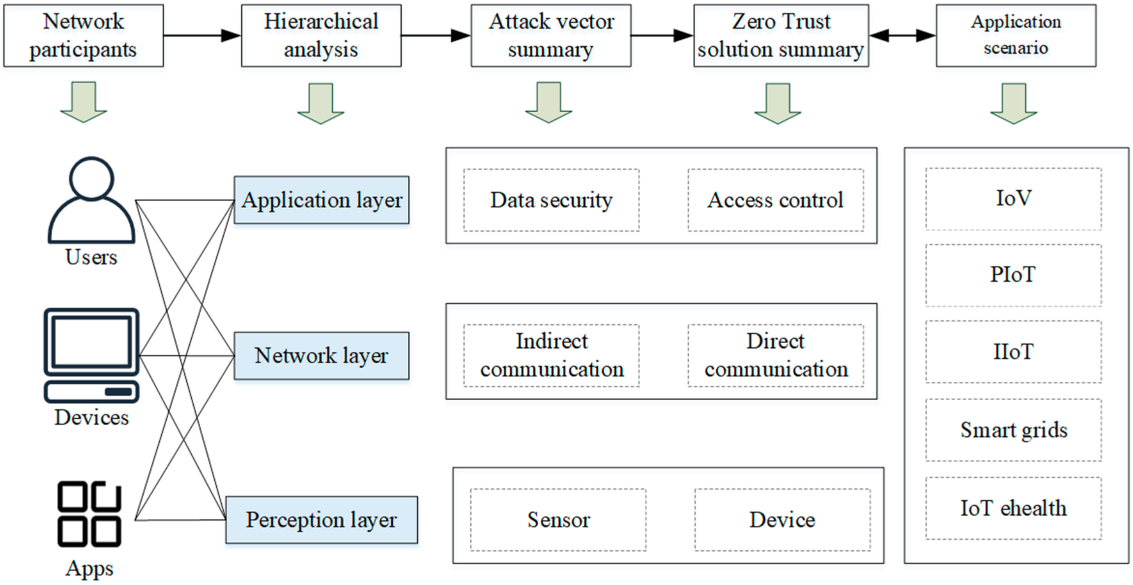

Fig. 5 Framework for analyzing zero trust in IoT

the latter focuses on the intellectual structure and evolution of topics related to zero trust.

Basic bibliometric analysis

The basic bibliometric analysis consists of two main parts. Firstly, we present general statistics on the growth trajectories of research related to zero trust. In the second part, a more detailed examination is conducted on the performance of countries/areas and their collaborations.

General statistics

We provide our results in a series of illustrations below: Figures and Tables. Further, we discuss each figure or table. We start with Fig. 6 below.

We show in Fig. 6 the general trajectories of research growth related to zero trust. The growth curve of the cumulative publications (*FCCPA*) is fitted and stimulated by a 4th-degree polynomial, where *FCCPA* indicates that fitted value of *CPA*. The correlation coefficient is 0.991, which implies a better curve fitting output. Fig. 6 illustrates that there has been a steady increase in research on zero trust during that period. We present this data as the number of scientific publications is a widely recognized metric for assessing scientific performance in specific technological domains, and can aid in elucidating the present state of technology as well as predicting its future development (Miyazaki and Islam 2007). The publication volumes for zero trust research exhibit an overall upward trend, which can be divided into three distinct periods: 2010–2012, 2013–2020, and 2021–2023. During the initial germination period, annual publications were below 15, with an average annual volume of 13. In the second exploration period, annual publications increased to less than 80, with an average annual volume of 32.25. Post 2020, zero trust research experienced a period of rapid growth, with 145 and 249 publications in 2021 and 2022, and a predictive curve fitting model estimates a total of 340.3 papers in 2023 and a cumulative count of 1023.4 documents from 2010 to 2023.

Countries/areas' performance and their collaborations analysis

A total of 814 publications on zero trust were contributed by 89 countries/areas worldwide, with 18 countries/areas contributing more than 10 articles each. This suggests an uneven distribution of scientific research on zero trust across different countries/areas. Table 1 displays the performance of the top 10 countries/areas in terms of productivity related to zero trust, as indicated by various indices. Out of these top 10 countries, only two are considered developing countries, namely China and India, which suggests that a strong foundation in science, technology, and industrial development is necessary for research on zero trust. The United States had the highest number of publications at 201, accounting for 24.69% of the total publications, which is approximately 1.38 times that of China in second place with 145 publications. India and Germany followed closely in third and fourth place, respectively, in terms of the number of publications. Additionally, the United Kingdom and Canada

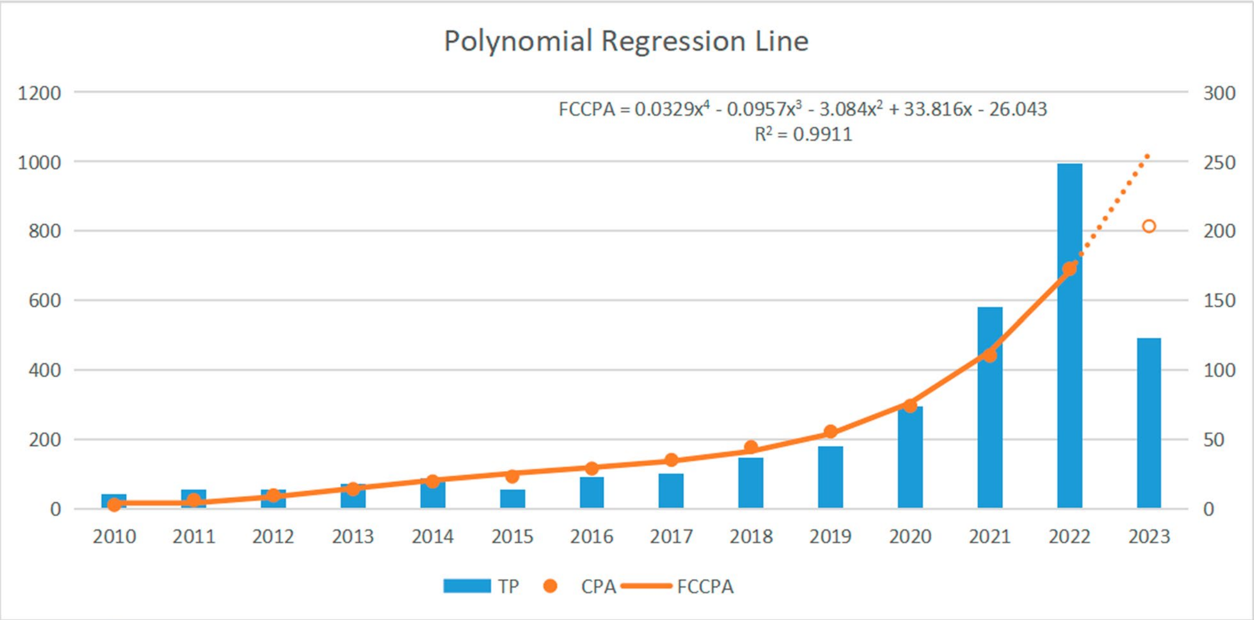

Fig. 6 General trajectories of research growth related to zero trust (*FCCPA*: fitting curve for *CPA*)

Table 1 The performance of the top 10 most productive countries/areas

Countries/areas	TP (%)	CP(%)	TC	TC/TP	ICR	H-index
United States	201 (24.69)	131 (65.17)	2506	12.47	0.26	20
China	145 (17.81)	71 (48.97)	352	2.43	0.15	10
India	103 (12.65)	61 (59.22)	498	4.83	0.10	12
Germany	68 (8.35)	55 (80.88)	520	7.65	0.19	13
United Kingdom	51 (6.27)	40 (78.43)	525	10.29	0.51	12
Australia	28 (3.44)	19 (67.86)	266	9.50	0.39	9
Italy	27 (3.32)	19 (70.37)	92	3.41	0.41	4
Japan	26 (3.19)	13 (50)	85	3.27	0.31	5
Canada	19 (2.33)	16 (84.21)	313	16.47	0.58	10
Finland	19 (2.33)	11 (57.89)	78	4.11	0.63	5

had a significant academic impact, as reflected in their TC and h-index indicators. Finland had the highest international collaboration ratio, which is an important factor for future development in this field.

The annual publications from the top 10 most productive countries in the zero trust field are shown in Fig. 7. The United States has consistently been the leader in article production and has maintained a steady growth in publications on zero trust. Notably, China has exhibited significant growth in zero trust research since 2020, and surpassed the United States in 2022. It continues to maintain a growth trend in this field. India also shows a fast growth rate in 2020–2022. However, the number of publications in other countries has shown a similar slow growth trend, indicating that the growth of zero trust publications is mainly driven by the efforts of China and the United States, and China holds the potential to surpass all others and emerge as the most productive country in this field in the future.

To investigate possible collaborations in the field of zero trust, Fig. 8 displays a co-authorship network of countries that have published at least five papers. The

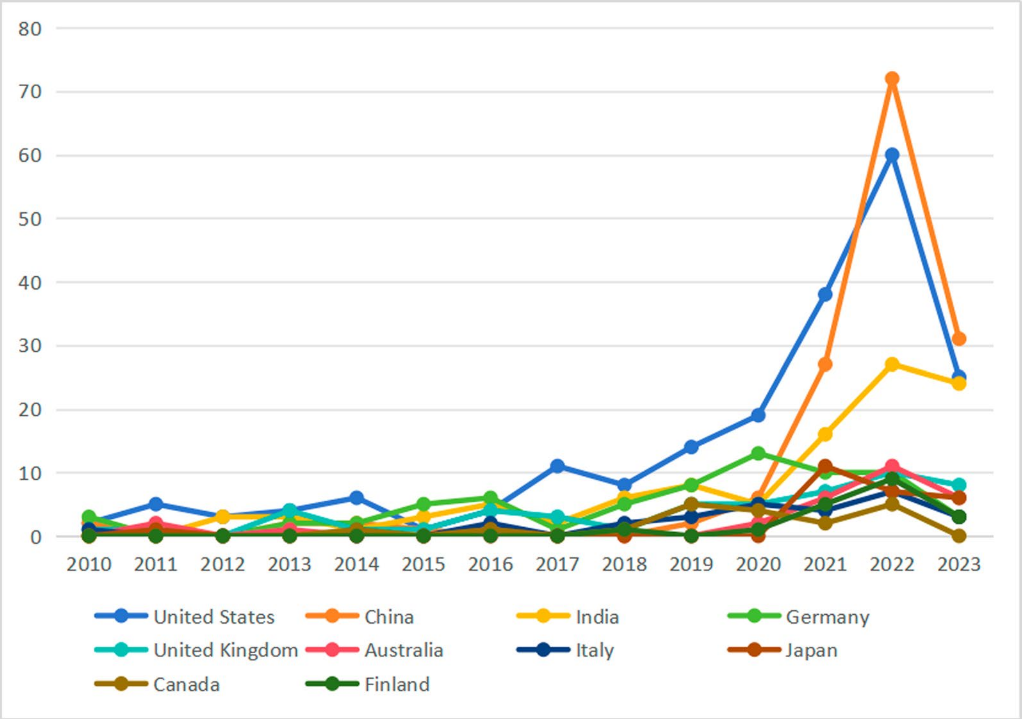

Fig. 7 The growth trends of the 10 most productive countries/areas

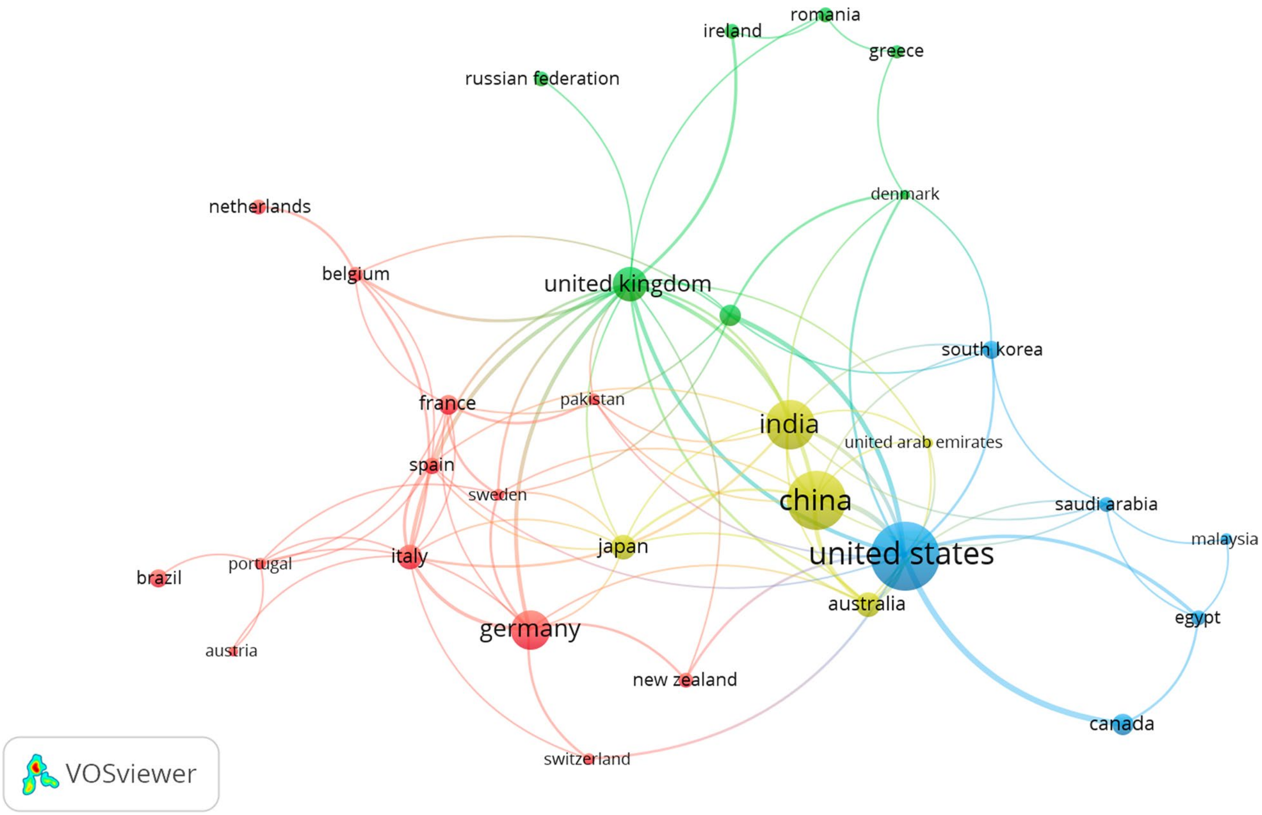

Fig. 8 Co-authorship network of Countries/areas with the threshold of minimum 5 publications

size of the nodes corresponds to the total link strength of the countries, while the edges depict collaborations between them. Nodes with high cohesion form clusters, and a total of 31 countries are represented in the network, categorized into four groups based on their color (red, green, blue, and yellow).

In general, the co-authorship relationships among countries exhibit spatial characteristics that are reflective of regional affiliations. The clusters' geographical positions show that the United States, the United Kingdom, Germany, and China have the strongest link strengths, as evidenced by the size of the corresponding nodes, which indicates their significant contributions to cooperative connections. The European cooperation network, centered on Germany, is the largest sub-network with nodes from 13 different countries. The second largest sub-network centers on the United States and involves countries from North America, Asia, Europe, and Africa, making it a cross-regional cooperation network. The third largest sub-network is centered on the United Kingdom and is also a European cooperation network, consisting of 6 nodes. On the other hand, the smallest cooperation network is located in Asia, centered on China, with only 5 nodes, and the other nodes in the cluster contribute less comparatively.

Knowledge structure analysis

We have divided our analysis into two sections. The first section focuses on the topic landscape and its evolution, providing useful insights into the hotspots of zero trust research. The second section delves deeper into the main research hotspots, offering a comprehensive understanding of the current research status and future opportunities for these topics.

The landscape of hot topics and evolution

The topic landscape maps are generated based on terms co-occurrence of document related to zero trust, which shows the most used keywords or the most favored research areas (please see Fig. 9). The topics are clustered based on their connections. We provide a different kind of detailed data in Tables 2 and 3.

At first sight, the results we placed in Fig. 9, Tables 2 and 3 indicate a strong relationship between zero trust and other technologies such as the IoT, cloud, and blockchain. This relationship is evident not only in the size of

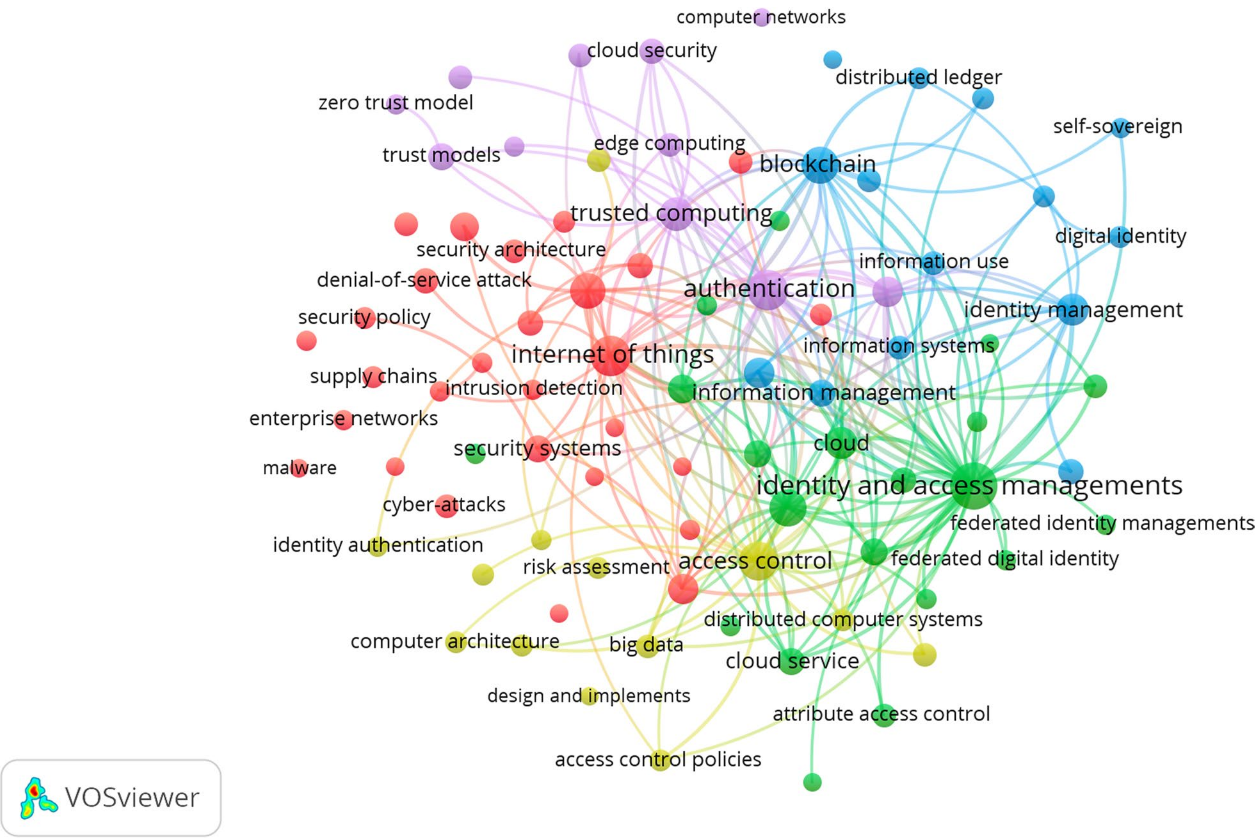

Fig. 9 Knowledge landscape and clusters based on terms with a threshold of 12 times

Table 2 Research topic clusters of zero trust based on topic keywords

Cluster #	No. of node	Research topic	Main keywords (frequency)
1	28	Zero trust in IoT	Internet of things (144), network architecture (88), sensitive data (55), zero trust architecture (44), security systems (39), 5g and beyond (32), machine learning (29), denial-of-service attack (28), security architecture (24), software defined networking (23), artificial intelligence (22), deep learning (21)
2	20	Zero trust in cloud computing	Cloud computing (108), cloud (70), cryptography (50), cloud service (39), web services (38), privacy (34), privacy and security (28), authentication and authorization (24), attribute access control (22), federated identity managements (17), role-based access control (17), service provider (14), service oriented architecture (13)
3	14	Blockchain enhanced zero trust security	Blockchain (100), identity management (71), data security (57), access management (28), digital storage (25), distributed ledger (21), decentralisation (18), electronic document identification systems (18), self-sovereign (14), public key cryptography (13)
4	13	Big data security	Big data (26), access control models (22), trust networks (22), risk assessment (21), computer architecture (19), distributed computer systems (19), dynamic access control (19), trust evaluation (19), access control policies (18), behavioral research (16), identity authentication (14), design and implements (12)
5	11	Zero trust in edge computing	Edge computing (22), trusted computing (82), authorization (59), zero trust model(15), continuous authentication(14), computer networks(13)

the keyword nodes, but also in the total link strength and average norm citations.

As shown in Table 3, in addition to the basic vocabulary related to IAM, including identity and access managment and authentication, the term that is most closely connected with zero trust is “internet of things” with a total link strength of 512, followed by “cloud computing” with a total link strength of 447. The average citation

Table 3 Strong connection keywords used in the zero trust (total link strength more than 290)

Rank	Keywords (frequency)	Total link strength	Avg. citations	Avg. pub. year	Cluster#
1	Identity and access managements (236)	819	11.89	2017	2
2	Authentication (136)	513	6.37	2019	5
3	Internet of things (144)	512	11.60	2021	1
4	Access control (124)	500	7.36	2019	4
5	Cloud computing (108)	447	20.31	2018	2
6	Blockchain (100)	377	17.38	2021	3
7	Network architecture (88)	354	5.38	2021	1
8	Trusted computing (82)	318	5.06	2021	5
9	Identity management (71)	303	4.94	2018	3
10	Cloud (70)	293	7.06	2019	2

frequency for these terms is 20.31 and 11.6, respectively, with "cloud computing" ranking first and "Internet of Things" ranking fourth. Furthermore, the average year of occurrence for keywords related to "internet of things" is 2021, indicating an increasing scholarly attention in recent years to this topic.

Nonetheless, we can also observe more granularity in the topics. The zero trust research landscape can be effectively summarized into five clusters: Cluster 1 (red) is characterized by central nodes such as"internet of things", "zero trust architecture", "5 G and beyond", and "machine learning"etc. These nodes highlight the intersection of zero trust and IoT, which appears to be the primary focus of the ongoing expansion of zero trust. Cluster 2 (green), frequent nodes such as "cloud computing", "cryptography", "privacy and security", and "authentication and authorization" etc. indicate a research focus on the application of zero trust in cloud computing. Cluster 3 (blue) highlights the integration of blockchain and zero trust, with "blockchain", "identity management", "data security", "distributed ledger", "self-sovereign", and "decentralisation" etc.being the most significant nodes. Significant nodes in Cluster 4 (yellow), such as "access control", "big data", "trust networks", "access control models", and "dynamic access control" etc., suggest a research emphasis on big data security. Finally, Cluster 5 (purple) concentrates on the application of zero trust in edge computing, with keywords like "edge computing", "trusted computing", "authorization", "trust models", and "software defined perimeter" etc. being the most frequent.

We generate a map showing how the topic of zero trust has evolved over the years by using the average publication year of keywords related to the topic (please see Fig. 10). Nodes on the map are color-coded based on their average publication year. Keywords with an average publication year after 2021 are considered emerging hot topics. The top 10 emerging hot topic keywords along with their corresponding link weights are shown in Table 4.

Based on the results presented in Fig. 10 and Table 4, we can see that research topics in Cluster 2, such as "privacy and security", "federated identity management", "identity and access management," and "role-based access control," have been present in zero trust research since around 2018. This suggests that zero trust research has evolved from exploring cutting-edge technologies to refining established practices. On the other hand, the remaining clusters have introduced new topics in recent years. For example, "deep learning," "zero trust architecture," "5 G and beyond," and "machine learning" in Cluster 1, "distributed ledger," "decentralization," and "self-sovereign" in Cluster 3, "trust evaluation," "trust networks," "behavioral research," and "dynamic access control" in Cluster 4, as well as "zero trust model," "edge computing," and "continuous authentication" in Cluster 5 represent emerging hot topics in the field of zero trust. The evolved clustering results provide a comprehensive view of zero trust research, showcasing both emerging trends and established practices. These findings highlight emerging hotspots and future trends in zero trust research, portraying the shift towards decentralized, behavior-based, and adaptive security approaches, as well as the exploration of advanced concepts such as edge computing and continuous authentication.

Analyzing key research hotspots and future trends for zero trust

Zero trust in IoT Resource-constrained IoT devices connected to the network are ubiquitous today, which motivates the integration of IoT and cloud services, but also expands the attack surface (Ameer et al. 2022; Refaey et al. 2019). The security of IoT devices, network architecture and resource is the primary issues to successfully implement zero trust in IoT in real practice. The concept

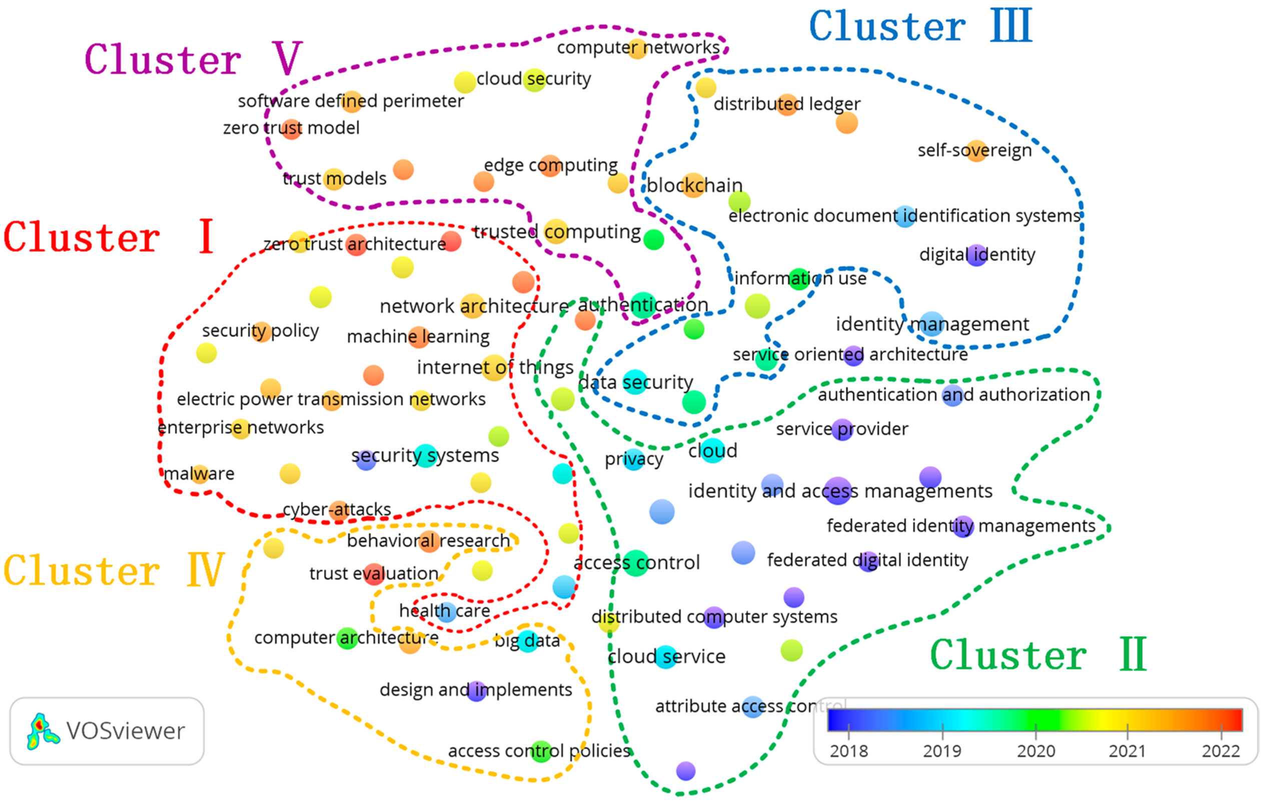

Fig. 10 Main clusters of keywords co-occurrence network with timeline

Table 4 Emerging hot topics based on avg. pub. year and links

Rank	Keywords (frequency)	Avg. pub. year	Links	Cluster #
1	Internet of things (144)	2021	82	1
2	Network architecture (88)	2021	78	1
3	Blockchain (100)	2021	77	3
4	Trusted computing (82)	2021	75	5
5	Zero trust architecture (44)	2021	54	1
6	5G and beyond (32)	2021	50	1
7	Trust models (34)	2021	46	5
8	Behavioral research (16)	2021	45	4
9	Dynamic access control (19)	2021	45	4
10	Edge computing (22)	2021	44	5

of zero trust in IoT means that all data traffic generated within the IoT ecosystem must be treated with skepticism and thoroughly evaluated, regardless of whether it originates from internal or external sources (Zolotukhin et al. 2022; Wang et al. 2023). To address the security challenges posed by the IoT, various dynamic (Wu et al. 2021), fine-grained (Abreu et al. 2020) and lightweight access (Wang et al. 2023; Ziegler et al. 2020; Ahmed et al. 2023) control models have been developed, using a combination of cryptography, machine learning, and SDP. These models are based on multi-source heterogeneous data, including attributes of users and devices, behavioral patterns, application integrity, and flow baselines. Micro-segmentation is another technology that can be utilized to secure the IoT network against internal attacks resulting from lateral movement(Osman et al. 2020).

In addition, there is an increasing integration of AI, machine learning, deep learning, and IoT, reflecting the urgent need to address the growing scale and complexity of IoT. These AI-based technologies have the capability to effectively enhance IoT security through real-time monitoring and dynamic security evaluation. As the number of IoT devices rapidly grows, traditional security measures are no longer sufficient to provide comprehensive protection for IoT. However, machine learning can detect abnormal behavior or malicious activities in network traffic, and deep learning can analyze vast amounts of data to discover threat patterns (Sedjelmaci et al. 2023). Automated policy configuration can enhance existing security intelligence engines by incorporating more complex rules and and minimizing time and effort (Hosney et al. 2022). A MSG model based on machine learning can mitigate lateral movement by attackers or malware (Arifeen et al. 2021), while an intelligent IAM model utilizes neural networks for training to maintain security and efficient file access (Duggal and Dave 2021). This application of AI empowers IoT's zero trust security architecture to effectively detect and respond to network threats, thereby enhancing security performance and mitigating vulnerabilities exploitation. Consequently, AI in IoT security represents a promising avenue for research, offering robust protection for zero trust security measures.

Zero trust in cloud computing Cloud computing has gained widespread popularity in recent years as organizations seek to optimize their IT infrastructure and cut costs. However, this shift also presents new security challenges as sensitive data and applications are transferred to remote servers, making trust management a concern due to threats such as identity theft, data breaches, data integrity and confidentiality (Mehraj and Banday 2020). The zero trust principle offers a promising solution to ensure cloud computing security, as it can be applied to help secure data and applications, even when they are stored and processed on remote servers. The focus of zero trust in cloud computing is to examine the zero trust principles and their implementation to the context of cloud computing (Ferretti et al. 2021; Zhao et al. 2022), with a specific emphasis on least privilege, dynamic access authorization control, encryption, and other related topics. For example, the work of (Mehraj and Banday 2020) addressed the issue of trust in cloud computing by examining the trust relationship between the user and the cloud service provider and establishing a zero trust strategy in the cloud computing environment. Dong et al. (2018) proposed a dynamic fine-grained cloud access control strategy based on Ciphertext Policy Attribute-Based Encryption, which includes identity-based user revocation. Yacob (2023) focused on achieving security in system design and providing users with the least privileged access to protect sensitive data in the cloud. Pero and Ekman Pero and Ekman (2023), on the other hand, emphasized the importance of adopting a zero trust strategy in the local cloud environment, which involves comprehensive user verification and authentication, distrusting any user, and assigning minimal access privileges to each user. Sanchez-Gomez et al. (2018) introduced the concept of Encrypted Cloud, which assumes a zero trust context and includes a comprehensive integrity verification protocol to ensure secure management of multiple cloud storage services. Rajasoundaran et al. (2021) proposed a machine learning-based approach to deep job exploration and secure transactions in virtual private cloud systems. By implementing a zero trust environment, the risks of cloud security vulnerabilities and data leakage can be minimized (Kang and Lee 2023).

Further more, as organizations exhibit a growing inclination to establish well-defined and effective multi-cloud strategies, the necessity for robust and secure architectures becomes increasingly pronounced. Consequently, researchers have dedicated their efforts to exploring the concept of zero trust architectures in multi-cloud environments. These architectures are designed to leverage service mesh technology (Martiradonna 2023) and implement granular application-level policies (Chandramouli and Butcher 2023). By doing so, they aim to meet the dynamic runtime requirements of zero trust architectures within the complexities of multi-cloud and hybrid environments.

Blockchain enhanced zero trust security Blockchain is a decentralized technology that incorporates cryptography into its core functions, making it tamper-proof and immune to manipulation or fraud on the data (Gao et al. 2018; Polychronaki et al. 2022; Partida et al. 2021). In the context of zero trust, blockchain can be seen as a perfect match. The decentralized nature of blockchain ensures the security and reliability of data through the use of cryptographic techniques and a decentralized manner of record-keeping. The data is stored across nodes throughout the network, eliminating the risk of a single point of failure. Even if any node is attacked, the data of the entire network is not affected, making the use of blockchain a more secure and efficient way of managing data without having to trust any single party. Thus, scholars are focused on using blockchain technology and low-energy distributed ledger technology to replace the trusted authorization of communication nodes (Meng et al. 2022) and establish decentralized identity management mechanisms (Wang et al. 2022; Li et al. 2022). These efforts aim to promote information sharing in a zero trust environment (Liu et al. 2022), achieve anonymous traceability, temporary identity verification and data privacy protection. As an example, the reference in Lin et al. (2021) proposed a system model of an optimized blockchain-based fair payment for outsourcing computations in a zero trust environment.

In addition, the application of blockchain technology provides a solution to the trust issue in cross-organizational and cross-domain data sharing. By utilizing blockchain technology, data integrity and trustworthiness can be ensured, and a distributed trust network can be established. Research on the security issues of digital identity management can further contribute to the development of a secure and efficient cross-organizational and cross-domain data management and identity verification system. For example, an approach proposed by Awan et al. (2023) utilizes a consortium blockchain to create a trustworthy environment. Within this environment, a role-based access control model is implemented using a multi-signature protocol and smart contract methods. Liu et al. (2023) proposed a novel multi-domain cloud-edge architecture based on sharded blockchain under the zero trust model. They have also designed a cross-domain data sharing scheme under partial trust models to achieve security, scalability, and high performance.

Big data security As a data asset, big data is huge in scale and grows exponentially with time. Every domain including health care, administration, education, retail has collected big data (Singh et al. 2022), which contains a lot of sensitive data, involving security and privacy issues (Sharma et al. 2021). Owing to their intricate nature, a majority of information systems frequently encounter vulnerabilities in data security, thereby increasing the likelihood of sensitive information leakage (Thapliyal and Gaur 2023). In order to alleviate this risk, the zero trust network provides improved access control and auditing mechanisms to safeguard big data (Han 2023). For example, the reference in Tao et al. (2018) proposed a unique strategy to enhance big data security, comprising three stages: user context recognition based on zero trust, fine-grained data access authentication control, and full network traffic-based data access auditing to identify and prevent potentially dangerous data access. Additionally, the references in Jasim et al. (2018) and Longstaff and Noble (2016) introduced a zero trust access control method using signature keys and attributes for big data security.

Additionally, big data does indeed raise security and privacy concerns, but at the same time, it provides opportunities to improve access control accuracy (Saleem et al. 2023). In a big data environment, more information and contextual factors can be combined to perform access control, ensuring that only authorized users can access specific data. For example, factors such as user behavior patterns (Nana and Yuanyuan 2022), network activities, and geographical locations can be considered to determine the legitimacy of accessing certain data. Moreover, big data is characterized by its vast volume, which contains a wealth of information and patterns. The available data and patterns from big data can be leveraged to improve the accuracy of access control policies (Muneer et al. 2023). By analyzing and mining big data, correlations between users and anomalies in behavior can be discovered, enabling more accurate determination of whether a user has permission to access certain resources (Cheng et al. 2023). For example, Zhao et al. (2022) successfully differentiated between legitimate and illegitimate access requests by developing a trust evaluation mechanism through mining user behavior-related data using a cloud-based big data fuzzy clustering algorithm.

Edge computing Edge computing shifts data processing and storage closer to data sources and end-user devices, addressing challenges such as increasing data volume, latency requirements, privacy concerns, and network limitations (Ali et al. 2023). It enables real-time processing, reduces data transfer costs, and enhances data privacy and security. However, it also introduces security challenges. One approach to enhance application security in mobile edge computing is implementing a zero trust strategy (Sharma et al. 2023). Various zero trust architectures and methods have been proposed, including MSG and intrusion detection for edge nodes. For example, Lei et al. (Lei et al. 2023) proposed a microservices-based edge segmentation solution with continuous authentication and dynamic access control mechanisms for physical system security. Another framework based on security rules and machine learning algorithms has been proposed for intrusion detection in 6 G edge computing, improving attack detection accuracy (Sedjelmaci et al. 2023). Sharma et al. (2023)introduced a probabilistic distributed collaborative intrusion detection system for detecting anomalies in service-to-service interactions across multiple edge clusters in a zero trust network setting.

Furthermore, researchers have recognized the problem of network cost overheads in edge computing, leading them to propose avenues for improvement. One approach is trust-aware task load balancing in multi-access edge computing based on blockchain and zero trust security capability framework (Ali et al. 2023). This framework does not assume any edge computing node to be trusted and uses Q-learning algorithms and blockchain technology to evaluate and record node trust values and trust relationships. Such a zero trust approach significantly improves the security of resource management and ensures that only reliable nodes participate in task processing, thereby reducing potential security risks. Furthermore, a technology called “Non-Intrusive Edge Observability Stack (Kumar et al. 2023)” has been introduced, which simplifies the process of collecting, analyzing, and visualizing telemetry data, whcih reduces the amount of code instrumentation needed to collect telemetry data up to 80% and offers extensive configuration capabilities within the subcomponents of the process.

IoT threat analysis and zero trust solutions

To effectively implement zero trust policies in IoT, it is important to have a thorough understanding of the latest attack methods and potential threats of IoT. This will allow us to adapt to the changing landscape of malicious attacks and take appropriate measures to protect against them. The IoT ecosystem is composed of three layers: the perception layer, network layer, and application layer. Each layer presents its own set of vulnerabilities and risks, which must be identified and addressed proactively.

In the subsequent sections, we will explore the key threats and zero trust solutions of IoT.

Perception layer

The perception layer plays a crucial role in the IoT ecosystem (Khattak et al. 2019). It is the foundation of the whole IoT architecture and provides key support for devices and sensors to interact with the physical environment (Wu 2022; Khattak et al. 2019). In the perception layer, sensors have the ability to detect objects and their surroundings, while devices are employed to manipulate and control the physical environment in order to carry out specific tasks. For example, in the Internet of Vehicles (IoV), sensors in the sensing layer can be used to collect the data of traffic, road conditions and weather, while devices can be used to control the operation of vehicle systems. In smart cities, sensors can detect changes in environmental conditions, such as air quality, and devices can adjust street lighting. In Internet of Health Things (IoHT), sensors can monitor patients' vital signs, and devices can manage drugs or provide treatment. The devices and sensors in the perception layer cooperate with each other to provide data support for the upper layer, which promotes the realization of various IoT application scenarios. However, the perception layer also poses a major security threat. To address these threats, zero trust solutions are available to protect both sensors and devices. Table 5 presents a comprehensive overview of the security threats that exist in the IoT perception layer and outlines the corresponding zero trust solutions to address them.

Sensor side

Unauthorized access to IoT devices can result from exploiting vulnerabilities at the sensor side. In the IoT, the collection of fingerprints (Marasco and Ross 2014) and voiceprints (Zhang et al. 2017) by sensors on devices are essential data sources for user authentication, and their security is closely related to the protection of users identity information. The forgery or theft of this data can lead to identity theft analysis or spoof attacks, where an attacker uses a fake or forged biometric sample to impersonate a genuine user and gain unauthorized access (Ratha et al. 2007). This scenario is particularly crucial in applications such as IoV, smart cities, and IoHT. For instance, in IoV, sensors onboard can collect

Table 5 Zero trust security solutions for IoT perception layer

Threat location	Vulnerabilities	Application scenarios	Types of attack	Zero trust solutions	Core technologies
SS	Biometric sample spoofing	IoT MD	Spoof attacks	Biometric finger vein identification (Darwish 2021)	IAM
SS	Easily subverted identity authentication	IoV	Impersonation attacks	Continuous facial recognition (Song et al. 2022)	IAM
SS	Easily subverted identity authentication	IoT device	Spoof attacks	Continuous and multifactor authentication (Alappat 2023)	IAM
SS	Biometric sample spoofing, Sensitive information leakage	IoHT	Spoof attacks, data leakage attacks	Multimodal biometric authentication (Cheng et al. 2023)	IAM
DS	Device intrusion and long-term infections caused by device vulnerabilities	IoT SD	Password cracking attacks	Dynamic intrusion detection model (Zolotukhin et al. 2022)	IAM
DS	Malicious users damaging devices and normal users misusing terminals	PIoT	Privilege attacks	Developing fine-grained and dynamic access control policies for IoT devices (Wu et al. 2021)	IAM
Ds	Exploiting device vulnerabilities in a LAN network	IoT LAN	APT attacks	Segmenting IoT devices into separate network segments (Da Rocha et al. 2021)	MSG
DS	Lateral movement threat	IIoT	APT attacks	Automated MSG model based on machine learning algorithms (Arifeen et al. 2021)	MSG
DS	Bluetooth protocol vulnerabilities and unsecure deployment policies vulnerabilities	IoHT	MITM, eavesdropping attacks, DoS	Divide network into micro-networks by criticality of devices and shared data, and use behavioral analysis for continuous authentication of devices (Satam et al. 2020)	IAM & MSG

SS, Sensor Side; DS, Device Side; IoT MD, IoT Mobile Devices; IoT SD, IoT Smart Devices the driver's fingerprints and voiceprints, which are used for user authentication and vehicle ignition. In scenarios like smart cities and IoHT, sensors contribute to securing access to city infrastructure or medical devices by collecting users' biometric data like fingerprints and voiceprints. However, if attackers manage to exploit vulnerabilities in sensors or forge biometric data, they could impersonate legitimate users and obtain unauthorized access. This poses security threats to vehicles, city infrastructure, and healthcare devices.

To enhance access control security at the sensor side, the zero trust approach emphasizes enhancing the recognition of individual features, continuous identity authentication, and continuous multifactor authentication. This enables the collected biometric data such as fingerprints and voiceprints by the sensor to stay within the edge devices, thus reducing the risk of data interception by attackers during network transmission. One example is an efficient personal identification model based on finger vein proposed by Darwish (2021). By incorporating local and global characteristics, this method improves vein images and then applies Gabor transformation to fuse them and obtain the vein pattern. Nevertheless, the extended identification time during testing restricts its applicability to big data samples. Due to its relatively low computational complexity in an online phase, this model is suitable for mobile device deployment. Another method proposed by Song et al. for periodic (continuous) identity establishment involves using NFC and fingerprint at entry points followed by facial recognition (Song et al. 2022). Driver images are captured periodically and transformed into an embedding vector, which is then compared against the enrolled image of the corresponding authorized driver by computing the Euclidean distance. However, in low-light conditions or when facial features change, this can result in legitimate drivers being denied entry or being falsely labeled as potential threats. Furthermore, scholars (Alappat 2023) have proposed a multi-factor authentication solution under the zero trust framework. This approach involves continuously verifying multiple factors of identity information (including biometrics, one-time passwords, smart cards, and mobile authenticators) to enhance the security of IoT device access. To enhance automation and accuracy, researchers have investigated a CNN-based federated learning approach for multi-factor authentication (Cheng et al. 2023). This innovative method utilizes photoplethysmography and electrocardiogram signals to discern users' biological characteristics, thereby improving identification precision. By integrating multiple modalities, it not only strengthens the authentication system but also safeguards user privacy and data security. Furthermore, this approach is highly applicable in the context of the IoHT, addressing the unique challenges and requirements of secure access to health devices and sensitive information.

Device side

IoT devices hold immense significance, particularly in scenarios like edge computing, IoV, smart cities, smart grids, and IoHT. To ensure the security of IoT systems, it is imperative that devices possess the capability to process massive volumes of data streams promptly and accurately, all the while safeguarding the confidentiality of sensitive information. On the IoT device side, intelligence threats can be categorized into three types: hardware vulnerabilities (Gnad et al. 2019; Kumar et al. 2017), firmware vulnerabilities (Ronen et al. 2017), and software vulnerabilities (Kumar et al. 2019). Bad actors can exploit unauthorized access resulting from unpatched vulnerabilities, outdated or malicious firmware, weak passwords, outdated communication interfaces, and a lack of authentication in update mechanisms to breach devices (Wu et al. 2021; Kumar et al. 2019). Additionally, smart devices often lack effective malware signature detection and intrusion detection, while firmware vulnerabilities may result in some devices remaining vulnerable for long periods, as not all devices support wireless secure updates or updates without downtime, requiring physical access or temporary halt of production (Zolotukhin et al. 2022). Malicious attackers may exploit these vulnerabilities to infiltrate vehicles, power equipment, and medical devices, among others. All these factors can lead to sensitive information theft or the launch of worm or Advanced Persistent Threat (APT) attacks. A core solution to combat this issue under the zero trust model is to implement IAM, and MSG strategies.

Device-side IAM strategies mainly aim to enforce the principle of least privilege for device access and implement intrusion detection based on traffic analysis. For instance, to ensure the normal operation of Power Internet of Things (PIoT) devices, researchers have adopted the concept of zero trust and studied security protection strategies for devices from four perspectives: user authentication, equipment trust, application integrity, and flow baselines (Wu et al. 2021). The aim is to establish minimum device access, preventing both malicious users from causing harm to the device and regular users from misusing the endpoints. However, implementing this approach presents challenges due to the need for constructing profiles and performing integrity validation for each PIoT device, which requires significant resources and time. Additionally, Zolotukhin et al. (2022) proposed a dynamic attack detection model for smart device that utilizes traffic analysis to adjust detection algorithms in response to changes in the network environment, such as the discovery of new applications or vulnerabilities. This facilitates optimizing security policies and responding promptly to crises, thereby reducing future attack risks and minimizing the attack surface.

Fine-grained access control logic based on MSG provides an efficient approach for preventing lateral propagation of malicious software by generating network traffic differentials and blocking malicious traffic. The MSG technique described in reference (Da Rocha et al. 2021) applies MSG and Next-Generation Firewall technology to segregate IoT LAN devices into distinct network segments. This effectively blocks lateral propagation of infected IoT LAN devices and foils advanced persistent threat attacks. The drawbacks of this approach are high operational complexity, lack of automation, significant human involvement required, complex communication mapping for each specific software on the 7th layer of the OSI model, potential communication inaccessibility in case of poor MSG implementation, and risks to reliability and stability. In response to these challenges, an automated MSG model that uses machine learning algorithms to automatically generate micro-segments and separates normal traffic while limiting redundant links and blocking malicious traffic was explored by Arifeen et al. (2021). It is particularly suitable for large and dynamic networks, such as the Industrial Internet of Things (IIoT).

The reference in Satam et al. (2020) proposed another approach, which is the combined mode of MSG and IAM used to address large Bluetooth networks. This method involves dividing the Bluetooth network into different levels of micro-networks based on the criticality of the connected devices and the importance of shared data. This segmentation can limit the exposure of critical devices and data to potential attacks. Additionally, a primary whitelist server and behavioral analysis can be used for continuous authentication and authorization of unidentified devices attempting to join the Bluetooth network. This approach can enhance the security of the Bluetooth network by detecting and blocking unauthorized or malicious access attempts in real-time. An effective scenario for applying this method is the IoHT, where devices communicate with each other through Bluetooth and share sensitive and critical information. This methodology can efficiently safeguard the Bluetooth network from attacks such as MITM, eavesdropping, and Dos.

Network layer

The network layer of the IoT is a crucial component responsible for connecting and facilitating communication between various IoT devices, sensors, and gateways (Shilpa et al. 2022). In a communication network, various communication methods and network topologies exist, including direct and indirect communication (Lin et al. 2009). The source and destination can connect either directly or indirectly, depending on the type of communication utilized. For different communication modes, solutions for zero trust are different. The details of the threats and zero trust security solutions for the IoT network layer are shown in Table 6.

Direct communication

Direct communication within IoT is crucial for various scenarios such as edge computing, IoV, smart cities, smart grids, and IoHT. These scenarios involve extensive direct communication among devices and systems. For instance, IoT technology enables vehicles to directly communicate with other vehicles and road infrastructure, enabling intelligent driving and traffic management. It also facilitates instant and direct communication and data exchange between smart meters and smart grid devices. In addition, IoT technology enables more efficient and direct interconnection of medical devices and sensors. Direct communication within IoT can allow for the direct transmission of secret messages from sender to receiver without network relay or cloud transmission (Sheng et al. 2022). However, IoT devices have limited resources, which makes it challenging to implement traditional communication and security protocols. This limitation exposes direct communication to various security threats. One such threat is the vulnerability of key exchange mechanisms in direct communication protocols. Attackers can exploit these vulnerabilities to intercept transmitted keys and gain unauthorized access to sensitive user data (Wen et al. 2020). A novel side-channel attack variant that aims to extract the global AES-CCM key used by Philips to encrypt and authenticate new firmware is one example of such a vulnerability (Ronen et al. 2017). Another type of threat involves vulnerability attacks targeting the TCP/IP communication mode, which poses significant risks because TCP/IP-focused security frameworks frequently allow devices to connect and communicate before authentication, leading to ineffective security foundations (Puthal et al. 2022), i.e.intruders get huge space to be part of the communication system before authentication happens (Puthal et al. 2020). Furthermore, the security issues associated with outsourced chip production pose a significant threat to the semiconductor supply chain. This vulnerability exposes direct communication between chips to various security attacks, including hardware Trojan injection, intellectual property theft, and overproduction. To address these concerns, a widely used security technology called Gls puf offers a relevant solution by providing a digital fingerprint for hardware security (Liao et al. 2022). However, authenticating a physically unclonable function (PUF) chip heavily relies on trusting the

Table 6 Zero trust security solutions for IoT network layer

Threat location	Vulnerabilities	Application scenarios	Types of attack	Zero trust solutions	Core technologies
DC	Insecure key exchange of direct communicate of E2E	SG	–	Generating dynamically changing session keys based on Time-based One Time Password (Abreu et al. 2020)	IAM
DC	Insecure key exchange of direct communicate of D2D	IIoT & SG	Replay attacks, MITM, cloning attacks, sybil attacks	Generating dynamically changing session keys based on tunable mathematical function (Shah et al. 2020, 2021)	IAM
DC	TCP/IP communication mode vulnerability	RIoT	Confidentiality attacks, integrity attacks, replay attacks, DDoS, Identity spoofing attacks	Perform identity authentication and establish a secure channel using an SDP controller (Puthal et al. 2022) or an enhanced SDP controller (Puthal et al. 2020)	SDP
DC	Vulnerabilities in identity authentication and session management	RIoT	Replay attacks	Chosing a lightweight approach to implementing the complex SPDM protocol and establishing chip-to-chip communications based on the principles of zero trust (Xiong et al. 2019)	IAM
IC	Vulnerabilities in identity authentication and session management	RIoT	Integrity attacks, network sniping, MITM, DoS	Authenticate and authorize requests using the SDP-SDN controller (Karimi et al. 2021); OTP-based software-defined cloud architecture for secure dynamic routing (Kim et al. 2022)	SDP
IC	Vulnerabilities MQTT	RIoT	DoS	SDP improvements for MQTT (Refaey et al. 2019)	SDP
IC	Vulnerabilities in identity authentication and session management	IoT ehealth	Forgery attacks	Token-based federated IAM mechanism for HTTP and COAP protocols (Beltrán 2018)	IAM
IC	Vulnerabilities in identity authentication and session management	IIoT	Forgery attacks	Pairing-free and provably secure certificateless parallel key-insulated signature scheme (Xiong et al. 2019)	IAM

DC, Direct Communication; IC, Indirect Communication; SG, Smart Grids; RIoT, Regular IoT System; DDoS, Distributed Denial-of-Service challenge-response table, which contradicts the principles of zero trust (Ahmed et al. 2023). Consequently, this reliance introduces potential attack vectors and security threats to secure communication between chips (Ahmed et al. 2023). To mitigate these threats, the zero trust architecture leverages technologies like IAM and SDP to secure direct communication channels, including device-to-device (D2D) and end-to-end (E2E) communications. This will facilitate the development of IoT technology and bring more convenience and security to various IoT scenarios.

To address the vulnerability of direct communication key exchange, one possible method for securing communication is continuous identity authentication. In a zero trust environment, endpoints do not have implicit trust, and continuous identity authentication is suggested as a potential solution. To protect D2D and E2E communication in scenarios where security is critical and resources are limited, researchers have put forth several secure communication protocols with high deployment potential. For example, the references in Shah et al. (2020, 2021) proposed an novel and lightweight continuous D2D authentication protocol. This protocol generates dynamically changing session keys to ensure uninterrupted device authentication, making it highly applicable in critical infrastructure scenarios such as smart grids and IIoT. Abreu et al. (2020) suggested the use of time-based one-time passwords to generate dynamically changing session keys for E2E secure communication in smart grids. They also implemented multicast communication for efficient messaging without compromising security. Bhattacharjya and Saiedian (2022) proposed a technique that enables the establishment of secret keys for resource-limited device-user pairs with minimal interaction. This approach utilizes elliptic curve cryptography and periodic key refreshing to mitigate side-channel attacks, thereby expanding the application of IoT to sectors like healthcare, industry, and other large-scale deployments.

The vulnerability of the TCP/IP communication mode has become a major concern in today's digital landscape. To address this issue and ensure enhanced security for sensitive data, a zero trust approach that leverages SDP for boundary-based security can be employed. By implementing this approach, as described in references (Puthal et al. 2022, 2020), E2E communication channels can be protected from unauthorized access by performing device authentication and verifying the authenticity of each device based on an SDP controller. In addition to authenticating devices, to further enhance secure communication, symmetric and asymmetric key mechanisms (Puthal et al. 2022) or mTLS connections (Singh et al. 2020) can be implemented with the SDP controller, providing an additional layer of protection against potential security breaches and unauthorized access to sensitive data.

Moreover, in response to the security threats posed by the reliance on the trust of a challenge-response table for chip authentication using PUF, Ahmed et al. (2023) presented a chip-to-chip zero trust architecture. This architecture prioritizes physical-level security for hardware systems by implementing an authentication and attestation procedure. Communication between two chips is permitted only if they successfully pass this procedure. The inclusion of physical-layer chip authentication plays a crucial role in safeguarding the system against potential risks, such as unauthorized information exchange with counterfeit chips.

Indirect communication

Indirect communication refers to a communication mode in which data transmission between two endpoints is facilitated by an intermediate layer or entity. This intermediate layer could be a gateway device, a router, a proxy server, or any other similar entity. Indirect communication is particularly vulnerable due to the unreliability of identity authentication and session management. In protocols like MQTT, CoAP, and AMQP, security vulnerabilities in the identity authentication and session management mechanisms can result in client identity theft, unauthorized message responses, and malicious topic subscription, as stated in Wang et al. (2021) and Jia et al. (2020). In particular in the fields of PIoT, IoHT, and IoV involve substantial amounts of sensitive data, making them susceptible to potential privacy harm from indirect communication attacks. To address the potential risk of exploitation in indirect communication, advanced control measures and flexible identity authentication processes may be necessary in certain contexts, according to Beltrán (2018). Strategies like SDP and IAM can prove useful in enhancing data access control and improving identity authentication in complex networked environments, thereby reducing the chances of security breaches associated with indirect communication.

SDP is an advanced technology that enhances the security of indirect communications by either designing new protocols or improving existing ones (Tanimoto et al. 2021). For example, Karimi et al. (2021) put forward a groundbreaking indirect communication protocol designed specifically for IoHT. This protocol incorporates gateway communication with an SDP-SDN controller, which handles authentication and processing of owner requests while facilitating data transmission to the relevant cloud servers. By leveraging this protocol, the unique aspects of IoHT can be emphasized, ensuring secure and efficient communication within the network.

Kim et al. (2022) proposed cloud architecture provides a secure data path through dynamic routing using one-time internet protocol algorithm between each layer, and use software-defined technology to provide efficient network management and data security. This approach is particularly suitable for scenarios involving large data flow, such as IIoT systems and smart cities. In addition, the use of SDP technology can also lead to improvements in the indirect communication protocol. For instance, SDP can enhance security measures for IoT indirect communication by offering an extra level of protection for MQTT, with or without SSL/TLS. This is achieved by replacing the traditional login process that uses a username and password with a SPA process, which can help prevent end devices from being compromised by attackers (Refaey et al. 2019).

Another effective approach to enhance the security of indirect communication is through the implementation of IAM-based strategies. With a dependable and secure framework for managing user identities, access controls, and authentication mechanisms, IAM can effectively prevent unauthorized access to the cloud and improve security. In one example, the reference in Beltrán (2018) proposed a IAM mechanism, allowing federated and token-based identification, authentication and authorization of IoT agents (mainly smart objects and network devices but also end users via smart objects) to cloud services and applications running on traditional data centers (deployed locally or in the cloud) or on fog computing nodes, i.e. IoT-cloud services. This new mechanism is federated and token-based, capable of working over HTTP and COAP with adaptive security. This mechanism has been validated and evaluated in real healthcare use cases, effectively safeguarding secure communication between medical devices and cloud servers, protecting the privacy and integrity of patient data. Xiong et al. (2019) proposed an efficient certificateless parallel key-insulated signature authentication scheme without pairing, ensuring strong key insulation security and existential unforgeability under the random oracle model for secure communication between IIoT cloud servers and devices.

Application layer

The application layer is a critical component of the IoT system, responsible for processing and analyzing data to enable real-time control, accurate management, and scientific decision-making (Gerodimos et al. 2023). It can implement application programs and user interfaces, providing data services, and access control to higher-level applications. Within the application layer, the data aspect primarily deals with data collection, storage, processing, and transmission. Meanwhile, access control logic is in charge of regulating user access and operations on higher-level applications. The main carrier of the application layer is the IoT app of the IoT manager or user, as well as various IoT cloud platforms. Exploiting application layer program vulnerabilities or access logic defects can cause security issues such as unauthorized access, device spoofing, data leakage, and remote control. Faced with application layer security threats, zero trust proposes solutions from both the data side and access control side. The details of the threats and zero trust security solutions for the IoT application layer are shown in Table 7.

Data security

In IoT systems, a significant portion of data is generated from real-time sensing across various application scenarios, especially in areas such as IoV, PIoT, and IoHT, which involve sensitive data from critical industries. Ensuring the security of IoT data is crucial for the sustainable development of IoT. The major threats to data security stem from issues with device state machine models or access control logic that can lead to unauthorized access. Such unauthorized access may result in illegal activities, including illegal theft (Bevish Jinila et al. 2022), destruction (Davoli et al. 2018), or manipulation of data resources (Sanchez-Gomez et al. 2018; Gerodimos et al. 2023). In order to mitigate potential risks and threats in the realm of data security, the zero trust approach prioritizes the discovery, classification, protection, and monitoring of sensitive information to prevent potential risks and threats in data security. To achieve this goal, data is categorized based on various security factors such as importance, sensitivity, and business-related elements. This enables the identification of sensitive data, with appropriate access permissions allocated to individual users, devices, and applications that require access to the data. For instance, (Liao et al. 2021) employed a zero trust approach to categorize business data in PIoT from different perspectives, including users, devices, data, and applications, for precise protection and access control. Similarly, Bevish Jinila et al. (2022) introduced a zero trust model to ensure secure handling of IoMT data by identifying sensitive information, limiting access, detecting threats, utilizing baselines, and applying analytics to isolate active internal and external attacks.

Access control

The application layer in IoT systems comprises both the cloud platform and user mobile applications, facilitating various interactions, including cloud-to-user, cloud-to-device, and cross-cloud instances. Access control is critical for secure interactions across all these scenarios. However, vulnerabilities of device authentication and

Table 7 Zero trust security solutions for IoT application layer

Threat location	Vulnerabilities	Application scenarios	Types of attack	Zero trust solutions	Core technologies
DS	Data access policy flaws	PIoT	–	Classifying data risk levels based on importance, and establishing fine-grained access policies for sensitive data (Liao et al. 2021)	MSG
DS	Data access policy flaws	IoMT	–	Identify sensitive data and restrict access to it (Bevish Jinila et al. 2022)	IAM
AC	Access control policy flaws in IoT platform	RIoT	–	Blockchain-enabled user authentication in zero trust IoT (Zhao et al. 2020); Decentralized identity and access management (Fan et al. 2020)	IAM
AC	Access control policy flaws in IoT platform	PIoT	–	Continuous authentication based on device state changes (Xiaojian et al. 2021)	IAM
AC	Access control policy flaws in IoT platform	TM	Flooding attacks	Continuously verify user equipment credentials (Ali et al. 2021)	IAM
AC	Access control policy flaws in IoT platform	SH	–	Trust aware continuous authorization for zero trust in consumer IoT (Dimitrakos et al. 2020)	IAM
AC	Access control policy flaws in IoT platform	SG	–	Dynamic fine-grained access control strategy based on trust evaluation mechanism (Tao et al. 2023)	IAM
AC	Malicious node injection in IoT platform	BSA	Botnet-based attacks	Suspicious node identification based on behavior analysis of the internal graph of the platform (Davoli et al. 2018)	IAM
AC	Weaknesses in application programs and IoT platform access policies	IoV	Switch attacks, novice attacks, replay attacks, internal attacks, integrity attacks	Developing fine-grained access control based on behavior and trust levels using deep learning (Fang et al. 2022)	IAM & SDP

DS, Data Security; AC, Access Control; IoMT, Internet of Medical Things; TM, Telemedicine; BSA, Big Stream Applications

authorization control policy in IoT platform can pose a significant threat to IoT applications. As outlined by Chen et al. (2019), a weakness in IoT device authentication makes it possible for attackers to create bogus devices using publicly available data like device IDs, MAC addresses, and models, thereby gaining illicit access to sensitive user information. Attackers may also secretly seize control of devices, leading to repeated service or connection interruptions. Furthermore, the massive number of devices and users accessing networks in IoT environments increases network exposure (Xiaojian et al. 2021). Similarly, weaknesses in the authorization control policies of IoT platforms can provide opportunities for malicious device manipulation, as demonstrated by the identification of security vulnerabilities in SmartThings subsystems. Design issues in access control may further allow applications to assume complete control over IoT devices, even if initial access was restrictive (Fernandes et al. 2016). To mitigate these security threats, zero trust-based solutions heavily rely on IAM techniques. The aim is to improve access control logic by enhancing device authentication and implementing trust-level-based access control mechanisms.

Enhanced device authentication Utilizing device enhanced methods is an effective way to improve IoT device access authentication security and address vulnerabilities like device impersonation attacks, particularly in emerging edge computing situations(Li et al. 2022). Deploying device authentication mechanisms at edge nodes can protect device authentication and secure the edge node, effectively reducing the risk of device impersonation attacks and other associated vulnerabilities. These device enhanced methods have a wide range of applications in various areas like smart grids (Wang et al. 2023), smart cities, and IoHT, where they can prevent device impersonation attacks on power equipment, transportation equipment, surveillance equipment, and medical equipment. Zero trust can improve device authentication in multiple ways, including the use of device identifiers, device fingerprints, as well as device states and equipment credentials as authentication mechanisms.

Guaranteeing the security of IoT heavily depends on the deployment of device authentication based on device identifiers. An instance of this method is integrating device authentication with the IoT device's IAM system, which is an effective approach for enhancing the current OAuth 2.0 authorization framework (Julku et al. 2021). This delegation-oriented architecture is reliable in managing trust in a distributed environment with many sensitive network resources and provides a scalable method. Another more powerful approach is the blockchain-based enhanced device authentication technology. This technique uses device attributes (such as, name, account number, imei number, address, serial number, or a combination of these) (Zhao et al. 2020), decentralized identifier and verifiable credentials (Fan et al. 2020) as identifiers. These identifiers are then stored on the blockchain, leveraging the technology's immutability and decentralization to provide secure identity verification. By implementing this approach, device owners can establish universal device identity representations on the blockchain and share their device data with other entities in the ecosystem. This helps overcome IoT application silos and unlocks the full potential of IoT on a global scale, paving the way for greater innovation and collaboration in the IoT space (Fan et al. 2020). Additionally, this method overcomes the centralized single point of failure of the IAM system (Polychronaki et al. 2022), making it more secure and reliable.

Another method of enhancing device authentication is based on device fingerprint extraction and the identification public key algorithm (Wang et al. 2023). This technique involves generating a device fingerprint by extracting relevant information, including the unique serial number of the device/module, general parameters, product detection serial number, and the running state of the embedded module. This approach achieves a lightweight and secure device security authentication method tailored for access scenarios in power terminals.

The third method of device authentication is to continuously verify the identities of devices and users based on the changes of device state and user equipment credentials. For example, the reference (Xiaojian et al. 2021) utilized a device list service to constantly gather, process, and publish status changes of registered devices. It then monitors and analyzes this data to ensure continuous authentication of devices and users. By combining this approach with dynamic policy controls, vulnerability scanning systems, and certificate issuance, a robust authentication framework can be created, guaranteeing the security of both devices and applications. Ali et al. (2021) employed zero trust techniques to continuously verify user equipment credentials and utilized the PRESENT encryption algorithm to protect these credentials, ensuring uninterrupted service continuity.

Access control logic based on trust level Access control logic based on trust level is a security mechanism that utilizes behavior information to assess trust levels and applies dynamic, fine-grained access control to cloud resources based on these trust level labels. This mechanism is widely used in various domains such as the IoV (Fang et al. 2022), smart cities, smart grids (Wang et al. 2023), and IoHT (Nana and Yuanyuan 2022). By leveraging behavior information of specific access subjects and evaluating trust levels, access control policies based on trust can establish secure mutual trust relationships. This approach enables continuous evaluation of device trustworthiness beyond traditional boundary security, ensuring that only authorized users and devices can access specific cloud resources, with access limited to authorized areas. For example Feng et al. (2022), Tao et al. (2023) and Huang et al. (2023) proposed utilizing power terminal behavior, device access delay, and other information to calculate the trustworthiness of access subjects using the beta distribution function, enabling fine-grained access control in the context of the PIoT. Dimitrakos et al. (2020) and Wang et al. (2023) proposed utilizing the attributes and behavior of access subjects, applying Bayes' rule and the TMBRE Model to calculate the trustworthiness of access subjects, and combining attribute-based access control policies to achieve fine-grained access control in the context of smart homes and intelligent healthcare systems. Furthermore, integration of self-earning techniques like CNN (Fang et al. 2022) and case-based reasoning (Jiang et al. 2022) algorithms allows the system to adapt to emerging threats and improve security overall. During the process, scholars also use the SPA packet transmission acceptance rate of SDP architecture as one of the factors for machine learning training to improve the accuracy of access subject trust evaluation (Fang et al. 2022).

Moreover, researchers have explored federated access policies, which aim to provide a more flexible and scalable approach to managing access control in distributed network environments, and to promote secure collaborations among various organizations and domains. In their study, Davoli et al. (2018) outlined a security approach for the Big Stream platform that involves controlling provider-node interactions, analyzing the internal graph for suspicious behavior by processing nodes, and promptly reacting to any malicious activities in order to protect other active nodes' operations. This solution is particularly advantageous in cloud environments that feature intricate network topologies and a diverse range of devices and applications.

Challenges and opportunities for implementing zero trust in IoT

The challenges and difficulties encountered in the current application of zero trust in IoT are outlined.

Challenges

Developing dynamic and granular zero trust security policies for millions of distributed devices in 5 G and beyond of IoT is a complex task

As 5 G and beyond continue to develop, the number of devices connected to IoT systems is increasing exponentially and may reach millions, distributed across different geographic locations. Different applications and services require different security policies, making the development of zero trust security policies highly complex. Security policies must consider the authentication and authorization of each device and protect their data and communication throughout the entire system. Additionally, the IoT landscape in the 5 G and beyond era involves multiple access edge networks and network slicing, which require specific security policies for each edge network and network slice that must be integrated into the entire IoT system. Moreover, the implementation of hybrid security policies also presents difficulties for network service providers.

Implementing MSG security policies for IoT presents major operational complexity

Implementing MSG security policies in large-scale and dynamic IoT networks, such as smart cities and IIoT, poses significant challenges in terms of operational complexity. The core concept of MSG is to divide the network into smaller areas, each containing a group of devices and users, and implementing targeted security policies to minimize the potential for attacks and decrease network vulnerabilities. The implementation of MSG for large and complex IoT networks requires a comprehensive analysis of device and user access requirements, as well as the establishment of precise security policies for each area, which requires a considerable amount of configuration work to ensure network security and performance. Moreover, continuous updates and management are essential for MSG implementation to adapt to the dynamic access requirements of devices and users, resulting in increased difficulty and complexity.

Reducing latency and minimizing resource costs in the zero trust IoT is a challenging task

The latency challenge of zero trust applications in the IoT mainly stems from the need for continuous monitoring and analysis of a large number of device and user activities. To ensure network security, the zero trust model requires authentication and authorization for every device and user and continuous monitoring and analysis of their activities. Implementing hybrid security policies in IoT devices requires the devices to locally execute security measures while transmitting data to a central cloud for tracking and in-depth analysis. However, this process may cause latency issues. Low latency is crucial in key areas such as IoV, smart cities, and IoHT to enhance the efficiency and reliability of IoT data transmission, ensuring real-time connectivity and fast decision-making. Real-time monitoring and analysis in a zero trust model may pose a substantial burden on computing resources and bandwidth, given the limitations of IoT device resources. This, in turn, can degrade network performance. Therefore, minimizing resource costs and reducing latency in the context of zero trust IoT is a challenging task.

Opportunities

To achieve more secure and efficient zero trust security policies in the IoT, this section proposes three future research directions.

Implementing intelligent zero trust policies

Leveraging automation tools and AI technology can be a promising solution to alleviate the challenges of executing dynamic, granular, and MSG zero trust security policies for millions of distributed devices in 5 G and beyond. By utilizing these technologies, security policies can be generated and deployed automatically, reducing human errors and ensuring policy consistency. Regular policy updates are also possible, adapting to the constantly changing network environment. Moreover, AI-driven automatic MSG technology demonstrates its effectiveness in optimizing MSG schemes for large-scale IoT networks like smart cities and IIoT. It intelligently identifies and isolates potential security risks, ensuring network stability and reliability. This technology effectively handles a vast number of devices, diverse security threats, and complex attack methods, providing robust MSG solutions. By automating the process, it reduces deployment and maintenance costs while enhancing system flexibility and security.

Exploring zero trust security in the context of digital twin technology for the IoT

With the continuous advancement and widespread adoption of IoT technology, the need for network communication and interaction among numerous distributed devices is increasing. This poses several challenges in implementing zero trust strategies in IoT. However, digital twin technology emerges as a promising solution to address these challenges and concerns. Digital twin can create an accurate model of a real-world physical system and synchronize it in real-time with the actual system, allowing for real-time monitoring and detection, automated decision-making and response, and targeted defense measures, ultimately achieving zero trust security through hyper-automation. Digital twin technology can also use automated tools to automatically deploy MSG strategies based on network topology, device and user attributes, and access requirements, significantly reducing the workload and complexity of network administrators while improving network security and performance. Furthermore, digital twin technology can perform identity authentication and authorization operations in a virtual environment, avoiding direct communication with physical devices and minimizing network communication and data transmission latency and security risks. Thus, in-depth research on zero trust security in IoT under digital twin technology is one of the most crucial research areas for the future.

Investigating distributed zero trust security strategies for edge computing in the IoT

Edge computing pushes computation and data processing to the edge of IoT devices, enabling real-time processing at the data source. Compared to sending all IoT data to the cloud for processing, edge computing reduces transmission and response latency, thereby improving system performance. This is essential for implementing zero trust strategies in IoT, which require real-time and low-latency applications. Furthermore, by transmitting only critical information to the cloud, edge computing preserves and protects the original data on edge devices, minimizing the risk of data leakage. In this context, research on distributed zero trust security strategies for edge computing helps to enhance system security. This involves utilizing advanced technologies such as distributed machine learning to improve anomaly detection and response capabilities. For instance, a zero trust security strategy based on federated learning allows IoT devices to participate in model training and security decision-making while maintaining user privacy. Each device trains its model locally, adjusts model parameters based on local data, and then transmits encrypted model updates to the central server, mitigating the risk of exposing raw data.

Conclusion

The widespread use of IoT, cloud computing, edge computing, and bring your own device has made the network boundary blurred and traditional perimeter security models cannot meet the current network security needs. Therefore, the zero trust model, as a new security solution, has gradually been widely accepted and plays an increasingly important role in the field of network security. This study utilizes bibliometric methods to analyze the current state of research on zero trust and conducts a comprehensive analysis of its practical applications in IoT. The first part of the study involves identifying the developmental stages of academic research on zero trust, analyzing leading countries and their collaboration relationships, and identifying current and emerging research hotspots. The second part of the study focuses on investigating security threats present in IoT landscape and outlining zero trust solutions that can be employed to counter security vulnerabilities and attack techniques in different layers of the IoT ecosystem. The study also delves into the difficulties of applying zero trust measures in IoT environments and explores possible avenues for resolving these challenges.

The analysis of the general trajectories of research related to zero trust reveals a consistent and sustained interest from the academic community, and is experiencing a phase of rapid growth. Additionally, a fitting analysis of the cumulative publications suggests that the trend of increasing research on this topic will continue into the foreseeable future.

The examination of countries/areas-level productivity and collaboration in zero trust research indicates that the number of publications is unevenly distributed across different countries/areas, with the United States taking the lead, followed by China and India. The co-authorship network analysis highlights the significant contributions of the United States, the United Kingdom, Germany, and China to cooperative connections, with potential for increased international collaboration in zero trust research. These findings emphasize the need for continued international collaboration in this field to advance the development of zero trust technologies and improve cybersecurity globally.

The study identifies five main clusters in the research landscape of zero trust, which include zero trust in IoT, zero trust in cloud computing, blockchain enhanced zero trust security, big data security, and zero trust in edge computing. Additionally, the study analyzes the main research hotspots for zero trust in detail and presents emerging hot topics in Clusters 1, 3, 4, and 5. While research in emerging hot topics areas is currently limited, there is significant potential for growth in the future. These findings will provide valuable insights into current research trends and future directions for zero trust.

The research on threat analysis and zero trust solutions for IoT has revealed that vulnerabilities and risks exist in the perception layer, network layer, and application layer. At the perception layer, zero trust security for IoT sensors and devices are achieved by improving personal feature recognition, continuous identity authentication, continuous multifactor authentication, assigning real-time trust levels, and segmenting the terminal device network into small segments to restrict user access etc. At the network layer, IAM and SDP technologies based on zero trust provide device authentication and encryption, enhancing the security of direct and indirect communication channels. At the application layer, zero trust solutions for data and access control involve activities such as categorizing the importance of data, and improving access control logic.

Supplementary Information

The online version contains supplementary material available at https://doi.org/10.1186/s42400-024-00212-0.

Additional file 1. Well-structured table of bibliometric analysis data.

Acknowledgements

The authors of the paper sincerely appreciate anonymous reviewers whoreviewed this manuscript and provided constructive comments.

Author contributions

CL participated in all the work, designed the framework and experiments, and wrote the manuscript. RT, YW, YF and FZ provided suggestions on the framework design and joined the discussion of this work. ZJ, YL and QL reviewed the manuscript and gave suggestions on the revision of the details of the article. All authors read and approved the final manuscript.

Funding

This work is supported by the Youth Innovation Promotion Association CAS, the Foundation Strengthening Program Technical Area Fund (No. 2021-JCJQ-JJ-0908), the Climbing Program of the Institute of Information Engineering, Chinese Academy of Sciences (No. E3Z0071116), the Key Laboratory of Network Assessment Technology at Chinese Academy of Sciences and Beijing Key Laboratory of Network security and Protection Technology.

Availability of data and materials

The data for bibliometric analysis are displayed in a structured table that can be found in Additional file 1.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 20 June 2023 Accepted: 22 January 2024
Published online: 03 May 2024

References

Abreu V, Santin AO, Viegas EK, Cogo VV (2020) Identity and access management for IoT in smart grid. In: Advanced information networking and applications: proceedings of the 34th international conference on advanced information networking and applications (AINA-2020). Springer, pp 1215–1226

Adahman Z, Malik AW, Anwar Z (2022) An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Comput Secur 122:102911

Ahmed A, Shoufan A, Belwafi K (2023) Formal verification of light-weight security protocol and data model for chip-to-chip zero trust. IEEE Access

Alappat MR (2023)Multifactor authentication using zero trust. Ph.D. thesis, Rochester Institute of Technology

Ali B, Gregory MA, Li S (2021) Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In: 2021 31st international telecommunication networks and applications conference (ITNAC). IEEE, pp 192–197

Ali B, Gregory MA, Li S (2023) Trust-aware task load balancing in multi-access edge computing based on blockchain and a zero trust security capability framework. Trans Emerg Telecommun Technol 4845

Al-Ruwaii B, De Moura G (2021) Why the time has come to embrace the zero-trust model of cybersecurity. In: World economic forum

Ameer S, Gupta M, Bhatt S, Sandhu R (2022) Bluesky: towards convergence of zero trust principles and score-based authorization for IoT enabled smart systems. In: Proceedings of the 27th ACM on symposium on access control models and technologies, pp 235–244

Arifeen M, Petrovski A, Petrovski S (2021) Automated microsegmentation for lateral movement prevention in industrial internet of things (IIoT). In: 2021 14th international conference on security of information and networks (SIN), vol 1. IEEE, pp 1–6

Awan SM, Azad MA, Arshad J, Waheed U, Sharif T (2023) A blockchain-inspired attribute-based zero-trust access control model for IoT. Information 14(2):129

Basta N, Ikram M, Kaafar MA, Walker A (2022) Towards a zero-trust microsegmentation network security strategy: an evaluation framework. In: NOMS 2022-2022 IEEE/IFIP network operations and management symposium. IEEE, pp 1–7

Beltrán M (2018) Identifying, authenticating and authorizing smart objects and end users to cloud services in internet of things. Comput Secur 77:595–611

Bevish Jinila Y, Prayla Shyry S, Christy A (2022) A multi-component-based zero trust model to mitigate the threats in internet of medical things. In: Data engineering for smart systems: proceedings of SSIC 2021. Springer, pp 605–613

Bhattacharjya S, Saiedian H (2022) Establishing and validating secured keys for IoT devices: using p3 connection model on a cloud-based architecture. Int J Inf Secur 21(3):427–436

Buck C, Olenberger C, Schweizer A, Völter F, Eymann T (2021) Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Comput Secur 110:102436

Campbell M (2020) Beyond zero trust: trust is a vulnerability. Computer 53(10):110–113

Chandramouli R, Butcher Z (2023) A zero trust architecture model for access control in cloud-native applications in multi-cloud environments. Technical report, National Institute of Standards and Technology

Chappin EJ, Ligtvoet A (2014) Transition and transformation: a bibliometric analysis of two scientific networks researching socio-technical change. Renew Sustain Energy Rev 30:715–723

Chen H, Jiang W, Yang Y, Yang Y, Man X (2015) Global trends of municipal solid waste research from 1997 to 2014 using bibliometric analysis. J Air Waste Manag Assoc 65(10):1161–1170

Cheng R, Chen S, Han B (2023) Towards zero-trust security for the metaverse. IEEE Commun Mag

Chen J, Zuo C, Diao W, Dong S, Zhao Q, Sun M, Lin Z, Zhang Y, Zhang K (2019) Your IoTs are (not) mine: on the remote binding between IoT devices and users. In: 2019 49th annual IEEE/IFIP international conference on dependable systems and networks (DSN). IEEE, pp 222–233

Da Rocha BC, de Melo LP, de Sousa RT (2021) Preventing apt attacks on LAN networks with connected IoT devices using a zero trust based security model. In: 2021 workshop on communication networks and power systems (WCNPS). IEEE, pp 1–6

Darwish SM (2021) Feature extraction of finger-vein patterns based on boosting evolutionary algorithm and its application for lot identity and access management. Multimedia Tools Appl 80(10):14829–14851

Davoli L, Belli L, Veltri L, Ferrari G (2018) THORIN: an efficient module for federated access and threat mitigation in big stream cloud architectures. IEEE Cloud Comput 5(1):38–48

Dhar S, Bose I (2021) Securing IoT devices using zero trust and blockchain. J Organ Comput Electron Commer 31(1):18–34

Dimitrakos T, Dilshener T, Kravtsov A, La Marra A, Martinelli F, Rizos A, Rosetti A, Saracino A (2020). Trust aware continuous authorization for zero trust in consumer internet of things. In: 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom). IEEE, pp 1801–1812

Dong Q, Huang D, Luo J, Kang M (2018) Achieving fine-grained access control with discretionary user revocation over cloud data. In: 2018 IEEE conference on communications and network security (CNS), pp 1–9

Duggal AK, Dave M (2021) Intelligent identity and access management using neural networks. Indian J Comput Sci Eng

Ellegaard O, Wallin JA (2015) The bibliometric analysis of scholarly production: how great is the impact? Scientometrics 105:1809–1831

Fan X, Chai Q, Xu L, Guo D (2020) DIAM-IoT: a decentralized identity and access management framework for internet of things. In: Proceedings of the 2nd ACM international symposium on blockchain and secure critical infrastructure, pp 186–191

Fang L, Wu C, Kang Y, Ou W, Zhou D, Ye J (2022) Zero-trust-based protection scheme for users in internet of vehicles. Secur Commun Netw 2022

Feng J, Yu T, Wang Z, Zhang W, Han G, Huang W (2022) An edge zero-trust model against compromised terminals threats in power IoT environments. J Comput Res Dev 59(5):1120–1132. https://doi.org/10.7544/issn1000-1239.20211129

Fernandes E, Jung J, Prakash A (2016) Security analysis of emerging smart home applications. In: 2016 IEEE symposium on security and privacy (SP). IEEE, pp 636–654

Ferretti L, Magnanini F, Andreolini M, Colajanni M (2021) Survivable zero trust for cloud computing environments. Comput Secur 110:102419

Gao F, Jia X, Zhao Z, Chen C-C, Xu F, Geng Z, Song X (2021) Bibliometric analysis on tendency and topics of artificial intelligence over last decade. Microsyst Technol 27:1545–1557

Gao W, Hatcher WG, Yu W (2018) A survey of blockchain: Techniques, applications, and challenges. In: 2018 27th international conference on computer communication and networks (ICCCN). IEEE, pp 1–11

Ge Y, Li T, Zhu Q (2023) Scenario-agnostic zero-trust defense with explainable threshold policy: a meta-learning approach. arXiv preprint arXiv:2303.03349

Gerodimos A, Maglaras L, Ferrag MA, Ayres N, Kantzavelou I (2023) IoT: communication protocols and security threats. Internet Things Cyber-Phys Syst 3:1–13. https://doi.org/10.1016/j.iotcps.2022.12.003

Gnad DR, Krautter J, Tahoori MB (2019) Leaky noise: New side-channel attack vectors in mixed-signal IoT devices. IACR Trans Cryptographic Hardw Embedded Syst 305–339

Han J (2023) Data access security monitoring system based on zero trust mechanism. In: Second international conference on electronic information technology (EIT 2023), vol 12719. SPIE, pp 735–740

Hosney ES, Halim ITA, Yousef AH (2022) An artificial intelligence approach for deploying zero trust architecture (ZTA). In: 2022 5th international conference on computing and informatics (ICCI). IEEE, pp 343–350

Huang W, Xie X, Wang Z, Feng J, Han G, Zhang W (2023) ZT-access: a combining zero trust access control with attribute-based encryption scheme against compromised devices in power iot environments. Ad Hoc Netw 145:103161

Indu I, Anand PR, Bhaskar V (2018) Identity and access management in cloud environment: mechanisms and challenges. Eng Sci Technol Int J 21(4):574–588

Jabar T, Mahinderjit Singh M (2022) Exploration of mobile device behavior for mitigating advanced persistent threats (apt): A systematic literature review and conceptual framework. Sensors 22(13):4662

Jasim AC, Tapus N, Hassoon IA (2018) Access control by signature-keys to provide privacy for cloud and big data. In: 2018 5th International conference on control, decision and information technologies (CoDIT). IEEE, pp 978–983

Ji L, Liu C, Huang L, Huang G (2018) The evolution of resources conservation and recycling over the past 30 years: a bibliometric overview. Resour Conserv Recycl 134:34–43

Jiang C, Xu H, Huang C, Huang Q (2022) An adaptive information security system for 5g-enabled smart grid based on artificial neural network and case-based learning algorithms. Front Comput Neurosci 16

Jia Y, Xing L, Mao Y, Zhao D, Wang X, Zhao S, Zhang Y (2020) Burglars' IoT paradise: understanding and mitigating security risks of general messaging protocols on IoT clouds. In: 2020 IEEE symposium on security and privacy (SP). IEEE, pp 465–481

Julku J, Suomalainen J, Kylänpää M (2021) Delegated device attestation for IoT. In: 2021 8th international conference on internet of things: systems, management and security (IOTSMS). IEEE, pp 1–8

Kang H, Lee K-H (2023) Cloud security scheme based on blockchain and zero trust. J Internet Things Converg 9(2):55–60

Karabacak, B., Whittaker, T.: Zero trust and advanced persistent threats: who will win the war? In: International conference on cyber warfare and security, vol 17, pp 92–101 (2022)

Karimi M, Krishnamurthy P (2021) Software defined ambit of data integrity for the internet of things. In: 2021 IEEE/ACM 21st international symposium on cluster, cloud and internet computing (CCGrid). IEEE, pp 737–745

Khattak HA, Shah MA, Khan S, Ali I, Imran M (2019) Perception layer security in internet of things. Future Gener Comput Syst 100:144–164

Kim TW, Pan Y, Park JH (2022) OTP-based software-defined cloud architecture for secure dynamic routing. Comput Mater Continua 71(1)

Kindervag J, Balaouras S (2010) No more chewy centers: Introducing the zero trust model of information security. Forrester Res 3

Klein D (2019) Micro-segmentation: securing complex cloud environments. Netw Secur 2019(3):6–10

Kumar A, Ahmed T, Saini K, Kumar J (2023) Neos: non-intrusive edge observability stack based on zero trust security model for ubiquitous computing. In: 2023 IEEE international conference on edge computing and communications (EDGE). IEEE, pp 79–84

Kumar P, Moubayed A, Refaey A, Shami A, Koilpillai J (2019) Performance analysis of SDP for secure internal enterprises. In: 2019 IEEE wireless communications and networking conference (WCNC), pp 1–6

Kumar S, Sahoo S, Mahapatra A, Swain AK, Mahapatra KK (2017) Security enhancements to system on chip devices for IoT perception layer. In: 2017 IEEE international symposium on nanoelectronic and information systems (iNIS). IEEE, pp 151–156

Kumar D, Shen K, Case B, Garg D, Alperovich G, Kuznetsov D, Gupta R, Durumeric Z (2019) All things considered: an analysis of IoT devices on home networks. In: USENIX security symposium, pp 1169–1185

Kunz M, Fuchs L, Hummer M, Pernul G (2015) Introducing dynamic identity and access management in organizations. In: Information systems security: 11th international conference, ICISS 2015, Kolkata, India, December 16-20, 2015. Proceedings 11. Springer, pp 139–158

Lei W, Pang Z, Wen H, Hou W, Zhang X (2023) Edge-enabled zero trust architecture for ICPS with spatial and temporal granularity. In: 2023 IEEE 6th international conference on industrial cyber-physical systems (ICPS). IEEE, pp 1–6

Li D, Zhang E, Lei M, Song C (2022) Zero trust in edge computing environment: a blockchain based practical scheme. Math Biosci Eng 19(4):4196–4216

Liao M, Yuan J, Huang F, Wang P, Wang W, Luo S, Yao Y (2022) On-chip silicon optical scattering physical unclonable function towards hardware security. J Lightwave Technol 41(5):1487–1494

Liao H, Li L, Cheng K (2021) Research and application of new business hierarchical security strategies for power internet of things. In: IOP conference series: earth and environmental science, vol 632. IOP Publishing, p 042017

Lin T-S, Tsai I-M, Kuo S-Y (2009) Quantum transmission integrity mechanism for indirect communication. In: 2009 proceedings of 18th international conference on computer communications and networks. IEEE, pp 1–6

Lin C, He D, Huang X, Choo K-KR (2021) OBFP: optimized blockchain-based fair payment for outsourcing computations in cloud computing. IEEE Trans Inf Forensics Secur 16:3241–3253

Liu Y, Hao X, Ren W, Xiong R, Zhu T, Choo KKR, Min G (2022) A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. IEEE Trans Comput

Liu Y, Xing X, Tong Z, Lin X, Chen J, Guan Z, Wu Q, Susilo, W (2023) Secure and scalable cross-domain data sharing in zero-trust cloud-edge-end environment based on sharding blockchain. IEEE Trans Dependable Secure Comput

Longstaff J, Noble J (2016) Attribute based access control for big data applications by query modification. In: 2016 IEEE second international conference on big data computing service and applications (BigDataService). IEEE, pp 58–65

Marasco E, Ross A (2014) A survey on antispoofing schemes for fingerprint recognition systems. ACM Comput Surv (CSUR) 47(2):1–36

Martiradonna A (2023) Zero trust architectures in a multi-cloud environment. Ph.D. thesis, Politecnico di Torino

Mehraj S, Banday MT (2020) Establishing a zero trust strategy in cloud computing environment. In: 2020 international conference on computer communication and informatics (ICCCI). IEEE, pp 1–6

Meng L, Huang D, An J, Zhou X, Lin F (2022) A continuous authentication protocol without trust authority for zero trust architecture. China Commun 19(8):198–213

Merigo JM, Blanco Mesa F, Gil Lafuente AM, Yager RR (2017) Thirty years of the international journal of intelligent systems: a bibliometric review. Int J Intell Syst 32(5):526–554

Misbahuddin M, Harish R, Ananya K (2022) Identity of things (IdoT): a preliminary report on identity management solutions for IoT devices. In: 2022 IEEE international conference on public key infrastructure and its applications (PKIA). IEEE, pp 1–9

Miyazaki K, Islam N (2007) Nanotechnology systems of innovation—an analysis of industry and academia research activities. Technovation 27(11):661–675

Moubayed A, Refaey A, Shami A (2019) Software-defined perimeter (SDP): state of the art secure solution for modern networks. IEEE Netw 33(5):226–233

Muneer SM, Alvi MB, Farrakh A (2023) Cyber security event detection using machine learning technique. Int J Comput Innov Sci 2(2):42–46

Nahar K, Gill AQ (2022) Integrated identity and access management metamodel and pattern system for secure enterprise architecture. Data Knowl Eng 140:102038

Nana H, Yuanyuan Y (2022) A research on data secure access control mechanism based on zero trust and attribute encryption in medical cloud. In: 2022 IEEE 8th international conference on computer and communications (ICCC). IEEE, pp 1400–1404

Omar RR, Abdelaziz TM (2020) A comparative study of network access control and software-defined perimeter. In: Proceedings of the 6th international conference on engineering & MIS 2020, pp 1–5

Osman A, Wasicek A, Köpsell S, Strufe T (2020) Transparent microsegmentation in smart home IoT networks. In: HotEdge

Palmo Y, Tanimoto S, Sato H, Kanai A (2021) Complementary methods of IoT reliability for embedding IoT devices into SDP. In: 2021 IEEE 11th international conference on consumer electronics (ICCE-Berlin). IEEE, pp 1–6

Partida A, Criado R, Romance M (2021) Identity and access management resilience against intentional risk for blockchain-based IoT platforms. Electronics 10(4):378

Pero V, Ekman L (2023) Implementing a zero trust environmentfor an existing on-premises cloud solution

Piya K, Au QA, Shrestha S, Singh A, Mohd TK (2021) IoT in health care industry: a promising prospect. In: 2021 IEEE 12th annual ubiquitous computing, electronics & mobile communication conference (UEMCON). IEEE, pp. 0466–0474

Polychronaki M, Kogias DG, Patrikakis CZ (2022) Identity management in internet of things with blockchain. In: Blockchain based internet of things. Springer, pp 209–236

Puthal D, Yang LT, Dustdar S, Wen Z, Jun S, Moorsel AV, Ranjan R (2020) A user-centric security solution for internet of things and edge convergence. ACM Trans Cyber-Phys Syst 4(3):1–19

Puthal D, Wilson S, Nanda A, Liu M, Swain S, Sahoo BP, Yelamarthi K, Pillai P, El-Sayed H, Prasad M (2022) Decision tree based user-centric security solution for critical IoT infrastructure. Comput Electr Eng 99:107754

Rajasoundaran S, Prabu AV, Routray S, Kumar SS, Malla PP, Maloji S, Mukherjee A, Ghosh U (2021) Machine learning based deep job exploration and secure transactions in virtual private cloud systems. Comput Secur 109:102379

Ramezanpour K, Jagannath J (2022) Intelligent zero trust architecture for 5g/6g networks: principles, challenges, and the role of machine learning in the context of O-RAN. Comput Netw 109358

Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572

Refaey A, Sallam A, Shami A (2019) On IoT applications: a proposed SDP framework for MQTT. Electron Lett 55(22):1201–1203

Ronen E, Shamir A, Weingarten A-O, O Flynn C (2017) IoT goes nuclear: creating a zigbee chain reaction. In: 2017 IEEE symposium on security and privacy (SP). IEEE, pp 195–212

Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero trust architecture. Technical report, National Institute of Standards and Technology

Saleem M, Warsi M, Islam S (2023) Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in saas cloud computing environment. J Inf Secur Appl 72:103389

Sanchez-Gomez A, Diaz J, Arroyo D (2018) Encrypted cloud: A software solution for the secure use of free-access cloud storage services. In: International joint conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, 2017, Proceeding 12. Springer, pp 683–692

Satam S, Satam , P, Hariri S (2020) Multi-level bluetooth intrusion detection system. In: 2020 IEEE/ACS 17th international conference on computer systems and applications (AICCSA). IEEE, pp 1–8

Sedjelmaci H, Ansari N (2023) Zero trust architecture empowered attack detection framework to secure 6g edge computing. IEEE Network

Shah SWA, Syed NF, Shaghaghi A, Anwar A, Baig Z, Doss R (2020) Towards a lightweight continuous authentication protocol for device-to-device communication. In: 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom). IEEE, pp 1119–1126

Shah SW, Syed NF, Shaghaghi A, Anwar A, Baig Z, Doss R (2021) LCDA: lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). Comput Secur 108:102351

Sharma P, Borah MD, Namasudra S (2021) Improving security of medical big data by using blockchain technology. Comput Electr Eng 96:107529

Sharma R, Chan CA, Leckie C (2023) Probabilistic distributed intrusion detection for zero-trust multi-access edge computing. In: NOMS 2023-2023 IEEE/IFIP network operations and management symposium. IEEE, pp 1–9

Sharma A, Sharma S, Dave M (2015) Identity and access management-a comprehensive study. In: 2015 international conference on green computing and internet of things (ICGCIoT). IEEE, pp 1481–1485

Sheng Y-B, Zhou L, Long G-L (2022) One-step quantum secure direct communication. Sci Bull 67(4):367–374

Shilpa V, Vidya A, Pattar S (2022) MQTT based secure transport layer communication for mutual authentication in IoT network. Global Transit Proc 3(1):60–66

Singh J, Bello Y, Hussein AR, Erbad A, Mohamed A (2020) Hierarchical security paradigm for IoT multiaccess edge computing. IEEE Internet Things J 8(7):5794–5805

Singh M, Dubey RK, Kumar S (2022) Vehicle telematics: an internet of things and big data approach. In: Artificial intelligence and machine learning for EDGE computing. Elsevier, pp 235–254

Song Y, Jiang F, Shah SWA, Doss R (2022) A new zero-trust aided smart key authentication scheme in IOV. In: 2022 IEEE international conference on pervasive computing and communications workshops and other affiliated events (PerCom workshops). IEEE, pp 630–636

Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R (2022) Zero trust architecture (ZTA): a comprehensive survey. IEEE Access

Tanimoto S, Sato Y, Chertchom P, Sato H, Kanai A (2021) Proposal of a perimeter line management method for fog and edge computing with SDP concept. In: Advances in networked-based information systems: the 23rd international conference on network-based information systems (NBiS-2020) 23. Springer, pp 290–302

Tao W, Cao Y, Li M, Lu L, Jiang Z, Zhang W (2023) Research on terminal security protection of zero-trust smart grid based on fog computing. In: 2023 5th international conference on intelligent control, measurement and signal processing (ICMSP). IEEE, pp 1–4

Tao Y, Lei Z, Ruxiang P (2018) Fine-grained big data security method based on zero trust model. In: 2018 IEEE 24th international conference on parallel and distributed systems (ICPADS). IEEE, pp 1040–1045

Teerakanok S, Uehara T, Inomata A (2021) Migrating to zero trust architecture: reviews and challenges. Secur Commun Netw 2021:1–10

Thapliyal N, Gaur M (2023) Security threats in healthcare big data: a comparative study. In: 2023 international conference on computational intelligence and sustainable engineering solutions (CISES). IEEE, pp 32–37

Vanickis R, Jacob P, Dehghanzadeh S, Lee B (2018) Access control policy enforcement for zero-trust-networking. In: 2018 29th Irish signals and systems conference (ISSC). IEEE, pp 1–6

Wang Zh, Jin Mh, Jiang L, Feng Cj, Cao Jy, Yun Z (2023) Secure access method of power internet of things based on zero trust architecture. In: International conference on swarm intelligence. Springer, pp 386–399

Wang S, Li H, Chen J, Wang J, Deng Y (2022) Dag blockchain-based lightweight authentication and authorization scheme for IoT devices. J Inf Secur Appl 66:103134

Wang Z, Yu X, Xue P, Qu Y, Ju L (2023) Research on medical security system based on zero trust. Sensors 23(7):3774

Wang Q, Ji S, Tian Y, Zhang X, Zhao B, Kan Y, Lin Z, Lin C, Deng S, Liu AX (2021) Mpinspector: a systematic and automatic approach for evaluating the security of IoT messaging protocols. In: USENIX security symposium, pp 4205–4222

Wen H, Lin Z, Zhang Y (2020) Firmxray: detecting bluetooth link layer vulnerabilities from bare-metal firmware. In: Proceedings of the 2020 ACM SIGSAC conference on computer and communications security, pp 167–180

Wu C (2022) Internet of things security: architectures and security measures. Springer Singapore

Wu K, Shi J, Guo Z, Zhang Z, Cai J (2021) Research on security strategy of power internet of things devices based on zero-trust. In: 2021 international conference on computer engineering and application (ICCEA). IEEE, pp 79–83

Xiaojian Z, Liandong C, Jie F, Xiangqun W, Qi W (2021) Power IoT security protection architecture based on zero trust framework. In: 2021 IEEE 5th international conference on cryptography, security and privacy (CSP). IEEE, pp 166–170

Xiao S, Ye Y, Kanwal N, Newe T, Lee B (2022) SOK: context and risk aware access control for zero trust systems. Secur Commun Netw 2022

Xiong H, Mei Q, Zhao Y (2019) Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments. IEEE Syst J 14(1):310–320

Yacob T (2023) Securing sensitive data in the cloud: a new era of security through zero trust principles

Yan X, Wang H (2020) Survey on zero-trust network security. In: Artificial intelligence and security: 6th international conference, ICAIS 2020, Hohhot, China, July 17-20, 2020, Proceedings, Part I 6. Springer, pp 50–60

Zhang G, Yan C, Ji X, Zhang T, Zhang T, Xu W (2017) DolphinAttack: inaudible voice commands. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, pp 103–117

Zhao S, Li S, Li F, Zhang W, Iqbal M (2021) Blockchain-enabled user authentication in zero trust internet of things. In: Security and privacy in new computing environments: third EAI international conference, SPNCE 2020, Lyngby, Denmark, August 6–7, 2020, Proceedings 3. Springer, pp 265–274

Zhao L, Sun M, Yang B, Xie J, Feng J (2022) Zero trust access authorization and control of network boundary based on cloud sea big data fuzzy clustering. J Intell Fuzzy Syst (Preprint), 1–13

Ziegler D, Marsalek A, Prünster B, Sabongui J (2020) Efficient access-control in the IIoT through attribute-based encryption with outsourced decryption. In: ICETE (2), pp 547–552

Zolotukhin M, Hämäläinen T, Kotilainen P (2022) Intelligent solutions for attack mitigation in zero-trust environments. In: Cyber security: critical infrastructure protection. Springer, pp 403–417

Publisher's Note