future internet

MDPI

Review

Using the Zero Trust Five-Step Implementation Process with Smart Environments: State-of-the-Art Review and Future Directions

Shruti Kulkarni *, Alexios Mylonas and Stilianos Vidalis

Cybersecurity Research Lab, School of Physics, Engineering and Computer Science, University of Hertfordshire, Hatfield AL10 9AB, UK; a.mylonas@herts.ac.uk (A.M.); s.vidalis@herts.ac.uk (S.V.)
* Correspondence: s.s.kulkarni@herts.ac.uk

Abstract

There is a growing pressure on industry to secure environments and demonstrate their commitment in taking right steps to secure their products. This is because of the growing number of security compromises in the IT industry, Operational Technology environment, Internet of Things environment and smart home devices. These compromises are not just about data breaches or data exfiltration, but also about unauthorised access to devices that are not configured correctly and vulnerabilities in software components, which usually lead to insecure authentication and authorisation. Incorrect configurations are usually in the form of devices being made available on the Internet (public domain), reusable credentials, access granted without verifying the requestor, and easily available credentials like default credentials. Organisations seeking to address the dual pressure of demonstrating steps in the right direction and addressing unauthorised access to resources can find a viable approach in the form of the zero trust concept. Zero trust principles are about moving security controls closer to the data, applications, assets and services and are based on the principle of "never trust, always verify". As it stands today, zero trust research has advanced far beyond the concept of "never trust, always verify". This paper provides the culmination of a literature review of research conducted in the space of smart home devices and IoT and the applicability of the zero trust five-step implementation process to secure them. We discuss the history of zero trust, the tenets of zero trust, the five-step implementation process for zero trust, and its adoption for smart home devices and Internet of Things, and we provide suggestions for future research.

Keywords: zero trust; smart home; authentication; authorisation; IoT; zero trust five-step implementation process; protect surface; transaction flows; zero trust architecture; zero trust policy

Academic Editors: Dimitris Karampatzakis, Thomas Lagkas and Kalliopi Kravari

Received: 9 June 2025
Revised: 3 July 2025
Accepted: 8 July 2025
Published: 18 July 2025

Citation: Kulkarni, S.; Mylonas, A.; Vidalis, S. Using the Zero Trust Five-Step Implementation Process with Smart Environments: State-of-the-Art Review and Future Directions. *Future Internet* **2025**, *17*, 313. https://doi.org/10.3390/fi17070313

1. Introduction

Growing pressure on the industry to secure smart environments and to demonstrate their commitment to taking the right steps in securing their products and services has been elaborated in the public domain [1]. The impact of security compromises on products and services include data breaches, data exfiltration, unauthorised access to devices with incorrect configurations and exploitation of vulnerabilities in software components [2], of not just IT systems, but also of Operational Technology (OT), Internet of Things (IoT) and smart home devices. The causes of these compromises include but are not limited to incorrect access decisions or stolen credentials or because of default, reusable credentials.

With the pervasiveness and interconnection of smart home devices [3], the security of smart home devices is under scrutiny, resulting in 200+ companies joining the Connectivity Standards Alliance (CSA) as members. The security of smart home devices has been highlighted in a cyber security certification program announced by the Biden–Harris government in the USA [4]. With the proliferation of cloud environments, the interconnectivity of devices, remote working and increasing digitisation, perimeter-based security does not address the prevailing threat landscape, as it lags behind the innovativeness of malicious actors. Zero trust provides a viable alternative approach with a paradigm shift that seeks to address compromises by mitigating unauthorised access [1,2] with continual authentication of access requests before granting access, thus never trusting but always verifying. This approach is encapsulated in the seven tenets of zero trust [5]. Zero trust includes moving security controls closer to data, applications, assets and services [2]. Lately, zero trust research has advanced beyond the concept of "never trust, always verify" [6].

Zero trust is implemented using the zero trust five-step implementation process [7], which includes (a) *Define your protect surface*, (b) *Map the transaction flows*, (c) *Build a Zero Trust architecture*, (d) *Create Zero Trust Policy* (e) *Monitor and maintain the network.* This paper surveys the adoption of the zero trust five-step implementation process for smart environments. Smart environments are elastic, i.e., (i) the number of devices expands and contracts, depending on the users' appreciation and attraction to the ever-increasing availability of IoT devices, and (ii) they use heterogeneous communication vectors, such as Bluetooth, ZigBee and Wi-Fi. This poses a challenging situation, as many smart devices are mass produced and are installed by users and consumers. However, unlike traditional devices like laptops and desktops, the security of such smart devices is not very well understood by both technology-aware and technology-unaware users [8], as has been noticed with any new smart device introduced into the market, e.g., smartphones [9,10] and smart locks [11].

In the face of such elasticity, coupled with the speed with which manufacturers ship smart devices to market, security considerations take a backseat [8,11]. The industry's response to the growing pressure to address security issues includes applying zero trust to smart environments [12]. This paper provides a state-of-the-art review of the adoption of the zero trust five-step implementation process in smart home environments and IoT, as well as providing directions for future research.

The major contributions of the paper are as follows:

(1) Contrary to most surveys that cover zero trust architecture and network security, this paper provides a comprehensive review of the adoption of zero trust five-step implementation for smart homes and IoT. To the best of our knowledge, we are the first to discuss the five-step zero trust implementation process for smart homes and IoT.
(2) We believe that zero trust cannot be applied without understanding the protect surface, which includes the data or the asset we seek to secure and the communication flows between assets. Unlike other studies, we devote a subsection to discussing the history of zero trust and the importance of the five-step implementation process.
(3) In this survey, we have not limited our work to presenting the reviewed works; we also compare and analyse them and identify the gaps in the research on zero trust and smart home devices and IoT. The context and reference for the identification of gaps is the five-step implementation process for smart home devices and IoT, and the problem that the papers seek to address with zero trust and the zero trust tenets is identified. In this way, we produce suggestions and recommendations for future work.
(4) We discuss open issues regarding the current implementations of zero trust and discuss how such systems need to look at zero trust implementation comprehensively,

as devised by authoritative sources, such that security controls are moved closer to resources to prevent compromises that occur as a result of unauthorised access.

The rest of this paper is organised as follows. Section 2 provides the background of zero trust and related work. Section 3 contains the literature review. Section 4 discusses open issues and directions for future work, before the paper concludes in Section 5.

2. Background

The National Security Telecommunications Advisory Committee (NSTAC) report [7] laid out a pragmatic approach to strategise and implement zero trust. The report traces the history of zero trust and USA federal guidelines/policy and moves on to describe zero trust foundational concepts and definitions along with the zero trust five-step implementation process. As the NSTAC report supersedes the earlier publications on zero trust, this paper considers this report as an authoritative source for zero trust.

Contrary to the obsolete castle-and-moat model of security, zero trust assumes that the perimeter is breached and does not trust the entities that gained access within the environment by providing the authentication details at the perimeter [1]. Zero trust architecture centres around the protect surface, which is a combination of data, applications, assets and services that an organisation seeks to protect [7]. The implementation process of zero trust applies not only to IT, but also to OT, IoT, smart home devices, etc. [2]. We first describe how the protect surface is different from the attack surface, which is ever evolving [13] and is traditionally used.

Figure 1 illustrates an example of the protect surface and the attack surface.

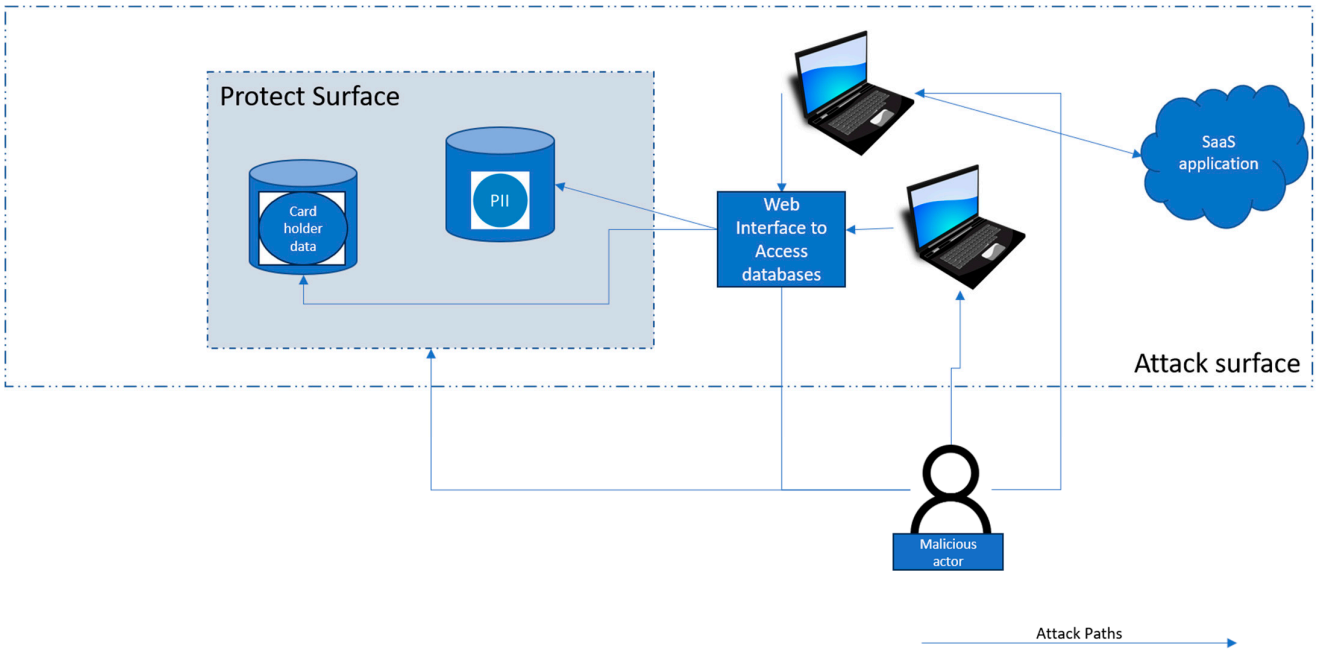

Figure 1. Example of attack surface and protect surface.

In Figure 1 we assume that the databases with Personally Identifiable Information (PII) and cardholder data are of value to the organisation, as any compromise of the data that persists in these databases (confidentiality-, integrity- and availability-wise) may lead to contractual, legal, regulatory and/or statutory impact. The organisation seeks to protect these two servers that are of prime importance from compromises. From a zero-trust perspective these two database servers form one protect surface. On the other hand, the attack surface consists of laptops, the Software-as-a-Service (SaaS) application and the web interface that connects to the database servers, as these assets provide attack paths

for a malicious actor to reach the databases in the protect surface, which may result in compromise(s).

Figure 2 illustrates the addition of assets (Additional asset and SaaS application 2) to the environment and the impact it has on the attack surface.

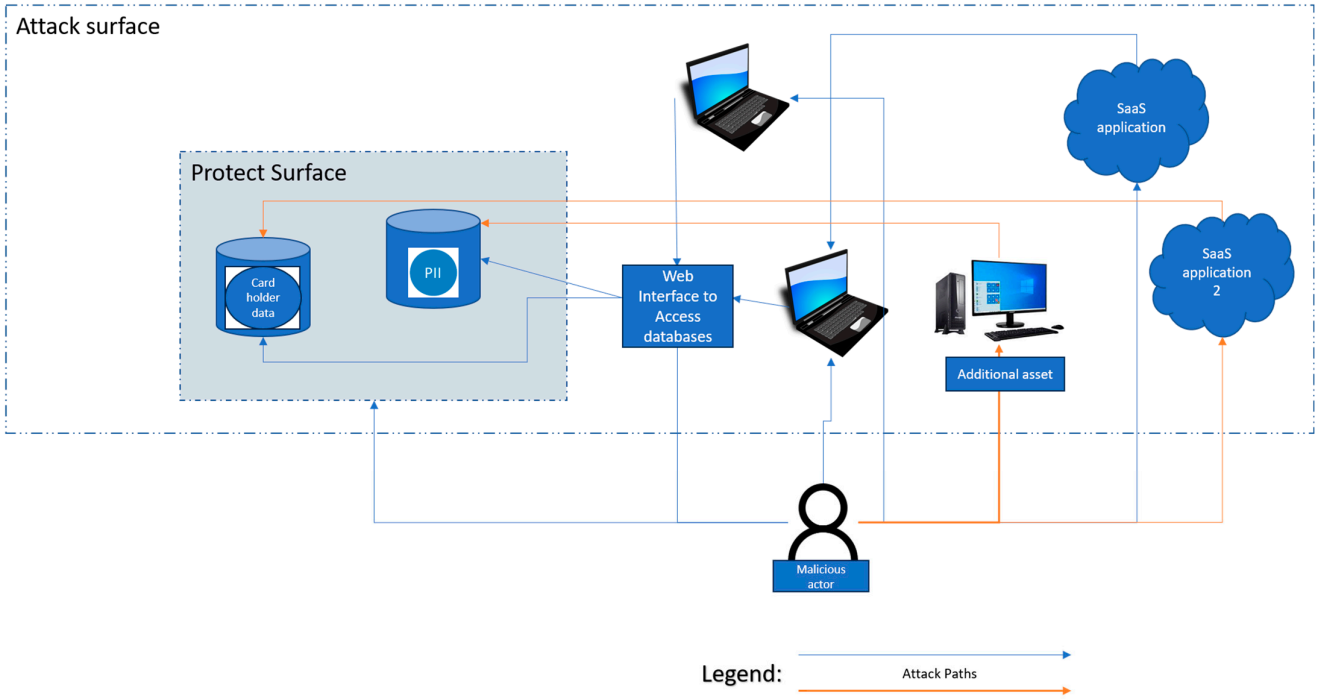

Figure 2. Example of how attack surface increases with addition of assets.

In Figure 2, assume the organisation adds a new desktop (Additional asset) and a new SaaS application (SaaS application 2) The addition of these two assets increases the attack surface, as they provide more attack paths for a malicious actor to compromise the databases in the protect surface, but does not change the protect surface identified in Figure 1. The protect surface does not change because the database servers that the organisation seeks to secure, the servers for the PII database and cardholder database, remain the same. The paths in orange depict the additional attack paths brought about by the additional assets.

This is illustrated in Figure 3.

In Figure 3 the smart home environment consists of three disparate smart devices from three different vendors, each of which provides a specific functionality distinct from the others. These are smart home devices that connect with their home clouds via a home router to receive updates and upgrades and perhaps share telemetry. Most smart devices also have an interface application (web and/or mobile) that serves as an interface to configure the device. However, smart devices do not communicate amongst themselves. For example, a smart TV does not have any interface to connect with a smart fridge or a smart boiler. A smart fridge does not communicate with a smart boiler to change the heating settings. To compromise the smart devices, a malicious actor needs to (a) compromise the home router (vulnerabilities, open ports, etc.) or (b) conduct a person-in-the-middle attack between the home cloud and the smart device or (c) compromise the home cloud or (d) compromise the interface application. In effect, the attack surface for the smart home environment is formed of the home router, the communication layer between the smart device and the home cloud, the home cloud, and the interface application.

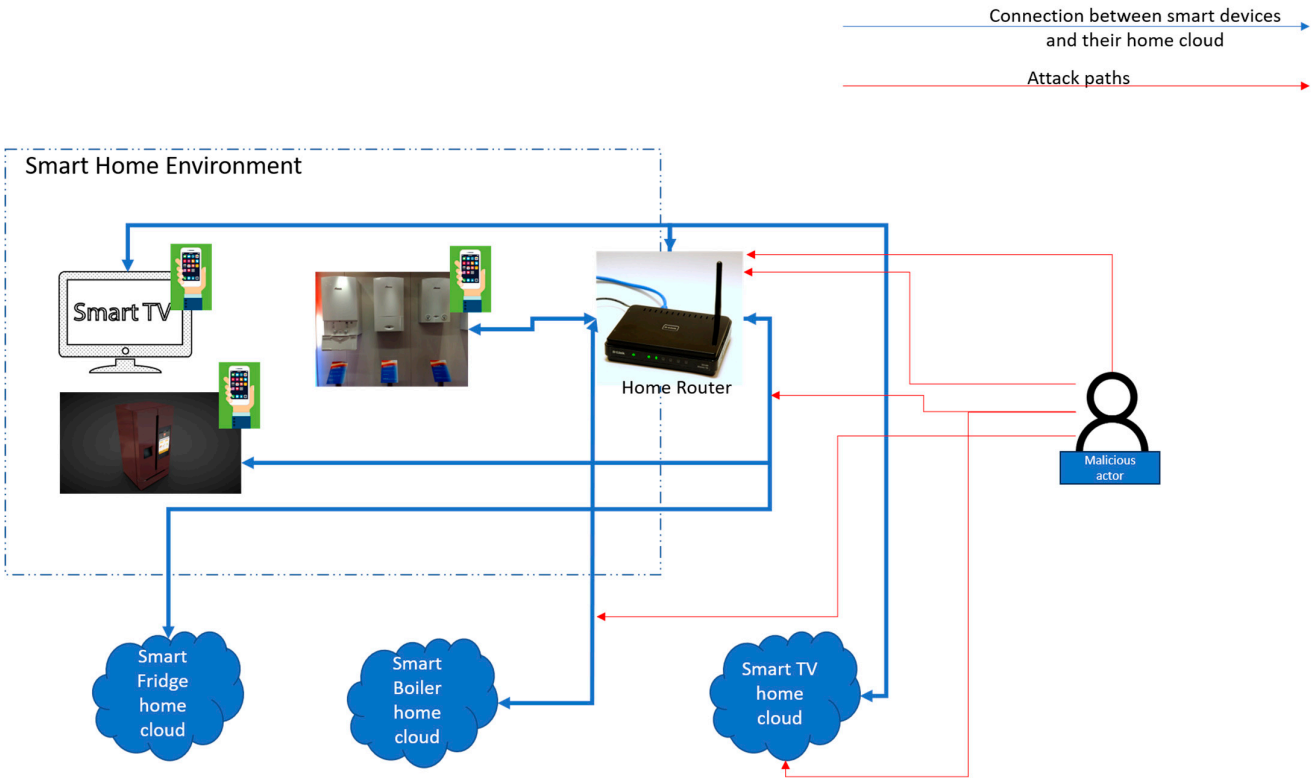

Figure 3. Example of smart home environment and attack surface.

Added complexity derives from the presence of home automation systems and their integration with smart home devices [14].

Due to home automation system integrations, the attack paths now increase multi-fold, as illustrated in Figure 4.

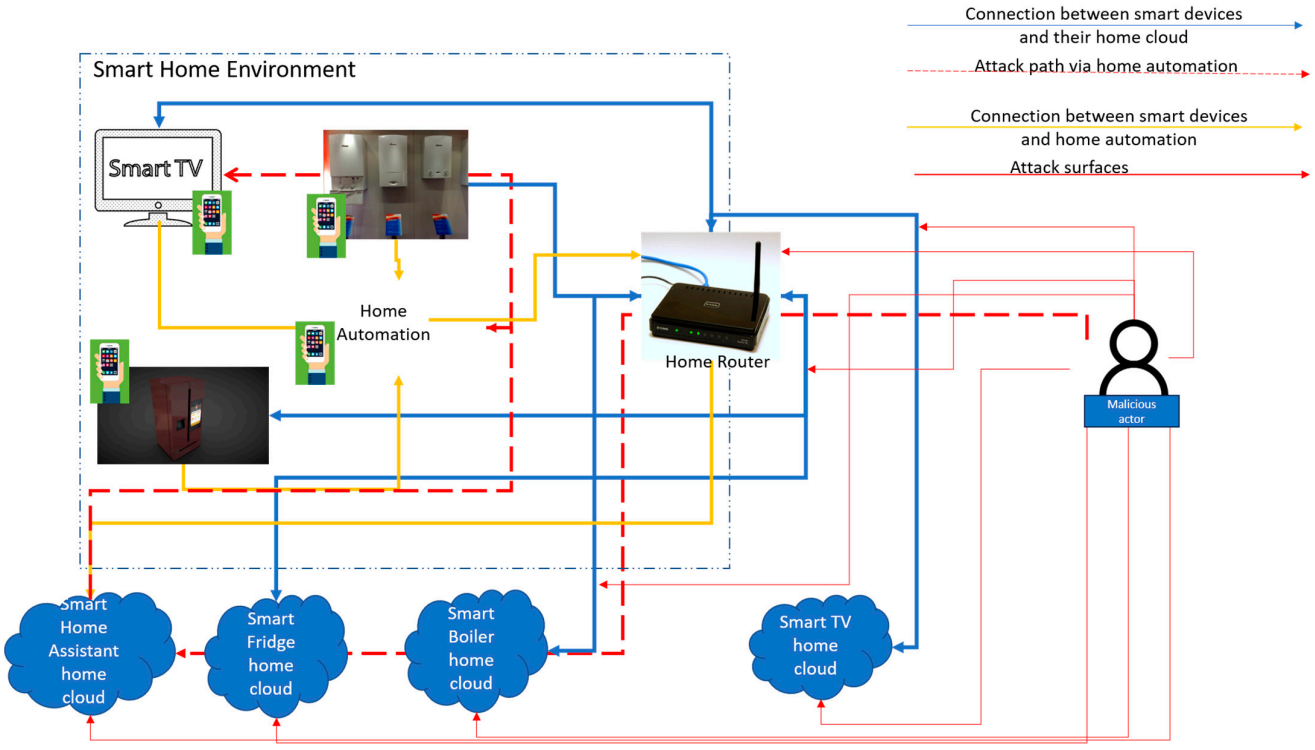

Figure 4. Increased attack paths with home automation system.

When used, to provide the required interface and the required value to smart homes, a home automation system connects with most, if not all, smart home devices. Home automation systems have their home cloud too. Home automation systems provide functionalities like setting alarms for re-order when inventory falls below a certain level in a smart fridge or controlling the heating with a smart boiler. These kinds of functionalities require that the homeowner configures settings on the home automation. For example, to take advantage of automatic re-ordering via a smart fridge, the homeowner would need to set an inventory threshold on the home automation. This interfacing leads to a lot more communication lines between the devices than those depicted in Figure 3. The attack surface now increases from the home router, the communication layer, the home cloud and the interface application to include the home automation and the interfaces that the home automation has with other smart home devices. The attack paths increase, and a malicious actor now only needs to compromise the home automation systems and gain access to the interconnected devices. Additional security complications come with the addition and removal of smart wear devices, home assistants and smart devices. These devices are mass-produced and are installed by users and consumers whose security capabilities range from no knowledge to a high level of knowledge.

Put in the context of zero trust, smart home devices, home clouds, home routers and home automation systems are assets and applications of a smart home environment that also persist and transmit data. Zero trust, which is implemented using the five-step implementation process [7], includes the identification of Data, Assets, Application, Services (DAAS) elements as the protect surface, which is an important step [2], as it allows the organisation to see how the elements that comprise a business system or an environment cohesively form a group. Any compromise of these elements impacts the delivered value—business or otherwise. Mapping transaction flows [15] is the next step in the implementation process, which involves identifying information flows between DAAS elements—within a protect surface, between protect surfaces and with external elements—and their current security maturity [7]. Zero trust architecture is built to protect key assets by adding/enhancing controls which includes but is not limited to definition and location of Policy Decision Point (PDP), Policy Enforcement Point (PEP), Policy Administrator (PA), etc. [7]. The next step is creation of zero trust policies for the full technical stack—network, applications, sessions, etc. [7]. Zero trust policies implement access controls and are based on considered factors, either allowing or denying access. The final step is monitoring and maintaining the network. Step 5 also involves a feedback process, as any failures noted during monitoring are fed back to Step 4 to ensure that policies are adjusted. Again, this statement should not be taken literally to mean the monitoring of networks only; it includes the monitoring and maintaining of applications and interface components like APIs and so on [7].

The five-step implementation process implements the tenets of zero trust [5].

Table 1 maps the tenets to the technology solutions through which the tenets are realised.

Table 1. Zero trust tenet descriptions and tenet realisations.

Tenet #	Tenet Description	Technology/Technology Solution Through Which the Tenet Is Realised
1	All data sources and computing services are considered resources	Authentication, authorisation and encryption of data
2	All communication is secured regardless of network location	Encryption of data-in-transit, micro-segmentation
3	Access to individual enterprise resources is granted on a per-session basis	Least privilege, continual authentication/session-based authentication

Table 1. *Cont.*

Tenet #	Tenet Description	Technology/Technology Solution Through Which the Tenet Is Realised
4	Access to resources is determined by dynamic policy—including the observable state of the client identity, the application/service and the requesting asset—and may include other behavioural and environmental attributes	Context-aware access control, context-based access control, risk-based access control
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets	Continuous monitoring
6	All resource authentications and authorisations are dynamic and strictly enforced before access is allowed	Trust algorithm, software-defined perimeter (SDP), device agent/gateway
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture	Continuous monitoring, feedback loop, contexts for access control

2.1. History of Zero Trust

The concept of trust as a computational concept was put forward by Stephen Paul Marsh [16] in his doctoral thesis at the University of Stirling. He formalised the definition of trust in the context of Distributed Artificial Intelligence (DAI) or Multi-Agent Systems (MAS), where the discussion is about two aspects of general trust—zero trust and distrust. The author has discussed how the two are not the same. With this perspective, it is important to note that while the phrase "zero trust" was coined in 1994, it was not used to define zero trust in the manner it is defined today.

In 2001, the authors of the OSSTMM manual [17] included "trust" as a concept which depends on authentication and authorisation, non-repudiation, data confidentiality and data integrity of the system. The manual discusses testing "trust" in various contexts. In 2010, the OSSTMM published version 3.0 of their manual, where the authors documented trust as a problem and a solution [18]. The authors also mentioned that, from an authentication perspective, trust is often placed in the credentials that are authenticated when an entity enters the environment and the entity is not authenticated again.

Then came the concept of "de-parameterisation", which was elaborated by the authors of [19]. They focused on how the early Internet was designed for a small group of people and that a trusted perimeter was implementable. They discussed the challenges of this concept posed in the early 2000s. The thoughts of a group of UK-based senior security leaders were formalised in 2003 by an interest group called the Jericho Forum [20]. The Jericho Forum researched and produced a body of literature to reveal the inadequacy of the perimeter in the face of the increasing digitisation of the economy and modernisation via digitisation. They also mentioned that the perimeter was increasingly turning into a sieve. The authors further documented their findings before the Jericho Forum formally closed in 2013.

In 2009 Google created BeyondCorp [21] by implementing the principles of zero trust. They did this by not depending solely on user credentials for authentication. Google included devices used for entering credentials and the security state of the device. They further included monitoring of the endpoints, logging all traffic and only communicating over encrypted channels, with multi-factor authentication. They thus eliminated using just static credentials for authentication.

In 2010 John Kindervag, an analyst with Forrester Research, published two technical reports which set the tone for the formalisation of zero trust, i.e., [22,23]. In these reports the author focused on the lack of verification in the phrase "trust, but verify" and gave a different thought process by bringing into focus the internal environment. Network packets on the internal environment cannot be trusted as if they were people. Access to

resources must be secured, irrespective of where the network traffic comes from, with least privilege access and strict access control. The author did not recommend role-based access control (RBAC) and pivoted from "trust, but verify" to "verify and never trust". Logging and inspecting all traffic provides visibility to the activities in the internal environment.

After 2010 there were few developments in the zero-trust-related literature until 2018, when the National Institute of Standards and Technology (NIST) published NIST SP 800-207—Zero Trust Architecture [5], which describes the seven tenets of zero trust. NIST sees the core components of zero trust as depicted in Figure 5. Variations of this architecture to suit use cases are also defined in the report. The architecture is focused on preventing unauthorised access to resources while making access as granular as possible. Any zone outside of the data plane is treated as an "implicit trust" zone, and all access is granted via a Policy Enforcement Point (PEP).

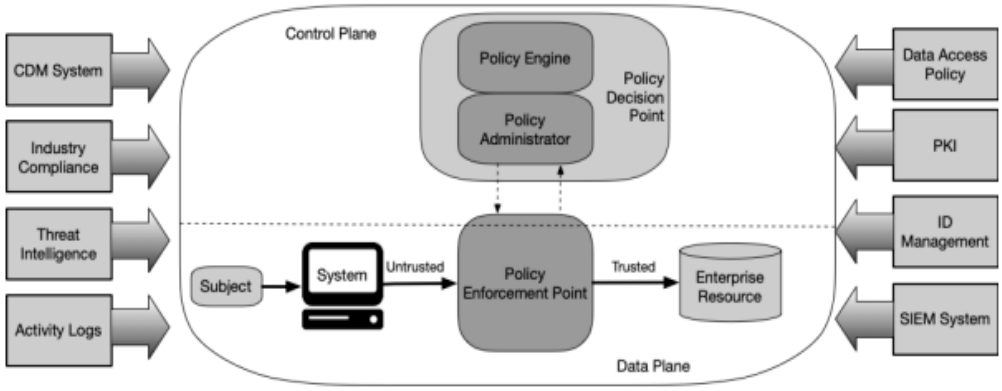

Figure 5. Core Zero Trust Logical Components [5].

In 2021 the US Department of Defense (US DoD) cleared their zero-trust reference architecture for publication [24]. This architecture was used internally by the US DoD and cleared for public consumption. Though based on zero trust principles, the UD DoD created their architecture around what they term as pillars. Each pillar is a group of strategic resources and provides specific functions. The pillars are designed to protect the data pillar, as data was seen by the department as an equivalent of the protect surface to be secured. The architecture is thus data-centric, which is illustrated in Figure 6.

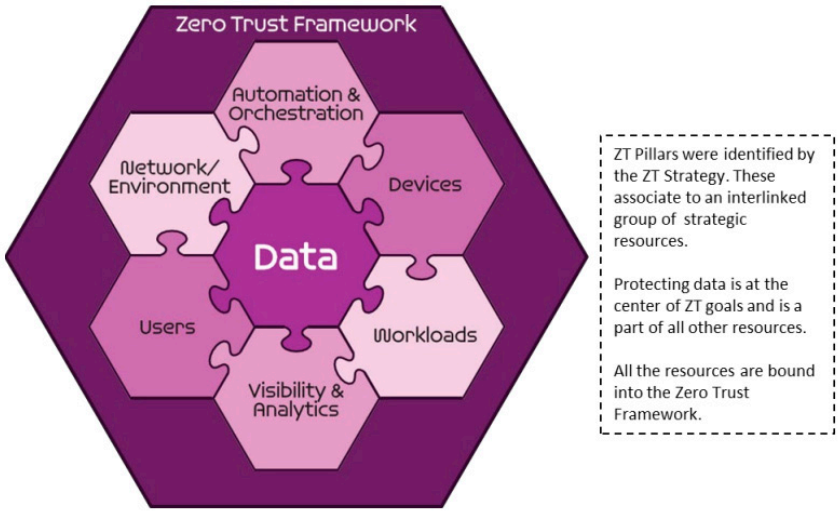

Figure 6. Zero Trust Pillars [24].

Other technical reports by the US Government exist, namely, the National Security Agency (NSA)'s "Embracing a Zero Trust Security Model" [25], the CISA's "Zero Trust

Maturity Model" [26] and the OMB's Federal Zero Trust Strategy: "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" [27].

However, a more rounded approach to zero trust came from the President's National Security Telecommunications Advisory Committee [7] in their report to the US President in February 2022. This technical report provides guidance around treating zero trust as a strategy, the continual journey of zero trust implementation, the focus on key zero trust foundational concepts and definitions, and the zero trust five-step process for the implementation of zero trust. The focus of zero trust implementations includes OT and IoT along with IT systems.

Further study of zero trust is being carried out by the Cloud Security Alliance. Examples include Defining the Zero Trust Protect Surface [2] and Mapping of Transactions Flows [15].

Though many definitions of zero trust are in existence, we treat the NSTAC report as the authoritative source of zero trust in its current form.

2.2. Reference Implementation

The zero trust five-step implementation process, as defined by the NSTAC report [7], is illustrated in Figure 7.

Figure 7. Zero Trust Five-Step Implementation Process [7].

Google has used the zero-trust five-step implementation process with Google Cloud and elaborated the journey in their document Applying Zero Trust on Google Cloud [28].

Google assembled a team to deliver the zero-trust journey. They started with definition of protect surface (Step 1) by identifying the DAAS elements and inventorying the elements. They created an inventory of signals, which fed into Step 4—*Create Zero Trust Policy*. Gap analysis was conducted to identify the current capability and the changes needed to reach the desired maturity of zero trust implementation. The gap analysis was conducted for the five pillars—identity, device, applications and workloads, network and data. Transaction flows were mapped (Step 2) between protect surfaces. Zero trust architecture (Step 3) was created to add Layer 7 context, which ensured that unauthorised users could not gain access to DAAS elements. Policies were created (Step 4) for each protect surface using Layer 7 dynamic context signals. Endpoints were monitored (Step 5) to ensure that network and other relevant technology stack were monitored and maintained.

2.3. Related Work

This section summarises the surveys that have been carried out by authors to apply zero trust (zero trust five-step implementation or otherwise) to smart home environments and IoT. We note that the relevant surveys are very few.

The authors of [29] survey the academic and practice-oriented literature to identify gaps that can explain the lack of widespread and holistic understanding of zero trust adoption. They explain that the increasing amount of digitisation and the number of digital devices (IoT, Bring Your Own Devices, etc.) leads to the ineffectiveness of perimeter security. Zero trust offers a novel solution to address the shortcomings of perimeter-based

security. The authors elaborate zero trust architecture, which consists of Policy Information Point (PIP), policy storage, Policy Enforcement Point (PEP) and zero trust engine. They also elaborate the core principles of zero trust. Their results demonstrate the influence of practice and academia on one another. Their review also demonstrates the implementation of zero trust in specific industries and IoT and considers the literature on architectural variations for IoT networks and smart home networks. Some of the literature demonstrates the applicability of zero trust to smart home infrastructures. They conclude that their survey results indicate unanswered questions that hinder zero trust's widespread adoption but that they have provided a framework to continue research in this space.

Zero trust architecture with PEP and zero trust engine as the main components for IoT and smart homes is studied by [29]. The authors discuss zero trust architecture and its common concepts, namely, enhanced governance of authentication systems, software defined perimeter (SDP), reverse proxies, and micro-segmentation. The authors discuss that owing to the innovativeness of zero trust, the existing security controls may not work. They conclude that the current research in zero trust is centred around small networks and is not spread uniformly across industry sectors. They also conclude that architecture for large scale networks is not very well researched and that the disadvantages of zero trust are not well understood.

The existing literature on zero trust architecture, including authentication, access control and trust assessment, is surveyed by [30]. A proposal is made for access control for smart homes based on zero trust, which in turn is based on context and continuous authentication. A trust evaluation mechanism uses edge computing for smart products for home IoT. The authors analyse survey results by identifying the advantages and disadvantages of architecture, authentication methods, access control methods and trust assessments. The results demonstrate that (a) user-to-device authentication is verified with biometrics acquired from smart wearables like smart watches and that (b) attribute-based access control provides fine grained access control. The authors conclude that their survey and the results have significance for migrating perimeter-based architectures to zero trust architecture.

Zero trust literature on IoT is surveyed by [31] based on a three-point approach and includes the following: (a) the principles of zero trust model; (b) the scope of zero trust in and challenges to address authentication, authorisation, data management, etc.; and (c) correlation between the latest developments in defence and the creation of resilience-preserving zero-trust models. The authors identify the essential components of zero trust as authentication, network segmentation, authorisation, encryption, network monitoring, PDP, PEP and Policy Administrator (PA) and highlight the difference between traditional security and zero trust. They look at the alignment between zero trust and MITRE ATT&CK framework. They use this alignment to highlight the risks posed by zero trust paradigm for the identified components. They then offer architectures to implement zero trust. The authors conclude that the survey reveals a number of zero trust systems that are cloud based which are implemented in centralised mode and in edge-based decentralised mode. They also conclude that zero trust is likely to reduce zero-day attacks and reduce the attack surface.

The authors of [32] survey access control solutions for IoT, including ones based onzero trust, which include PEP, Policy Definition Point (PDP) and PIPs as components of attribute-based access control (ABAC), which are also the components of zero trust access architecture as documented by NIST SP 800-207 [5]. They introduce various access control models, both centralised and distributed. The authors mention that due to the large-scale use cases of IoT network, access control between devices for which a distributed model works best is a critical security control. Blockchain is a suitable distributed technology that addresses this requirement. They conclude that their survey is expected to facilitate effective

guidance to enable understanding of access control solutions. They further conclude that the categorisation of access control models and approaches is important to industries and organisations, as it helps in selecting the right approaches and models for their needs.

Dhiman, Poonam et.al. [33] survey the literature on zero trust architecture framework, access control, evaluation methods for access control and trusted authentication. They compare traditional security and zero trust security paradigms and summarise key strengths and shortcomings of zero trust network approaches. Their literature review discusses how perimeter-based security is no longer trusted because of the prevalence of cloud applications and IoT networks. They design a taxonomy of zero trust features and compare zero trust cloud networking approaches. Their study reveals the importance of including zero trust principles in 5G/6G networks, as IoT devices interact among themselves while delivering services. They compare zero trust techniques used by IoT platform. The authors conclude that their survey emphasises the necessity of continuous authentication and authorisation based on context, behaviour and perceived threats, which are the tenets of zero trust.

The authors of [34] survey the literature that discusses digital signatures used in IoT environments. Digital signatures are used to address integrity, non-repudiation and authenticity to secure devices and data. Because of the heterogeneity of IoT devices, their small footprints and the limited compute power of IoT applications, they cannot consume more features than that supported by modern digital signatures. Working in zero-trust environments requires a Trusted Third Party (TTP) for key distribution, which is difficult for some applications and platforms. The authors survey digital signatures that have been recently designed and that address the challenges of IoT, which are (a) working in zero trust environment (b) privacy preserving and (c) functionality. They analyse the survey results to show that lightweight scenarios can use Keyless Digital Signature (KDS), Randomizable Digital Signature (RDS) and Double Authentication Preventing Digital Signature (DAPS) schemes, some of which can be implemented without TTP. These schemes also address insider attacks from reliably registered IoT entities but which try to maliciously access and compromise security and/or privacy. They compare advanced digital signatures that address zero trust management. They conclude that five of their selected digital signature schemes address security and privacy concerns while being compatible in zero trust environments.

Lone et.al. [35] survey the literature studying the various types of applications of IoT in cybersecurity, for example, using IoT devices on the edge network to detect threats and using IoT equipment to respond automatically to breaches by blocking access to network or systems. They discuss the essential characteristics of IoT, the architectural layers (applications, network and perceptions) and attacks against the layers. The authors discuss IoT issues like the lack of standardisation, network issues, scalability, availability and reliability, including security and privacy. They present a comparative study of vulnerable IoT devices. As current research trends, the authors discuss a potential solution using blockchain to implement zero trust tenets to address security and privacy issues of IoT devices. Blockchain can facilitate trust-less environments that supports zero trust's principle of "never trust, always verify". They conclude that the results of their survey indicate that although research on IoT and cybersecurity is extensive, there is lack of research on blockchain and zero trust, along with other challenges like lightweight security and decision-based security techniques.

Studies of various models of zero trust based on four principles (the principle of separating trust from location, the principle of least privilege, treating data and services as resources, and continuous monitoring and evaluation) are conducted by [36], whose authors make deductions by surveying zero trust literature. The models that they focus

on are—Cloud Security Alliance's Software Defined Perimeter, Google's BeyondTrust and NIST's Zero Trust Architecture. They present an overview of the various publications in the zero-trust space along with an abstract of the contents. The authors then expand on how zero trust is applied in cloud environments and IoT environments. They analyse the application of zero trust, explaining the definition of "trust" in the context of zero trust. The authors then conclude that the literature review indicates that implicit trust can no longer be relied upon.

Campbell, Mark [37] has studied zero-trust architecture and their paper includes references to the five-step implementation method, including defining the protect surface and not the attack surface. The author documents the software defined perimeter (SDP) defined by CSA, BeyondCorp, Adaptive Security Architecture (ASA), continuous adaptive risk and trust assessment (CARTA), zero trust network access (ZTNA) and Zero Trust eXtended (ZTX) to explain the various implementations of zero trust. The author studies the manner in which the principles of ZTA are potentially bent by vendors to suit their products. The author deduces that the adoption of zero trust is on the rise and enables security teams to make the shift from perimeter-based architecture to verification-based access environment where all access is by default denied. The author concludes that although zero trust solutions today are often based in marketing hype or as a technology or as a tool, the solutions will improve and mature over time and zero trust will become the security strategy standard as zero trust solutions become more automated and smarter.

The authors of [38] review NIST SP 800-207 and discuss the non-feasibility of zero trust architecture in real life. The authors argue that real life systems do not exist without trust. They point out that zero trust as a concept is not very well defined. The authors quote other researchers saying that the main tenets of zero trust are not practical and are challenging to implement technically, ill-advised and inconsistent. The authors argue that it may be economically and/or technically not possible for an organisation to uplift legacy systems to systems that are zero trust aware. They are concerned that zero trust architecture has gained momentum in recent times without the organisations' required understanding of zero trust architecture. The authors touch upon "certification" based on zero trust principles. They also conclude that the implementation of zero trust would be made easier by moving to cloud.

3. Literature Review

This section includes a literature review on the application of the zero trust five-step implementation process to (i) smart home devices and (ii) IoT.

3.1. Collection Methodology

This subsection elaborates on the methodology that was used in searching for and compiling the considered papers. We reviewed the literature that was published in the last five years that focused on zero trust to improve the security of smart devices. Papers, technical articles and conference papers were acquired via searches in the ACM Digital Library, IEEE Xplore and Google Scholar, using keywords like (i) "zero trust and IoT", (ii) "smart homes and zero trust", (iii) "zero trust architecture and IoT", (iv) "zero trust architecture and smart home devices", (v) "zero trust and smart home devices", (vi) "five step zero trust implementation process and smart homes", (vii) "5-step zero trust implementation process and smart homes", (viii) "protect surface and smart homes" and (ix) "five-step implementation process for zero trust and IoT". In addition, specific papers were added in our paper collection, based on the authors' personal knowledge.

These criteria were based on the elaboration of similarities between smart home devices and other IoT devices drawn by the authors of [8]. These similarities include limited

resources like the small hardware footprint and the software footprint, the applicable threats, and available security controls (lack of preventive controls and monitoring tools on the devices).

Finally, the papers were analysed based on their consideration of the five-step implementation process as elaborated in the NSTAC report [7], namely, (a) *Defining the Protect Surface*, (b) *Mapping Transactions Flows*, (c) *Build Zero Trust Architecture*, (d) *Create Zero Trust Policy* and (e) *Monitor and Maintain the network*.

3.2. Smart Home Devices

This section describes the survey conducted for the literature that has researched the implementation of zero trust for smart home devices.

To address security risks, access control solutions based on zero trust network architecture in smart home environments are researched by [39]. To meet zero trust principle of "never trust, always verify" for any new device introduced into the start home environment, the authors use mutual authentication between devices. They achieve this with the new device, generating a random number that is encrypted using quadratic residues and sending it to multiple devices for verification. The verification result and a hash value are sent by the verifying device. The authors claim that the basis of their device access solution is based on zero trust architecture. However, they do not include any zero trust architecture components like PEP, PDP PA. The authors conclude that their solution provides higher efficiency and better security than traditional methods.

The authors of [40] survey various techniques and approaches to implementing zero trust architecture based on NIST SP 800-207 [5] for smart home devices. The authors discuss communication layer encryption, software defined perimeter and micro-segmentation as essential components of zero trust architecture (ZTA). The logical components of their study include Policy Engine (PE), Policy Administrator (PA), PEP and trust algorithm. The ZTA implementation techniques include identity management, access control, logging and monitoring, consuming threat intelligence, continuous monitoring and maintenance, and compliance with various applicable and industry acknowledged standards. The authors study issues with traditional access control methods and the fulfilment of ZTA implementation techniques to address issues in conventional access control methods. They conclude that ZTA cannot be implemented with any technology or any defined architecture. They also conclude that successful realisation of ZTA can be achieved with a constant evaluation of trust in access control techniques by considering an organisation's context, threats and behavioural analytics.

da Silva et. al. [41] apply zero trust principles for access control like contextual awareness and user behaviour to smart home systems (SHS). Their system, Zero-Aware Smart Home (ZASH), uses zero trust architecture in the form of continuous authentication for smart home devices. Their paper is an extension of [42], written for the Department of Computer Science of the Federal University of Minas Gerais, Brazil, by the same set of authors and an additional author, Daniel F. Macedo. ZASH considers active and passive devices in SHS that collect user behaviour data. The authors consider user categories (like admin user and normal user) and state machine representation for server authorisation and client authorisation. An ontology manager contains user categories mapped to devices, and any request by a user category for a device is verified by a context manager. The authors conclude that ZASH protects users' privacy, blocks most attacks and ensures that all interactions are access controlled.

Challenges of privacy protection in smart homes that use IoT devices are a subject of research by [43]. The authors designed the Smart Home Privacy Protection (SHPP) standard framework that includes terminology, a reference framework and criteria for

guidelines. The relationship between various parts of the SHPP is explained with the reference framework to data managers. They discuss challenges related to privacy risk evaluation, demand diversity and privacy protection methodology. They propose that zero trust offers data security to address internal and external threats. The data manager monitors the ingress and egress of data and locates sensitive data and uses the zero-trust model to check for data compliance and identify any privacy issues. They conclude that the development of the SHPP has provided support for data security governance.

In summary, the surveyed literature applying zero trust to smart home environment is rather limited when compared to the papers on IoT devices. The researchers identified security issues with authentication and authorisation that were addressed with the zero trust principle of "never trust, always verify", which essentially addresses implicit trust. Usage of zero trust architecture (PEP, PDP, PIP, PA and PE) as defined by NIST was also used to address identified access control issues. However, the solutions defined and identified by the authors do not adopt the five-step implementation process. In the surveyed papers, the researchers applied Step 3, which is *Build Zero Trust architecture*, for which the authors used PEP, PIP, PA and PE [39–41,43].

3.3. IoT

This section describes the survey conducted for the literature that has researched the implementation of zero trust for IoT devices.

3.3.1. Addressing Security and Privacy Issues by Adopting Zero Trust

The authors of [44] study security and privacy issues related to IoT brought about by interconnected networks which bring in accessibility from anonymous users and the Internet. The authors discuss IoT/OT alignment, as IoT devices are used in OT environments. The reasons for security challenges include the non-standard nature of IoT devices, security requirements for the large amount of data generated by IoT, vulnerabilities developed in IoT devices over a period of time due to the difficulty of patching and upgrading them, the lack of security awareness in the IoT industry, and skills shortages. They discuss the importance of resiliency in strategy in protecting IoT assets, which in turn helps achieve resiliency in network. The operational resiliency and cyber resiliency can be achieved with zero trust. The authors discuss the elimination of implicit trust by zero trust using continuous verification of all assets. They further discuss the zero trust architecture and access to assets granted only after continuous evaluation. They conclude that the security of IoT devices remains a major concern. These concerns are addressed with respect to the resilience of these devices using technology and organisational policies.

The application of a blockchain's cross-chain to achieve value exchange or value transfer for IoT is a focus of study for [45]. The authors specifically focus on information and transactions related to the security of personal assets. Their framework is based on a virtual blockchain address generator and an authentication scheme using zero-knowledge proof. They introduce a protocol named cross-chain privacy protection, which is interactive. They further study the loyalty of each node of blockchain IoT in a zero trust environment and analyse the interaction protocol for security threats, including replay attack, man-in-the-middle attack, zero knowledge proofs and anonymity. The authors elaborate that the common blockchain addresses were replaced with virtual blockchain addresses for anonymity of the transactions. Virtual blockchain addresses provide anonymity for each of the transactions by not repeating the existing external addresses. The privacy of a user's transactions is secured with multiple layers of security, as a malicious actor can only reach a user's transaction by obtaining all block records by compromising the main chain. They conclude that their experiment shows that their

proposal demonstrates efficiency in terms of performance, as the time taken by the virtual address generation to anonymise external addresses is shorter than the transaction time. In terms of storage and transmission, the proofs are smaller in size. To effectively address IoT blockchain cross-chain privacy, multiple smart contracts that are compatible with existing framework standards can be used.

The authors of [46] state that IoT devices share information in a decentralised way which can be addressed with zero trust, as zero trust addresses authentication and information sharing in decentralised and untrusted environments and supports fairness and privacy awareness in information sharing. They propose an information sharing protocol that is blockchain based and which operates in zero trust environment. To address authentication for ad-hoc information sharers, their blockchain based authentication protocol has a mechanism that is based on smart contracts to detect and filter synthesised information, thus preventing unauthenticated users from sharing information. This approach reinforces fairness, which is one of the privacy principles, in processing information. The smart contract also removes dependencies on trusted third parties for sharing information. The authors conclude that their proposed protocol proves that it is universally composable. They additionally conclude that future research can be conducted to reduce latency in the protocol.

3.3.2. Addressing Access Control Issues by Adopting Zero Trust

The study of context aware attribute-based access control with minimised computational and memory footprint for commercial Internet of Things is a focus of [47]. The authors study the zero-trust architecture (PE, PA, PEP) and the trust algorithm, both from NIST, to calculate the level of certainty of the access request. They use attributes of the policy, calculate the level of certainty and compare it with the policy. To demonstrate different system behaviours, they run tests by varying the number of attributes of policy and by varying the evaluator types between attribute-based access control (ABAC) and the Trust-Level -Evaluation-Engine (TLEE). Variation in the evaluators, as they are additional, adds metrics related to the introduced penalty. In the end, the authors compare the various ABAC evaluators. They conclude that their test results obtained with Huawei's Smart Home test bed prove significant improvements in efficiency of their ABAC policy evaluator when compared with popular ABAC policy services.

Xiao et.al. [48], review research in context aware access control for IoT. They provide a background for zero trust principles and zero trust architecture (PA, PE and PEP). They review research in context aware access control (CAAC) using Role Based Access Control (RBAC)-based context schemes, ABAC-based context schemes and situation awareness in CAAC. They then research studies related to decision making in CAAC using risk and trust. They use patterns in context, risk and trust and apply them to zero trust. The authors conclude that context awareness is a well-researched area. The previous research in CAAC has commonalities that the authors apply to zero trust models and deployments. Areas for future research are identified. They conclude that, based on their findings, they intend to develop a language for access control policy for zero trust systems that is based on context and that is risk aware.

The authors of [49] study zero trust as a security paradigm and apply it to IoT. They study access control requirements that are compliant with zero trust principles and that apply to IoT. The access control requirements are security related metadata (subject properties, object properties and context properties), least privilege (granular access and ephemeral privileges) and dynamic decisions for access control and architectural aspects (policies, Policy Decision Point, and decentralised and distributed approaches). They review the start-of-the-art access control solutions for IoT, which are (a) capability-based access control,

(b) usage control, (c) role based access control and (d) attribute-based access control. Their studies demonstrate the lack of an access control framework for IoT that meets the zero trust access control requirements. They discuss the architectural requirements of access control, namely, PDP, PEP, PAP and PIP. The authors conclude that the access control requirements relate to both the adopted model and the implementation mechanism of the access control requirements. Their review of the existing literature demonstrates a lack of solutions which consider and implement solutions for all the requirements identified. They conclude that access control in IoT has significant issues that are not addressed by zero trust and that a completely different way of looking at the access control framework, including a redesign, is also required to enable a well-rounded adoption of zero trust in IoT environments.

Research on the challenges and potential enablers for zero trust architecture's automation and orchestration is studied by Cao et. al. [50]. The focus of the research is using AI for automation and orchestration, with IoT considered as a use case. The authors use NIST to model and define the control plane, the data plane and the data source using PA, PE and PEP. The authors discuss authentication and identity management as being more than just verification of user identity alone and including device authentication as well, along with cloud services. Access control methods are reviewed and discussed for IoT, namely, role based access control (RBAC), attribute-based access control (ABAC) and fine grained access control (FGAC). For physical layer authentication, they review a survey that classified IoT device features to detect devices. They review [51] for device-to-device authentication. They conclude that, with least privilege, ZTA solves security problems like lateral movement and insider attacks in perimeter-based security.

To determine the authenticity of any access requests made by an entity, by using a combination of zero trust access control with attribute-based access control is studied by [52]. The research is based on the zero-trust gateway, validating whether the access entity can request access to data. To achieve this, the study uses a list of approved and empanelled devices, IP addresses of the devices and the data that each entity can access. If these validations fail, the zero-trust gateway rejects the access request. The access request is validated not just with a request from the access entity but also by using additional parameters like an IP address. The authors conclude that their scheme secures confidentiality of sensitive data and that the scheme improves the detection and interception of access requests from malicious actors.

The authors of [53] study the application of zero trust principles to remote access to network and to edge. They discuss the solution for network remote access via the zero trust access control architecture of PEP, PDP, PE, trust algorithm etc., which is quite well aligned with the zero trust architecture described by NIST (NIST Special Publication 800-207 [5]). The solution for remote access to edge is via a Gateway Portal, which is aligned with one of the software defined perimeter [54] architectures promoted by Cloud Security Alliance. The authors conclude that fine grained access control can be achieved with this two-layered model.

3.3.3. Addressing Issues with Authorisation Using Zero Trust

In the interconnected world of IoT devices, the authors of [55] studied the security concerns around authorisation mechanisms related to IoT devices and proposed OUTSIDE (which is the name of the solution and is not an acronym), which is a zero trust IoT network designed to provide fine grained authorisation for IoT applications. The authors worked on a threat model and identified connection-based attacks and application impersonation attacks that can disrupt the IoT network. Their solution, OUTSIDE, verifies each packet generated by the IoT application. The authors used zero trust architecture with a Policy Manager (PM) and a Policy Administrator (PA). The PEP is a combination of server-

side application aware authorisation and capability verification. The architecture uses application aware authorisation policies to generate a token that is integrated into the application packet. The PM configures both client side and server-side policies with the designed attributes. The capability verification module verifies the packets to ensure that only authorised packets access the target service. The authors tested OUTSIDE and discussed how it prevents connection-based attacks and application impersonation attacks. They implemented and evaluated the results, and they concluded that OUTSIDE protects IoT devices from unauthorised interactions and unauthorised access requests.

The authors of [56] studied the impact of weak authorisation controls for IoT devices, which they attribute mainly to the heterogeneous nature of these devices, limited memory and limited computation, which creates a challenge for any access control solution. In the paper, the authors survey the literature on access control solutions for IoT and the progress made in this area. They look at policy-based architecture which is mapped to the zero trust architecture as defined by NIST [5]. The architecture consists of PAP, PEP, PDP, PIP and another component, a Policy Refinement Point (PRP). The authors also look at the OAuth architecture and a hybrid User Management Access (UMA) architecture. They infer that zero trust architecture could be used to secure IoT devices and data movement among users, applications, services and devices. They note that research is thin on how micro-segmentation helps realise zero trust in IoT. Based on their survey, the authors discuss the emerging research area related to IoT and zero trust architecture. Their study suggests applying micro-segmentation, monitoring of resources, verification or access requests and fine-tuning of access control policies can strengthen access control in IoT devices. They conclude that the integration of the OAuth architecture and the UMA architecture along with zero trust can be studied further.

Awan et. al. [57] researched integration and automation achieved with IoT that may provide an attack path for cyberattacks that impact services and people's lives. In their paper, they discuss the challenges of perimeter-based security for IoT devices. They say that perimeter-based security is not possible because of the nature of the distribution of IoT devices. They propose zero trust architecture (ZTA) as defined by NIST [5], using PE, PA and PEP. Along with ZTA, they propose using attribute-based access control (ABAC) to address security challenges in authentication and authorisation. They propose a framework which is named Zero trust and ABAC for IoT using Blockchain (ZAIB). Devices are registered on blockchain which provides anonymity with smart contracts along with device to device (D2D) communication. An InterPlanetary File System (IPFS) stores the properties of all IoT devices connected to the network, smart contracts and associated access policies. The authenticity of the policies is checked with the hashes of IPFS blocks. Access policies are enforced using a Policy Decision Point Oracle (PDPO). The trust engine calculates the trustworthiness of access requests. The authors conclude that their framework provides a mechanism to prevent cyberattacks with secure device-to-device communication by considering anomalous behaviour of access request, which is evaluated by the trust engine along with security levels of the network.

Provisioning of data using blockchain by utilising a publish/subscribe policy is a focus of study by [58]. The authors do not trust both the infrastructure and transactions carried out by the infrastructure. To ensure that a reliable network is available to IoT, the authors develop Amatista, a middleware built based on blockchain and that has two level mining that applies zero trust hierarchical management. The first level mining validates the infrastructure, and the second level mining validates the transactions. The authors conclude that the results of the evaluations demonstrate that the transactions executed by the infrastructure along with the infrastructure are validated by Amatista.

Along with its validation, Amatista demonstrates a satisfactory performance during the validation of transactions.

3.3.4. Addressing Security Issues with Zero Trust and Network Segmentation

The authors of [59] researched the usage of blockchain for network segmentation and device identification to implement zero trust principles for IoT devices. They used zero trust to centralise an access control engine for all policies and an agent on all endpoints for policy enforcement. Network segmentation is achieved with a segmentation gateway (SG) and a microcore and perimeter (MCAP) with a switch that connects to SG for centralised management of MCAPs. Any communication between devices is authenticated with the presence of smart contracts in the blockchain nodes of the partners. The authors concluded that multiple security concerns are addressed with their framework, including (a) the concern about device security, which is addressed with MCAPs for IoT devices and security services from the blockchain (partners); and (b) data security, which is enhanced with secure storage that has cryptography controls; and (c) data related to network administration is communicated securely, leading to comprehensive network management.

Li et. al. [12] focused on the difficulty of implementing network segmentation and zero trust policies in 5G-IoT networks due to the presence of millions of devices. The authors studied zero trust architecture and applied it to the IoT environment. They used blockchain enabled authentication leveraging digital signature-based authentication. This resulted in software defined perimeter using the blockchain enabled authentication and zero trust. The authors additionally used PEP, PA and PE to implement access control in IoT devices. The authors concluded that their study introduced zero trust by design for IoT and that device authentication is achieved with blockchain.

The authors of [60] proposed an architecture that is zero trust aligned, which uses software defined network to implement micro-segmentation in heterogeneous environments. They defined policies to grant/deny access requests between networks. This was combined with configuration management to generate and distribute certificates that are driven by defined policies. This action ensures that all participating resources have credentials to participate in interactions within networks. The authors concluded that their approach provides flexibility and adaptability to meet the complex requirements of industries without making any modifications to the application layer.

The shortcomings of IoT devices in terms of compatibility with 5G network is researched by [61], as 5G offers increased bandwidth, better speed and a higher capacity to handle more devices. The authors study the network slicing that is made possible in 5G networks and the ways of addressing security issues with IoT. Network slicing provides isolation but allows sharing of network functions. However, dynamic allocation is preferred, which addresses the issue. The authors propose zero trust architecture to address the risk of IoT devices being used as attack vector in 5G networks. They propose NIST's [5] zero trust architecture. The zero trust architecture principles that the authors apply to IoT devices are (a) continuous authentication and authorisation of IoT devices, (b) least privilege, (c) micro-segmentation and (d) continuous monitoring. They conclude that zero trust and network slicing present innovative solutions to security issues with IoT using 5G. However, they recommend that similar solutions should be applied to all situations and that organisations should identify the components that are important to them and apply zero trust and network slicing to secure them.

Enhancement of zero trust security for IoT with authentication using emerging technologies like blockchain and AI-driven anomaly detection is studied by [62]. The authors summarise the existing authentication methods for IoT with zero trust. The authentication methods include biometric, cryptography, identity and access management—federated and

otherwise, blockchain-based and physically unclonable functions (PUFs). These methods are evaluated against the background of the limitations of IoT, which include resource constraints and low battery life. The methods are matched with the benefits of emerging technologies. Finally, the researchers compare the evaluations with zero trust in the IoT environment, including (but not limited to) access control, micro-segmentation, data encryption, zero trust policies, integrating IoT security with zero trust principles and developing IoT environments that are aligned with zero trust principles. The authors conclude that their study provides an understanding of the changes taking place for IoT and in transitioning IoT to zero trust environment from a perimeter-based environment.

The challenges of perimeter-based security are discussed by the authors of [63], who discuss its being overtaken by cloud and edge computing, IIoT, etc. Access control in this challenging environment can be addressed with risk-based access control. The challenges of perimeter-based security can be addressed with zero trust networking, which can be achieved with zone-based network segmentation. The zones themselves are restricted with firewalls and risk-based access control policies. The authors devised a policy management framework, the Fuzzy Risk Framework for Zero Trust Networking (FURZE). They trialled the framework as a proof of concept. The results demonstrate that existing policies were successfully changed based on the calculated risk and that existing permissions were revoked. They concluded that their risk-based access control enforcement framework supports zero trust networking and can be extended to smart manufacturing.

3.3.5. Addressing Implicit Trust with Zero Trust

The authors of [64] studied the integration of zero trust concepts with IoT systems. They arrived at seven tenets based on access policies to secure communications and to reduce implicit trust. They proposed the zero trust authorisation requirements framework (ZT-ARF) and the zero trust score based authorisation framework (ZT-SAF). Their paper considers ZT-SAF as it is directly related to the implementation of zero trust authorisation principles as opposed to the authorisation policy models proposed in ZT-ARF. ZT-SAF is based on attribute-based access control and considers zero trust principles in reducing implicit trust, such that the confidence levels and the level of certainty of an access request can be determined based on calculations of contexts and the anomalies that may be present in the environment. The score engine of ZT-SAF considers the created sessions, states of context (environments, systems, and threats and logs), the actors who initiate the access request, the action to be performed by the actor and the resources to which access is requested. The framework algorithm considers the score and the threshold and via the access decision enforcement engine produces the result that either grants or denies an access request. Through their results they conclude that ZT-SAF provides a structured approach to develop authorisation models for zero trust systems.

Applying the zero trust principle of "never trust, always verify" to IoT is the focus of [65]. The authors focus their study on perimeter-based security for IoT and the impact of implicit trust in such an environment. The authors researched the applicability of physical, unclonable function-based device continuous authentication (PUFDCA) and the verification of device identity. The authors presented a threat analysis for the physical, unclonable function and concluded by saying that by using zero trust principles, like strong device identity, continuous authentication and least privilege, it is possible to reduce implicit trust along with providing secure communication without implicit trust.

The presence of implicit trust in IoT network that arises from perimeter-based security has been studied by the authors of [66]. In their paper, they propose continuous authentication between devices using blockchain. They implement initial authentication with cryptology based on ECC and include continual authentication with an operation that is

lightweight, such as XOR Hash. The authors discuss that blockchain is decentralised by nature and hence eliminates "trust". By eliminating trust in the environment, the authors propose that their research is consistent with ZTA. The authors conclude that the existing schemes require an authority that is trusted, which is inconsistent with ZTA.

The authors of [36] studied implicit trust and perimeter-based security with zero trust as a potential alternative to secure devices, including cloud and IoT devices. The authors discussed zero trust in the context of software defined perimeters (SDP) and the logical components of zero trust architecture (PE, PA PEP) as described by NIST [5], Google's BeyondCorp and the zero trust container architecture (ZTCA). The authors then introduced partial zero-trust solutions for IoT (and cloud) devices. They surveyed the body of literature that researched using blockchain based decentralised approach for authentication and as segmentation gateway. They also surveyed a body of literature that researched using SDP with IoT. The authors concluded that their survey confirms that zero trust aims to address implicit trust and aims at transforming implicit trust into explicit trust. They further concluded that their research introduced "trustbase", a novel concept serving as a foundation for both implicit and explicit trust.

The deployment and use of Security Attribute Based Dynamic Access Control (SADAC), a dynamic access control based on the security attributes for IoT, was researched by [67]. SADAC is based on the zero trust principle of granting access to resources once the requestor has been verified. SADAC makes dynamic decisions based on monitoring using a machine learning model and detection of anomalies. Security profiles for users and devices are built using a feature generator and an estimator module. Essentially, the authors use a machine learning model to identify features of users and devices and, using the estimator, model user and device behaviour. SADAC then identifies anomalies between expected behaviour and actual observed behaviour. If an anomaly is within the accepted limits, access is granted, or else it is denied. The authors concluded that SADAC is a viable option for IoT devices on wireless corporate environments.

The authors of [51] discuss critical infrastructures like smart grids, Industrial IoT and other physical systems and their associated security requirements. They consider NIST's definition of ZTA [5] and propose that the principles of ZTA are authentication and authorisation, which are considered as key principles, and discuss the role of implicit trust during the granting of access request by an entity to a resource. Based on their research, they propose that the authentication process is limited at the login stage. Once the entity is authenticated, the entity gains access within the environment. To address this implicit trust the authors proposed continuous authentication of device-to-device (D2D) communication using their proposed protocol called Lightweight Continuous Device-to-Device Authentication (LCDA). The protocol operates in two phases: (a) authentication to ensure that the devices mutually authenticate each other in a continuous manner and (b) continuous authentication to ensure that the devices do not talk to any unauthenticated devices. An informal security analysis of the LCDA protocol is performed and a formal security analysis of the protocol using Scyther Cremers [68] is conducted. They conclude that LCDA addresses both mutual authentication and continuous authentication phases with a channel state modification using a refreshed dynamic secret key. Attacks to secure D2D communication are addressed with an adaptation of a light-weight tuneable linear function. Conformation to security properties, such as integrity, confidentiality and resistance to protocol, is evaluated using the Scyther tool.

Perimeter-based security and its security concerns for cloud environments are studied by [69]. The authors discuss addressing these concerns with zero trust architecture as described by NIST [5]. To understand the current state of cloud security concerns, the authors survey the literature that discusses architecture and technical features of zero trust

architecture. They discuss the concepts of zero trust architecture and compare them with traditional security. Their description of zero trust architecture is centred around the core concept of origination of network threats being both internal and external. Thus, any access to the network is to be granted by a process of verification at a designed interval of time. They discuss zero trust maturity and comparative analysis of zero trust technologies as applicable to cloud network. They conclude by saying that zero trust offers case specific solutions to security issues that are applicable to network in cloud environments.

The authors of [70] studied using hardware device fingerprints to create identities for IoT authentication. The authors proposed a framework using a radio frequency-based device that generates identity using a Convolutional Neural Network (CNN). The framework includes the constraints that are related to resources of IoT devices. The hardware signature is captured as the Double-Sided Envelope Power Spectrum (EPS). The hardware signature includes only related device information. The framework supports one of the zero trust principles related to the authentication of devices. It is worth noting here that whilst the research does not include any other zero trust principles, it provides a good basis for extending it to zero trust architecture and implementation, using EPS as an identity in dynamic access control decisions. Using an identity in a resource constrained environment is a step forward in reducing implicit trust where devices may communicate with each other without any authentication in place.

The impact of rapidly changing technology, evolving business models, remote work, regulatory requirements, etc., on IoT is studied by [71]. The authors discuss the principles of zero trust that apply to IoT and the future directions for applying zero trust. The principles of zero trust the authors discuss are (a) least privilege, (b) risk alignment, (c) policy alignment and automation, (d) and asset-centric security. They further discuss the integration of zero trust with emerging technologies, enhancing resilience with continuous authentication and behaviour analytics, the application of zero trust to edge computing, the application of zero trust to supply chain and user-centric privacy controls. They conclude that as the threat landscape changes, traditional assumptions and security will be challenged. In the face of such challenges, zero trust offers a framework to mitigate such threats.

Szymanski, Ted H. [72] proposes that the paradigm of determinism provides hardware support in layer 3 and level 4 for the US NIST Zero Trust Architecture (ZTA) [18,19] (see Section 2). Specifically, all communications within a Deterministic Virtual Private Network (DVPN) are encrypted with quantum resistant long Quantum Safe keys (QS), and every network packet requires an Authorisation-Check (see Section 3). The author has built zero trust architecture (ZTA) with access control systems that are extended to individual resources, and access requests are ascertained for certainty with access rule-based policy engines. Software defined networking (SDN) control plane creates deterministic traffic flows (D-flows), that are verified and approved by the policy-engines. Cybersecurity is enhanced with the combination of the SDN control-plane, access control systems that are part of the ZTA, and an intrusion detection system. The packets in DVPN and packet headers are encrypted that secure the confidentiality of the data. Insecure layer three protocols are not implemented by deterministic packet switches (D-Switches). The author concludes that this paradigm improves national security by reducing cyberattacks on critical infrastructure.

3.3.6. Addressing Authentication Issues in Supply Chain with Zero Trust

Collier et. al. [73] used zero trust in supply chain management. Using a process adapted from Sarkis and Sundarraj 2000 [73], the authors arrived at a strategy to move from perimeter-based security to zero trust security. The propositions made by the authors are

closer to zero trust principles. They researched the impact of zero trust on other components in the ecosystem, the logical point at which the implementation of zero trust may not yield any returns, and the influence of zero trust on other factors like regulation and in turn the influence of other factors on zero trust implementation. The authors concluded that supply chain management in an organisation is critical to its competitiveness. Managing the supply chain addresses its risks, improves the quality of service and reduces disruptions. They provide exemplary cases which demonstrate that the usage of zero trust has secured organisations against safety and health concerns, from financial losses and from poor farming practices.

The semiconductor supply chain industry and the alignment of semiconductor development with zero trust is the focus of [74]. The authors focused on securing intellectual property because of IP's competitiveness and the security required around it. The authors mention that the confidentiality of proprietary information is impacted by malicious insiders. By using the zero-trust approach, they consider all the entities in the design process to not be trusted, avoiding any trust anchors in the process. They propose a framework, Assuring Confidential Electronic Design Against Insider Threats (ACED-IT), to address this supply chain risk. The authors elaborate the design process for a typical semiconductor product and threat model for insider threats. The system-on-chip design process involves many entities, including external entities. The authors consider the original system-on-chip specifications, the role of a system administrator and the tools that are used in software to be trusted. The ACED-IT tool creates an emulated environment that defines requirements for engineers to access tools and carry out required operations. The system administrators create accounts for engineers with required permissions. The software wrapper contains scripts to process the entire designs through system-on-chip (SoC) processes and to perform action logging. The authors evaluated the security of ACED-IT and concluded that their framework provides solutions to prevent intellectual property (IP) theft by applying zero trust principles.

Crowther, Kenneth G. [75] researched the shared responsibility between the original equipment manufacturers (OEM) of the different layers (perception layers, network layer, processing layers and application layers) of IIoT and how it can impact the security of these devices. The author discusses using zero trust to address the prevalent challenges with many OEMs and end users to improve security. The shared responsibility model considers the aspects of (a) segregation of responsibilities; (b) IIoT lifecycle management; (c) multi-layer supply chain defence; (d) security underpinning business requirements, i.e., security costs not overrunning the business requirements; and (e) compliance with standards like those of the NIST. ZTA reduces the attack surface and fosters faster detection of compromises, as it advocates monitoring of devices and the technology stack. The author concludes that ZTA and the shared responsibility model bring visibility to security requirements and secure the design and early detection of compromises to secure IIoT devices.

The applicability of zero trust for IoT as per the guidance from the NIST was studied by [76]. The authors studied the definition of "zero trust", the inconsistencies in NIST's guidance of ZTA and the lack of support of ZTA for legacy IT and OT. They mention that because of ZTA, delays will be introduced. Power grids are designed to operate with or without SCADA, and any downtime (due to cyber-attacks on OT) can be remediated manually by bringing up SCADA. They concluded that overlaying ZTA on a control system might break the established available coordination in the control systems. Hence, implementing zero trust would neither be advisable nor support the electric power grid.

A technology framework to facilitate zero trust for Industrial IoT (IIoT) was researched by [77]. The paper describes zero trust requirements for IIoT and proposes a three-step

framework for wireless IIoT. The steps include (a) creating security zones with artificial noise encoding based on physical layer, (b) industrial devices being authenticated within the security zones with physical fingerprints and (c) physical layer based key distribution to secure critical transaction flows within security zones. The authors conclude that the feasibility of the framework was demonstrated with the experiments conducted. The paper refers to zero trust five-step implementation and implements Step 1 for the protect surface by defining security zones and Step 2 by mapping transactions and securing the flows with physical layer based key distribution.

The influence of emerging technologies (like artificial intelligence/machine learning, blockchain, quantum computing, etc.) on zero trust has been researched by [78]. Joshi, Hrishikesh has discussed the latest developments in network connected IoT and emerging technologies and the resultant cyber threats due to the diversification of attack vectors. The author has discussed the White House Executive Order [79] that advocated using zero trust across US federal agencies to address the new threat landscape. They have used the six pillars of zero trust (data, device, application, identity, infrastructure and network) to study the influence and use of emerging technologies to improve security. The focus of this study is the trust algorithm used in implementation of zero trust environments, which is implemented using emerging technology like machine learning based trust evaluation, Bayesian network models, graph-based trust propagation, behaviour analysis and quantum inspired algorithms. This helps achieve risk evaluation of edge devices with (a) continuous device posture assessment, (b) device identity and authentication, (c) behaviour analysis and anomaly detection, (d) micro-segmentation and access control, (e) vulnerability scanning and prediction, and (f) innovation in identity and access management. The author discusses key points for implementing zero trust systems with (a) continuous adaptive trust, (b) intent-based security, (c) zero trust data security, (d) software defined perimeter (e) zero trust edge (f) secure access service edge (SASE), (g) zero trust as code, (h) AI-driven zero trust and (i) quantum-safe zero trust. The author concludes that as a part of this research they will deep-dive into each focus area and conduct experiments with a variety of use cases to further provide recommendations and assess the impact of these advancements on the zero trust posture of organisations.

In summary, zero trust has been used to address various security issues identified in IoT devices and environments. The following conclusions arise from the study of the literature:

- Addressing privacy issues in interconnected IoT devices has been researched, resulting in authors advocating zero trust for resiliency and for authentication [44–46].
- Reducing the risks of malicious access requests has been studied by authors, which has resulted in using zero trust to address context aware access control for IoT devices by calculating risk and trust values of the access requests made by entities [47,48].
- Requests for IoT devices from malicious actors have been a prevalent problem, as studied by various authors. Zero trust architecture with PEP, PDP, PIP, PA and PE have been applied by authors to address malicious access requests, authentication issues and the zero trust principle of "authentication before authorisation" [47–53].
- Authorisation issues related to IoT devices have been studied by researchers, and many have applied zero trust architecture to address the issues [55,56,58].
- Network segmentation to address lateral movement is one of the zero trust principles. Authors have used blockchain to achieve segmentation [12,59–63]. Network segmentation and credential management have been achieved without blockchain by [61]. Network security to support zero trust principles has been achieved with network slicing by [62].
- Issues with authentication and authorisation in IoT environments leading to implicit trust has been studied by authors who have included mutual authentication and zero trust to address the identified issues [64].

- Implicit trust is a byproduct of perimeter-based security, where an identity, when authenticated at the perimeter, is not verified when an access request is made. Researchers have studied this problem and provided proposals/solutions using zero trust principles [36,51,65–67,69,70]. Access control issues and addressing them with zero trust has been studied by [71]. Access control issues have been addressed using quantum safe keys by [72].
- Issues in supply chain leading to compromises of intellectual property (IP) and competitive edge has been researched by [73–75].
- The authors of [76] studied the applicability of zero trust to power grids to address cyber-attacks and concluded that zero trust does not address prevalent issues.
- Researchers have studied technology frameworks to facilitate zero trust and used zero trust to address the changing threat landscape [77,78].
- Researchers have studied network topology to address authentication and authorisation issues in IoT by including network segmentation to limit lateral movement [80–83].

Regarding the zero trust five step implementation process, authors and researchers have generally not considered Steps 1, 2, 4, and 5. One author has considered Steps 1 and 2 [77]. A few authors have considered Step 4 [62] and Step 5 [61], but these considerations were more from a perspective of including policies and continuous monitoring in their work than from a perspective of considering the adoption of the five-step implementation process.

4. Discussion and Open Issues

In today's environment, traditional perimeter-based security does not work well, as demonstrated by the breaches that regularly take place and the revenue generating business that data breaches have become [84,85]. Zero trust offers a viable alternative to address security by verifying the requestor of access before granting access to a resource.

Zero trust has gained a lot of attention in the past few years and continues to gain attention. As with any other computing environment, the tenets of zero trust are applicable to smart environments. However, the nuances of smart environments should be factored in. One of the nuances is the presence of disparate devices in such environments. For example, a smart television offers a very different functionality to a smart boiler. Any physical damage caused to a smart television may not result in damage to a smart boiler. When the zero trust five-step implementation process is applied to smart devices, each device could be considered a protect surface, as a device owner would want to secure each one of them [86]. In the above example the smart homeowner would want to secure both devices, the smart television and the smart boiler. The communication between these devices is also limited, but due to the centralising administration and integrating devices for visibility, for example, the development of smart home automation systems like Alexa, Google home, etc., device-to-device communication between a smart device and hubs has gained in prevalence [87]. Communications between smart devices and home clouds and applications continue. This development brings into focus the other steps of the zero trust implementation process, namely, mapping transaction flows, creating zero trust policies, and monitoring and maintaining the network. Nonetheless, as this survey has uncovered, the current state of the art in both academia and industry seems to omit these interactions and their respective flows.

Though research has been conducted to apply zero trust to smart homes and IoT, the whole paradigm of zero trust has not been investigated and focused on in the literature. For example, zero trust is not a technology or a tool or a standard or an architecture on its own [37]. Zero trust is a security strategy, which is described as a journey. Zero trust has its tenets in the form of pillars and cross-cutting capabilities [5,7,26] and it has its implementation process [7], which have not been considered in the past literature.

Existing research mainly considers identities as a part of the zero trust tenets/pillars and uses zero trust architecture to address security issues with identities. Zero trust has other pillars like devices, data, application and workloads and network [7,26].

Moreover, as discussed in Section 1 and summarised in Tables 2–7 and Tables 3–7, none of the surveyed papers researched the adoption of the zero trust five-step implementation process for smart environments. Researchers have studied the implementation of zero-trust architectures [12,36,39–41,47–50,53,55–57,75]. The authors identified security issues with authentication and authorisation that were addressed with the zero trust principle of "never trust, always verify", which essentially addresses implicit trust. The zero trust architecture (PEP, PDP, PIP, PA and PE) as defined by NIST, was also used to address identified access control issues, lateral movement, intellectual property and misinformation. There is one paper that has studied the applicability of the definitions of the protect surface and mapping transaction flows [77].

Applying NIST 800-207's zero trust core architecture components (PDP, PEP, PA, etc.) is a good starting point. However, the past literature has not considered protect surfaces. In the absence of a defined protect surface, the studies may have applied zero trust architecture to devices that are not critical to the environment [86]. It is worth mentioning here that in theory there is a possibility that any threat may materialise. However, when one considers the relevant risk, it is critical to know the likelihood of threat materialisation. Defining protect surfaces facilitates information acquisition at this level [2].

Step 2, which is mapping transaction flows, identifies the communication lines between devices. This helps in identifying device-to-device communication requirements. This information feeds into Step 4, which is creating zero trust policies for granting or denying access based on the communication that is required.

The past literature has highlighted the gap of not using preventive controls in smart home devices [8]. Though this gap cannot be closed by installing or including preventive controls in the firmware or hardware of devices, alternative ways of including zero-trust architecture and creating policies can be considered. Step 4, which is *Create Zero Trust Policies*, helps to reduce the attack surface by restricting communication, for example, between home automation systems and devices and between devices and their respective home clouds. The attack surface can further be reduced by consolidating all devices to communicate with one cloud and creating zero trust policies for each device. We saw the absence of studies related to Step 4 for smart homes and IoT. Restricting communication addresses the gap identified by [8], as this action is a preventive measure in securing smart devices.

Whilst preventive controls are important, it is equally relevant to monitor and maintain network, applications, devices and other components of the technical stack. Step 5—*Monitoring and Maintain the Network*—supports the security of smart environments in detecting malicious activities. It also helps in establishing a feedback loop for any ill-construed policies and further refinement of policies. Monitoring and maintaining network should not be construed literally to mean just the network. It includes network activities and application activities. This step gains prominence in the presence of smart automation systems and probable malicious activities carried out by malicious devices. As communication lines between devices increase with the introduction of automation devices, compromise of one device may lead to lateral movement between other available and connected devices. The relevance of monitoring traffic and logs has been demonstrated by the authors of [8]. Monitoring should not be construed to mean passive listening to device traffic. It can be extended to detecting the materialisation of threats as well. This gap is a consideration for a future research project.

Table 2. Summary of literature review for smart home environments.

Ref.	Defining the Protect Surface	Mapping of Transactions	Build Zero Trust Architecture	Create Zero Trust Policies	Monitor and Maintain the Network	Problem Sought to Be Addressed by Zero-Trust	Zero Trust Tenets Adopted
[39]	No	No	Yes	No	No	Security risks for smart home devices	• Mutual authentication between devices. • Zero trust architecture but without PDP, PEP, PA or PE
[40]	No	No	Yes	No	No	Issues with traditional access control methods	• Zero trust architecture (with PEP, PA and PE) • Micro-segmentation • Software Defined Perimeter
[41]	No	No	Yes	No	No	Privacy issues and issues with access control	• Zero trust architecture but without PDP, PEP, PA, or PE • Context aware access control
[43]	No	No	No	No	No	Privacy issues	Authors have proposed using zero trust to secure data but have not actually applied any zero trust principles
[44]	No	No	No	No	No	Issues related to security and privacy brought about by interconnected devices	• Operational resilience • Cyber resiliency • The authors have proposed that zero trust can help in cyber resilience and explained how it can be achieved • The authors have not explained how the ZTA can be implemented to address operational and cyber resiliency
[45]	No	No	No	No	No	Information and transactions related to security of personal assets and cross-chain privacy	The authors have studied the loyalty of each node of blockchain IoT in a zero trust environment but have not applied any zero trust principles
[46]	No	No	No	No	No	Sharing of information by IoT devices leading to privacy issues	Blockchain based authentication protocol

Table 3. Summary of literature review for IoT devices addressing access control issues.

Ref.	Defining the Protect Surface	Mapping of Transactions	Build Zero trust Architecture	Create Zero Trust Policies	Monitor and Maintain the Network	Problem Sought to Be Addressed by Zero Trust	Zero Trust Tenets Adopted
[47]	No	No	Yes	No	No	Low efficiency of attribute based access control policy servers	Zero trust architecture with PEP, PE and PA
[48]	No	No	Yes	No	No	Review of research in context aware access control for IoT	Zero trust architecture with PEP, PA and PE
[49]	No	No	Yes	No	No	Lack of access control framework for IoT that meets zero trust access control requirements	Zero trust architecture with PDP, PEP, PAP, PIP
[50]	No	No	Yes	No	No	Authentication and identity management as being more than just verification of user identity	• Zero trust architecture with PEP, PA, PE • Device authentication • Least privilege
[51]	No	No	No	No	No	Lateral movement and insider attacks in perimeter based security that are a result of access control issues	Least privilege
[52]	No	No	No	No	No	Authenticity of access requests	Zero trust gateway validating access requests to data
[53]	No	No	Yes	No	No	Remote access to network and to edge	Zero trust architecture with PEP, PDP, PE

Table 4. Summary of literature review for IoT devices addressing issues with authorisation.

Ref.	Defining the Protect Surface	Mapping of Transactions	Build Zero Trust Architecture	Create Zero Trust Policies	Monitor and Maintain the Network	Problem Sought to Be Addressed by Zero Trust	Zero Trust Tenets Adopted
[55]	No	No	Yes	No	No	Concerns around authorisation related to IoT devices	Zero trust architecture with PEP, PM, PA
[56]	No	No	Yes	No	No	Weak authorisation controls for IoT devices	Zero trust architecture with PAP, PEP, PDP, PIP, PRP
[57]	No	No	Yes	No	No	Security challenges in authentication and authorisation	Zero trust architecture with PEP, PE, PA
[58]	No	No	No	No	No	Lack of trust with infrastructure and the transactions carried out by infrastructure	Zero trust hierarchical management using blockchain and two level mining. This however, is not zero trust tenet

Table 5. Summary of literature review for IoT devices addressing security issues with zero trust and network segmentation.

Ref.	Defining the Protect Surface	Mapping of Transactions	Build Zero Trust Architecture	Create Zero Trust Policies	Monitor and Maintain the Network	Problem Sought to Be Addressed by Zero Trust	Zero Trust Tenets Adopted
[59]	No	No	No	No	No	Lack of centralised access control engine for all policies	• Network segmentation • Cryptography controls for secure storage for data
[12]	No	No	Yes	No	No	Challenges with implementation of network segmentation and zero trust policies due to the presence of millions of 5G-IoT devices	• Zero trust architecture with PEP, PA, PE • SDP using blockchain enabled authentication and zero trust.
[60]	No	No	No	Yes	No	Challenges related to implementation of micro-segmentation in heterogeneous networks	Polices to grant/deny access requests between networks
[61]	No	No	No	No	Yes	Challenges related to the compatibility of IoT devices with 5G network and the resulting security issues	• Continuous authentication and authorisation of IoT devices • Least privilege • Micro-segmentation • Continuous monitoring
[62]	No	No	No	Yes	No	Enhancement of zero trust security for IoT using emerging technology	• Access control • Micro-segmentation • Data encryption • Zero trust policies
[63]	No	No	No	No	No	Challenges of perimeter based security	• Risk based access control

Table 6. Summary of literature review for IoT devices addressing implicit trust.

Ref.	Defining the Protect Surface	Mapping of Transactions	Build Zero Trust Architecture	Create Zero Trust Policies	Monitor and Maintain the Network	Problem Sought to Be Addressed by Zero Trust	Zero Trust Tenets Adopted
[64]	No	No	No	No	No	Implicit trust	Assessing confidence levels and the level of certainty for access requests
[65]	No	No	No	No	No	Perimeter based security and the impact of implicit trust in such an environment	• Strong device identity • Continuous authentication • Least privilege
[66]	No	No	No	No	No	Perimeter based security and the impact of implicit trust in such an environment	• Continuous authentication using blockchain • Eliminating trust with the decentralised nature of blockchain
[36]	No	No	Yes	No	No	Perimeter based security and the impact of implicit trust in such an environment	• Authentication and segmentation gateway with decentralised approach of blockchain
[67]	No	No	No	No	No	Inadequate verification of access requestor	Assessing the gap between expected and observed behaviour of users and devices before granting access
[51]	No	No	No	No	No	Role of implicit trust during granting of access request by an entity to a resource	• Continuous authentication of device-to-device communication • Mutual authentication
[69]	No	No	No	No	No	Perimeter based security and its security concerns for cloud environments	Access to network to be granted by a process of verification at a designed interval of time
[70]	No	No	No	No	No	Challenges related to authentication in a resource constrained environment like IoT	Using hardware device fingerprints to create identities for IoT authentication
[71]	No	No	No	Yes	No	Changing threat landscape	• Least privilege • Risk alignment • Policy alignment and automation • Asset-centric security
[72]	No	No	No	No	No	Cyberattacks on critical infrastructure	• Encryption of communication • Access control systems • Intrusion detection system

Table 7. Summary of literature review for IoT—issues in supply chain.

Ref.	Defining the Protect Surface	Mapping of Transactions	Build Zero Trust Architecture	Create Zero Trust Policies	Monitor and Maintain the Network	Problem Sought to Be Addressed by Zero Trust	Zero Trust Tenets Adopted
[73]	No	No	No	No	No	Security issues in supply chain management	Moving away from perimeter-based security, which is not one of the tenets of zero trust
[74]	No	No	No	No	No	Securing intellectual property	Least privilege
[75]	No	No	Yes	No	No	Shared responsibility between original equipment manufacturers for different layers	Zero trust architecture but without PDP, PEP, PA or PE
[76]	No	No	No	No	No	Lack of support of ZTA for IT and OT	The authors have expressed views that zero trust is not advisable in electric power grids
[77]	Yes	Yes	No	No	No	Technology framework to facilitate zero trust for IIoT	• Defining protect surface by defining security zones • Mapping of transaction flows
[78]	No	No	No	No	No	Cyber threats due to diversification of attack vectors	• Trust algorithm for risk based access control

5. Conclusions

The proliferation of smart home devices and IoT has come with security risks. With the growing number of compromises, the industry is under pressure to demonstrate steps being taken to secure these devices. Zero trust has emerged as a promising alternative. Vendors of smart environments can demonstrate their commitment to security by using the zero trust five-step implementation process to create preventive controls and detective controls to secure smart environments and secure the privacy of the data generated and consumed by smart devices. This paper surveys the zero trust five-step implementation process as applied to smart environments.

Zero trust is not a technology or a tool or just an architecture. It is a strategy and is implemented with the zero trust five-step implementation process. As our survey reveals, most papers have studied the implementation of zero trust architecture, which is Step 3—*Build a Zero Trust Architecture*. In particular, the existing research has not studied the zero trust five-step implementation process for smart homes and IoT. Through our survey we have highlighted the reasons to use this process, as zero trust is not just about zero trust architecture. Its principle of "never trust, but verify", least privilege, and the assumption of breaches are achieved with Step 3, along with the other steps in the zero trust five-step implementation process that have been described. Whilst Step 1 has less relevance in smart environments due to the disparity of smart devices and each device being a protect surface in its own right, Step 2, Step 3, Step 4 and Step 5 can be addressed by vendors. Researchers and vendors can look towards providing a mechanism for (a) identifying the interfaces between the devices; (b) architecting solutions to segment network, identities and data; (c) creating access policies—both network and applications; and (d) monitoring the connections to ensure that compromises are prevented and that when they materialise they are detected in near-real time. Finally, as discussed in this paper, the research can be extended with works that demonstrate the inclusion of these steps in not just reducing the attack surface by creating tightly controlled policies, but also with monitoring applications and network traffic for malicious activities.

Author Contributions: Conceptualization, S.K.; methodology, S.K. and A.M.; formal analysis, S.K.; writing—original draft preparation, S.K.; writing—review and editing, S.K., A.M. and S.V.; visualization, S.K. and A.M.; supervision, A.M. and S.V.; validation, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

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

Abbreviations

Abbreviation	Definition
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PE	Policy Engine
PA	Policy Administrator
ZTA	Zero-Trust Architecture
PIP	Policy Information Point
PAP	Policy Administrator Point
OT	Operational Technology
IoT	Internet of Things

IT	Information Technology
IIoT	Industrial Internet of Things
SDP	Software-Defined Perimeter

References

1. Juniper. The Rise of Zero Trust | White Paper. 2019. Available online: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/security/the-rise-of-zero-trust.pdf (accessed on 20 August 2024).
2. CloudSecurityAlliance. Defining the Zero Trust Protect Surface. Available online: https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface (accessed on 12 July 2024).
3. Amazon and Google. Amazon, Google Back Global Cybersecurity Standard for Smart Home Devices. 2024. Available online: https://www.pymnts.com/cybersecurity/2024/amazon-google-back-global-cybersecurity-standard-for-smart-home-devices/ (accessed on 8 September 2024).
4. The White House. *Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers*; The White House: Washington, DC, USA, 2023.
5. NIST. SP 800-207. 2020. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed on 14 August 2024).
6. Kerman, A. Zero Trust Cybersecurity: 'Never Trust, Always Verify'. 2020. Available online: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify (accessed on 20 September 2024).
7. CISA. Nstac Report to the President. NSTAC Report to the President on Communications Resiliency. Available online: https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20(10-17-22).pdf (accessed on 12 September 2024).
8. Kulkarni, S.; Mylonas, A.; Vidalis, S. Preventing and Detecting Malware in Smart Environments. The Smart Home Case. In *Malware: Handbook of Prevention and Detection*; Gritzalis, D., Choo, K.R., Patsakis, C., Eds.; Springer Nature: Cham, Switzerland, 2025; pp. 395–410.
9. Mylonas, A.; Gritzalis, D.; Tsoumas, B.; Apostolopoulos, T. A qualitative metrics vector for the awareness of smartphone security users. In *Trust, Privacy, and Security in Digital Business, Proceedings of the 10th International Conference, TrustBus 2013, Prague, Czech Republic, 28–29 August 2013*; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2013; pp. 173–184.
10. Mylonas, A.; Kastania, A.; Gritzalis, D. Delegate the smartphone user? Security awareness in smartphone platforms. *Comput. Secur.* **2013**, *34*, 47–66. [CrossRef]
11. Allen, A.; Mylonas, A.; Vidalis, S.; Gritzalis, D. Smart homes under siege: Assessing the robustness of physical security against wireless network attacks. *Comput. Secur.* **2024**, *139*, 103687. [CrossRef]
12. Li, S.; Iqbal, M.; Saxena, N. Future industry internet of things with zero-trust security. *Inf. Syst. Front.* **2024**, *26*, 1653–1666. [CrossRef]
13. Blog, J.K. Protect Surface and Attack Surface. Available online: https://www.illumio.com/blog/john-kindervag-zero-trust-government-agencies#:%20:text=Define%20your%20protect%20surface:%20You,element,%20service,%20or%20asset (accessed on 20 October 2024).
14. Assistants, H. List of Available Integrations with Home Assistant. Available online: https://www.home-assistant.io/integrations/ (accessed on 21 October 2024).
15. CSA. Map the Transaction Flows for Zero Trust. Available online: https://cloudsecurityalliance.org/artifacts/map-the-transaction-flows-for-zero-trust (accessed on 23 October 2024).
16. Marsh, S.P. Formalising Trust as a Computational Concept. 1994. Available online: https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf (accessed on 15 August 2024).
17. Herzog, P.; Barceló, M.; Chiesa, R.; Ivaldi, M.; Guasconi, F.; Sensibile, F.; Rudolph, H.; Brown, A.; Mitchell, R.; Feist, R.; et al. Open-Source Security Testing Methodology Manual. 2003. Available online: https://www.isecom.org/OSSTMM.3.pdf (accessed on 20 September 2024).
18. Herzog, P. OSSTMM 3.0. 2010. Available online: https://dl.packetstormsecurity.net/papers/unix/osstmm.pdf (accessed on 24 October 2024).
19. Spencer, M.; Pizio, D. The de-perimeterisation of information security: The Jericho Forum, zero trust, and narrativity. *Soc. Stud. Sci.* **2024**, *54*, 655–677. [CrossRef]
20. Jericho. Forum, "Jericho Forum™ Commandments,". Available online: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf (accessed on 20 October 2024).
21. Assunção, P. A zero trust approach to network security. In Proceedings of the Digital Privacy and Security Conference, Porto, Portugal, 16 January 2019.
22. Kindervag, J.; Balaouras, S. No more chewy centers: Introducing the zero trust model of information security. *Forrester Res.* **2010**, *3*, 1–16.

23. Kindervag, J. Build Security into Your Network's DNA: The Zero Trust Network Architecture. 2012. Available online: https://www.forrester.com/report/Build-Security-Into-Your-Networks-DNA-The-Zero-Trust-Network-Architecture/RES57047 (accessed on 31 January 2025).
24. U.S.D. of Defense. Department of Defense (DoD) Zero Trust Reference Architecture. 2022. Available online: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf (accessed on 20 January 2025).
25. NSA. Embracing a Zero Trust Security Model. 2021. Available online: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF (accessed on 6 February 2025).
26. CISA. Zero Trust Maturity Model. 2024. Available online: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (accessed on 6 February 2025).
27. Office Of MANAGEMENT and BUDGET. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. 2022. Available online: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf (accessed on 6 February 2025).
28. Google. Zero Trust Five Step Implementation Process. 2023. Available online: https://services.google.com/fh/files/misc/zt_implem_guide_800_27.pdf (accessed on 13 June 2025).
29. Buck, C.; Olenberger, C.; Schweizer, A.; Völter, F.; Eymann, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Comput. Secur.* **2021**, *110*, 102436. [CrossRef]
30. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A survey on zero trust architecture: Challenges and future trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274. [CrossRef]
31. Azad, M.A.; Abdullah, S.; Arshad, J.; Lallie, H.; Ahmed, Y.H. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet Things* **2024**, *27*, 101227. [CrossRef]
32. Trabelsi, R.; Fersi, G.; Jmaiel, M. Access control in Internet of Things: A survey. *Comput. Secur.* **2023**, *135*, 103472. [CrossRef]
33. Dhiman, P.; Saini, N.; Gulzar, Y.; Turaev, S.; Kaur, A.; Nisa, K.U.; Hamid, Y. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors* **2024**, *24*, 1328. [CrossRef]
34. Alagheband, M.R.; Mashatan, A. Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: Taxonomy, capabilities, and objectives. *Internet Things* **2022**, *18*, 100492. [CrossRef]
35. Lone, A.N.; Mustajab, S.; Alam, M. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Secur. Priv.* **2023**, *6*, e318. [CrossRef]
36. Kang, H.; Liu, G.; Wang, Q.; Meng, L.; Liu, J. Theory and Application of Zero Trust Security: A Brief Survey. *Entropy* **2023**, *25*, 1595. [CrossRef]
37. Campbell, M. Beyond zero trust: Trust is a vulnerability. *Computer* **2020**, *53*, 110–113. [CrossRef]
38. Michael, J.B.; Dinolt, G.C.; Cohen, F.B.; Wijesekera, D. Can You Trust Zero Trust? *Computer* **2022**, *55*, 103–105. [CrossRef]
39. Liu, P.; Xu, Y.; Wang, Y.; Fan, P. A Blockchain Empowered Smart Home Access Scheme Based on Zero-trust Architecture. *J. Electr. Syst.* **2024**, *20*, 43–49. [CrossRef]
40. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero trust architecture (zta): A comprehensive survey. *IEEE Access* **2022**, *10*, 57143–57179. [CrossRef]
41. Da Silva, G.R.; Santos, A.L.D. Adaptive Access Control for Smart Homes Supported by Zero Trust for User Actions. *IEEE Trans. Netw. Serv. Manag.* **2024**. [CrossRef]
42. Da Silva, G.R.; Macedo, D.F.; Santos, A.L.D. Zero trust access control with context-aware and behavior-based continuous authentication for smart homes. In *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*; Sociedade Brasileira de Computação: Porto Alegre, Brazil, 2021.
43. Liu, D.; Wu, C.; Yang, L.; Zhao, X.; Sun, Q. The development of privacy protection standards for smart home. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9641143. [CrossRef]
44. Prasad, S.G.; Badrinarayanan, M.K.; Sharmila, V.C. Internet of Things (IoT): Resilience as a key Parameter in Security Management. In Proceedings of the 2023 4th IEEE Global Conference for Advancement in Technology (GCAT), Bengaluru, India, 6–8 December 2023.
45. Yang, Y.; Bai, F.; Yu, Z.; Shen, T.; Liu, Y.; Gong, B. An Anonymous and Supervisory Cross-Chain Privacy Protection Protocol for Zero-Trust IoT Application. *ACM Trans. Sens. Netw.* **2024**, *20*, 1–20. [CrossRef]
46. Liu, Y.; Hao, X.; Ren, W.; Xiong, R.; Zhu, T.; Choo, K.-K.R.; Min, G. A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. *IEEE Trans. Comput.* **2022**, *72*, 501–512. [CrossRef]
47. Dimitrakos, T.; Dilshener, T.; Kravtsov, A.; La Marra, A.; Martinelli, F.; Rizos, A.; Rosetti, A.; Saracino, A. Trust aware continuous authorization for zero trust in consumer internet of things. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2021.
48. Xiao, S.; Ye, Y.; Kanwal, N.; Newe, T.; Lee, B. SoK: Context and risk aware access control for zero trust systems. *Secur. Commun. Netw.* **2022**, *2022*, 7026779. [CrossRef]

49. Colombo, P.; Ferrari, E.; Tümer, E.D. Access Control Enforcement in IoT: State of the art and open challenges in the Zero Trust era. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021.
50. Cao, Y.; Pokhrel, S.R.; Zhu, Y.; Doss, R.; Li, G. Automation and orchestration of zero trust architecture: Potential solutions and challenges. *Mach. Intell. Res.* **2024**, *21*, 294–317. [CrossRef]
51. Shah, S.W.; Syed, N.F.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). *Comput. Secur.* **2021**, *108*, 102351. [CrossRef]
52. Huang, W.; Xie, X.; Wang, Z.; Feng, J.; Han, G.; Zhang, W. ZT-Access: A combining zero trust access control with attribute-based encryption scheme against compromised devices in power IoT environments. *Ad Hoc Netw.* **2023**, *145*, 103161. [CrossRef]
53. Federici, F.; Martintoni, D.; Senni, V. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics* **2023**, *12*, 566. [CrossRef]
54. Cloud. Security. Alliance. Software Defined Perimeter. 2022. Available online: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2 (accessed on 18 March 2025).
55. Zhang, H.; Wang, Q.; Zhang, X.; He, Y.; Tang, B.; Li, Q. Toward Zero-Trust IoT Networks via Per-Packet Authorization. *IEEE Commun. Mag.* **2024**, *62*, 90–96. [CrossRef]
56. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors* **2023**, *23*, 1805. [CrossRef]
57. Awan, S.M.; Azad, M.A.; Arshad, J.; Waheed, U.; Sharif, T. A blockchain-inspired attribute-based zero-trust access control model for IoT. *Information* **2023**, *14*, 129. [CrossRef]
58. Samaniego, M.; Deters, R. Zero-trust hierarchical management in IoT. In Proceedings of the 2018 IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, USA, 2–7 July 2018.
59. Dhar, S.; Bose, I. Securing IoT devices using zero trust and blockchain. *J. Organ. Comput. Electron. Commer.* **2021**, *31*, 18–34. [CrossRef]
60. Zanasi, C.; Russo, S.; Colajanni, M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Netw.* **2024**, *156*, 103414. [CrossRef]
61. De Almeida, A.O.; Salvador, L.R. Securing IoT Devices: ZTA Principles and Network Slicing. In Proceedings of the 2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY), Pula, Croatia, 19–21 September 2024.
62. Bast, C.; Yeh, K.-H. Emerging Authentication Technologies for Zero Trust on the Internet of Things. *Symmetry* **2024**, *16*, 993. [CrossRef]
63. Vanickis, R.; Jacob, P.; Dehghanzadeh, S.; Lee, B. Access control policy enforcement for zero-trust-networking. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018.
64. Ameer, S.; Gupta, M.; Bhatt, S.; Sandhu, R. 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, New York, NY, USA, 8–10 June 2022.
65. Alshomrani, S.; Li, S. PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 235–244. [CrossRef]
66. Meng, L.; Huang, D.; An, J.; Zhou, X.; Lin, F. A continuous authentication protocol without trust authority for zero trust architecture. *China Commun.* **2022**, *19*, 198–213. [CrossRef]
67. García-Teodoro, P.; Camacho, J.; Maciá-Fernández, G.; Gómez-Hernández, J.A.; López-Marín, V.J. A novel zero-trust network access control scheme based on the security profile of devices and users. *Comput. Netw.* **2022**, *212*, 109068. [CrossRef]
68. DeCusatis, C.; Liengtiraphan, P.; Sager, A.; Pinelli, M. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. In Proceedings of the 2016 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 18–20 November 2016.
69. Sarkar, S.; Choudhary, G.; Shandilya, S.K.; Hussain, A.; Kim, H. Security of zero trust networks in cloud computing: A comparative review. *Sustainability* **2022**, *14*, 11213. [CrossRef]
70. Elmaghbub, A.; Hamdaoui, B. Domain-Agnostic Hardware Fingerprinting-Based Device Identifier for Zero-Trust IoT Security. *arXiv* **2024**, arXiv:2402.05332. [CrossRef]
71. Ismail, M.; El-Gawad, A.F.A. Revisiting Zero-Trust Security for Internet of Things. *Sustain. Mach. Intell. J.* **2023**, *3*, 1–8. [CrossRef]
72. Szymanski, T.H. The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access* **2022**, *10*, 45893–45930. [CrossRef]
73. Collier, Z.A.; Sarkis, J. The zero trust supply chain: Managing supply chain risk in the absence of trust. *Int. J. Prod. Res.* **2021**, *59*, 3430–3445. [CrossRef]
74. Stern, A.; Wang, H.; Rahman, F.; Farahmandi, F.; Tehranipoor, M. ACED-IT: Assuring Confidential Electronic Design Against Insider Threats in a Zero-Trust Environment. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2021**, *41*, 3202–3215. [CrossRef]

75. Crowther, K.G. Blending Shared Responsibility and Zero Trust to Secure the Industrial Internet of Things. *IEEE Secur. Priv.* **2024**, *22*, 96–102. [CrossRef]
76. Swearingen, M.T.; Michael, J.B.; Weiss, J.; Radvanovsky, R. Resilient Without Zero Trust. *Computer* **2024**, *57*, 120–122. [CrossRef]
77. Lei, W.; Pang, Z.; Wen, H.; Hou, W.; Li, W. Physical Layer Enhanced Zero-Trust Security for Wireless Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2024**, *20*, 4327–4336. [CrossRef]
78. Joshi, H. Emerging Technologies Driving Zero Trust Maturity Across Industries. *IEEE Open J. Comput. Soc.* **2024**, *6*, 25–36. [CrossRef]
79. The White House. *Improving the Nation's Cybersecurity*; The White House: Washington, DC, USA, 2021. Available online: https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/executive-order-14028 (accessed on 21 September 2024).
80. Nahar, N.; Andersson, K.; Schelén, O.; Saguna, S. A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks. *IEEE Access* **2024**, *12*, 94753–94764. [CrossRef]
81. Son, S.; Kwon, D.; Lee, S.; Kwon, H.; Park, Y. A Zero-Trust Authentication Scheme With Access Control for 6G-enabled IoT Environments. *IEEE Access* **2024**, *12*, 154066–154079. [CrossRef]
82. HKholidy, A.; Disen, K.; Karam, A.; Benkhelifa, E.; Rahman, M.A.; Rahman, A.-U.; Almazyad, I.; Sayed, A.F.; Jaziri, R. Secure the 5G and beyond networks with zero trust and access control systems for cloud native architectures. In Proceedings of the 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 4–7 December 2023.
83. Nie, S.; Ren, J.; Wu, R.; Han, P.; Han, Z.; Wan, W. Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment. *Sensors* **2025**, *25*, 550. [CrossRef]
84. Alliance, Cyber Management. Biggest Cyber Attacks, Ransomware Attacks, Data Breaches of March 2025. 2025. Available online: https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-ransomware-attacks-data-breaches-of-march-2025 (accessed on 21 April 2025).
85. Kosinski, M.; Holdsworth, J. What is ransomware as a service (RaaS)? 2024. Available online: https://www.ibm.com/think/topics/ransomware-as-a-service (accessed on 1 April 2025).
86. Kindervag, J. Define a Protect Surface to Massively Reduce Your Attack Surface. 2018. Available online: https://www.paloaltonetworks.com/blog/2018/09/define-protect-surface-massively-reduce-attack-surface/ (accessed on 22 April 2025).
87. Gartner. Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022. Available online: https://www.gartner.com/en/newsroom/press-releases/2014-09-08-gartner-says-a-typical-family-home-could-contain-more-than-500-smart-devices-by-2022 (accessed on 22 April 2025).