Journal of Computer and Communications, 2024, 12, 252-282
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security

Fazal Raheman

Blockchain 5.0 Ltd Kesklinnalinnaosa, Tallinn, Estonia
Email: drfazal@bc5.eu

How to cite this paper: Raheman, F. (2024) From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. *Journal of Computer and Communications*, **12**, 252-282.
https://doi.org/10.4236/jcc.2024.123016

Received: January 23, 2024
Accepted: March 26, 2024
Published: March 29, 2024

Abstract

Cybercrime is projected to cost a whopping $23.8 Trillion by 2027. This is essentially because there's no computer network that's not vulnerable. Fool-proof cybersecurity of personal data in a connected computer is considered practically impossible. The advent of quantum computers (QC) will worsen cybersecurity. QC will be a boon for data-intensive industries by drastically reducing the computing time from years to minutes. But QC will render our current cryptography vulnerable to quantum attacks, breaking nearly all modern cryptographic systems. Before QCs with sufficient qubits arrive, we must be ready with quantum-safe strategies to protect our ICT infrastructures. Post-quantum cryptography (PQC) is being aggressively pursued worldwide as a defence from the potential Q-day threat. NIST (National Institute of Standards and Technology), in a rigorous process, tested 82 PQC schemes, 80 of which failed after the final round in 2022. Recently the remaining two PQCs were also cracked by a Swedish and a French team of cryptographers, placing NIST's PQC standardization process in serious jeopardy. With all the NIST-evaluated PQCs failing, there's an urgent need to explore alternate strategies. Although cybersecurity heavily relies on cryptography, recent evidence indicates that it can indeed transcend beyond encryption using Zero Vulnerability Computing (ZVC) technology. ZVC is an encryption-agnostic absolute zero trust (AZT) approach that can potentially render computers quantum resistant by banning all third-party permissions, a root cause of most vulnerabilities. Unachievable in legacy systems, AZT is pursued by an experienced consortium of European partners to build compact, solid-state devices that are robust, resilient, energy-efficient, and with zero attack surface, rendering them resistant to malware and future Q-Day threats.

Keywords

Cybersecurity, Quantum Computers, Post Quantum Cryptography, Q-Day, Zero Trust

1. Introduction

Cybercrime is predicted to skyrocket to become over $23.8 Trillion industry by 2027 [1]. A hack attack occurs every 39 seconds, and about 300,000 new malwares are created daily [2]. By 2025, ~75 billion devices will be connected to the Internet [3]. If the state-of-the-art had a perfect solution, cybercrime would not have shown a persistent upward trajectory with exponential growth doubling in 5 years from $8.44 trillion in 2022 to $23.84 trillion by 2027 (**Figure 1**) [1]. These estimates do not even consider the catastrophe Q-Day may unleash upon our daily lives when Internet-breaking Quantum Computers (QC) become a reality. With the exponential proliferation of IoT devices and the ever-growing vulnerabilities of connected devices, the cybercrime industry is poised for unstoppable growth.

Experts unanimously agree that fool-proof cybersecurity is "practically impossible" essentially because our legacy computer architecture mandates third-party permissions that third-party applications need to run, but which bad actors often exploit to attack with malware [4]. Experts unanimously agree that data within a connected device can never be entirely secure because network exposure can never be risk-free. A World Economic Forum report warns that a "catastrophic cyber event" is coming (**Figure 2**). It claims that "93% of cyber leaders, and 86% of cyber business leaders, believe that the geopolitical instability makes a catastrophic cyber event likely in the next two years." [5]

The situation will worsen when quantum computers (QC) with sufficient qubits arrive to break current encryption algorithms, and 6G communication devices will premiere in 2030 to reach a connection density of 10 million devices per square kilometer [6] (**Figure 3**).

6G is targeted as a global communication facility with approximately 1 Tb/s user bit rate with less than 1 microsecond latency [7]. Zhang *et al.* argue in their article that 1000 times price reduction from the customer's viewpoint is the key to the success of 6G [8]. Post Quantum Cryptography (PQC) is being aggressively developed to secure our cryptography-dependent digital infrastructure in a Zero Trust (ZT) cloud computing architecture recommended by NIST (National Institute of Standards and Technology) [9]. However, with over 90% of PQC candidates failing after the final round of NIST's PQC standardization process, QC appears more detrimental to human interests than the benefits it delivers [10].

PQC deployment will make the 6G goals almost unachievable as most promising PQC algorithms rely on keys much larger than those in classical algorithms

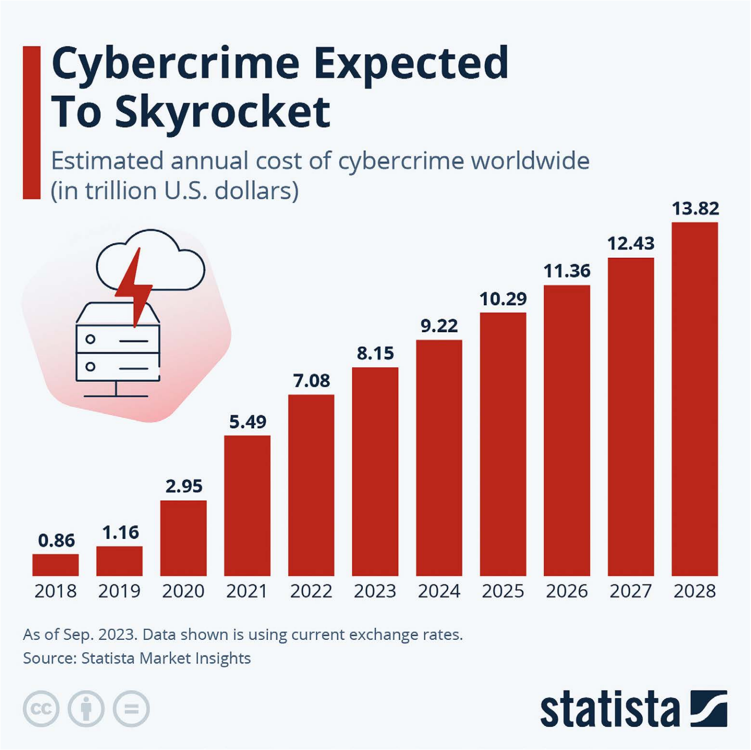

Figure 1. Exponential growth of cybercrimes. Image Source: Statista.com [1].

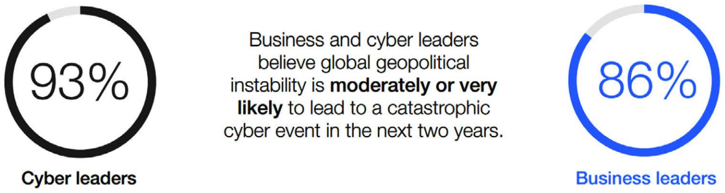

Figure 2. Possibility of catastrophic cyber event in by 2025. Credit: WEF Global Cybersecurity 2023 Report [5].

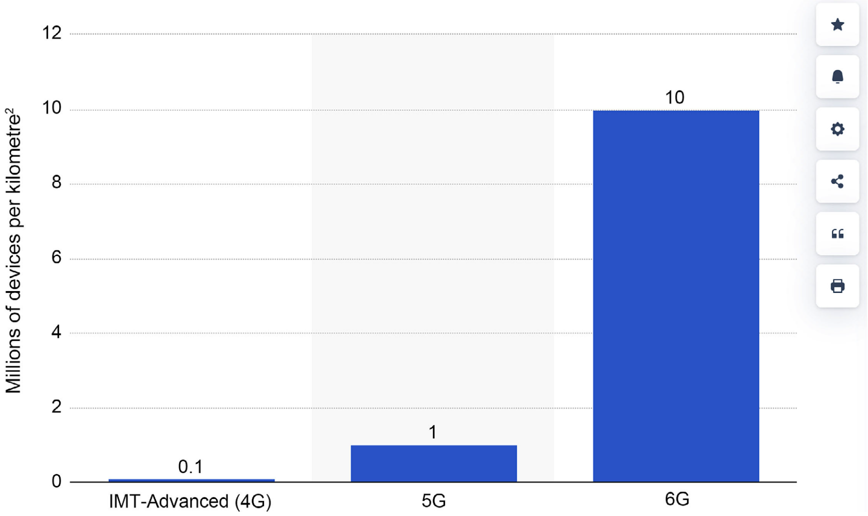

Figure 3. Connection density of 4G, 5G, and 6G mobile broadband technologies (in millions of devices per kilometre². Image credit: Statista.com [6]

and will likely have a higher computational cost than the current RSA methods. These large keys consume more storage space and processing power, increasing the time and costs. Not counting its operational cost or its energy efficiency, a recent high-performance implementation of CRYSTALS-Dilithium achieved the best-known latency as low as 16.8 microseconds on an Artix-7 at 142 MHz chip [11]. This is manifold higher than the 1-microsecond target set for 6G. There are substantial storage and computational costs and latency implications of PQC depending on the length of the keys ciphertext and signature size, the computational efficiency of their encryption, encapsulation, signature verification and private key decryption, decapsulation, and signing operations.

Even if PQC succeeds in NIST's standardization process, the critical challenge of latency looms large over 6G networks as these networks demand ultra-low latency (beyond current PQC capabilities) to power real-time applications seamlessly. Therefore, the necessity for cybersecurity solutions that offer blazing-fast, low-latency performance is undeniable. Regardless of the fate of PQC algorithms, the urgency for such solutions remains paramount in fortifying future 6G networks against quantum threats.

A solution is therefore urgently needed. This research explores & and extends the initial promising results of the H2020-funded ZVC experiments [4] and builds on the findings to create a robust quantum-resilient 3SoC (Solid-State Software-on-a-Chip) framework. Pursued by an experienced consortium of 9 European partners [12], this solid state Absolute Zero Trust (AZT) by design approach can potentially render computers quantum-resistant by banning all third-party permissions, which remains the root cause of most computer vulnerabilities.

Section 2 articulates a problem statement that the state-of-the-art needs to resolve to stop the worsening state of cybersecurity. **Section 3** describes the purpose of this research in the form of 3 research questions that this paper attempts to answer and briefly presents a concise summary of the related work. In **Section 4**, the state-of-the-art is challenged with each of the 3 research questions that set the backdrop for this paper. **Section 5** reviews the Zero Vulnerability Computing (ZVC) approach and its impact on a computer's operating system. **Section 6** discusses from a historical perspective and projects the possible future if our research agenda meets its goal. **Section 5** details the proposed solution that eliminates the complexities ingrained in legacy systems to build support for the quantum-safe hypothesis on the future of cybersecurity. **Section 6** demonstrates that ZVC/3SoC architecture is "*Absolute Zero Trust*" *by Design*, while the legacy system's "*Zero Trust*" strategies are policy-based and cannot be autonomous and seamless. **Section 7** compares the ZVC/3SoC architecture with other operating systems and bare machine systems (BMS). **Section 8** lays down the limitations of the study. **Section 9** concludes that future computers may be rendered more robust, resilient, and secure if they get rid of the complexities that their vulnerability-prone operating systems introduce.

2. Problem Statement

"*Complexity is the worst enemy of security, and this is especially true for computers & and the Internet*" [13]. Complexity opens the door to vulnerabilities. Unfortunately, computer advancements have always been associated with increased complexities. With the proliferation of IoT devices predicted to reach 75 billion by 2025 [14], the attack surface will exponentially grow, sharing a significant common attack surface and increasing security vulnerabilities across the board [15]. The time frame for vulnerability exploitation has also compressed. Now it is only 15 minutes before a vulnerability is exploited, compared to days in the past [16]. Zero-day cyber-attacks are predicted to rise from one per week to one per day [17]. Such extraordinary growth of cybercrime will get worse when the Q-day arrives. Q-Day is when quantum computers, with computing speeds millions of times faster than the fastest classical computer, will break the Internet [18].

State-of-the-art cybersecurity techniques are limited to strategies that reduce the attack surface and encrypt data stored in online devices to counter the vulnerabilities. These approaches, however, have known limitations and are often complex, making cybersecurity experts conclude that "*perfect cybersecurity is impossible*" [4] [19].

In 2016, NIST (National Institute of Standards and Technology) published a report on the rising threat to the encrypted Internet data by quantum computers and the catastrophic impact that would have on the integrity of the global IT infrastructure [20]. Traditional computers store data in binary "bits" (like ones and zeroes) and function by creating and storing long strings of these bits. However, quantum computers (QC) "qubits" (quantum bits) can do both simultaneously. This enables them to do millions of trial-and-error calculations at once. A QC could do what might have taken an ordinary computer week or even years in seconds. Thus, a QC can decrypt standard encryption instantly, exacerbating serious cybersecurity issues across the Internet. Following the NIST report, experts have been warning of the apocalyptic Q-Day when QC will have enough power to break the Internet [18]. The non-linear exponential growth in QC has opened up the possibility of performing attacks based on Shor's and Grover's algorithms that threaten the PKI and hash functions in the near future [21]. Therefore, it has become necessary for the development of post-quantum secure signature schemes. The nightmare scenario of a QC falling into rogue hands for hacking government systems, shutting down power grids, clearing bank accounts and crypto wallets, and triggering financial chaos has been played out umpteen times by experts [22]. Q-Day, the *day when quantum computers will be able to render all current encryption methods meaningless*, is predicted to arrive sooner than one thinks [23]. Some believe quantum networks can be expected to be operational before 2030 [24]. In fact, at least 6 companies have already started offering their current quantum computing capabilities as a commercial cloud service [25].

In April 2021, the Ransomware Task Force, a group of industry experts, submitted a report entitled "*Combatting Ransomware - A Comprehensive Framework for Action*" to the US government [26]. On May 12, 2021, in response to this report from the Ransomware Task Force, President Biden issued an Executive Order entitled "*Improving the Nation's Cybersecurity*" [27], which requires that the US advance towards a "*Zero Trust Architecture*", as described by the NIST [23].

Post-Covid ubiquity of work-from-home and bring-your-own-device (BYOD) strategies have driven the European Commission to upgrade its NIS2 Directive for cybersecurity to move workloads from client devices to the cloud [28]. This has accelerated the adoption of the Zero Trust Architecture in Europe and redefined the approach to cybersecurity [29]. In a recent RSA2023 event, experts suggested that PQC will become a core part of IT infrastructure with the goal of extending zero trust to future quantum computing [30]. Last year, the Cloud Security Alliance launched a countdown to Y2Q (years to quantum) that predicts just under seven years until quantum computing is able to crack current encryption [31]. They arbitrarily specify April 14, 2030, as the deadline by which the world must upgrade its IT infrastructure to meet the Y2Q threat (**Figure 4**). Even NATO and the White House recognize the threat and are preparing for Y2Q [32]. If we don't do anything, the Internet as we know it now may simply cease to exist.

The EuroQCI (European Quantum Communication Infrastructure) initiative was launched in 2019. The EuroQCI Declaration was initially signed by seven Member States, and all EU Member States subsequently joined the initiative [29]. The US Congress passed the Quantum Computing Cybersecurity Preparedness Act (H.R. 7535) in July 2022 [30], and on December 21, 2022, President Biden signed it into law [31]. The Act encourages "*federal government agencies to adopt technology that will protect against quantum computing attacks.*" This marks a major milestone in the global effort to develop and deploy quantum-resilient cybersecurity. These legislations made the world move quickly against the coming QC threat since upgrading existing governmental and commercial cryptography infrastructure takes significant effort and years.

Post-quantum cryptography (PQC) is being aggressively pursued worldwide as a defense from potential quantum threats to the Internet. In 2017, NIST initiated its long journey to standardize a defense against this impending catastrophe and, in 2019, published the results of its first round of 82 PQC candidates

Figure 4. Countdown to Q-Day (Y2Q). Credit: Cloud Security Alliance [31].

entering the standardization process [32]. In 2022, 2 of the 4 finalist PQC candidates were decimated by ethical hackers using standard computing devices, sending a shockwave within the cybersecurity community [33] [34] [35]. Last year, a Swedish group also cracked the remaining finalist PQCs (CRYSTALS-Kyber and CRYSTALS-Dilithium) [36] and a French team of cryptographers [37].

3. Research Purpose and Related Works

The principal objective of this research is to address the perpetually worsening cybersecurity landscape, which is further aggravated by the looming catastrophic threats from QC. Two major NIST (National Institute of Standards & Technology) initiatives taken in recent years aimed at mitigating the cybersecurity crisis include:

1) Post Quantum Cryptography Standardization Project [20].

2) Zero Trust Architecture (ZTA) [26] [27] [28] [29].

These initiatives are also supported by the ENISA (EU cybersecurity agency) in its revised EU directive on the security of network and information systems (NIS2) [38]. Both these initiatives are facing implementational challenges. This paper examines these initiatives de novo in the light of a new encryption-agnostic cybersecurity approach [4] by formulating the following research questions (RQ):

3.1. RQ1: Why Are Computers Inherently Vulnerable, and Why Foolproof Cybersecurity Is Impossible?

Cybersecurity experts unanimously agree that 100% cybersecurity is impossible [4] [19]. Although logically obvious, peer-reviewed literature lacks an explicit, technologically pertinent answer to this question. This research articulates an explicitly defined answer to this question.

3.2. RQ2: Is PQC the Ideal Solution to Secure 75 Billion Connected Devices in the Near Future?

Today's Internet security is almost entirely cryptography-dependent [39], and therefore it remains vulnerable to the impending threats from the enormous computing power of the future QC. PQC is obviously the logical defense against the Q-Day threat. However, PQC algorithms are expensive and consume relatively more computing resources than legacy cryptography schemes. A good majority of IoT devices are low-cost with low computational power. Running PQC algorithms may not be techno-economically feasible on the majority of IoT devices. An answer to RQ2 will help us explore alternate possibilities.

3.3. RQ3: Is Absolute Zero Trust (AZT) Achievable in Prior Art?

AZT is not achievable [40] [41]. Nevertheless, several research reports claim to implement ZT by design, although all of them are policy-based models (see section 4.3) that cannot run without continuously monitoring and maintaining zero-trust policy-based rules defined by the organization running the ZT system. An affirmative answer to this question will make real build-time AZT possible and make implementing ZT seamless and autonomous.

Answers to these research questions may help researchers target cybersecurity solutions to the root cause of computer vulnerabilities, better prepare our digital infrastructure to deal with the Q-Day threat and make the implementation of ZT more robust, resilient, autonomous, and seamless.

PQC is the only defence currently explored by researchers and regulatory authorities to secure the Internet from the Q-Day threat. A recent report discloses a novel way to deal with the impending Q-Day threat by segregating all quantum computing activities from mainstream Internet instead of deploying resource-intensive PQC on every Internet device [42]. It deployed a new Zero Vulnerability Computing (ZVC) paradigm that proposed a new computer architecture banning all third-party permissions to reduce the computer's attack surface to zero and achieve zero vulnerability [4]. This approach delivers QC services to customers in a Quantum-as-as-Service (QaaS) business model [42] [43]. Although computer security heavily relies on cryptography, recent evidence indicates that it can indeed transcend beyond encryption by deploying ZVC technology. ZVC is an encryption-agnostic approach that can potentially render computers quantum-resistant by banning all third-party permissions, a root cause of most vulnerabilities [4] [42]. Recently, 9 European organizations, including four universities, three SMEs, a research organization, and a non-profit, built a consortium to develop a quantum-resistant computing infrastructure, further deploying this new ZVC paradigm [44]. This paper expounds on the principle objective of the consortium to design a ZVC computing environment that eliminates the complexities of the traditional multi-layered architecture of legacy computers and builds a minimalist, compact Solid-State Software on a Chip (3SoC) device that's robust, resilient, energy efficient, and with zero attack surface, rendering it resistant to malware, as well as future Q-Day threats [4] [42] [43].

4. State-of-the-Art

With the advent of IoT and the proliferation of connected devices, attack surfaces, and vulnerabilities have exponentially grown. Over the past decade, malware has grown from about 100 million in 2012 to 1.33 billion in 2021 [45]. In the current state-of-the-art, the approach to improving the security of a computer system is to measure the attack surface [46] and minimize it with the following strategies:

1) reducing the amount of code running,

2) reducing entry points available to untrusted users, &,

3) eliminating services requested by relatively few users [47].

The Zero Trust architecture by NIST suggests a similar strategy [48]. Although attack surface reduction helps prevent many security failures, it does not mitigate the damage an attacker could inflict once a software vulnerability is found [49].

Computer encryption is vital for protecting users, data, and infrastructure in the digital age [50]. Using traditional computing, even common desktop encryption could take decades for specialized "crackers" to break, and government and infrastructure-grade encryption would take *billions* of times longer. In light of these facts, it may seem that today's computer cryptography is a rock-solid way to safeguard everything from online passwords to the backbone of the entire internet. Unfortunately, many current cryptographic methods will soon be obsolete when the Q-Day arrives [51].

This paper reviews and challenges the state-of-the-art de novo with three grassroots-level questions. The first question targets the very design and architecture of computers that render them vulnerable in the first place. The second question challenges the techno-economic feasibility of current approaches to counter the impending Q-Day threat. The third and final question investigates whether the legacy systems permit the much-desired ZTA by Design implementation possible. The answers may unveil a solution to the intractable cybersecurity problem that appears to be so far unassailable.

4.1. Why Are Computers Inherently Vulnerable, and Why Is Foolproof Cybersecurity Impossible?

All modern computing devices follow at least two mandatory design rules to make them usable [4] [42] [43]

1) *All computer hardware and software are designed to grant third-party permissions that third-party applications need to run.*

2) *The inherent vulnerability of in-computer data storage.*

In prior art, no hardware or software is devoid of third-party permissions, and these permissions are mandated for a good reason—allowing vendors to supply a diverse range of applications. Without third-party applications, a computer will be useless. Although permissions allow computers to run applications, most, if not all, computer vulnerabilities originate from those inherent permissions, creating an attack surface that hackers use to deploy attack vectors [4] [42] [43]. In legacy computing systems, the attack surface cannot be eliminated. It can only be reduced by deploying policy-based measures. Consequently, third-party permissions and the resulting attack surface are necessary evils legacy computing systems must live with. This situation compels cybersecurity experts to conclude that fool-proof cybersecurity is practically impossible [4] [19] [39]. Those rules, although perfect for the pre-Internet era, have failed to stop cybercrimes in the age of the Internet and, in fact, allowed the exponential growth of cybercrimes [47]. Without unlearning that deeply ingrained knowledge about the "*necessary evil*," it is difficult to comprehend the new **ZVC** (Zero Vulnerability Computing) paradigm that the proposed solution builds on to solve the cybersecurity quagmire [4] [8] [42] [43].

4.2. Is PQC the Ideal Solution to Secure 75 Billion Connected Devices in the Near Future?

All the evidence suggests that QC is experiencing an inflection point. compelling us to get ready for this new computing paradigm [30]-[36]. More importantly, because companies like IBM, Amazon, *et al.* have already commenced offering their QC capabilities to their qualified clients as cloud services [25], the need to secure the Internet from Q-Day threats is greater than ever. Experts believe the transition of the billions of old and new devices to PQC will be a multidecade transition process that has to account for aspects such as security, algorithm performance, ease of secure implementation, compliance, etc. [50]. By 2025, there will be ~75 billion devices connected to the Internet [10], a good majority of which will be IoT devices with minimal resources posing significant computational restrictions on their hardware and software. The communication between these devices, their limited energy resources, and their limited processing power make running any cryptographic algorithm with longer keys challenging. 95% of current Internet security is cryptography-based [52], bearing significant resource and cost consequences on these devices connected to the Internet. The IoT devices with limited resources are impacted the most. The advent of QC will make the cybersecurity situation worse. There is a race among countries to get supremacy in QC because QC will drastically reduce the computing time from years to minutes. Although the power of QC will be a boon for data-intensive industries, it raises serious threats to the cybersecurity of connected devices. Theoretically, all cryptographic algorithms are vulnerable to quantum attacks. The availability of a practical QC with millions of qubits capacity will be able to break nearly all modern public-key cryptographic systems, threatening an impending Quantum apocalypse [53]. Before the QCs arrive with sufficient qubits, we must be ready with quantum-safe cryptographic algorithms, tools, techniques, & and deployment strategies to protect our ICT infrastructure.

In 2016, the National Institute of Standards and Technology (NIST) predicted that QCs would soon be able to break the most popular forms of public key cryptography. The encryption technologies we rely on every day—HTTPS, TLS, WIFI protection, VPNs, cryptocurrencies, PKI, digital certificates, smartcards, etc. will be virtually useless. In 2022, after a rigorous 5-year process, four finalists out of 82 PQC candidates for standardization were announced, two of whom got cracked within months [36] [37] [38]. Subsequently, the remaining PQC were also breached by a Swedish and a French team of cryptographers [39] [54], placing the PQC standardization process in serious jeopardy [42] [43]. Moreover, encryption algorithms, in general, are neither resource-efficient nor cost-effective because of the high cost of encryption and decryption of data [55]. A recent report estimates the current cost of quantum cryptography for connecting two computers at a whopping $50,000 [56]. Notwithstanding the cost and failing state of PQCs, most IoT devices with limited resources will be unable to support the implementation of PQC algorithms computationally. Implementing PQC on

75 billion devices is a techno-economic futility that PQC advocates often ignore. These circumstances warrant an urgent need to explore alternate strategies. Although state-of-the-art security heavily relies on cryptography, recent evidence indicates it can indeed transcend beyond encryption using Zero Vulnerability Computing (ZVC) technology [4] [42] [43]. ZVC is an encryption-agnostic approach that can potentially render devices quantum-resistant by banning all third-party permissions, a root cause of most computer vulnerabilities [4]. ZVC eliminates the complexities of the multi-layered architecture of legacy devices and builds a minimalist, compact Solid-State Software on a Chip (3SoC) device that's robust, resilient, energy-efficient, and with zero attack surface rendering it resistant to malware as well as future quantum threats [42] [43].

Recent setbacks may jeopardize the original NIST timeline for PQC standardization, estimated at 15 years for a full transition to Quantum-safe Internet [43] [53]. Global PQC implementation is a massive undertaking impacting each of the billions of computing devices in the entire Internet ecosystem. It is not just a time-consuming but resource-intensive undertaking. However, the alternate approach for quantum resilience that this proposal proposes limits its implementation to QC service providers offering discerning QaaS (Quantum-as-a-Service) subscription exclusively to highly selective special needs clients, warranting no Internet-wide implementation of QC [42] [43]. Thus, keeping the QC exploiting bad actors at bay, the proposed 3SoC architecture can accelerate the process of securing the Internet from the Q-Day threat [42] [43].

4.3. Is Absolute Zero Trust (AZT) by Design Possible in Prior Art?

In legacy computing environments, trust itself is a vulnerability and, like all vulnerabilities, should be eliminated [57]. Zero Trust was created because traditional security models operate on the outdated assumption that everything inside an organization's network should be implicitly trusted. This implicit trust means that all users, including threat actors and malicious insiders, can access sensitive data once on the network due to a lack of lateral security controls [57]. First proposed by John Kindervag in 2010 [58], zero trust is a systemic approach to information security that trusts no user, transaction, or network traffic unless verified. In 2020, NIST defined it as "*a term for an evolving set of cybersecurity paradigms that move defenses from traditional static, network-based perimeters to focus on users, assets, and resources.*" [59] It lays out a user-centric security vision as compared to its perimeter-focused predecessors. It is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction. Rooted in the principle of "*never trust, always verify,*" Zero Trust (ZT) is designed to protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing threat prevention, and simplifying granular, "least access" policies. However, at the end of the day, zero trust remains just a vision, not a recipe, a strategy, not a toolset, a policy-based protocol implemented by humans, not an autonomously implemented algorithm that runs seamlessly by default.

A zero-trust architecture (ZTA) uses zero-trust principles to plan industrial and enterprise infrastructure and workflows. ZT assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (*i.e.*, local area networks versus the internet), or based on asset ownership (enterprise or personally owned) [58] [59]. Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring-your-own-device (BYOD) implementations, and cloud-based assets that are not located within an enterprise-owned network boundary. ZTA focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component of the security posture of the resource [57] [58] [59].

NIST's Zero Trust Architecture (ZTA) defines three policy-related core components (**Figure 5**):

1) Policy Engine: The policy engine is the core of ZTA. The policy engine decides whether to grant access to any resource within the network. It relies on policies designed and managed by the enterprise's security team and data from external sources like threat intelligence to verify and determine context. Access is then granted, denied, or revoked based on the parameters defined by the enterprise. The policy engine communicates with a policy administrator component that executes the decision.

2) Policy Administrator: The policy administrator component is responsible for executing access decisions determined by the policy engine. It can allow or deny the communication path between a subject and a resource. Once the policy engine makes an access decision, the policy administrator kicks in to allow or deny a session by communicating a third logical component called the policy enforcement point.

3) Policy Enforcement Point: The policy enforcement point is responsible for enabling, monitoring, and terminating connections between a subject and an

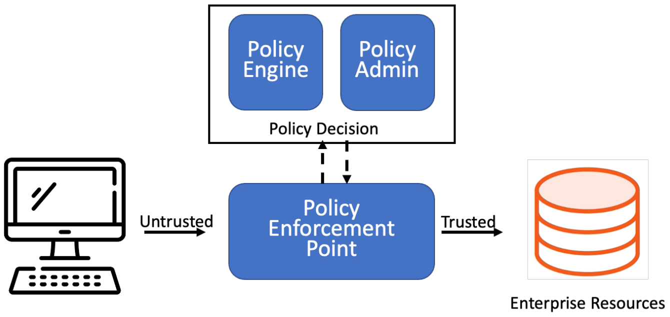

Figure 5. Simplified anatomy of NIST's policy-based zero trust architecture.

enterprise resource. In theory, this is treated as a single component of ZTA, but in practice, it has a client-side agent on a PC or a server and the resource-side access control gateway.

Simply put, ZTA is a policy-based system that authenticates the user many times during the user's online activity, but these are done behind the scenes so as not to bother the user at every step of the process.

5. Zero Vulnerability Computing: A New Cybersecurity Paradigm

Zero Vulnerability Computing is a new encryption-agnostic cybersecurity approach that bans all third-party permissions that all legacy hardware and software inherently grant to allow running diverse applications that third-party vendors offer [4] [42] [43]. These permissions are the principal cause of almost all computer vulnerabilities. Because only native applications are allowed access to the zVC resources and all non-native codes are outright rejected by default, there is no need for deploying complex cryptographic keys for authenticating an authorized user.

5.1. How Does ZVC Become a Security Strategy for Resistance to Quantum Computers (QC)

As discussed in Section 2, traditional computers store data in binary "bits" (like ones and zeroes) and function by creating and storing long strings of these bits. However, quantum computers (QC) "qubits" (quantum bits) can do both simultaneously. This enables them to do millions of calculations at once. A QC could do what might have taken an ordinary computer week or years in seconds. Thus, a QC can decrypt standard encryption instantly, exacerbating serious cybersecurity issues across the Internet. Q-Day, the day when quantum computers will be able to render all current encryption methods meaningless, is predicted to arrive soon [23].

Our previous reports on ZVC [4] [42] [43] provided experimental validation of the ZVC hypothesis. This novel approach to cybersecurity does not depend on user-facing cryptographic schemes; therefore, it is encryption agnostic and inherently resistant to the cryptography-breaking power of future quantum computers [4] [42] [43].

5.2. The Quantum-Safe Zero Vulnerability Computing (ZVC) Hypothesis and Its Impact on Operating System

However, the ZVC approach drastically changes our current IT practices at the grassroots level, imposing certain significant limitations on the traditional OS and installable applications as supported by the 3SoC hypotheses [42]. As a consequence of banning all third-party permissions, all the traditional computing layers are merged, resulting in zero attack surface, introducing the revolutionary "*zero moving parts*" concept of traditional solid-state electronics to the computer's software framework. Because of its solid-state nature that does not rely on user-facing cryptography for its security, 3SoC turns out to be a novel approach to developing, storing, and running any software in a computing environment that's inherently bequeathed with robustness, resilience, energy efficiency, and resistance to any malware and future quantum threats. Such a ZVC/3SoC framework achieved security without the policy-based ZTA and hence serendipitously resulted in absolute zero trust (AZT) architecture by design.

To overcome the legacy computing environments' disadvantages in terms of permissions for the storage of data & and execution of programs, the 3SoC computing environment demands a new protocol that discriminates non-native data from the data generated by native applications [42]. Such file management protocol essentially builds a gateway to authorize access to the nonvolatile memory for data privileges. As illustrated in **Figure 6**, the Soft Gate works at the firmware level, filtering all data with permission to store and execute data files in two steps. The 1st step only allows the data files with the .3SoC extension, and the 2nd step checks for the private key before authorizing any storage rights to the data file. The Hardware Gate is a tiny controller that assigns memory registry addresses only to the native 3SoC file format (**Figure 6**). All non-native, non-3SoC data are denied access. To pass the 3SoC gateway, a natively generated file ingrains at least two unique attributes. The first attribute assigns a .3SoC file extension to all the native files, and the second deploys public key cryptography in the file compilation algorithm for encapsulating a private key within the file. The gateway permitting access to the memory thus passes through two checks before granting access, denying all files not recognized by the gateway (**Figure 6**).

In comparing 3SoC architecture with the multi-layered architecture of traditional computing systems, as illustrated in **Figure 7**, it is amply clear that the concept is heading toward a minimalist computing system that is devoid of a full-featured Operating System (OS). Discussed in more detail subsequently in Sections 6.3 and 7, ZVC/3SoC takes another well-researched concept of BMS

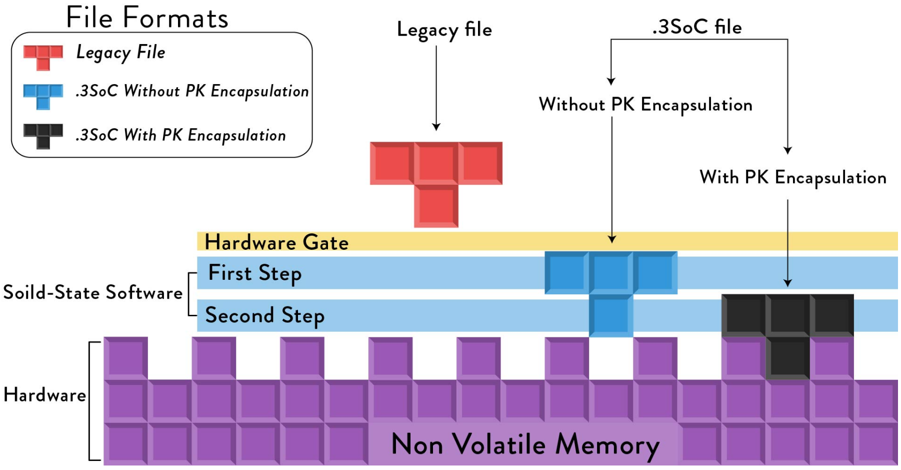

Figure 6. Hardware level banning of non-native data by 3SoC. Adapted: Future Internet, 14(11), 33 (2022).

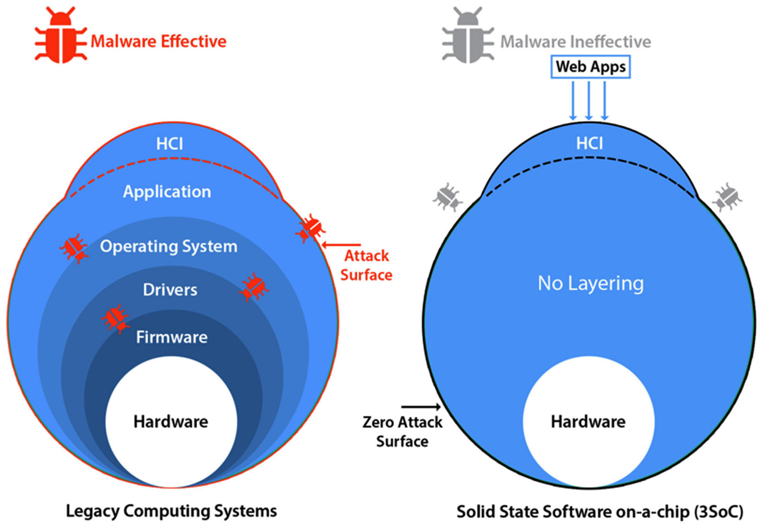

Figure 7. Layered legacy system vs compact 3SoC.

(Bare Machine Systems) [60] to the next level. BMS is a minimalist computing environment devoid of a proper OS designed to improve computer security. Unlike the BMS, 3SoC is not limited to running a single custom application but integrates a user interface that can run any traditional web application (**Figure 8**). 3SoC remains an active subject of research pursued by our consortium, having far-reaching insinuations on our understanding of solid-state electronics and computer hardware/software [8] [42] [43]. It delivers a fully functional computing device without a classical OS and zero installable applications but with web-delivered features and user experience on par with the legacy computing systems running legacy operating systems, such as Windows, Android, Linux, MacOS or iOS.

6. How Does the Zero Trust Strategy Playout in the ZVC/3SoC Framework?

Hype surrounds any new concept or phenomenon, as with "Zero Trust Architecture" (ZTA). Michael, et al claim that the concept of ZTA is currently a moving target, and developing and sustaining ZTA is essentially impossible [61]. Some experts consider Zero Trust as a misnomer [62]. When a good majority of cybersecurity experts believe ZTA itself is impossible or illusive [63], the legitimacy of research reports claiming ZTAbD (Zero Trust Architecture by Design) is at best questionable. An in-depth review of these reports will deliver a fair answer to the question of ZTAbD or absolute zero trust (AZT) feasibility in the real world.

In legacy systems, security is often an afterthought and an overlay on the original network, mostly placing the traditional security controls at the perimeter of the network [64]. Acknowledging that full lifecycle security of software and systems is more successful than when it is treated as an afterthought, Dwight & Nair argued that the benefits of the ZT strategy cannot be fully realized without extending the notion of ZT beyond the network architecture to include ZT

Figure 8. Graphic illustration of a 3SoC hardware without OS.

protocol design and full lifecycle ZT software engineering [65]. However, their proposed ten foundational principles of the ZT by Design architecture are also policy-based. Since policy-based protocols are human-configured, implemented, and supervised, they cannot be fully autonomous, self-governing, and universally relevant by design, at least not at build time. This essentially means that a rule-based or policy-dependent ZTA that introduces application-specific trust rules during each runtime execution cannot integrate universal trust rules during build-time.

A typical ZT architecture implements different pillars of zero-trust as different functions, with each function providing functionality for a different zero-trust principle pertaining to data, device, application, user identity, infrastructure, and network [66]. Each of these pillars is layered in legacy computing systems mandating third-party permissions, which are governed by a policy engine, policy administration, and policy enforcement process defined by the system's varying operational circumstances (**Figure 9**). Although several reports [62]-[67] claim the merit of ZT by Design or absolute zero trust (AZT), technically all those proposed ZT implementations in the prior art are policy based [61]-[69], and therefore strictly speaking cannot be ZTbD or AZT. Embedding full, seamless, and autonomous ZT in any legacy computing system is wishful thinking that can only be desired but not achieved. This is because if third-party permissions exist in any build-time computing environment, there will always be policies to govern those permissions that third-parties deploy in diverse computing scenarios [4] [8] [42] [43]. Therefore, in all legacy systems, true universal AZT is a myth that can only be desired but never achieved. However, as illustrated in **Figure 8**, the AZT framework powered by ZVC/3SoC devices, governance does not involve any layering or third-party permissions (**Figure 6**, **Figure 7** & **Figure 9**) and, therefore, can be built into the architecture of the 3SoC computing environment for seamless autonomous operation without having to design, implement and monitor ZT policies.

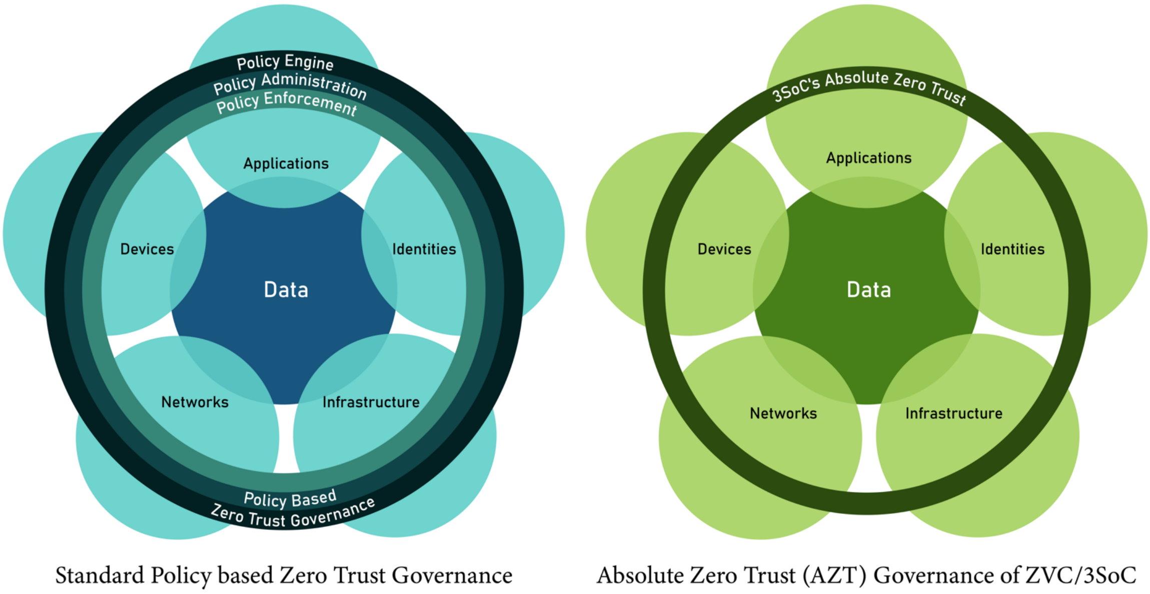

Figure 9. Pillars of zero trust governance: legacy (policy based) vs 3S0C's absolute zero trust (AZT) by design.

6.1. Absolute Zero Trust (AZT) Architecture by Design Extends ZT to "Trust No Application" & "Trust No Code"

Implementing the Zero Trust strategy is a multi-step process that entails defining the protection surface, mapping the transaction flows, defining the relevant architecture, creating the zero trust policy, and monitoring and maintaining the zero trust environment (**Figure 10**). Integrating all of these steps into ZT by design at the build-time is impossible as these conditions change during the runtime according to the prevailing circumstances and require continuous monitoring by a dedicated team. Therefore, "Absolute Zero Trust" (AZT) is not achievable because its complex policy implementation cannot run autonomously 24/7 without human intervention [61]-[70]. However, by banning all third-party permissions, the principle cause of all vulnerabilities and resulting attack surface, ZVC's 3SoC architecture, whether at build-time or runtime, is inherently "Zero Trust" by design. This means no attack surface needs to be defined, and no strategy, rules, or policy must be designed, planned, created, or monitored. For the reasons explained here and in the previous subsection, legacy zero trust systems will always be policy-based, and as such, the elements of zero trust cannot be coded into their architecture at build-time. In other words, self-implementing AZT by design is an impossibility in legacy computing systems.

In essence, prior art ZT is built on the principle of "*trust no one*, *trust no device*, *and trust no network.*", whereas the AZT by Design framework described in this paper extends the concept of ZT and ZTA beyond "*trust no one*, *trust no device and trust no network*," to "*trust no application and trust no code*" (**Figure 9**). The legacy ZT implementation remains a policy-based strategy or model and not a product, while ZVC/3SoC's AZT is a product that delivers AZT by design coded into the program at build-time. In ZVC/3SoC-based architecture,

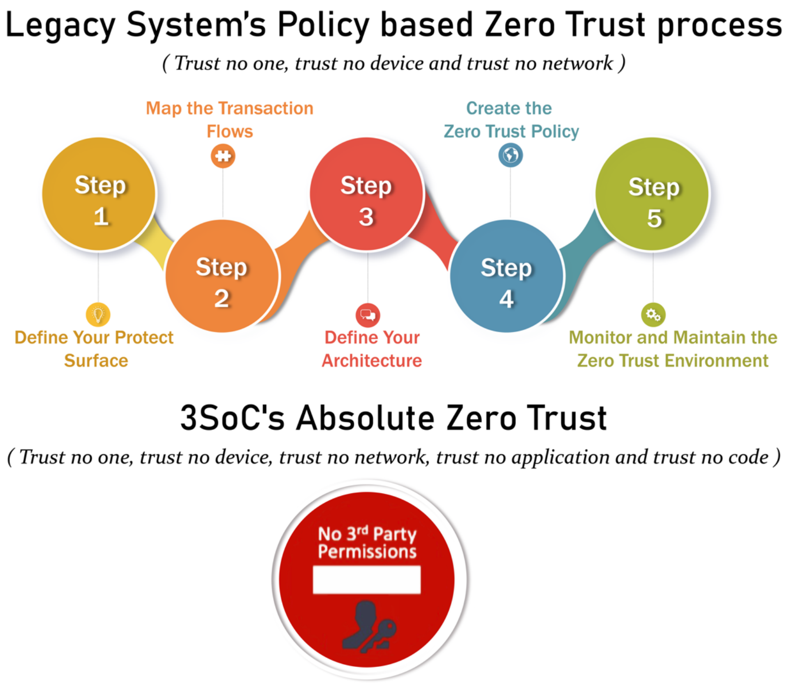
Legacy System's Policy based Zero Trust process
(Trust no one, trust no device and trust no network)
Map the Transaction Flows
Create the Zero Trust Policy
Step 1
Step 2
Step 3
Step 4
Step 5
Define Your Protect Surface
Define Your Architecture
Monitor and Maintain the Zero Trust Environment
3SoC's Absolute Zero Trust
(Trust no one, trust no device, trust no network, trust no application and trust no code)
No 3rd Party Permissions

Figure 10. 5-Step zero trust process vs autonomous absolute zero trust (AZT) by design of 3SoC.

AZT implementation is automatic by default without defining or continuously monitoring policies.

6.2. AZT: A Cloud Continuum

AZT should be designed as a cloud continuum to maximize its impact, not just a vaulted computer terminus operating in a sequestrated environment. Cloud computing is one of the fastest-growing markets in the software industry predicted to hit $791.48 Billion by 2028 [71]. This is despite cloud computing facing the triple whammy of privacy breaches, security threats, and interoperability flaws [72]. Notwithstanding these shortcomings, the "**-as-a-Service**" cloud computing model has grown exponentially because of its advantages over legacy systems. The cloud computing environment is quickly evolving from an entirely centralized architecture to a more distributed continuum.

6.2.1. Four-Layered AZT Cloud Continuum

The cloud-computing continuum continues to shift. Shifts, not only in terms of distribution of services but also in terms of distribution of resources. In terms of services, that continuum has evolved from basic software, platform, or infrastructure as-a-Service to Everything-as-a-Service (XaaS). In terms of the distribution of resources, it has evolved from isolated remote servers in the cloud to the Cloud-Fog-Edge computing continuum. Recently, Moreschini, et al, analyzed 36 studies [73] to formulate the definition of cloud continuum as "*an extension of the traditional Cloud towards multiple entities* (*e.g., Edge, Fog, IoT*) *that provide analysis, processing, storage, and data generation capabilities.*"

The AZT by Design framework proposed in this study can significantly contribute to the evolving cloud continuum by taking the traditional 3-layered Cloud-Fog-Edge continuum to a novel 4-layered Cloud-Fog-Edge-EN (End Node) continuum. Thus, extending the redistribution of computing resources of the cloud continuum beyond traditional fat, fog, and edge devices to the EN, placing users in full control of their personal data stored in personal online data stores (PODs) within the EN [74], and decentralizing the continuum to bring the resources closer to the EN client device (**Figure 11**). In legacy systems, EN is considered no more than a user interface with plenty of *EN Problems* that introduce vulnerabilities into the network [75], warranting its exclusion from the cloud continuum. However, in the proposed AZT framework, EN plays a key role in not only boosting processing speeds and minimizing latency but also ensuring the privacy, security, and interoperability of users' personally identifiable information (PII) (**Figure 10**). Most importantly, in the proposed AZT architecture the only change warranted is in the EN client devices. The rest of the infrastructure (edge, fog, fat server) can remain the same, requiring no hardware-level changes to those devices. This is because, as illustrated in **Figure 11**, the only way to access the edge, fog, or server devices is via the EN or client device, and a bad actor would not be able to access any of the continuum resources using a legacy client device. Only the 3SoC client devices have authorized access rights to the continuum resources, and none of the legacy devices can be authenticated to the AZT cloud continuum infrastructure layers (**Figure 11**). It is like enabling 2-factor authentication at each layer of the AZT continuum the second factor being the special 3SoC identity of the authorized EN client device. Thus, access to any data space on the continuum mandates 3SoC authentication at every step by default without the need for any policy or exclusion/inclusion rule. Additionally, in the most computation-intensive artificial intelligence use cases, the PII data is secured in the PODs stored at the EN as the machine learning

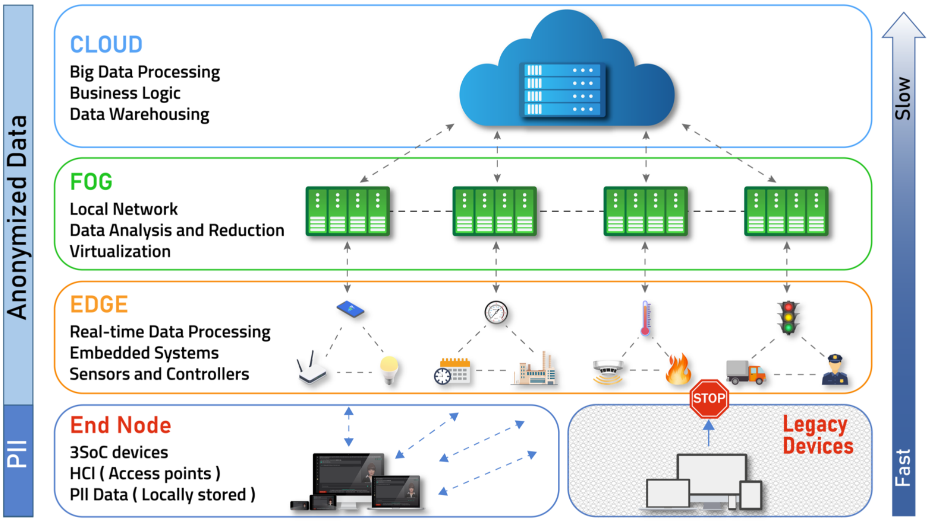

Figure 11. Four-layered AZT by design cloud continuum with 3SoC End-Node vs. Legacy Devices.

models running on edge, fog, and cloud servers can efficiently operate on anonymized data. Hence, because of the efficient use of computing resources and sequestering of the private PII data in user-controlled PODs, the proposed AZT framework is private, secured, interoperable, fast, energy-efficient, and deployed with low capital and operational costs.

6.2.2. Absolute Zero Trust (AZT) Framework for Futureproof Cloud Continuum

AI is fast becoming an essential constituent of our cloud infrastructure [76]. Therefore, designing any cloud ecosystem cannot ignore AI or at least make provisions for securely integrating ML modules as part of the continuum (Figure 12).

6.3. Other Ways AZT Potentially Changes Legacy Security Models

6.3.1. Zero Touch Security

As seen in Section 4.3, Zero Trust systems are always policy-based and not self-implementing. A concept of Zero Touch is fast emerging that deploys computationally efficient and trustable AI-driven autonomous network management operations [77]. AZT changes that and renders the network operation autonomous without any extra AI tools.

6.3.2. Operating Systems: A Historical Perspective from "No OS" to "OS" and Beyond

The first digital computers, developed after World War II had no operating systems (OS). They ran one program at a time, which had command of the entire system (Figure 13). The programs were often entered into the computer one bit

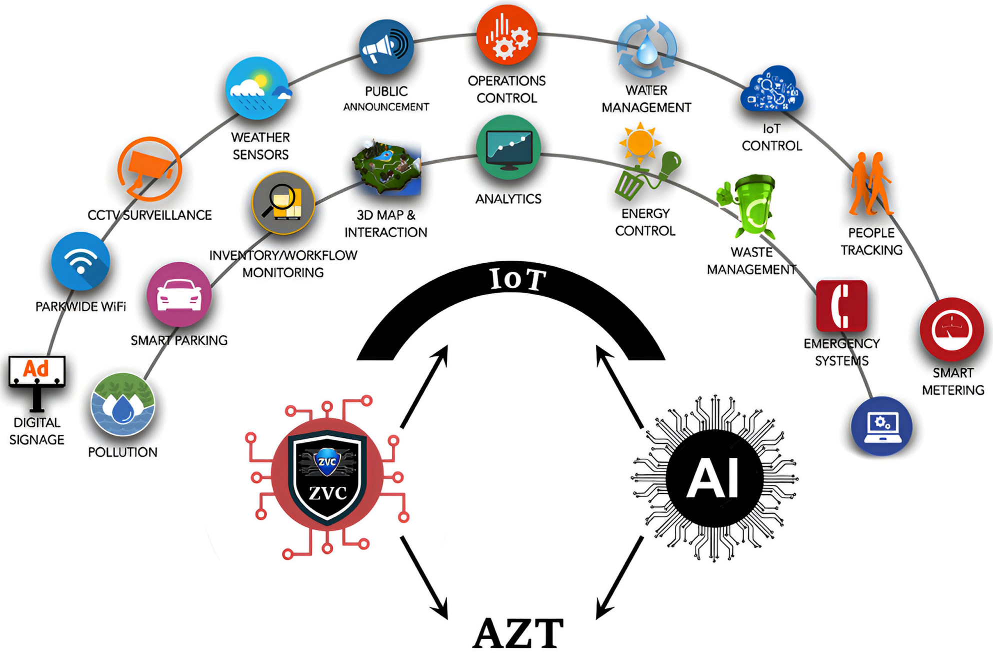

Figure 12. Achieving absolute zero trust (AZT) to secure an AI-powered cloud infrastructure.

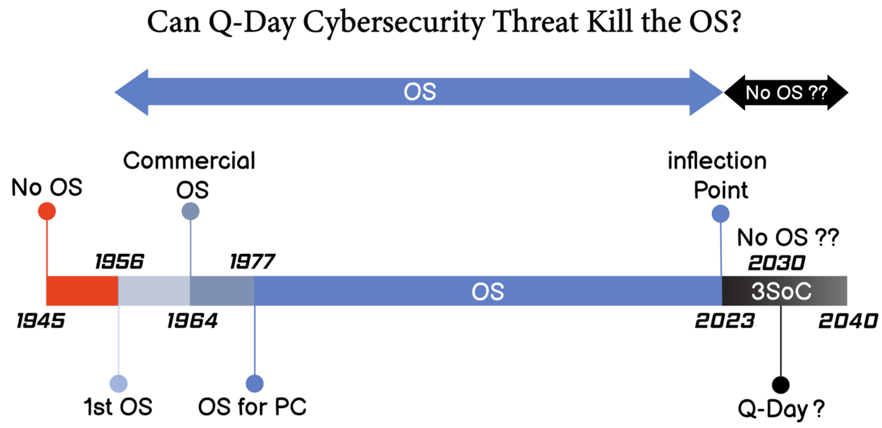

Figure 13. History of OS & its potential role in future computers.

at a time on rows of mechanical switches. Eventually, machine languages (consisting of strings of the binary digits 0 and 1) were introduced, accelerating the programming process [78]. The systems of the 1950s generally ran only one job at a time. It allowed only a single person at a time to use the machine, placing all the machine's resources at the user's disposal. There was no such thing as Operating System (OS) resources. A human operator would provide all the special resources needed to operate the computer. The concept of OS started evolving in the mid-1950s, and with it emerged the rise of systems software and the software industry [79]. In the 1960s, the turn from user-driven software to manufacturer's software made the concept of an OS viable, gradually making OS a part of the computer's system structure as the actual hardware. Most computers were designed to be rented or sold with an OS so that customers would be able to write their own applications or contract vendors to develop according to their needs, giving birth to a whole new software industry [80]. Today, we cannot imagine using a computer without an OS. It shapes and frames how we access the computer and its peripherals and supports our interaction with it throughout. During the mid-1960s, IBM's OS/360 for the IBM machines or Multics for an integrated time-sharing system premiered, laying the foundation of a more systematic framework that defined our modern view of the OS [81].

An OS manages resources and interfaces between the users and the hardware in a layered architecture. The layers of hardware, firmware, middleware, drivers, OS, and application are all designed and built with mandatory third-party permissions at each level. OS serves as the core that binds all the layers together. As much as OS is the heart of a computer, it is also directly or indirectly responsible for almost all the reported vulnerabilities [72]. Can we make the OS more reliable and secure? Tanenbaum *et al.* tried answering that question by reviewing four different attempts to improve operating system reliability, focusing on preventing buggy code and device drivers [82]. One of the first reports on multiple problems originating from OS came from MIT as early as 1995, contending that OS abstractions are the root of all OS problems, which can be minimized by the systematic extermination of OS abstractions [83]. The authors claimed this would result in lowering the interface enforced by the OS to a level close to the raw hardware to improve the OS performance. Taking the cue from this MIT report, various groups have tried designing bare machine systems (BMS) by eliminating the OS altogether to improve the performance and security of the system in specific use case scenarios, such as running SQL [84], USB Storage [85], VOIP [86], etc. All these BMS initiatives, however, fall short of delivering a fully functional computing device with features and user experience on par with legacy computing devices running legacy operating systems, such as Windows, Android, Linux, MacOS, or iOS.

7. Comparing 3SoC with Legacy Operating Systems (OS) & Bare Machine Systems (BMS)

The legacy OS and BMS (Bare Machine System) computing environments of prior art discussed in detail in the preceding section have certain disadvantages that the proposed 3SoC computing environment overcomes. Most importantly, such shortcomings are attributed to the mandatory third-party permissions to universally allow any data, program, or code to access the computing resources for storage or execution [4] [42] [43]. Consequently, access to such permissions exclusively relies on cryptographic protocols, which in turn are governed by the rules and policies that determine the zero-trust strategy. As explained earlier, this makes absolute zero trust or AZT impossible, as policies cannot be coded into any software architecture at build-time. Moreover, eliminating the dependency on encryption for preventing third-party intrusion renders the proposed system resistant to threats from future QC. Getting rid of the complexities of legacy systems also improves the user experience of the proposed AZT framework.

Beyond security and improved user experience, the 3SoC ecosystem is much more resilient to the obsolescence risk that legacy systems are vulnerable to in terms of losing the competitive edge with time. In the words of Bill Gates, "*In three years, every product my company makes will be obsolete. The only question is whether we will make them obsolete or somebody else will*" [87]. **Table 1** highlights key differences between the 3SoC computing environment and the prior art operating systems and bare machine systems (BMS).

Table 1. Comparison between OS, BMS and 3SoC.

Attributes	Legacy OS Windows, MacOS, Android, Linux, iOS	Bare Machine Computing	3SoC
Layered	Yes	No	No
Applications	Environment sensitive	Application-driven	Web-driven
third-party permissions	Yes	Limited	None
Complexity	Too complex	Simple	Very simple
Size of code	Large	Much smaller	Much smaller
User Experience	Normal	With Limitations	Improved in speed & performance

Continued

Open ports	Many	None	Optional
Inter-OS compatibility	None	None	Switchable within multiple OSs
Vulnerabilities	Many	Limited	None
Frequent patching	Not required	Not required	None
Zero-day vulnerability	High	Limited	None
Zero Trust Approach	Policy based implementation	Application-driven policy	Built-in by design
AZT Cloud Continuum	Impossible	Not possible	By default
End Node	Highly vulnerable	Vulnerable	Highly secure
Resilience	Fragile	Robust	Very robust
Thread/process creation	User-driven	Application Driven	Pre-defined
System Calls	Many	Application Calls	Predefined
Local IoT Portability	Extensive	None	Within 3SoC ecosystem
Universal Portability	Extensive	Limited	Extensive via WiFi only
Hardware	Rapid changes	Less often	Lot Less
Software	Rapid changes	Less often	Less often
Software Upgrades	Frequent	Rare	Rare
Heterogeneity	More	None	None
External code dependencies	Substantial	None	None
People skills	Diverse	App-centric	Diverse
Hardware Life	Less	Lot More	Lot more
Software Life	Less	Extensible	Extensible
Global/Local Centric	Global Centric	Local Centric	Local & Global
App developers’ development time	Faster due to existing tools	Slower due to non-existing tools	Faster as all apps are web based
Malware	Susceptible	Less susceptible	Resistant
Attack surface	Large	Not totally obliterated	Totally obliterated
Quantum threat	Vulnerable	Vulnerable	Resistant
Obsolescence	High	Low	Low
Learning curve	More due to complexities	Less due to App focus	Less due to simplicity

8. Limitations of the Study

The proposed ZVC /3S0C framework has the potential to not only afford protection against future quantum threats but also secure the current computing infrastructure in a way that is less resource-intensive and more cost-effective than the cryptographic approaches. This novel approach to cybersecurity does not depend on user-facing cryptographic schemes; therefore, it is encryption agnostic and inherently resistant to the cryptography-breaking power of future quantum computers [4] [42] [43]. However, it drastically changes our current IT practices at the grassroots level, imposing certain significant limitations on the traditional

OS and installable applications. How that pans out in real-world practice cannot be precisely predicted. This research on banning third-party permissions to achieve quantum-resistant zero vulnerability computing (ZVC) is ongoing [4] [42] [43]; all observations and results are interim and cannot be considered conclusive until replicated and established by peer researchers in diverse real-world settings. It must be clearly understood that non-deployment of user-facing cryptography in ZVC does not imply that cryptography is not used for file management protocols at the firmware and hardware level (see Section 5) [42]. However, cryptographic deployments remain oblivious to adversarial confrontations as they are not user-facing. Although several use case scenarios are currently being explored in several research projects that may have far-reaching implications on our understanding of computer hardware/software and their security and resilience, the principal objective of this study was to address the following two major cybersecurity strategies that our regulatory regimes have initiated to defend our computing infrastructure against the perpetually worsening cybersecurity landscape:

1) Post Quantum Cryptography Standardization Project [20]

2) Zero Trust Architecture Initiative [26] [27] [28] [29]

These initiatives aimed at mitigating the cybersecurity crisis need to be carefully reviewed, considering the new possibilities that this paper presents in terms of keeping our ICT infrastructure sanitized with banned third-party permissions, resulting in zero attack surface in an AZT cloud ecosystem. The answers to the three research questions presented in this paper provide theoretical support to the proposed new cybersecurity paradigms and need further research to validate their role in eliminating the complexities present in the legacy systems to render the Internet more secure, resilient, energy efficient, and sustainable.

9. Conclusions and Future Prospects

"*Today, we run billions of computer programs on globally connected machines without any formal guarantee of their absolute safety. We cannot prove that when we launch an application on our smartphones, we would not trigger a chain reaction that leads to the transmission of missile launch codes that start a nuclear war.*"—Alfonseca, *et al.*, Journal of Artificial Intelligence [88].

Although Alfonseca *et al.* made comment about the unstoppable superintelligence, it also holds in the context of cybersecurity.

Life without computers is unimaginable, and so is a computer without third-party permissions or an OS. Moving from "OS" to "No OS" will indeed be a radical departure from the legacy computing systems that may also sound like going back to the ancient times when computers premiered without a proper OS. A computer with no third-party permissions would also mean no installable third-party applications and, consequently, no marketplace for installable apps. Moving from OS to No OS, from installable to no installable apps, will be quite a Quantum Leap from the prevailing norms. It will be too drastic a challenge to the status quo. A departure from our current comfort zone is always extremely difficult and challenging. But "*necessity is the mother of invention*," they say. With the speed at which quantum technology is progressing, Q-Day may not be too far off. The need to prepare for the Q-Day is now more than ever. "*The pending upgrade to post quantum-resilient cybersecurity will be the largest upgrade in information technology history*" [19]. Universal PQC deployment, particularly in low-cost, low-resource IoT devices, appears techno-economically impracticable to protect the entire Internet within a reasonable time and budget, even if the recent PQC setbacks are overcome. The timeline for the launch of 6G is more or less in sync with the timeline for the availability of quantum computers [6] [31]. Not taking into account the Q-Day threat when designing 6G networks will be disastrous. With the existing PQC performance standards on latency [11] and cost [55] [56], meeting the 6G goals for one-microsecond latency [7] and 1000 times cost reduction [8] seems impossibly difficult. These circumstances may create a dire necessity to justify mothering as radical an invention as the AZT framework of this research. Research efforts will be more productive if the initial focus of the AZT research remains low-cost, low-resource IoT devices with low computational power.

Fear has the power to trump the status quo and rekindle hope. In the given circumstances, the AZT strategy offers the best hope of averting the perils of the impending Q-Day. Time will tell if the Q-Day fear delivers the quantum leap computers need to take to save the Internet from QC threats. There are, however, plenty of unanswered questions about how to build and integrate these systems into the mainstream, but significant progress can be made by pursuing the ideas laid out in this report. The earlier this work begins, the more opportunity there will be for unforeseen difficulties to surface and get resolved to tackle the cybersecurity challenges of a post-quantum future.

Authorship Contribution Statement

Fazal Raheman: Conceptualization, Methodology, Software, Validation, Writing—original draft, Writing—review & editing.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability

All data are either included in the paper or can be found in the sources cited in the paper. Any additional data will be made available on request.

Acknowledgements

The author is grateful to Dr Brecht Vermeulen and Professor Peter Van Daele (IMEC—Ghent University, IDLab iGent Tower—Department of Information

Technology, Technologiepark-Zwijnaarde 126, *B* 9052 Ghent, Belgium) for support in the initial hypothesis building research, and to Mr Tejas Bhagat and Ms Sadiya Khan for their help in preparing this manuscript. The author is also grateful to Dr Kotzaniko laou Panayiotis of University of Piraeus and Dr Kostas Kolomvatsos of University of Thessaly for being trusted partners in several consortia and initiatives involved in the development of the Zero Vulnerability Computing (ZVC) concept.

Conflicts of Interest

The author declares that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Fleck, A. (2022) Cybercrime Expected to Skyrocket in Coming Years. Statista. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[2] Satoh, A., Fukuda, Y., Hayashi, T. and Kitagata, G. (2020) A Superficial Analysis Approach for Identifying Malicious Domain Names Generated by DGA Malware. *IEEE Open Journal of the Communications Society*, **1**, 1837-1849. https://doi.org/10.1109/OJCOMS.2020.3038704

[3] Banafa, A. (2023) How to Secure the Internet of Things. In: Banafa, A., Ed., *Introduction to Internet of Things* (*IoT*), River Publishers, New York, 57-62. https://doi.org/10.1201/9781003426240-10

[4] Raheman, F., Bhagat, T., Vermeulen, B. and Van Daele, P. (2022) Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet*, **14**, Article 238. https://doi.org/10.3390/fi14080238

[5] Raina, S. (2023) Geopolitical Instability Raises Threat of 'Catastrophic Cyberattack in Next Two Years'. World Economic Forum. https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/

[6] Taylor, P. (2023) Connection Density of 4G, 5G, and 6G Mobile Broadband Technologies (in Millions of Devices Per Kilometre^2). Statista. https://www.statista.com/statistics/1183690/mobile-broadband-connection-density/

[7] Aslam, A.M., *et al.* (2023) Metaverse for 6G and Beyond: The Next Revolution and Deployment Challenges. *IEEE Internet of Things Magazine*, **6**, 32-39. https://doi.org/10.1109/IOTM.001.2200248

[8] Zhang, S., Xiang, C. and Xu, S. (2020) 6G: Connecting Everything by 1000 Times Price Reduction. *IEEE Open Journal of Vehicular Technology*, **1**, 107-115. https://doi.org/10.1109/OJVT.2020.2980003

[9] Szymanski, T.H. (2022) The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access*, **10**, 45893-45930. https://doi.org/10.1109/ACCESS.2022.3169137

[10] Dobberstein, L. (2022) Post-Quantum Crypto Cracked in an Hour with One Core of an Ancient Xeon. The Register. https://www.theregister.com/2022/08/03/nist_quantum_resistant_crypto_cracked/

[11] Beckwith, L., Nguyen, D.T. and Gaj, K. (2022) High-Performance Hardware Im-

plementation of Lattice-Based Digital Signatures. Cryptology ePrint Archive.

[12] 3SoC Consortium (2023) Solid State Software on a Chip (3SoC): A Novel Approach for Quantum Safe Computing. Blockchain 5.0 OÜ (BC5), Tallinn. https://www.bc5.eu/3SoC/

[13] Dickson, B. (2016) What Bruce Schneier Teaches Us about IoT and Cybersecurity. TechTalk. https://bdtechtalks.com/2016/11/29/what-bruce-schneier-teaches-us-about-iot-and-cybersecurity/

[14] Statista Research Department (2016) Internet of Things (IoT) Connected Devices from 2015 to 2025 (in Billions). https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[15] Zhang, M., Xin, Y., Wang, L., Jajodia, S. and Singhal, A. (2019) CASFinder: Detecting Common Attack Surface. 33*rd Annual IFIP WG* 11.3 *Conference*, *DBSEC* 2019, Charleston, 15-17 July 2019, 338-358. https://doi.org/10.1007/978-3-030-22479-0_18

[16] Islam, Z. (2022) Hackers Now Exploit New Vulnerabilities in Just 15 Minutes. Digital Trends. https://www.digitaltrends.com/computing/hackers-now-exploit-new-vulnerabilities-in-just-15-minutes/

[17] Cybersecurity Ventures and Herjavec Group (2018) Hackerpocalypse: A Cybercrime Revelation. Cyentia Cybersecurity Research Library. https://library.cyentia.com/report/report_001392.html

[18] Grimes, R.A. (2019) Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. John Wiley & Sons, Hoboken. https://doi.org/10.1002/9781119618232

[19] Yoo, C.S. and Lee, B.C. (2023) Optimizing Cybersecurity Risk in Medical Cyber-Physical Devices. *William & Mary Law Review*, **64**, 1513-1554.

[20] Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Smith-Tone, D., *et al.* (2016) Report on Post-Quantum Cryptography. US Department of Commerce, National Institute of Standards and Technology, Vol. 12, Gaithersburg. https://doi.org/10.6028/NIST.IR.8105

[21] Fernandez-Carames, T.M. and Fraga-Lamas, P. (2020) Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, **8**, 21091-21116. https://doi.org/10.1109/ACCESS.2020.2968985

[22] Dupraz, F. and Rollin, M. (2022) Why Everyone's Talking about…the Quantum Apocalypse. Natixis Investment Managers. https://www.im.natixis.com/intl/research/everyone-s-talking-about-the-quantum-apocalypse

[23] Ford, P. (2023) The Quantum Cybersecurity Threat May Arrive Sooner than You Think. *Computer*, **56**, 134-136. https://doi.org/10.1109/MC.2022.3227657

[24] Křelina, M. (2022) Quantum Technology in Future Warfare: What Is on the Horizon? Future Warfare and Technology: Issues and Strate-Gies. *Global Policy Journal*, **1**, Article 107.

[25] Fulton III, S. (2022) A Buyer's Guide to Quantum as a Service: Qubits for Hire. ZDNET. https://www.zdnet.com/article/a-buyers-guide-to-quantum-as-a-service-qubits-for-hire/

[26] Biden, J.R. (2021) Executive Order on Improving the Nation's Cybersecurity. White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[27] Kerman, A., Borchert, O., Rose, S. and Tan, A. (2020) Implementing a Zero Trust Architecture. National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf

[28] Ali, R. (2021) Looking to the Future of the Cyber Security Landscape. *Network Security*, **2021**, 8-10. https://doi.org/10.1016/s1353-4858(21)00029-5

[29] Olufon, T. (2023) Zero Trust Comes into the Mainstream in Europe. Forrester. https://www.forrester.com/report/zero-trust-comes-into-the-mainstream-in-europe/res178958

[30] Columbus, L. (2023) How Post Quantum Cryptography Will Help Fulfil the Vision of Zero Trust. Venture Beat. https://venturebeat.com/security/how-post-quantum-cryptography-will-help-fulfill-the-vision-of-zero-trust/

[31] Huttner, B. and Kalsi, M. (2022) Countdown to Y2Q: Working Group, Quantum-Safe Security. Cloud Security Alliance. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

[32] Keary, T. (2022) NATO and White House Recognized Post Quantum Threats and Prepared for Y2Q. Venture Beat. https://venturebeat.com/business/nato-and-white-house-recognize-post-quantum-threats-and-prepare-for-y2q/

[33] Ribezzo, D., *et al.* (2023) Deploying an Inter-European Quantum Network. *Advanced Quantum Technologies*, **6**, Article 2200061. https://doi.org/10.1002/qute.202200061

[34] Lin, H. (2023) The Mother of All Data Breaches: Quantum Com-Puting Holds New Promises and Dangers. Such Devices Could Overturn Our Whole Cybersecurity Regime, Revealing Not Just Mountains of Data But Secrets from Years Past. *Hoover Digest*, **2023**, 79-83.

[35] Sanzeri, S. (2023) What the Quantum Computing Cybersecurity Preparedness Act Means for National Security. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quan-tum-computing-cybersecurity-preparedness-act-means-for-national-security/

[36] Alagic, G., *et al.* (2019) Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. US Department of Commerce, National institute of Standards and Technology, Washington, DC. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303

[37] Mathew, S. (2022) Encryption Meant to Protect against Quantum Hackers Is Easily Cracked. New Scientist. https://www.newscientist.com/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/

[38] Castryck, W. and Thomas, D. (2022) An Efficient Key Recovery Attack on SIDH. Cryptology ePrint Archive. https://eprint.iacr.org/2022/975

[39] Berzati, A., Viera, A.C., Chartouni, M., Madec, S., Vergnaud, D. and Vigilant, D. (2023) Exploiting Intermediate Value Leakage in Dilithium: A Template-Based Approach. Cryptology ePrint Archive. https://eprint.iacr.org/2023/050

[40] National Security Agency (2021) Embracing a Zero Trust Security Model.

https://media.defense.gov/2021/feb/25/2002588479/-1/-1/0/csi_embracing_zt_security_model_uoo115131-21.pdf

[41] Nivarthi, K.S.P. and Gatla, G. (2022) Fighting Cybercrime with Zero Trust. *American Academic Scientific Research Journal for Engineering, Technology, and Sciences*, **90**, 371-381.

[42] Raheman, F. (2022) The Future of Cybersecurity in the Age of Quantum Computing. *Future Internet*, **14**, Article 335. https://doi.org/10.3390/fi14110335

[43] Raheman, F. (2022) The Q-Day Dilemma and the Quantum Supremacy/Advantage Conjecture. Research Square. https://doi.org/10.21203/rs.3.rs-2331935/v1

[44] Nyári, N. (2021) The Impact of Quantum Computing on IT Security. *Biztonságtudományi Szemle*, **3**, 25-37.

[45] Malware (2023) Total Amount of Malware and PUA. AV-TEST.org. https://www.av-test.org/en/statistics/malware/

[46] Canella, C., *et al.* (2019) A Systematic Evaluation of Transient Execution Attacks and Defenses. *Proceedings of the* 28*th USENIX Security Symposium*, Santa Clara, 14-16 August 2019, 249-266.

[47] Filho, A.S., *et al.* (2020) Reducing the Attack Surface of Dynamic Binary Instrumentation Frameworks. In: Rocha, Á. and Pereira, R., Eds., *Developments and Advances in Defense and Security*, *Smart Innovation*, *Systems and Technologies*, Vol 152, Springer, Singapore, 3-13.

[48] Stafford, V.A. (2020) Zero Trust Architecture. NIST Special Publication 800-207.

[49] Manadhata, P.K. and Wing, J. (2011) An Attack Surface Metric. *IEEE Transactions on Software Engineering*, **37**, 371-386. https://doi.org/10.1109/tse.2010.60

[50] Swire, P. and Ahmad, K. (2011) Encryption and Globalization. *Columbia Science and Technology Law Review*, **23**, 416-481. https://doi.org/10.2139/ssrn.1960602

[51] Joseph, D., *et al.* (2022) Transitioning Organizations to Post-Quantum Cryptography. *Nature*, **605**, 237-243. https://doi.org/10.1038/s41586-022-04623-2

[52] Google (2019) Transparency Report: HTTPS Encryption by Chrome Platform. https://transparencyreport.google.com/https/overview

[53] Sharma, S. and Harjani, M. (2022) Rethinking the 'Quantum Apocalypse'. RSIS Commentay.

[54] Ji, Y. and Dubrova, E. (2023) A Side-Channel Attack on a Masked Hardware Implementation of CRYSTALS-Kyber. *Proceedings of the* 2023 *Workshop on Attacks and Solutions in Hardware Security*, Copenhagen, 30 November 2023, 27-37. https://doi.org/10.1145/3605769.3623992

[55] Li, X., Luo, C., Liu, P., Wang, L.E. and Yu, D. (2019) Injecting Differential Privacy in Rules Extraction of Rough Set. *Proceedings of the* 2*nd International Conference on Healthcare Science and Engineering*, Guilin, China, 10-12 September 2018, 175-187. https://doi.org/10.1007/978-981-13-6837-0_13

[56] Markets and Markets (2023) Quantum Cryptography Market by Offering (Solutions and Services), Security Type (Network Security and Application Security), Vertical (Government, Defense. BFSI, Healthcare, Retail, and eCommerce) and Region—Global Forecast to 2028. https://www.marketsandmarkets.com/market-reports/quantum-cryptography-market-45857130.html

[57] Campbell, M. (2020) Beyond Zero Trust: Trust Is a Vulnerability. *Computer*, **53**, 110-113. https://doi.org/10.1109/MC.2020.3011081

[58] Kindervag, J. (2010) No More Chewy Centers: The Zero Trust Model of Information Security. Forrester Research Inc, Cambridge. https://www.ndm.net/firewall/pdf/palo_alto/Forrester-No-More-Chewy-Centers.pdf

[59] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. National Institute of Standards and Technology, Gaithersburg. https://doi.org/10.6028/nist.sp.800-207

[60] Okafor, U., *et al.* (2013) Eliminating the Operating System via the Bare Machine Computing Paradigm. 5*th International Conference on Future Computational Technologies and Applications* (Future Computing), Saint-Laurent-du-Var, 26-30 June 2023, 1-6.

[61] Michael, J.B., Dinolt, G.C., Cohen, F.B. and Wijesekera, D. (2022) Can You Trust Zero Trust? *Computer*, **55**, 103-105.

[62] Georgsen, R.E., and Myrdahl Køien, G. (2022) Serious Games with SysML: Gamifying Threat Modelling in a Small Business Setting. *INCOSE International Symposium*, **32**, 119-132.

[63] Whitmore, T. (2022) The Elusive Promise of (and Maddening Obstacles to Implementing) a Cloud Zero Trust Architecture. Frost & Sullivan Report. https://www.frost.com/frost-perspectives/elusive-promise-and-obstacles-to-cloud-zero-trust-architecture/

[64] Kindervag, J. (2011) Applying Zero Trust to the Extended Enterprise. Forrester Research, Cambridge.

[65] Horne, D. and Nair, S. (2021) Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.-S. and Tinetti, F.G., Eds., *Advances in Security*, *Networks*, *and Internet of Things*, Springer, Cham, 512-525.

[66] Manan, A., *et al.* (2022) Extending 5G Services with Zero Trust Security Pillars: A Modular Approach. 2022 *IEEE*/*ACS* 19*th international Conference on Computer Systems and Applications* (*AICCSA*), Abu Dhabi, 5-8 December 2022, 1-6.

[67] Home, D. (2022) Leveraging Software Defined Perimeter (SDP) Soft-Ware Defined Networking (SDN) and Virtualization to Build a Zero Trust Testbed with Limited Resources. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.-S. and Tinetti, F.G., Eds., *Advances in Security*, *Networks*, *and Internet of Things*, Springer, Cham.

[68] Lefebvre, M., Engels, D.W., and Nair, S. (2022) On SDPN: Integrating the Software-Defined Perimeter (SDP) and the Soft-Ware-Defined Network (SDN) Paradigms. 2022 *IEEE Conference on Communications and Network Security* (*CNS*), Austin, 3-5 October 2022, 353-358.

[69] Karabacak, B. and Whittaker, T. (2022) Zero Trust and Advanced Persistent Threats: Who Will Win the War? *International Conference on Cyber Warfare and Security*, **17**. No. 1. https://doi.org/10.34190/iccws.17.1.10

[70] Gligor, V.D. (2022) Zero Trust in Zero Trust. CMU CyLab Technical Report 22-002. https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab22002.pdf

[71] Singh, C. and Kaur, R. (2023) Relevance of Multi-Factor Authentication for Secure Cloud Access. In: Rani, S., Bhambri, P., Kataria, A., Khang, A. and Sivaraman, A.K., Eds., *Big Data*, *Cloud Computing and IoT*: *Tools and Applications*, CRC, Boca Raton, 13.

[72] Ouda, A.J., *et al.* (2022) The Impact of Cloud Computing on Network Security and the Risk for Organization Behaviors. *Webology*, **19**, 195-206.

[73] Moreschini, S., *et al.* (2022) Cloud Continuum: The Definition. *IEEE Access*, **10**, 131876-131886.

[74] Zichichi, M., Ferretti, S. and D'Angelo, G. (2020) On the Efficiency of Decentralized File Storage for Personal Information Management Systems. 2020 *IEEE Symposium on Computers and Communications* (*ISCC*), Rennes, 7-10 July 2020, 1-6.

[75] Bickley, A. (2017) Securing IoT Nodes. Arrow Electronics. https://static4.arrow.com/-/media/arrow/files/pdf/s/securing-iot-nodes.pdf

[76] Mohamed, N., *et al.* (2023) In-Depth Review of the integration of AI in Cloud Computing. 2023 3*rd international Conference on Advance Computing and innovative Technologies in Engineering* (*ICACITE*), Greater Noida, 12-13 May 2023, 1431-1434.

[77] Benzaid, C. and Taleb, T. (2020) AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions. *IEEE Network*, **34**, 186-194.

[78] Stern, N. (1981) From ENIAC to UNIVAC: An Appraisal of the Eckert-Mauchly Computer. Digital Press, Bedford.

[79] Hansen, P.B. (2001) The Evolution of Operating Systems. In: Hansen, P.B., ed., *Classic Operating Systems*: *From Batch Processing to Distributed Systems*, Springer, New York, 1-34.

[80] Bullynck, M. (2019) What Is an Operating System? A Historical Investigation (1954-1964). *Reflections on Programming Systems*: *Historical and Philosophical Aspects*, Vol. 133, Springer, Cham.

[81] CVE Details. Top 50 Products by Total Number of "Distinct" Vulnerabilities. https://www.cvedetails.com/top-50-products.php

[82] Tanenbaum, A.S., Herder, J.N. and Bos, H. (2006) Can We Make Operating Systems Reliable and Secure? *Computer*, **39**, 44-51.

[83] Engler, D.R. and Frans Kaashoek, M. (1995) Exterminate All Operating System Abstractions. *Proceedings* 5*th Workshop on Hot Topics in Operating Systems* (*HotOS*- *V*), Orcas Island, 4-5 May 1995, 78-83.

[84] Okafor, U., *et al.* (2012) Transforming SQLITE to Run on a Bare PC. *Proceedings of the* 7*th International Conference on Software Paradigm Trends* (*ICSOFT*-2012), Rome, 24-27 July 2012, 311-314.

[85] Karne, R.K., Liang, S., Wijesinha, A.L. and Appiah-Kubi, P. (2013) A Bare PC Mass Storage USB Driver. *International Journal of Computers and Their Applications*, **20**, 32-45.

[86] Khaksari, G.H., Wijesinha, A.L., Karne, R.K., He, L. and Girumala, S. (2007) A Peer-to-Peer Bare PC VoIP Application. 2007 4*th IEEE Consumer Communications and Networking Conference*, Las Vegas, 11-13 January 2007, 803-807.

[87] WDN (WebDevelopersNotes.com). Every Product Becomes Obsolete in 3 Years. https://www.webdevelopersnotes.com/every-product-becomes-obsolete-in-3-years

[88] Alfonseca, M., *et al.* (2021) Superintelligence Cannot Be Contained: Lessons from Computability Theory. *Journal of Artificial Intelligence Research*, **70**, 65-76.