IEEE SA
STANDARDS
ASSOCIATION

INDUSTRY CONNECTIONS
REPORT

CYBERSECURITY FOR NEXT-GENERATION CONNECTIVITY SYSTEMS

RETHINKING DIGITAL ARCHITECTURES TO SAFEGUARD THE NEXT GENERATION FROM CYBERSECURITY BREACHES

IEEE

Authored by

Vikas Malhotra
Founder & CEO, WOPLLI Technologies
Chair – IEEE Cyber Security for Next Generation Connectivity Systems group
Co-Chair – Artificial Intelligence and Metaverse taskforce at Trust over IP foundation

Merrick S. Watchorn, DMIST, QIS, QSAR
Chair – Sub-Committee for Quantum Computing at IEEE Cyber Security for Next Generation Connectivity Systems group
Co-Founder, Quantum Security Alliance (QSA)

Keeper L. Sharkey
Vice Chair – Sub-Committee for Quantum computing at IEEE Cyber Security for Next Generation Connectivity Systems group
Founder and CEO, ODE, L3C and Chair for Quantum Applied Chemistry at Quantum Security Alliance (QSA)

Deepayan Chanda
Principal Cybersecurity Architect – Strategy, Design and Governance (Lab49)
Board of Advisor (Binalyze, FlexibleIR), Advisor to Woplli Technologies
Chair – Sub-Committee for Webx.0 in IEEE Cyber Security for Next Generation Connectivity Systems

Albert H. Carlson
Chair for Entropy and Encryption, Quantum Security Alliance (QSA) & Associate Professor, Austin Community College

Mark Lizar
CEO and Principal Engineer @ Zero Public Network
Vice Chair – Sub-Committee for Human Centricity & Control at IEEE Cyber Security for Next Generation Connectivity Systems group
Flow Editor and Co-Author of the Notice Record Specification for Operational Security and Privacy Trans-border
Editor of the Consent Receipt Specification (now at ISO/IEC 27560)

Pamela Gupta
CEO Co-President OutSecure, Inc.
Co-Chair NIST GCTC Smart Secure Communities Cybersecurity & Privacy
Chair – Sub Committee for AI & Autonomous Systems at IEEE Cybersecurity for Next Generation Connectivity Systems group

Michael A. Enright
CEO/President of Quantum Dimension, Inc.
Chair – IEEE SA Sub-Committee Chair for 5G/6G of Cyber Security for Next Generation Connectivity Systems
Secretary – IEEE SA P3120 Standard for Quantum Computing Architecture Working Group
Member – IEEE ComSoc Future Networks Initiative in Security Working Group
Member – Cloud Security Alliance Zero Trust Working Group

Alex Polyakov
Co-Founder, CEO, Adversa AI.
Member, Forbes Technology Council
Chair – Sub-Committee for Heterogeneous control applications at IEEE Cyber Security for Next Generation Connectivity Systems group

Debbie Reynolds
CEO and Chief Data Privacy Officer of Debbie Reynolds Consulting LLC
Chair – IEEE Sub Committee Chair for Human Centricity & Control at IEEE Cyber Security for Next Generation Connectivity Systems group.

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGMENTS

Special thanks are given to the following reviewers of this paper:

Vinoth Kumar Venkatesan
Ajay Singh

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA25737 978-1-5044-9134-1

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the ICCom members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

RETHINKING DIGITAL ARCHITECTURES TO SAFEGUARD THE NEXT GENERATION FROM CYBERSECURITY BREACHES

ABSTRACT

This paper outlines the reasons why next-generation architecture is needed that can protect technology, systems, networks, and data in a dynamic risk environment. Although the Internet is integral to the flow of information across the globe and national boundaries, it was not built for the highly sensitive, critical data we see today. Architecture throughout protocol and software application stacks is not set up to face the cybersecurity issues.

The forward-facing and strategic approach introduced here promotes an architecture inherently resilient to cybersecurity threats. This approach would also address the needs for 6G technologies, Web X.0, Metaverse, and any evolutionary technologies envisioned.

To overcome the issues and challenges related to current architecture and to develop a framework for next-generation connectivity, we propose an architecture built on the principles of (1) human centricity, (2) decentralized identity, (3) distributed storage and processing, (4) heterogenous control application and assessment, and (5) self-healing. This novel approach, when applied to current applications, can help secure them. More importantly, when applied to the following five new and upcoming critical areas, this approach will not only enhance security but will also help us to better prepare for future Cyber Black Swan Events (CBSEs):

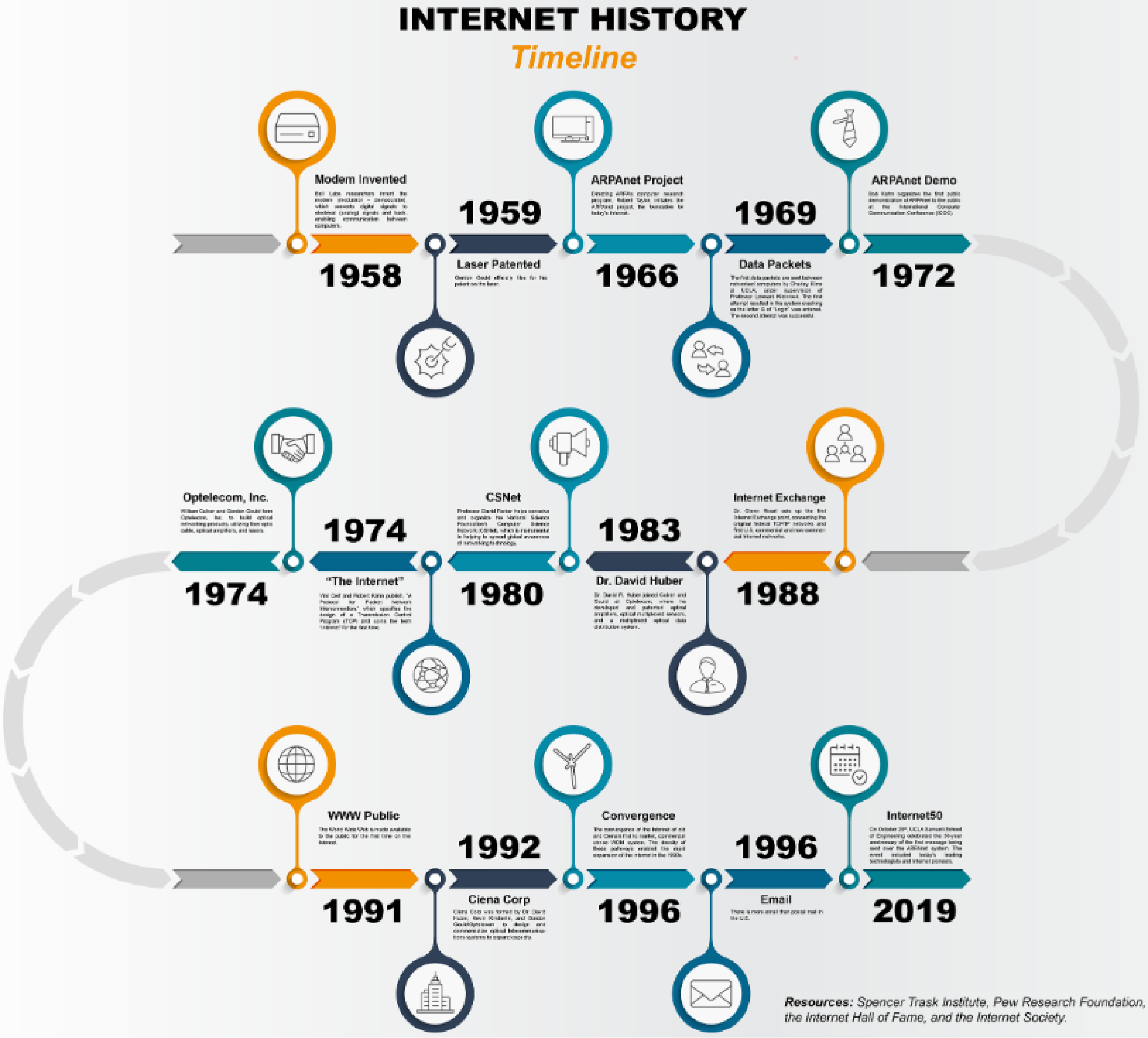
- Artificial Intelligence (AI) and Autonomous Systems
- Internet of Things (IoT)
- Web X.0+
- 5G/6G
- Quantum Computing

The IEEE Industry Connection group on “Cyber Security for Next Generation Connectivity Systems” investigates the five proposed architecture principles and their application on the five new and upcoming areas above in different subcommittees led by industry leaders in these fields. More information on this group can be found at IEEE SA - Cyber Security for Next Generation Connectivity Systems.

1. INTERNET AND SECURITY

The Internet has enabled groundbreaking communication leading to new forms of research and capabilities. The brief history of the Internet shown in FIGURE 1 outlines how the Internet has progressed and how humans have benefited.

FIGURE 1 Brief history of the Internet



Resources: Spencer Trask Institute, Pew Research Foundation, the Internet Hall of Fame, and the Internet Society.

Although the benefits of the Internet have been many, the Internet has also brought along security and safety issues for the consumers of Internet-driven technologies. These issues are rooted in the design of new digital information security architectures. In his groundbreaking series of essays published in 2005 called "The Laws of

Identity" [7], Kim Cameron—Microsoft's Chief Architect for Identity from 2004 to 2019—said:

> *The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust on the Internet.*

Kim's prophecy has come frighteningly true despite 20 years of collective work trying to solve these problems. In 2015, at the European Identity & Cloud (EIC) Conference, in his keynote address, Kim presented on what the future of the Internet would be like in 2020 [6]: "Attacks will be proliferating, and attack protection will be the number one concern."

The following statistics and data points support Kim's assertion:

- Nineteen percent of breaches occur because of stolen or compromised credentials. Sixteen percent of them occur because of phishing. Cloud misconfiguration causes 15% (IBM [26]).
- As of 2020, cyber-criminals use phishing most often in their attacks (FBI Internet Crime Complaint Centre [19]).
- In the first six months of 2021, 1,767 publicly recorded data breaches exposed a total of 18.8 billion records (Risk Based Security [46]).
- Major breaches have increased year over year as per the Center of Strategic and International Studies (CSIS Staff [10]).
- More than 90% of all healthcare organizations reported at least one security breach in the last three years with 61% acknowledging they lack effective mechanisms to maintain proper cybersecurity (Frost Radar**Error! Reference source not found.**).
- In 2021, a corporate data breach cost an average of US $4.24 million (IBM [26]).
- Most Web traffic (82%) contains Google third-party scripts, and almost half of them are tracking users (WhoTracks.Me [55]).
- Most Internet users (74%) feel they have no control over the personal information collected on them (Ponemon Institute [43]).

- Most Americans (72%) report feeling that all, or most, of what they do online or with their cellphone is being tracked by advertisers, technology firms, or other companies (Pew Research Center [40]).

- Rampant misinformation and unverified sources abound. In third-quarter 2020, 1.8 billion fake news engagements occurred on Facebook (German Marshall Fund [22]).

- Unrealized dangers can occur with modern technologies. For instance, 62% of the companies adopting AI are concerned that it will increase their cybersecurity vulnerabilities and 57% are concerned about the consequences of their AI systems using personal data without consent (Deloitte [11]).

- Most mobile device applications (71%) track people by copying and pasting code called “SDKs” (software development kits) to integrate subprocessing services, which add features and functionalities like Google Analytics, routinely disclosing (not sharing) information with so-called “third parties” without any transparency or legal authority to process personal data or consent, per research by Feal et al. [18].

- Feal et al.’s research [18], presented at the Commission Nationale de l'Informatique et des Libertés (CNIL), indicated that less than 10.0% of sites provided any privacy or security notice, and only 3.5% continued to work if consent was declined. At the same event, researchers demonstrated that even privacy tools leak personal data. One researcher demonstrated how 17.0% of forms collect data before the form is submitted, and that most people leak data about those close to them to third-party social media services. This process circumvents the individual, with terms and a software license used to get around privacy regulation.

- In 2019, an article exposed how public services in the United Kingdom use code from unauthorized third parties to systemically leak the data of the vulnerable and poor so when they can access basic government services (Eich [14]).

- The current data security environment highlights the lack of data control, the leakage, and the dominance of surveillance-based capitalism (Lessig [32]). Code regulates the Internet, not the consent of the individual.

- University of California (UC) Berkley research (Nair et al. [34]) has highlighted unprecedented privacy risks (from data collection) of the Metaverse from an environment clearly designed to extract personal data to expose people and their data in public formats on an unprecedented scale.

Many of these situations arise from large and uncontrollable data collection, its centralized storage, and the inability to stop its leakage from a variety of attacks. The data may be associated with identity or profiles, or it may be any other type of data, whether collected in a personal context or in the context of an organization.

2. INTERNET IS AT AN INFLECTION POINT

The rise of cybersecurity attack patterns and breach characteristics continues to evolve, and in most instances, security professionals must play “whack-a-mole” as part of their daily activities. Adequate security of data and information systems is fundamental; however, in this context, we are not doing well.

The Internet’s founders saw its promise but did not foresee users attacking one another. In a series of articles published in 2015 (Timberg [48]), Virginia Tech historian Janet Abbate said, “It would have taken enormous foresight for those planting these early seeds of Internet to envision the security consequences years later, when it would take a principal place in the world’s economy, culture, and conflicts.” Abbate added, “People don’t break into banks because they’re not secure. They break into banks because that’s where the money is. People thought they were building a classroom, but it was a bank.”

At the same time, more digitalization is happening. The Internet continues to grow, the way we deploy technology for remote work and communication is changing, and new areas and technologies are appearing on the horizon.

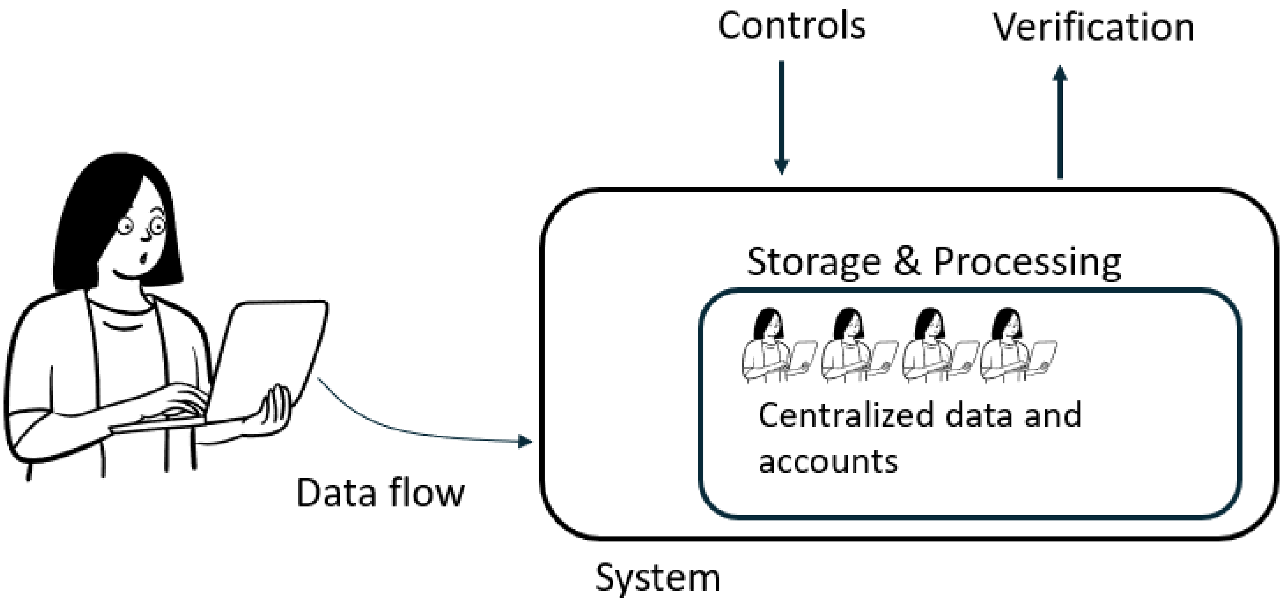
Cybersecurity has become such a key national issue in many countries that on September 14, 2022, the United States White House released a memorandum for enhancing the security of the software supply chain (DeRusha [12]). Such efforts will be undertaken globally.

We must prepare for the following five technology and application areas of the future:

- IoT
- AI
- Web X.0+
- 5G/6G
- Quantum Computing

These areas each include methods of data input or collection a process to manage the identity of a person or a thing in the system, storage and processing, control management, and some form of recovery mechanism. As systems grow in complexity, access control is a concern for systems distributed across multiple computers. We need to examine these areas in the context of the data input or collection methods to figure out better and more secure architectures (FIGURE 2).

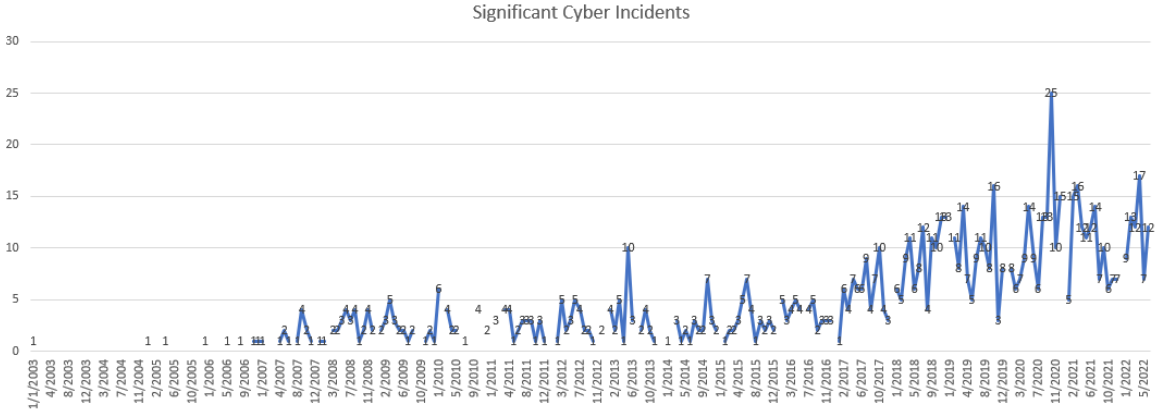
FIGURE 2 Typical digital environments



2.1.1. INCIDENTS AND VULNERABILITIES

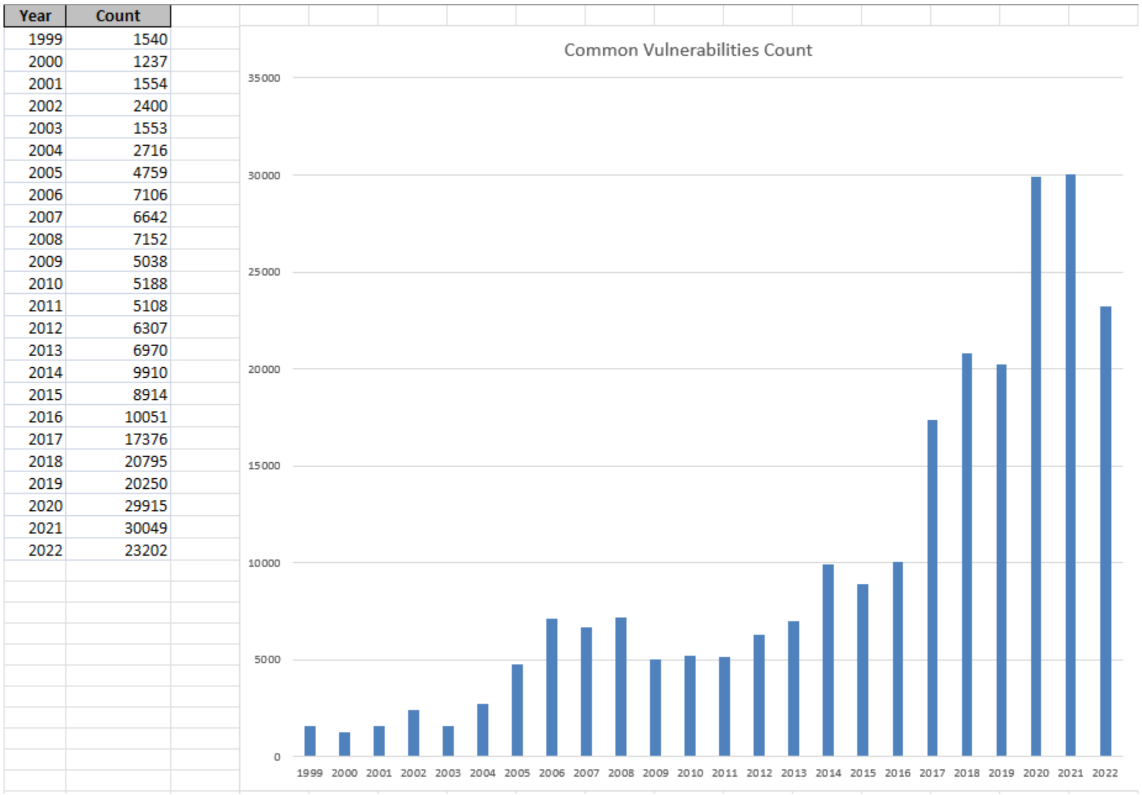
The number of attacks on the Internet, usually categorized as “incidents,” has been steadily growing. The CSIS has recorded significant cyber incidents since 2003 (FIGURE 3). The CSIS report [10] on cyber incidents focused on cyber-attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million US dollars.

FIGURE 3 Number of Cyber Incidents Since 2003



In addition, a steady rise in the number of vulnerabilities has occurred according to the Common Vulnerabilities Research Framework (CVRF). The numbers have been recorded by CVRF since 1999 (FIGURE 4).

FIGURE 4 Common Vulnerabilities Since 1999



Year	Count
1999	1540
2000	1237
2001	1554
2002	2400
2003	1553
2004	2716
2005	4759
2006	7106
2007	6642
2008	7152
2009	5038
2010	5188
2011	5108
2012	6307
2013	6970
2014	9910
2015	8914
2016	10051
2017	17376
2018	20795
2019	20250
2020	29915
2021	30049
2022	23202

To further analyze this area, we must look at the nature of the wicked security problem in regard to dynamism (threats, assets, structures, risks), pernicious dependencies, and complex coupled systems.

We also must look at the nature of the breaches, the reasons behind their increased severity, their frequency, and their velocity.

2.1.2. COSTS

Securing enterprise and its information asset has never been cheap, and it likely will become more expensive unless we change. The cost of security cannot be measured in currency alone; we should consider the effort and time as well. Although everything seemingly can be attributed a dollar value, we need to think about the overall cost and not just the expense. Given the limited time available for the purpose of this paper, an exact cost is challenging to ascertain; however, we can talk about the cost to an enterprise of a data breach.

Statistically the average cost to deal with such an incident has increased by 12.7% from USD 3.86 million in 2020 to USD 4.35 million in 2022 (IBM [26]).

The cost of a security breach is not only operational, but it also involves data loss or theft. A security breach can be of any nature; for example, an attack on a banking system can be entirely for money (the Bangladesh Bank SWIFT Heist in 2016 is a great example as the bank lost US $81 million). Regardless of the reason, a reputation loss occurs, and to rebuild that reputation, it will cost money, effort, and time. Regulatory fines can or will incur, and they will have to be paid. Under certain General Data Protection Regulation (GDPR) laws, for example, noncompliance could cost severe fines ranging between EUR €10 million and EUR €20 million.

A security breach response is another area where the cost cannot be calculated based solely on what is spent on incident response and related services, tools, and investigation processes. Legal responses need to be considered too, and in almost all security breaches, legal liabilities exist. For example, the litigation cost was approximately US $15.3 million in the Home Depot case in 2014 (ArcTitan [3]). And the most concerning area where the cost will be higher is the operational downtime of the business; any business closed because of a disruption will cost an organization money, which will be a combination of loss in sales during the time it is down and then the cost to bring it back online. Therefore, the cost is double fold, the amount of which is tough to determine as it will be dependent on the type and nature of the business.

Among other factors, we must also consider the cost spent to maintain the IT environment. Was the money spent on the right set of security architecture solutions and tools, or was it wasted on failed options? If the latter, then that money was an expensive mistake. For example, in the case of the Colonial Pipeline ransomware breach, the adversaries compromised the company simply because of a legacy VPN solution that did not have the capability of providing two-factor authentication paving the way to breach the single password. Although the company did spend approximately US $200 million in IT solutions that included security expenses in a span of five years, without the two-factor authentication for the VPN solution, the breach still occurred. Therefore, can we learn from this costly mistake and say that the money should be spent on the right set of solutions and tools rather than on just any option?

2.1.3. RATE OF DIGITAL TRANSFORMATION

The rapid rate at which digital transformation happens is certainly a concern from a cybersecurity point of view. The growth of digital transformation in 2020 alone was the equivalent of US $469.8 billion, and it is expected to cross US $1 trillion by 2025. This increase in the digital landscape has also increased the attack surface at a rapid speed, which also will lead to massive costs and a significant impact on business processes. One key aspect of digital transformation is integration and absorption of third-party services, which alone can lead to a high degree of security risks. It is very common to use third-party software libraries, packages and other tools during cloud-related transformations; attackers may use these third-party services as a pivot point to infiltrate enterprises. Thus, the increase in data breaches can also be attributed to third party usage in cloud adoption. Although we cannot avoid the fast pace of digital transformation for each business to stay relevant, at the same time, we must not let our guard down in securing our digital assets (see Bresnahan [4] and Eira [15]).

2.1.4. EVOLVING WORKPLACE CULTURE

During and after the COVID-19 pandemic, the workplace environment in most businesses either changed completely or evolved from the way it used to be. Employees often no longer only work from the confines of the organizational boundaries. As a result, various security challenges have emerged, involving identity, access to data, security monitoring, and risk and compliance security controls. In addition, insider threats are more of a reality now that employees no longer operate within the corporate boundary.

Those employees working remotely have access to company assets and data, and some of them use a home or a public Internet, which is not necessarily secured. Home wireless networks provide less security compared with a corporate network. As a result, adversaries might find a weak link to attack corporate assets, access confidential and sensitive information, and/or steal data. With the sudden increase in demand for portable computing devices (laptops, tablets, etc.), many employees must use personal devices for their official work, and these devices do not meet the security baseline and corporate standards in almost all cases.

Both situations are a realization that we should expect distributed environments in the future, so the question is, how do we secure data and assets with this new reality?

Remote work has also created another problem: colleagues who may be deep fakes (Dujmovic [13]).

It is not only about strengthening the infrastructure to tackle potential leakage from remote locations or distributed infrastructure, but also it is about whether you are dealing with a real colleague and a real person at the other end.

3. RETHINK

New and previously unrealized attack vectors require new protection and response architectures. Our current methods will fail with a continued rise in incidents and vulnerabilities. Our costs when a breach occurs only increase, and new patterns of our work and life emerge with remote communications.

Given the evolving landscape and ever-increasing breaches, we must create new approaches to how architectures are built. We must aim to create safe and secure digital environments for people to connect with and perform various functions and transactions in their personal lives or at work. We propose the following five principles as the basis of the architectures of the next-generation systems:

- Data collection and locus of control:
    - All data are collected before being stored or processed. Data may be collected in different contexts, either personal, organizational, or community. The data could be about a person, generated by a person, or about a thing, generated by a thing. Too often today we see data collection happen without the knowledge and consent of the person or thing sharing it. The data are stolen and then shared. Furthermore, that leads to potential breach situations. Per a *Newsweek* article by Piore [41], we conclude that if we enable systems to harness data without someone's knowledge, then bad actors or nation-states will use the same techniques to harness data as well. Therefore, we must consider how people can secure their information, including personal information, so it is not harnessed and out there, waiting to be breached.

The question that often arises is, who has control when that collection is happening? Can we push more control to a person to discourage unabated data collection and, hence, reduce these risks?

- Identity, applicable to anything anywhere:
  - Most digital constructs are based on the digital identity of people and things. When applied to humans in digital constructs, they take the form of online accounts. Many “things” out there do not even have an identity and no processes exist for how they should be managed. Two situations arise from current identity systems that are centralized and federated constructs: (1) A person may end up with multiple digital accounts and passwords in various properties, which then are the subject of privacy and security issues; and (2) a person, or a thing, cannot be truly verified in current identity systems, which can lead to situations in which bad actors can perform actions in an anonymous fashion or commit identity fraud.

The question is whether identity systems can be decentralized to mitigate security related problems and enable some form of verification, which can verify a person or a thing with real identity when communicating over the network. Current identity methods cannot.

- Storage and processing:
  - Collected data require proper storage and processing, which is typically done in a centralized manner. We advocate, however, that data should not be processed in a centralized manner but in a distributed one. As a result, we may evade bad actors (enemies) by not being in a place where the bad actor expects us to be and will strike. Also, with new constructs for how we work and live in general and for how computing happens with IoT, we should expect more distributed environments, which need to be managed well against cyber threats.

With this context, the question is, could we change storage and processing architectures in such a way that they are not centralized anymore? Can we distribute the data so that the sum of all pieces will form the whole and in the context of the data owner?

- Control assessment and application:
  - Too often controls are being applied and verified in digital environments. Controls help with governance and often in a security context. Usually, they come from a single source for an environment. Failure of a control or of the source of controls should not lead to failure of the environment.

The question is whether we could create environments where controls are sourced from different vendors and sources to avoid failures if a control or a vendor fails.

- Recovery in case of a failure:
    - We have observed that when a failure occurs, usually prolonged recovery battle ensues. It begins with figuring out a bad component (or vulnerabilities) and then another effort to replace it. The list of vulnerabilities has been increasing each year, and finding vulnerabilities quickly has become more difficult. In most cases, the bad component or a breach is not even discovered for a long time. We advocate for continuous verification at the component level and for forming possibilities to recover quickly when failures are detected.

The question is, how do we identify that something has gone wrong and recover from it quickly?

4. CYBERSECURITY APPROACH FOR NEXT GENERATION

The Internet is at an inflection point and with it are our experiences. As technologies progress, people are realizing the risks and dangers they face in their lives from cybersecurity issues. We should not reach a place where people relate the Internet to security problems and, hence, not trust it, leading to its avoidance. As we discussed, organizations are increasingly under pressure to maintain secure environments, but given our current architectures, policies, and processes, the breaches keep happening every day, with the average cost per breach increasing year over year, reaching its highest in 2021.

Recalling Virginia Abbate’s quote that with the Internet, we have built a bank that people want to break into, we must consider whether the bank (aka “the Internet”) should continue to collect all the currency (aka “the data”) often without people’s knowledge and store it centrally. Instead, wouldn’t it be better to allow people to have more control over their currency (data) and to store it in a more distributed fashion? In 2022, the onslaught of daily breaches should be a reminder that the Internet’s architecture needs to approach cybersecurity for the next generation differently. We should aim to be in a much better situation by 2030 or even 2025. New technology areas and our inability to control breaches today present us with a real danger of CBSEs or cyber-attacks (Herbolzheimer [24]).

We propose the following five principles based on the methods discussed earlier:

A. *Human Centricity:* Given that more and unnecessary data collection can lead to both privacy and security problems, could we create situations in which a person can control their data and information flow into the environment? We recommend a “human-centric” environment where a person has control on how their data flows in and is used. As a result, the locus of control shifts to the holder or generator of data. Therefore, we propose “human centricity” as the first principle.

Benefits: Prevents unwanted data flow into the system. Enables privacy and hence security at the edge.

With human centricity, we propose to build better controls for the flow of information from a human standpoint that may lead to less but relevant and compliant data collection. We would assess whether these controls can lead to lowering unabated data collection, which has implications on privacy and security, at both the personal and national levels.

B. *Decentralized Identity:* Human centricity goes hand in hand with identity. On the one hand, a person or a thing needs to be verified against the real identity so that fakes, bots, or malicious actors (such as originators of phishing emails) can be removed; on the other hand, a move should occur toward less central storage of account information, passwords, and so on. In today’s centralized and federated environments, this cannot be overcome; however, new constructs of identity, such as decentralized identifiers (DIDs; as recommended by W3C [52]), self-sovereign identities, and verifiable credentials, together can help achieve these goals. Hence, we propose “decentralized identity” as the second principle.

Benefits: Reduces centralization of information, avoids single points of failures, provides for stronger authentication, provides for peer–peer communication channels, reduces identity fraud, and enables two-way verification and single sign-on.

As a result, we propose defining a decentralized and self-sovereign identity with verifiable credentials, which is applicable to both humans and things (such as IoT) and assess whether such a situation will lead to less centralization of identity and realization of benefits, as stated previously.

C. *Distribution of Data Storage and Processing:* Although the identity data are decentralized back to a person or a thing, which can help manage large, distributed environments, such as IoT or software popping up everywhere, we recognize that some data flow and storage will occur into the systems. Could we create situations in which data cannot be constructed as a whole if a single system is breached? Hence, we propose "data storage and processing distribution" as the third principle.

Benefits: Increased resilience, in which failure of one part does not lead to failure of the whole system.

With distribution in storage and processing, we propose to define methods by which the data and information are not stored or processed in entirety in a single place, but they are spread across various systems in the context of the owner. With such methods, we will ensure that if part of the storage or processing system fails, then the entire system does not fail.

D. *Heterogeneous Control Applications:* Systems fail if a control or set of controls from a single provider or source fails. This issue is especially important when we work with the next-generation solutions, such as AI or Quantum, in which 100% reliable defense approaches have not yet been invented, and a need exists for combinations of controls on each step of the solution lifecycle from development to operations. Hence, we propose that controls sourced from various places and vendors be applied, making "heterogenous control applications" the fourth principle.

Benefits: Increased resilience, which reduces dependence on a single set of controls or service.

With heterogenous control systems, we propose finding ways to apply controls from multiple sources to a system and assessing whether failure of one control or a source of control leads to failure of a system.

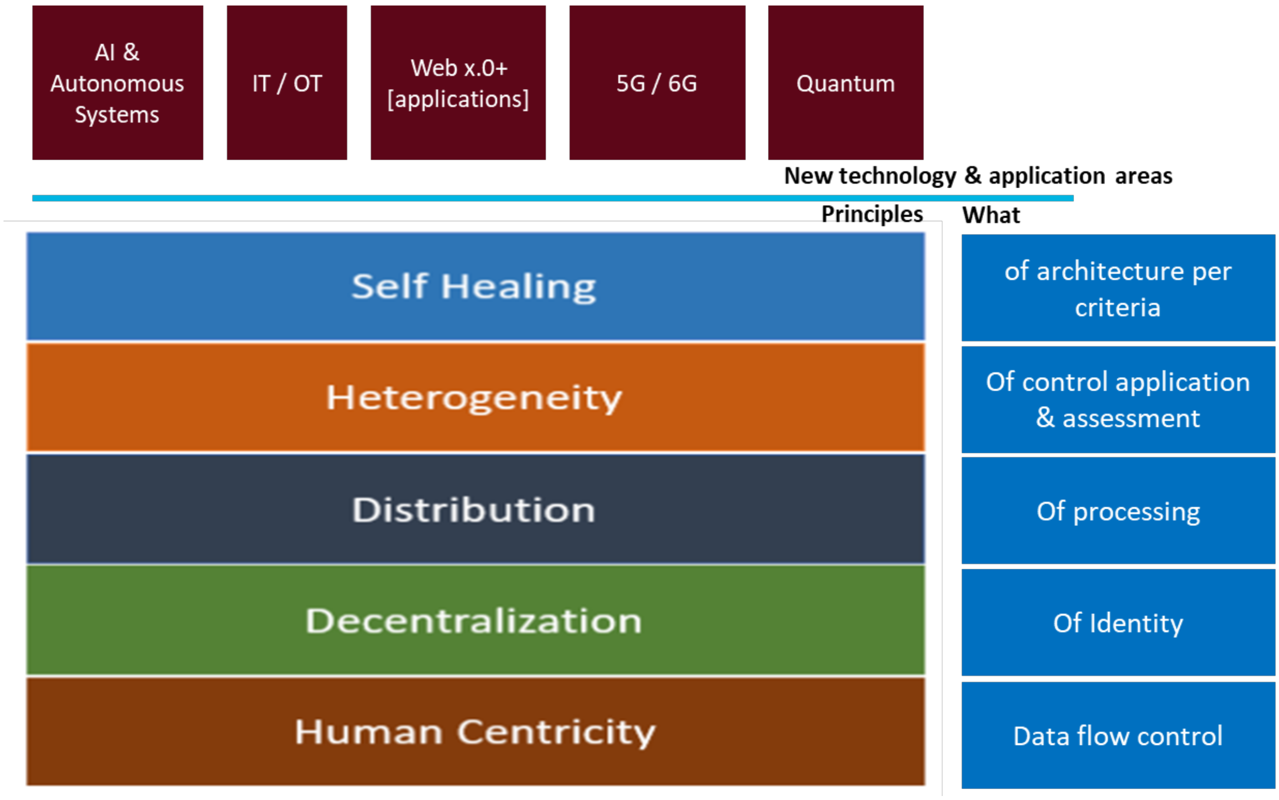
E. *Self-healing:* Despite our best efforts, failures and breaches will still occur. The key lies in identifying the failure situation quickly and in recovering from it in a seamless fashion. To do so, continuous verification and identification of the components and their failure states must occur using the criteria of security. Hence, we propose "self-healing" as the fifth principle.

Benefits: Continuous verification for quick recovery from an incident.

With self-healing, we propose finding methods and ways for how a system, service, or product can adjust and self-heal based on various types of triggers or criteria. The triggers or criteria could have many types, including regulatory changes, software updates, better control availability, or failure (or potential failure) of a subcomponent. Building self-healing systems will require us to continuously measure systems, services, or products at a subcomponent level and to keep adjusting the security configuration based on observed triggers or criteria. As a vision, we would like to explore how a system, service, or product can be dynamically protected (in a self-healing manner) based on those observed criteria.

We propose these five principles as the basis of the assessment of innovative technology areas, which are (1) AI and autonomous systems, (2) IT/OT, (3) Web X.0+, (4) 5G/6G, and (5) quantum computing (FIGURE 5). The aim is to build systems that would avoid CBSEs.

FIGURE 5 Proposed Architecture Principles and New Areas



How do we ensure that data remain secure to increase human, societal, and national security when using such systems? How do we ensure security is maintained during these situations? Can we build more secure next-generation systems with the five proposed principles, or do we need to consider more principles?

4.1. ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS

AI systems are software (and possibly hardware) systems that act in the physical or digital dimension by perceiving their environments through data acquisition, interpreting data, and reasoning/making decisions on the knowledge, or processing the information, derived from these data. AI systems can either use symbolic rules or learn a numeric model, and they can adapt their behavior by analyzing how the environment is affected by their previous actions.

As a scientific discipline, AI includes several approaches and techniques, such as machine learning (ML, of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).

> *"Machine learning systems differ from traditional software-based systems in that the behavior of ML systems is not specified directly in code but is learned from data."*
>
> *(Breck et al. [4])*

With regard to how AI and autonomous systems work, we will examine how AI transforms the threat landscape. We will discuss the cybersecurity threat models of AI systems and how they differ from conventional systems, as well as discuss ways to make these systems resilient and self-healing so that they can be reliably used for decision-making.

In various situations, data must be secured for AI and autonomous systems, for instance, during data input, data storage and processing, and run time when an AI or autonomous system takes an action. AI is a new way of developing solutions called "Software 2.0." Here, instead of code, we have algorithms, and these algorithms offer a new attack surface. Therefore, the stakes are higher as the responsibilities of AI are more significant than the ones of traditional software. Examples of AI incidents are already happening. For instance, Zillow lost US $6 billion of its valuation due to its problems with AI algorithms. Tesla's autonomous cars, as another example, can be made to crash into airplanes or can be fooled into changing lanes. Even cybersecurity solutions such as the Cylance AI-driven Malware detection engine can became vulnerable to attacks.

In the old paradigm, software vulnerabilities often occurred because of improper command filtering, incorrect data handling, or design flaws. Now, however, AI commands can be visual, audial, or textual. Thus, filtering, handling, and detecting malicious inputs and interactions is much more difficult. Only in the last decade have researchers released more than 2,000 papers about different types of vulnerabilities in AI algorithms, also called "adversarial attacks." Adversarial attacks on AI can be separated into the following three categories:

1. Manipulation attacks, such as evasion, allow adversaries to bypass expected AI behavior or even make AI systems perform unexpected jobs.
2. Infection attacks, such as poisoning, can sabotage the quality of AI decisions and enable stealth control of AI systems.
3. Exfiltration attacks aim to steal data or algorithm logic from AI systems.

Unfortunately, AI cannot be secure out of the box, and current cybersecurity solutions like code analysis or firewalls cannot deal with AI vulnerabilities as software security solutions cannot help with hardware security. Autonomous systems such as modern autonomous vehicles could be enormously complex. This complexity may lead to thorny cybersecurity challenges with real-world consequences. Unlike a classic cyberattack in which data are stolen or ransomware locks down a system, cyberattacks on cars could lead to property damage or injuries (IEEE Staff [27]).

We need new solutions for assessing and securing AI applications and autonomous systems. Could we leverage the architecture principles we proposed earlier to establish secure AI and autonomous systems? Different environments may require different solutions. Therefore, depending on the environment, these principles could be sufficient, other principles could be needed, or a completely different paradigm could be required. For example, in the **development environment in ML, which is used for discovery and model training,** large amounts of production data are necessary; thus, the development environment for ML should be secure and have strict access controls and back-up, and recovery should be required. The development environment for traditional software engineering, on the other hand, looks more like a production environment.

4.2. INTERNET OF THINGS

With the convergence of IT systems and operational technologies like smart sensors and actuators, the IoT covers everything from wireless heart monitors to autonomous cars. The IoT can supercharge the global economy by enabling a variety of new business models and applications. But it can also expose industries and consumers to unanticipated security issues. The IoT promises to deliver substantial productivity improvements over the coming decade, but very few IoT assets feature adequate security, something many business leaders do not know. As a result, many companies expect to run what they presume to be high-integrity applications in what they do not realize are low-integrity environments.

With our work in IoT, we plan to do the following:

- **Engineer trust into connected products.**

  Apply "secure-by-design" principles throughout a product's development, from concept ideation to series manufacturing, instead of addressing security issues at the end of the cycle. Designers should also build in operational controls when originally configuring systems to verify that all component behaviors conform to expected operational norms and undertake a complete analysis of a system's threat-versus-risk profile. Engineering responses should focus on eliminating undesirable outcomes (e.g., breached customer data).

- **Adopt a new operational mindset.**

  Monitor the IoT's operational and security health continuously—a big data challenge that requires a big data solution. Furthermore, an IoT system might depend on other such systems, so we should design for failure survival and focus on resiliency, starting with anomaly detection capabilities enabled by machine learning and effective responses.

- **Develop contextualized threat models.**

  Build tailored threat models that consider key business goals, the underlying technical infrastructure, and potential threats that can disrupt the business. Such models can help to prioritize IoT security threats and uncover blind spots.

  The IoT is now a fixture of modern digital life, but as technology improves, we will see more reliance on complex, Internet-connected devices that will be deployed in consumer and commercial uses over time, and we will witness the exponential growth of IoT devices now and in the future. IoT devices are modern marvels with the ability to collect data and track information in ways that were not possible in the past.

To get an idea of the scope, scale, and ubiquitous nature of IoT device uses, the following statistics help to tell the story:

- The number of Internet-connected devices is expected to increase from 31 billion in 2020 to 35 billion in 2021 and 75 billion in 2025 (Statista Research Department [47]), making it a widely distributed infrastructure that needs management.

- By 2026, experts estimate that the IoT device market will reach US $1.1 trillion (Security Today).

- IoT connections worldwide generated 13.6 zettabytes (ZB) of data in 2019. This data volume of IoT devices is expected to reach 79.4 ZB by 2025 (IDC**Error! Reference source not found.**). How much of this data should be collected?

IoT devices have many security-related problems as cited by Langkemper [31]. They range from access control issues to vulnerability management to privacy-related issues. The rapid growth of technologies expanded availability, and combinations of technological innovations that can be used in IoT devices create more complexity and difficulty in preventing cybersecurity and data privacy risks. A few points that highlight challenges with IoT include the many devices distributed out, the difficulty IoT device users have in knowing what data are being captured, and the challenge of properly identifying devices. The consumer and commercial marketplaces are hungry for innovations in the IoT space, but these IoT uses require careful consideration, planning, and tracking to understand not only the benefits but also the risks. As IoT becomes more vital to the digital future, we must proactively look at potential human harm, cybersecurity risks, and data privacy challenges created by IoT that we likely have never contemplated.

4.3. WEB X.0+

The Web was first designed to connect a handful of scientists who wanted to have more interaction and collaboration. It, however, kept evolving rapidly and ultimately became what it is today. The Web has massively influenced everything that we have been doing so far and will continue to do. It is generally categorized as Web 1.0, 2.0, 3.0, and X.0 (for all future expansions). Our focus of this paper is on Web X.0 and beyond (Web X.0+).

Historically, Web 1.0 provided a static content delivery platform. Web 2.0 then allowed users to be more interactive and had the ability to generate some content, which evolved into Web 3.0, which we experience today. Web 3.0 revolutionized the Internet completely by allowing people to be creative and have more ability to build multi-user applications that allow others to use it for various purposes, business, and collaboration.

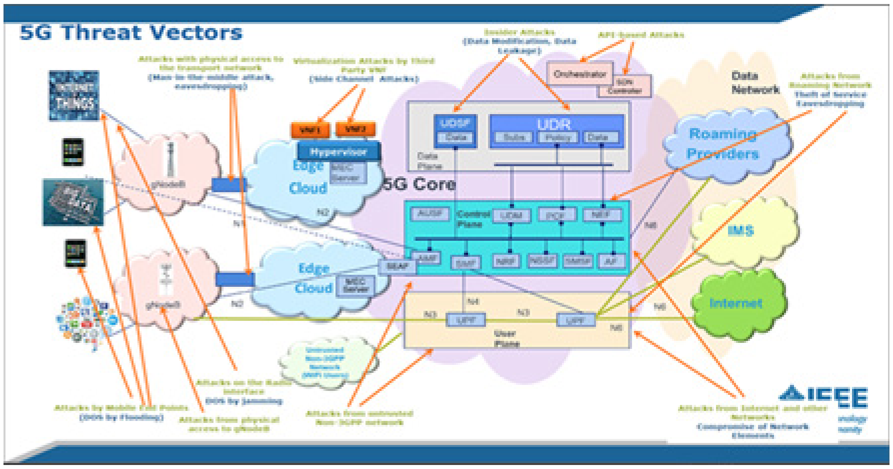
Web X.0 represents the next generation of Internet where human–machine interactions will be possible, along with many other advanced applications, like transactions via blockchain technologies and the Metaverse. With a combination of AI and Web X.0+, many experts also speculate that the next generation of users could interact with Web X.0+ via human implants with ease. Even though this possibility feels exciting at this moment, with some of its features already available to use, for instance, using one of the virtual assistant control home appliances (interaction with the physical world) and other devices remotely via a smart watch, a mass transformation is still a distant future.

As we have discussed, no Web technology is fully secure, and they all have massive security risks with exposure to many threats. Web X.0 will be no different, and in fact, it will be more prone to security risks and threats and more attacks might be possible. But unlike its predecessors, Web 1.0, 2.0, and 3.0, we can create it more securely from the ground up. The charter of the subcommittee for Web X.0+ calls for researching, identifying, and evaluating possible security risks and then making recommendations and/or suggestions to address them.

4.4. 5G/6G

The 5G, 6G, and future networks have many more threat vectors as shown in FIGURE 6. The different 5G service classes—eMBB, mMTC, and URLLC—will bring great security challenges, as will O-RAN. With such a broad attack surface, a new way of thinking about network security is needed. In addition, the vast nature of these systems means that they will require a greater use of autonomy. These networks must learn on the fly to cope with new and improved threats to the ecosystem. AI and ML can provide some level of autonomy. However, to date for 5G/6G systems, performance optimizations have been focused on channel and network optimizations; learning-based security architecture and security signal processing algorithm has been lacking.

FIGURE 6 5G Threat Vectors


5G Threat Vectors
Insider Attacks (Data Modification, Data Leakage)
API-based Attacks
Attacks with physical access to the transport network (Man-in-the-middle attack, eavesdropping)
Virtualization Attacks by third Party VNF (Side Channel Attacks)
Orchestrator
SDN Controller
Data Network
Attacks from Roaming Network Theft of Service Eavesdropping
INTERNET THINGS
VNF1
VNF2
Hypervisor
Edge Cloud
MEC Server
UDSF
Data
UDR
Subs
Policy
Data
Data Plane
5G Core
Roaming Providers
gNodeB
N2
N1
AUSF
Control Plane
UDM
PCF
NEF
N6
IMS
BIG DATA
AMF
SEAF
SMF
NRF
NSSF
SMSF
AF
Edge Cloud
MEC Server
gNodeB
N2
N4
N3
N3
UPF
UPF
N6
N6
Internet
User Plane
Untrusted Non-3GPP Network (WiFi Users)
Attacks on the Radio Interface DOS by Jamming
Attacks by Mobile End Points (DOS by Flooding)
Attacks from physical access to gNodeB
Attacks from untrusted Non-3GPP network
Attacks from Internet and other Networks Compromise of Network Elements
IEEE

New cybersecurity architectures for 5G/6G systems need to be developed that challenge the traditional way of thinking about security (i.e., simply thinking that firewalls and anti-virus software are the answer) to protect a wide range of systems that include terrestrial, satellite, and IoT. Furthermore, there are homogeneous systems, which comprise a single service provider, and heterogeneous systems, which comprise more than one provider. Consequently, new thinking about securing the 5G/B5G ecosystem is needed.

A good starting point to begin this journey is the security work done as part of the IEEE Future Networks Initiative (FNI) Security Working Group from IEEE's Communication Society as illustrated in their 2022 International Network Generations Roadmap (INGR) on Security and Privacy. Important topics from security management and orchestration to AI/ML security to trust and privacy were presented in this work. However, more work needs to be done.

How could we apply the architecture principles to establish secure 5G/6G networks?

We at IEEE "Cyber Security for Next Generation Connectivity Systems" plan to further this work by looking at new advances in security and privacy such as zero trust architecture implementations, real-time network security monitoring and situational awareness, open interfaces for security notification, security signal processing via artificial intelligence and machine learning, and more. In addition, 5G/6G are the next-generation wireless systems that will bring processing closer to the user. Although these communication technologies will be the impetus behind Web X.0+ applications and more ubiquitous processing, new security challenges will appear as these technologies evolve.

4.5. QUANTUM INFORMATION SYSTEMS (QIS)

In 1999, the National Science Foundation (NSF) held a workshop on quantum information science (QIS) to explore how this emerging field could affect the science and technology effort in computer science. The workgroup declared that QIS has the potential to cause revolutionary advances in the fields of science and engineering involving computation, communication, precision measurement, and fundamental quantum science (NSF [36]). The NSF-WG-QIS also helped to define areas of specific interest that would aid in the worldwide development of theories and validation of proof that the emerging field would need to document. The roots of this field go back approximately 20 years to when pioneers such as Charles Bennett, Paul Benioff, Richard Feynman, and others began thinking about the implications of combining quantum mechanics with the classic Turing computing machines (NSF [36]). In addition, the NSF-WG-QIS also posited that advances in the field would increase geopolitical, transnational, and localized competitiveness for IT during the coming century.

Although not meant to be comprehensive, the following core concepts should be understood when conducting analysis of the possibilities that QIS may provide:

1. Quantum Information Theory
    a. Computing
        i. Software (CSL)
            1. Implementation
        ii. Hardware (BRL)
            1. Integration Stabilization
            2. Types of Qubits
    b. Cryptography
    c. Communications
    d. Distributed Algorithms
        i. Quantum Proof Algorithms
            1. Complexity Theories
        ii. Quantum Programming Language (QPL)
            1. High-Level Programming Language (HLPL)
    e. Quantum Circuit Design
    f. Quantum Compilers

The field of QIS saw a large expansion because Peter Sho demonstrated that a quantum computing capability could factor exceptionally large numbers super efficiently (NSF [36]). For the last 20 years, the field of QIS has continued to grow and has finally reached a major milestone, the potential to provide increased performance in several areas of research as posited by the NSF-WG-QIS in 2000, to include the ability to begin to break security encryption, elements of sensing, quantum key distribution (QKD) solutions, and enhancements to random number generators. Thus, these types of enhancements also have a downside, which the IEEE Cyber Security for Next Generation Connectivity Systems Group is researching to create new architectures.

The group has determined that the need to understand the quantum-attack threat patterns may take time, and it has started the collection process to better inform its members of the emerging potential threat and to establish workgroups with a multidiscipline approach to include both a cyber and a QIS fusion workgroup. The next generation of fusion-based cybersecurity and QIS-trained persons will be able to develop the needed cyber doctrine required to build the next generation of architectures to enhance security while increasing protections required to thwart a quantum-based cyber-attack. Elements of the CVRF, which is the super dataset collected by

MITRE and the National Institute of Standards and Technology (NIST), also have reverse mappings to known vulnerabilities to the NPC Repository, NIST 800-53 Rev. 4 controls, SCAP Validations Tools, and United States Government Configuration Baseline (USGCB) initiative discussed in 2.1.1.

The group has begun the process of exploring the impact of the threat vulnerability report to include the Common Vulnerableness and Exposure (CVE)'s dataset in FIGURE 4. The graphic demonstrates that the CVE dataset has grown as the threat vectors and vulnerabilities of software and hardware have been developed. If the use of QIS creates the ability to increase these numbers, it will become a much larger attack-surface space that must be understood to provide the next generation of cyber protection.

5. CITATIONS

The sources in the following list have either been referenced within this paper or may be useful for additional reading:

[1] Adebayo, K. S., "Why CISA wants to release a new version of its Zero Trust Maturity Model," *VentureBeat*, July 29, 2022. https://venturebeat.com/security/cisa-wants-to-release-a-new-version-of-its-zero-trust-maturity-model-%ef%bf%bc/.

[2] Adversa Staff, "The road to secure and trusted AI," *Adversa*, 2022. https://adversa.ai/report-secure-and-trusted-ai/.

[3] ArcTitan Staff, "Case study: Home Depot data breach cost $179 million," *ArcTitan*, Aug. 20, 2021. .https://www.arctitan.com/blog/case-study-data-breach-cost-home-depot-179-million/.

[4] Eric Breck, Eric, Shanqing Cai, Eric Nielsen, Michael Salib, and D. Sculley, *Proceedings of IEEE Big Data* (2017). The ML Test Score: A Rubric for ML Production Readiness and Technical Debt Reduction.

[5] Bresnahan, E., "How digital transformation impacts IT And cyber risk programs," *CyberSaint Security*, 2022. https://www.cybersaint.io/blog/managing-risk-in-digital-transformation/.

[6] Cameron, K., "Identity services 2020," *KuppingerCore Analysts*, May 13, 2015. https://www.kuppingercole.com/watch/eic15_keynote_cameron/.

[7] Cameron, K., “The laws of identity,” *Computer Science*, 2005. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf/.

[8] Columbus, L., “Why the future of APIs must include zero trust,” *VentureBeat*, Aug. 1, 2022. https://venturebeat-com.cdn.ampproject.org/c/s/venturebeat.com/2022/08/01/why-the-future-of-apis-must-include-zero-trust/amp/.

[9] Computer Hope Staff, “What are the advantages of the Internet?” *Computer Hope*, Jan. 12, 2019. https://www.computerhope.com/issues/ch001808.htm/.

[10] CSIS Staff, “Significant cyber incidents,” *Center for Strategic & International Studies Blog*, Aug. 2022. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents/.

[11] Deloitte’s State of AI in the Enterprise, 3rd Edition, https://www2.deloitte.com/cn/en/pages/about-deloitte/articles/state-of-ai-in-the-enterprise-3rd-edition.html.

[12] DeRusha, C., “Enhancing the security of the software supply chain to deliver a secure government experience,” *The White House*, Sept. 14, 2022. https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/.

[13] Dujmovic, J., “Remote work has created yet another problem—Colleagues who may be deepfakes,” *MarketWatch*, Aug. 5, 2022. https://www-marketwatch-com.cdn.ampproject.org/c/s/www.marketwatch.com/amp/story/remote-work-has-created-yet-another-problem-colleagues-who-may-be-deepfakes-11659727993/.

[14] Eich, B., “Surveillance on UK council websites,” *Brave*, Feb. 2020. https://brave.com/static-assets/files/Surveillance-on-UK-council-websites_compressed_version.pdf.

[15] Eira, A., “72 vital digital transformation statistics: 2021/2022 spending, adoption, analysis & data,” *FinancesOnline*, 2022. https://financesonline.com/digital-transformation-statistics/.

[16] Elgan, M., “You just hired a deepfake. Get ready for the rise of imposter employees,” *Protocol*, Aug. 22, 2022. https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/.

[17] Ermetic Team, “93% of security professionals say their identity breaches could have been prevented,” *Ermetic*, Undated. https://ermetic.com/blog/cloud/93-of-security-professionals-say-their-identity-breaches-could-have-been-prevented/.

[18] Feal, Á., J. Gamba, J. Tapiador, P. Wijesekera, J. Reardon, S. Egelman, and N. Vallina-Rodriguez, *Don't Accept Candy from Strangers: An Analysis of Third-Party Mobile SDKs*. IMDEA Network Institute. https://dspace.networks.imdea.org/handle/20.500.12761/1565.

[19] FBI Internet Crime Complaint Centre, 2021, Internet Crime Complaint Center - Wikipedia.

[20] Franceschi-Bicchierai, L., “Hackers took over a commercial satellite to broadcast hacker movies,” *VICE*, Aug. 15, 2022. https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en/article/y3pwqx/hackers-took-over-a-commercial-satellite-to-broadcast-hacker-movies/.

[21] Frost Radar™: US Healthcare Cybersecurity Market, 2020.

[22] German Marshall Fund, 2020. Technology and Innovation | Strengthening Transatlantic Cooperation (gmfus.org).

[23] Help Net Security Staff, “Ransomware is not going anywhere: Attacks are up 24%,” *Help Net Security*, Aug. 12, 2022. https://www.helpnetsecurity.com/2022/08/12/increase-ransomware-attacks/.

[24] Herbolzheimer, C., “Preparing for a Black Swan cyberattack,” *Harvard Business Review*, Sept. 14, 2016. https://hbr.org/2016/09/preparing-for-a-black-swan-cyberattack/.

[25] Huitema, C., et al., *Introduction to Trust over IP* (White paper). Trust over IP (ToIP) Foundation, Nov. 17, 2021. https://trustoverip.org/permalink/Introduction-to-ToIP-V2.0-2021-11-17.pdf.

[26] IBM Staff, “Cost of a data breach 2022,” *IBM*, 2022. https://www.ibm.com/reports/data-breach/.

[27] IDC, IoT devices to generate 79.4ZB of data in 2025, says IDC.

[28] IEEE Staff, “Autonomous vehicles: Cyber-physical risk on a massive scale,” *IEEE Transmitter*, July 13, 2022. https://transmitter.ieee.org/autonomous-vehicles-cyber-physical-risk-on-a-massive-scale/?utm_campaign=Autonomous+Vehicles,Cyber+Security,IEEE+Transmitter+-

+BD&utm_content=why_is_cybersecurity_a_cr&utm_medium=organic&utm_source=linkedin/.

[29] Kelly, S., and J. Resnick-ault, “One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators,” *Reuters*, June 8, 2021. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

[30] Krebs, B., “It might be our data, but it’s not our breach,” *Krebs on Security*, Aug. 11, 2022. https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/.

[31] Langkemper, S., “The most important security problems with IoT devices,” *Eurofins*, Sept. 10, 2020. https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices/.

[32] Lessig, L., “Code is law,” *Harvard Magazine*, Jan. 1, 2000. https://www.harvardmagazine.com/2000/01/code-is-law-html/.

[33] Maguire, M., “Politicians warned not to discuss work near Alexa, Google Home,” *Newstalk*, Aug. 14, 2022. https://www.newstalk.com/uncategorized/big-brother-politicians-warned-not-to-discuss-work-near-alexa-google-home-1372431/.

[34] Nair, V., G. M. Garrido, and D. Song, “Exploring the unprecedented privacy risks of the Metaverse,” *arXiv:2207.13176v1*, July 26, 2022. https://arxiv.org/pdf/2207.13176.pdf.

[35] Nash, J., “ID.me finds itself accused of biometric data privacy violation,” *Biometric Update*, Aug. 10, 2022. https://www.biometricupdate.com/202208/id-me-finds-itself-accused-of-biometric-data-privacy-violation/.

[36] NSF Staff, “Quantum information science and engineering research at NSF,” *National Science Foundation*, 2000. https://www.nsf.gov/mps/quantum/quantum_research_at_nsf.jsp/.

[37] Palmer, D., “Critical infrastructure is under attack from hackers. Securing it needs to be a priority - before it's too late,” *ZDNET*, Aug. 21, 2022. https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/critical-infrastructure-is-under-attack-from-hackers-securing-it-needs-to-be-a-priority-right-now/.

[38] Pegoraro, R., “Ex-CISA chief's advice at Black Hat: Make security valuable and attacks costly,” *PCMag*, Aug, 10, 2022. https://www.pcmag.com/news/ex-cisa-chiefs-advice-at-black-hat-make-security-

valuable-and-attacks-costly/.

[39] Pelzer, L. M., “The true cost of cybersecurity incidents: The problem,” *Palo Alto Networks*, June 25, 2021. https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/.

[40] Pew Research Center, 2019, https://www.pewresearch.org/.

[41] Piore, A., “Beijing's plan to control the world’s data: Out-google Google,” *Newsweek,* Sept. 7, 2022. https://www.newsweek.com/2022/09/16/beijings-plan-control-worlds-data-out-google-google-1740426.html/.

[42] Plumb, T., “SBOMs: What they are and why organizations need them,” *VentureBeat*, July 29, 2022. https://venturebeat.com/security/sboms-what-they-are-and-why-organizations-need-them/.

[43] Ponemon Institute, 2020, https://www.ponemon.org/.

[44] Preukschat, A., and D. Reed, *Self-Sovereign Identity*. Shelter Island, NY: Manning, May 2021.

[45] Reed, D., and V. Syntez, *Design Principles for the Trust over IP Stack*. Trust over IP (ToIP) Foundation, Nov. 17, 2021. https://trustoverip.org/permalink/Design-Principles-for-the-ToIP-Stack-V1.0-2022-01-17.pdf.

[46] Risk Based Security, 2021, https://www.riskbasedsecurity.com/2021/.

[47] Statista Research Department, “Internet of Things—Number of connected devices worldwide 2015-2025,” *Statista*, Nov. 27, 2016. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[48] Timberg, C., “The real story of how the Internet became so vulnerable,” *The Washington Post*, May 30, 2015. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

[49] Toulas, B., “FBI warns of residential proxies used in credential stuffing attacks,” *Bleepingcomputer.com*, Aug. 22, 2022. https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/fbi-warns-of-residential-proxies-used-in-credential-stuffing-attacks/amp/.

[50] Toulas, B., “Hackers scan for vulnerabilities within 15 minutes of disclosure,” *Bleepingcomputer.com*, July 26, 2022. https://www.bleepingcomputer.com/news/security/hackers-scan-for-vulnerabilities-within-15-minutes-of-disclosure/.

[51] Toulas, B., “Hackers stole $620 million from Axie Infinity via fake job interviews,” *Bleepingcomputer.com,* July 12, 2022. https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/.

[52] W3C Staff, “Decentralized Identifiers (DIDs) v1.0,” *W3C*, July 19, 2022. https://www.w3.org/TR/did-core/.

[53] W3C Staff, “Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation,” *W3C*, July 19, 2022. https://www.w3.org/2022/07/pressrelease-did-rec.html.en/.

[54] Watchorn, M. S., Cyber Black Swan Event—Cyber security landscape ontology and taxonomy—Integration analysis and the critical infrastructure protection,” *LinkedIn*, Aug. 28, 2018. https://www.linkedin.com/pulse/cyber-black-swan-event-security-landscape-ontology-dr-merrick-s-/.

[55] WhoTracks.Me, 2019, WhoTracks.me: Find out where you're being tracked on the web (cliqz.com).

[56] Winder, D., “Cisco hacked: Ransomware gang claims it has 2.8GB of data,” *Forbes*, Aug. 13, 2022. https://www.forbes.com/sites/daveywinder/2022/08/13/cisco-hacked-ransomware-gang-claims-it-has-28gb-of-data/amp/.

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571