IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS REPORT

IEEE

CYBERSECURITY FOR NEXT-GENERATION CONNECTIVITY SYSTEMS

RETHINKING DIGITAL ARCHITECTURES TO SAFEGUARD THE NEXT GENERATION FROM CYBERSECURITY BREACHES

Documents
Document Sharing Hub

Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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.

Documents
Document Sharing Hub
Copyright © 2022 IEEE. All rights reserved.
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 4 November 2022. Printed in the United States of America.

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

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

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

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

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

Copyright © 2022 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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.

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

TABLE OF CONTENTS

ABSTRACT 6

1. INTERNET AND SECURITY 7

2. INTERNET IS AT AN INFLECTION POINT 10

2.1.1. INCIDENTS & VULNERABILITIES 11
2.1.2. COSTS 13
2.1.3. RATE OF DIGITAL TRANSFORMATION 14
2.1.4. EVOLVING WORKPLACE CULTURE 14

3. RETHINK 15

4. CYBER SECURITY APPROACH FOR NEXT GENERATION 17

4.1. ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS 21
4.2. INTERNET OF THINGS 22
4.3. WEB X.0+ 24
4.4. 5G/6G 25
4.5. QUANTUM INFORMATION SYSTEMS (QIS) 26

5. CITATIONS 28

Documents
Document Sharing Hub

Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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.

Copyright © 2022 IEEE. All rights reserved.

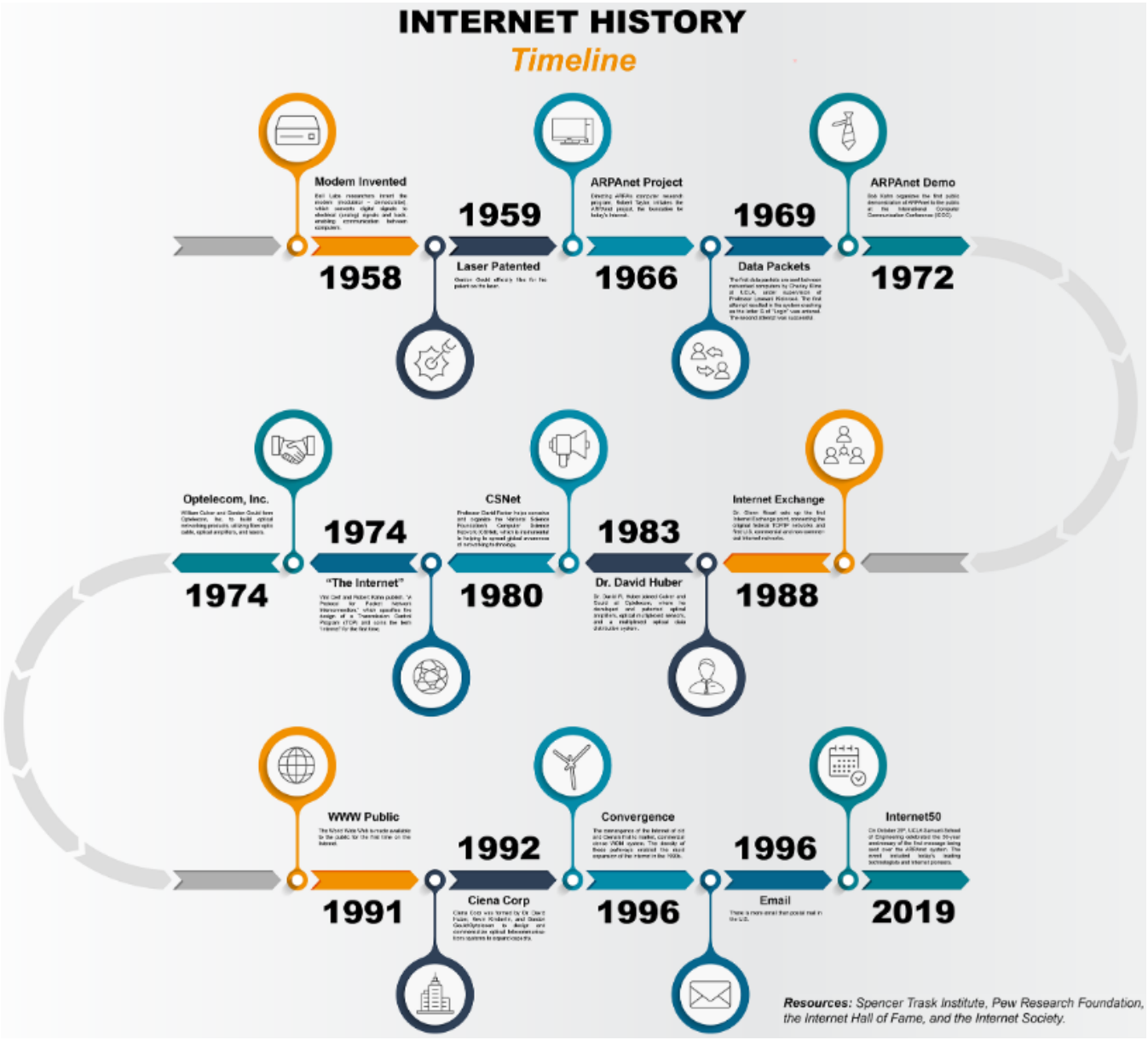
Documents
Document Sharing Hub

Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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



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

Copyright © 2022 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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]).

Copyright © 2022 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

- 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.

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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.

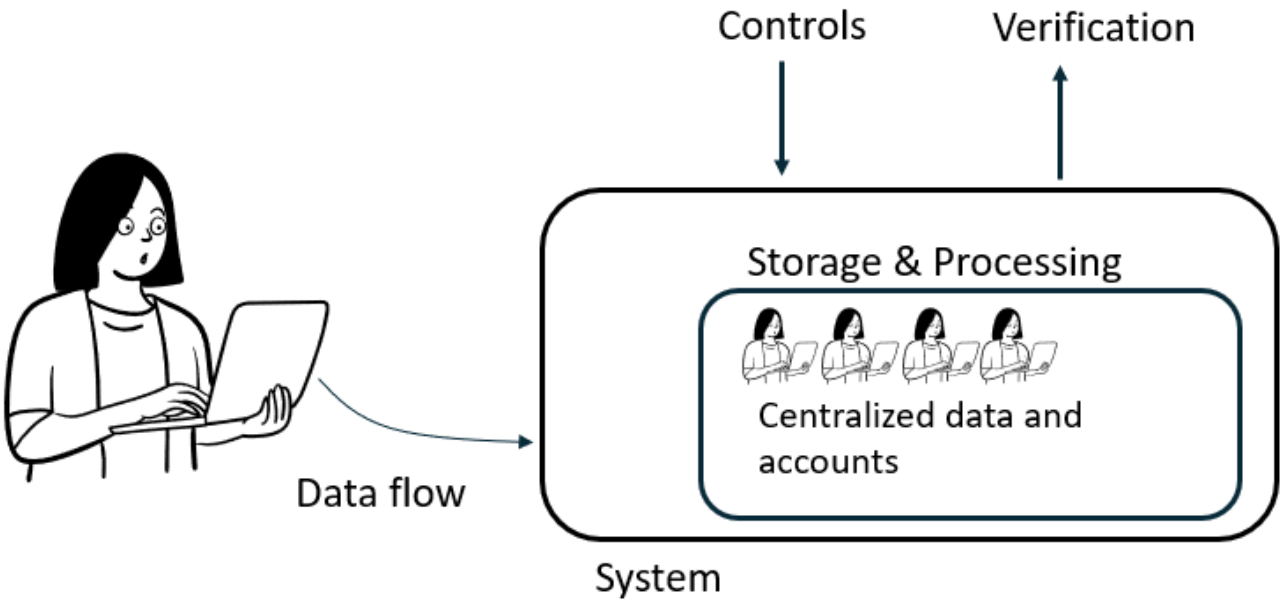
We must prepare for the following five technology and application areas of the future:

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

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...

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.

Copyright © 2022 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Cybersecurity for Next-Generation Connectivity Systems—Rethinking Digital Architectures to Safeguard the Next Generation Fro...