

cybersecurity topics for research

cybersecurity topics for research are crucial for advancing knowledge and developing innovative solutions to combat the ever-evolving threats in the digital world. As cyberattacks become more sophisticated, the demand for in-depth research in cybersecurity grows significantly. This article explores a wide range of cybersecurity topics for research, providing valuable insights into current trends, challenges, and emerging technologies. Researchers and professionals can benefit from understanding these topics to enhance security measures, protect sensitive data, and improve overall cyber resilience. From threat detection to cryptography, this article covers diverse areas that are vital for securing digital infrastructure. The following sections outline some of the most relevant and impactful cybersecurity topics for research today.

- Emerging Cyber Threats and Attack Vectors
- Cryptography and Data Protection
- Network Security and Intrusion Detection
- Artificial Intelligence in Cybersecurity
- Cloud Security Challenges
- Cybersecurity Policies and Compliance
- Human Factors in Cybersecurity

Emerging Cyber Threats and Attack Vectors

Understanding emerging cyber threats and attack vectors is fundamental in cybersecurity research. Attackers continuously evolve their methods to exploit new vulnerabilities, making it essential to study these trends to develop effective defenses. Research in this area involves analyzing malware, ransomware, phishing techniques, and advanced persistent threats (APTs) that target individuals, organizations, and governments.

Ransomware and Malware Evolution

Ransomware attacks have surged in prevalence, demanding ransom payments to restore access to encrypted data. Research focuses on the evolution of ransomware strategies, infection mechanisms, and mitigation techniques. Malware analysis also includes studying polymorphic and metamorphic malware that can evade traditional detection methods.

Phishing and Social Engineering

Phishing remains one of the most common attack vectors, exploiting human psychology to gain unauthorized access. Research in this domain examines the effectiveness of phishing campaigns, detection algorithms, and user awareness strategies to minimize success rates.

Zero-Day Exploits and Vulnerability Research

Zero-day vulnerabilities are unknown security flaws exploited by attackers before patches become available. Research targets identifying these vulnerabilities early, understanding their impact, and developing proactive defense mechanisms to reduce risks.

Cryptography and Data Protection

Cryptography is a cornerstone of cybersecurity, ensuring confidentiality, integrity, and authenticity of data. Research topics in cryptography focus on developing robust encryption algorithms, key management practices, and secure communication protocols to protect sensitive information against unauthorized access.

Post-Quantum Cryptography

With the advent of quantum computing, traditional cryptographic algorithms face potential obsolescence. Post-quantum cryptography research aims to design algorithms resistant to quantum attacks, securing data for the future.

Blockchain and Cryptographic Applications

Blockchain technology leverages cryptographic principles to provide decentralized and tamper-proof ledgers. Research explores blockchain's security implications, consensus mechanisms, and applications in identity management and secure transactions.

Data Encryption Standards and Protocols

Research also investigates the effectiveness of current encryption standards such as AES and RSA, evaluating their strengths and weaknesses in various applications, including cloud storage, communications, and IoT devices.

Network Security and Intrusion Detection

Network security research focuses on protecting data transmission and preventing unauthorized access to network resources. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are critical components studied to detect and respond to malicious activities in real time.

Intrusion Detection System Techniques

Research in IDS includes signature-based, anomaly-based, and hybrid detection methods. Advances in machine learning and behavioral analysis enhance the accuracy and speed of detecting network intrusions.

Firewall and Access Control Mechanisms

Firewalls remain vital for filtering traffic and enforcing security policies. Research explores next-generation firewall capabilities, dynamic access controls, and adaptive security models to address increasingly complex network environments.

Network Traffic Analysis

Examining network traffic patterns helps identify suspicious activities and potential breaches. Research includes developing tools to analyze encrypted traffic, detect botnets, and monitor IoT networks for anomalous behavior.

Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) and machine learning (ML) are transforming cybersecurity by automating threat detection, response, and prediction. Research in this area focuses on leveraging AI to enhance security systems, while also addressing challenges such as adversarial attacks against AI models.

AI-Powered Threat Detection

AI algorithms analyze vast amounts of data to identify patterns indicative of cyber threats. Research improves the precision and recall of these systems to reduce false positives and enable timely interventions.

Adversarial Machine Learning

Attackers may manipulate AI systems through adversarial inputs to bypass detection. Research aims to develop robust AI models resilient to such attacks, ensuring reliability in cybersecurity applications.

Automation and Incident Response

Automated response systems powered by AI can contain threats rapidly and reduce human workload. Research investigates the integration of AI in security orchestration, incident response, and forensic analysis.

Cloud Security Challenges

Cloud computing introduces unique security challenges due to its multi-tenant architecture and distributed nature. Research addresses data privacy, access control, and threat mitigation methods suitable for cloud environments.

Data Privacy and Confidentiality in the Cloud

Ensuring data privacy when using cloud services involves encryption, anonymization, and strict access controls. Research explores techniques to protect data both at rest and in transit within cloud infrastructures.

Cloud Access Security Brokers (CASB)

CASBs provide visibility and control over cloud usage. Research focuses on enhancing CASB capabilities to detect shadow IT, enforce policies, and prevent data leaks effectively.

Secure Multi-Cloud and Hybrid Cloud Strategies

Many organizations adopt multi-cloud or hybrid cloud solutions. Research investigates security frameworks and best practices that ensure consistent protection across diverse cloud platforms.

Cybersecurity Policies and Compliance

Policies and regulatory compliance play a critical role in shaping cybersecurity strategies. Research examines the impact of legal frameworks, standards, and best practices on organizational security postures.

Regulatory Frameworks and Standards

Research covers major regulations such as GDPR, HIPAA, and CCPA, analyzing their requirements and implications for data protection and breach notification.

Risk Management and Governance

Effective cybersecurity governance involves risk assessment, policy development, and continuous monitoring. Research explores methodologies to align security practices with organizational objectives and compliance mandates.

Incident Reporting and Legal Considerations

Timely and accurate incident reporting is essential for compliance and mitigation. Research examines legal obligations, reporting frameworks, and the role of transparency in building trust.

Human Factors in Cybersecurity

The human element remains one of the most significant vulnerabilities in cybersecurity. Research focuses on understanding user behavior, training effectiveness, and the psychological aspects of security compliance.

Security Awareness and Training

Educating employees and users on security best practices reduces the risk of human error. Research evaluates training programs' efficacy and develops tailored approaches to improve security culture.

Insider Threats and Behavioral Analysis

Insider threats pose serious risks due to privileged access. Research investigates detection methods based on behavioral analytics and access patterns to identify potential malicious insiders.

Usability of Security Systems

Balancing security and usability is critical for effective adoption. Research explores designing user-friendly security solutions that encourage compliance without compromising protection.

- Emerging Cyber Threats and Attack Vectors
- Cryptography and Data Protection
- Network Security and Intrusion Detection
- Artificial Intelligence in Cybersecurity
- Cloud Security Challenges
- Cybersecurity Policies and Compliance
- Human Factors in Cybersecurity

Frequently Asked Questions

What are the emerging threats in cybersecurity that require further research?

Emerging threats include ransomware evolution, supply chain attacks, AI-powered cyberattacks, quantum computing vulnerabilities, and IoT device exploitation. Research is needed to develop advanced detection and mitigation techniques for these evolving threats.

How can artificial intelligence and machine learning enhance cybersecurity defense mechanisms?

AI and ML can analyze large volumes of data to detect anomalies, predict potential attacks, automate threat response, and improve malware detection. Research focuses on improving accuracy, reducing false positives, and developing explainable AI for cybersecurity.

What role does blockchain technology play in improving cybersecurity?

Blockchain offers decentralized and tamper-proof data storage, which can enhance security in identity management, secure transactions, and supply chain integrity. Research explores scalable blockchain solutions and integration with existing cybersecurity frameworks.

How are quantum computers expected to impact current cryptographic systems?

Quantum computers have the potential to break widely used cryptographic algorithms like RSA and ECC. Research in post-quantum cryptography aims to develop new algorithms resistant to quantum attacks to secure data in the future.

What are the challenges and solutions for securing Internet of Things (IoT) devices?

IoT devices often have limited resources and weak security, making them vulnerable to attacks. Research focuses on lightweight encryption, secure firmware updates, network segmentation, and anomaly detection to enhance IoT security.

How can privacy-preserving techniques be integrated into cybersecurity research?

Privacy-preserving techniques like homomorphic encryption, differential privacy, and federated learning enable data analysis without compromising user privacy. Research aims to balance security needs with privacy protection in various applications.

Additional Resources

1. *Cybersecurity and Cyberwar: What Everyone Needs to Know*

This book provides a comprehensive overview of the key issues in cybersecurity and cyberwarfare. It explains complex concepts in accessible language, making it suitable for both beginners and professionals. The authors discuss the technical, political, and legal aspects of cybersecurity, along with real-world case studies that highlight current challenges.

2. *The Art of Invisibility*

Written by cybersecurity expert Kevin Mitnick, this book explores practical steps individuals and organizations can take to protect their privacy online. It delves into how data is collected, tracked, and potentially exploited, and offers actionable advice on maintaining anonymity and security in the digital age. The book is a valuable resource for anyone interested in enhancing their personal cybersecurity.

3. *Hacking: The Art of Exploitation*

This book provides a deep dive into the technical side of hacking, explaining how vulnerabilities are discovered and exploited. It covers topics such as programming, shellcode, and network communications, making it ideal for readers with some technical background. The hands-on approach helps readers understand the mindset of attackers to better defend against them.

4. *Security Engineering: A Guide to Building Dependable Distributed Systems*

Ross Anderson's book is a seminal work on the principles and practice of security engineering. It covers a wide range of topics including cryptography, system design, and threat modeling. The book is known for its thorough analysis and real-world examples, making it a foundational text for researchers and professionals designing secure systems.

5. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*

This classic book by Bruce Schneier provides detailed coverage of cryptographic protocols and algorithms. It includes practical examples and source code, making complex topics more accessible for implementation. The book serves as a vital resource for anyone researching or working in the field of cryptography and data security.

6. *Blue Team Field Manual (BTFM)*

The Blue Team Field Manual is a concise reference guide for cybersecurity defense professionals. It compiles essential commands, techniques, and best practices for monitoring, detecting, and responding to cyber threats. This manual is especially useful for incident responders and security analysts working in real-time environments.

7. *Social Engineering: The Science of Human Hacking*

This book explores the human element of cybersecurity, focusing on how attackers manipulate individuals to gain unauthorized access. It covers psychological principles, common tactics, and defense strategies to mitigate social engineering attacks. Researchers interested in the intersection of psychology and cybersecurity will find this a valuable resource.

8. *Network Security Essentials: Applications and Standards*

This book offers a clear and concise introduction to network security concepts and protocols. It covers topics such as firewalls, VPNs, intrusion detection systems, and wireless

security. The text is well-suited for those conducting research or working on securing network infrastructures.

9. *Metasploit: The Penetration Tester's Guide*

Focused on the popular Metasploit framework, this guide teaches readers how to conduct penetration testing and identify vulnerabilities. It includes practical examples and step-by-step instructions to simulate attacks ethically. The book is essential for researchers and security professionals aiming to understand offensive security techniques.

Cybersecurity Topics For Research

Find other PDF articles:

<https://staging.devenscommunity.com/archive-library-801/pdf?trackid=ulF46-9617&title=whole-food-s-vegan-soup.pdf>

cybersecurity topics for research: *Foundational Cybersecurity Research* National Academies of Sciences, Engineering, and Medicine, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, 2017-08-24 Attaining meaningful cybersecurity presents a broad societal challenge. Its complexity and the range of systems and sectors in which it is needed mean that successful approaches are necessarily multifaceted. Moreover, cybersecurity is a dynamic process involving human attackers who continue to adapt. Despite considerable investments of resources and intellect, cybersecurity continues to pose serious challenges to national security, business performance, and public well-being. Modern developments in computation, storage and connectivity to the Internet have brought into even sharper focus the need for a better understanding of the overall security of the systems we depend on. Foundational Cybersecurity Research focuses on foundational research strategies for organizing people, technologies, and governance. These strategies seek to ensure the sustained support needed to create an agile, effective research community, with collaborative links across disciplines and between research and practice. This report is aimed primarily at the cybersecurity research community, but takes a broad view that efforts to improve foundational cybersecurity research will need to include many disciplines working together to achieve common goals.

cybersecurity topics for research: Research Anthology on Advancements in Cybersecurity Education Management Association, Information Resources, 2021-08-27 Modern society has become dependent on technology, allowing personal information to be input and used across a variety of personal and professional systems. From banking to medical records to e-commerce, sensitive data has never before been at such a high risk of misuse. As such, organizations now have a greater responsibility than ever to ensure that their stakeholder data is secured, leading to the increased need for cybersecurity specialists and the development of more secure software and systems. To avoid issues such as hacking and create a safer online space, cybersecurity education is vital and not only for those seeking to make a career out of cybersecurity, but also for the general public who must become more aware of the information they are sharing and how they are using it. It is crucial people learn about cybersecurity in a comprehensive and accessible way in order to use the skills to better protect all data. The Research Anthology on Advancements in Cybersecurity Education discusses innovative concepts, theories, and developments for not only teaching cybersecurity, but also for driving awareness of efforts that can be achieved to further secure sensitive data. Providing information on a range of topics from cybersecurity education requirements, cyberspace security

talents training systems, and insider threats, it is ideal for educators, IT developers, education professionals, education administrators, researchers, security analysts, systems engineers, software security engineers, security professionals, policymakers, and students.

cybersecurity topics for research: Research Anthology on Business Aspects of Cybersecurity Management Association, Information Resources, 2021-10-29 Cybersecurity is vital for all businesses, regardless of sector. With constant threats and potential online dangers, businesses must remain aware of the current research and information available to them in order to protect themselves and their employees. Maintaining tight cybersecurity can be difficult for businesses as there are so many moving parts to contend with, but remaining vigilant and having protective measures and training in place is essential for a successful company. The Research Anthology on Business Aspects of Cybersecurity considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest. This comprehensive reference source is split into three sections with the first discussing audits and risk assessments that businesses can conduct to ensure the security of their systems. The second section covers training and awareness initiatives for staff that promotes a security culture. The final section discusses software and systems that can be used to secure and manage cybersecurity threats. Covering topics such as audit models, security behavior, and insider threats, it is ideal for businesses, business professionals, managers, security analysts, IT specialists, executives, academicians, researchers, computer engineers, graduate students, and practitioners.

cybersecurity topics for research: Research in Multidisciplinary Subjects (Volume-11) Chief Editor- Biplab Auddya, Editor- Rukhsar Parveen, Dr. G. Jyothi Olivia, Prathigadapa Anuradha, Shraddha Gaikwad, Dr. Lata Sharma, Dr. Arif M. Khan, 2023-11-07

cybersecurity topics for research: Cybersecurity Research Analysis Report for Europe and Japan Anna Felkner, Youki Kadobayashi, Marek Janiszewski, Stefano Fantin, Jose Francisco Ruiz, Adam Kozakiewicz, Gregory Blanc, 2020-11-20 This book contains the key findings related to cybersecurity research analysis for Europe and Japan collected during the EUNITY project. A wide-scope analysis of the synergies and differences between the two regions, the current trends and challenges is provided. The survey is multifaceted, including the relevant legislation, policies and cybersecurity agendas, roadmaps and timelines at the EU and National levels in Europe and in Japan, including the industry and standardization point of view, identifying and prioritizing the joint areas of interests. Readers from both industry and academia in the EU or Japan interested in entering international cybersecurity cooperation with each other or adding an R&D aspect to an existing one will find it useful in understanding the legal and organizational context and identifying most promising areas of research. Readers from outside EU and Japan may compare the findings with their own cyber-R&D landscape or gain context when entering those markets.

cybersecurity topics for research: Holistic Approaches to Cybersecurity Enabling Network-centric Operations United States. Congress. House. Committee on Armed Services. Subcommittee on Terrorism, Unconventional Threats, and Capabilities, 2009

cybersecurity topics for research: Cybersecurity Tugrul U Daim, Marina Dabić, 2023-08-23 Cybersecurity has become a critical area to focus after recent hack attacks to key infrastructure and personal systems. This book reviews the building blocks of cybersecurity technologies and demonstrates the application of various technology intelligence methods through big data. Each chapter uses a different mining method to analyze these technologies through different kinds of data such as patents, tweets, publications, presentations, and other sources. It also analyzes cybersecurity methods in sectors such as manufacturing, energy and healthcare.

cybersecurity topics for research: Unsettled Topics Concerning Airport Cybersecurity Standards and Regulation Aharon David, 2021-09-13 A large international airport is a microcosm of the entire aviation sector, hosting hundreds of different types of aviation and non-aviation stakeholders: aircraft, passengers, airlines, travel agencies, air traffic management and control, retail shops, runway systems, building management, ground transportation, and much more. Their associated information technology and cyber physical systems—along with an exponentially

resultant number of interconnections—present a massive cybersecurity challenge. Unlike the physical security challenge, which was treated in earnest throughout the last decades, cyber-attacks on airports keep coming, but most airports lack essential means to confront such cyber-attacks. These missing means are not technical tools, but rather holistic regulatory directives, technical and process standards, guides, and best practices for airports cybersecurity—even airport cybersecurity concepts and basic definitions are missing in certain cases. *Unsettled Topics Concerning Airport Cybersecurity Standards and Regulation* offers a deeper analysis of these issues and their causes, focusing on the unique characteristics of airports in general, specific cybersecurity challenges, missing definitions, and conceptual infrastructure for the standardization and regulation of airports cybersecurity. This last item includes the gaps and challenges in the existing guides, best-practices, standards, and regulation pertaining to airport cybersecurity. Finally, practical solution-seeking processes are proposed, as well as some specific potential frameworks and solutions. Click here to access *The Mobility Frontier: Cybersecurity on the Air & Ground* Click here to access the full SAE EDGETM Research Report portfolio. <https://doi.org/10.4271/EPR2021020>

cybersecurity topics for research: *Handbook of Research on Advancing Cybersecurity for Digital Transformation* Sandhu, Kamaljeet, 2021-06-18 Cybersecurity has been gaining serious attention and recently has become an important topic of concern for organizations, government institutions, and largely for people interacting with digital online systems. As many individual and organizational activities continue to grow and are conducted in the digital environment, new vulnerabilities have arisen which have led to cybersecurity threats. The nature, source, reasons, and sophistication for cyberattacks are not clearly known or understood, and many times invisible cyber attackers are never traced or can never be found. Cyberattacks can only be known once the attack and the destruction have already taken place long after the attackers have left. Cybersecurity for computer systems has increasingly become important because the government, military, corporate, financial, critical infrastructure, and medical organizations rely heavily on digital network systems, which process and store large volumes of data on computer devices that are exchanged on the internet, and they are vulnerable to “continuous” cyberattacks. As cybersecurity has become a global concern, it needs to be clearly understood, and innovative solutions are required. The *Handbook of Research on Advancing Cybersecurity for Digital Transformation* looks deeper into issues, problems, and innovative solutions and strategies that are linked to cybersecurity. This book will provide important knowledge that can impact the improvement of cybersecurity, which can add value in terms of innovation to solving cybersecurity threats. The chapters cover cybersecurity challenges, technologies, and solutions in the context of different industries and different types of threats. This book is ideal for cybersecurity researchers, professionals, scientists, scholars, and managers, as well as practitioners, stakeholders, researchers, academicians, and students interested in the latest advancements in cybersecurity for digital transformation.

cybersecurity topics for research: *The Cybersecurity Guide to Governance, Risk, and Compliance* Jason Edwards, Griffin Weaver, 2024-03-19 The *Cybersecurity Guide to Governance, Risk, and Compliance* Understand and respond to a new generation of cybersecurity threats Cybersecurity has never been a more significant concern of modern businesses, with security breaches and confidential data exposure as potentially existential risks. Managing these risks and maintaining compliance with agreed-upon cybersecurity policies is the focus of Cybersecurity Governance and Risk Management. This field is becoming ever more critical as a result. A wide variety of different roles and categories of business professionals have an urgent need for fluency in the language of cybersecurity risk management. The *Cybersecurity Guide to Governance, Risk, and Compliance* meets this need with a comprehensive but accessible resource for professionals in every business area. Filled with cutting-edge analysis of the advanced technologies revolutionizing cybersecurity, increasing key risk factors at the same time, and offering practical strategies for implementing cybersecurity measures, it is a must-own for CISOs, boards of directors, tech professionals, business leaders, regulators, entrepreneurs, researchers, and more. The *Cybersecurity Guide to Governance, Risk, and Compliance* also covers: Over 1300 actionable

recommendations found after each section Detailed discussion of topics including AI, cloud, and quantum computing More than 70 ready-to-use KPIs and KRIs This guide's coverage of governance, leadership, legal frameworks, and regulatory nuances ensures organizations can establish resilient cybersecurity postures. Each chapter delivers actionable knowledge, making the guide thorough and practical. —GARY McALUM, CISO This guide represents the wealth of knowledge and practical insights that Jason and Griffin possess. Designed for professionals across the board, from seasoned cybersecurity veterans to business leaders, auditors, and regulators, this guide integrates the latest technological insights with governance, risk, and compliance (GRC). —WIL BENNETT, CISO

cybersecurity topics for research: Global Information Warfare Andrew Jones, Gerald L. Kovacich, 2015-09-25 Since the turn of the century much has happened in politics, governments, spying, technology, global business, mobile communications, and global competition on national and corporate levels. These sweeping changes have nearly annihilated privacy anywhere in the world and have also affected how global information warfare is waged and what must be do

cybersecurity topics for research: US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments IBP, Inc., 2013-07-01 US National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments

cybersecurity topics for research: Open-Source Security Operations Center (SOC) Alfred Basta, Nadine Basta, Waqar Anwar, Mohammad Ilyas Essar, 2024-11-20 A comprehensive and up-to-date exploration of implementing and managing a security operations center in an open-source environment In Open-Source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC, a team of veteran cybersecurity practitioners delivers a practical and hands-on discussion of how to set up and operate a security operations center (SOC) in a way that integrates and optimizes existing security procedures. You'll explore how to implement and manage every relevant aspect of cybersecurity, from foundational infrastructure to consumer access points. In the book, the authors explain why industry standards have become necessary and how they have evolved – and will evolve – to support the growing cybersecurity demands in this space. Readers will also find: A modular design that facilitates use in a variety of classrooms and instructional settings Detailed discussions of SOC tools used for threat prevention and detection, including vulnerability assessment, behavioral monitoring, and asset discovery Hands-on exercises, case studies, and end-of-chapter questions to enable learning and retention Perfect for cybersecurity practitioners and software engineers working in the industry, Open-Source Security Operations Center (SOC) will also prove invaluable to managers, executives, and directors who seek a better technical understanding of how to secure their networks and products.

cybersecurity topics for research: Digital Sovereignty in Cyber Security: New Challenges in Future Vision Antonio Skarmeta, Daniele Canavese, Antonio Lioy, Sara Matheu, 2023-06-15 This book constitutes papers presented during the workshop session titled “CyberSec4Europe - Research to Innovation: Common Research Framework on Security and Privacy” during the Privacy Symposium hosted by Università Ca' Foscari in Venice, Italy, in April 2022. The 11 peer-reviewed selected papers present findings, conclusions, research, and recommendations in various security-related areas, from highly technical ones (e.g., software and network security) to law and human-centric ones (e.g., governance and cybersecurity awareness).

cybersecurity topics for research: Research Perspectives on Software Engineering and Systems Design Radek Silhavy, Petr Silhavy, 2025-09-12 This book offers a broad range of ideas from CoMeSySo 2024, highlighting theory and practice in modern computing. Researchers from diverse backgrounds present their latest findings on systems design, software engineering, and innovative problem-solving. Topics include new methods to improve modeling, testing, and optimization across various fields. This book also shows how data-driven approaches and well-structured architectures can increase reliability. These proceedings foster meaningful teamwork and shared learning by bringing together experts from many areas. Readers will gain insights into advanced techniques that can be adapted to real-world situations. Industry specialists,

academic researchers, and students will benefit from the breadth of approaches. Case studies reveal common hurdles and present workable solutions for upcoming challenges. With a clear focus on advancement, this resource is an essential guide to the next steps in computational development.

cybersecurity topics for research: Economics of Grids, Clouds, Systems, and Services

Maurizio Naldi, Karim Djemame, Jörn Altmann, José Ángel Bañares, 2025-02-05 This book constitutes the refereed proceedings of the 20th International Conference on Economics of Grids, Clouds, Systems, and Services, GECON 2024, held in Rome, Italy, during September 26-27, 2024. The 12 full papers and 10 short papers presented in this book were carefully reviewed and selected from 37 submissions. They focus on topics such as: Function as a Service: Resource Management and QoS; Cloud Business Models, Pricing, Trading, Network Neutrality; Edge Computing and Energy Awareness; AI/Forecasting/Prediction Sales; and Resource Management in Cloud Applications: Simulation, Streaming Processing and Workflows.

cybersecurity topics for research: Cyber Security in Parallel and Distributed Computing

Dac-Nhuong Le, Raghvendra Kumar, Brojo Kishore Mishra, Jyotir Moy Chatterjee, Manju Khari, 2019-03-20 The book contains several new concepts, techniques, applications and case studies for cyber securities in parallel and distributed computing The main objective of this book is to explore the concept of cybersecurity in parallel and distributed computing along with recent research developments in the field. Also included are various real-time/offline applications and case studies in the fields of engineering and computer science and the modern tools and technologies used. Information concerning various topics relating to cybersecurity technologies is organized within the sixteen chapters of this book. Some of the important topics covered include: Research and solutions for the problem of hidden image detection Security aspects of data mining and possible solution techniques A comparative analysis of various methods used in e-commerce security and how to perform secure payment transactions in an efficient manner Blockchain technology and how it is crucial to the security industry Security for the Internet of Things Security issues and challenges in distributed computing security such as heterogeneous computing, cloud computing, fog computing, etc. Demonstrates the administration task issue in unified cloud situations as a multi-target enhancement issue in light of security Explores the concepts of cybercrime and cybersecurity and presents the statistical impact it is having on organizations Security policies and mechanisms, various categories of attacks (e.g., denial-of-service), global security architecture, along with distribution of security mechanisms Security issues in the healthcare sector with existing solutions and emerging threats.

cybersecurity topics for research: Emerging Trends in Intelligent Systems & Network

Security Mohamed Ben Ahmed, Boudhir Anouar Abdelhakim, Bernadetta Kwintiana Ane, Didi Rosiyadi, 2022-08-31 This book covers selected research works presented at the fifth International Conference on Networking, Information Systems and Security (NISS 2022), organized by the Research Center for Data and Information Sciences at the National Research and Innovation Agency (BRIN), Republic of Indonesia, and Moroccan Mediterranean Association of Sciences and Sustainable Development, Morocco, during March 30-31, 2022, hosted in online mode in Bandung, Indonesia. Building on the successful history of the conference series in the recent four years, this book aims to present the paramount role of connecting researchers around the world to disseminate and share new ideas in intelligent information systems, cyber-security, and networking technologies. The 49 chapters presented in this book were carefully reviewed and selected from 115 submissions. They focus on delivering intelligent solutions through leveraging advanced information systems, networking, and security for competitive advantage and cost savings in modern industrial sectors as well as public, business, and education sectors. Authors are eminent academicians, scientists, researchers, and scholars in their respective fields from across the world.

cybersecurity topics for research: Internet of Things A to Z

Qusay F. Hassan, 2025-09-29 A fully updated guide to cutting-edge Internet of Things (IoT) technology The Internet of Things (IoT) has revolutionized the way we interact with technology in a highly connected world, bringing a host of new objects and points of entry into global communications networks. Internet of Things A to Z:

Technologies and Applications, Second Edition, is a thorough and accessible resource to IoT for undergraduate and postgraduate students, as well as practitioners and implementers. With a contributor team led by an editor who has decades of experience in information and communication technology (ICT), it covers all foundational subjects for understanding IoT. Now fully updated to reflect the latest developments in the field, it is an indispensable volume for students, researchers, and IT learners looking to keep pace with this rapidly growing technology. Organized into five thematic parts, this edition offers foundational theory, emerging technologies, domain-specific applications, security and trust models, and hands-on tutorials that bridge theory and practice. Each chapter offers a research-informed overview with extensive references, making the book equally valuable as a course text and a scholarly reference. Readers of the second edition will also find: Three additional chapters covering applications of artificial intelligence, machine learning, and deep learning, including information on the Internet of Military Things Detailed chapters on IoT architecture and ecosystems, security issues such as trust management and IoT authentication methods, big data analytics, and more Expanded treatment of essential technologies not covered in the first edition, including edge computing and edge intelligence, with coverage of applications such as tinyML, Digital Twins, AR/VR, and the metaverse Practical tutorials on building IoT prototypes and developing streaming data pipelines using widely adopted tools and platforms New information on design and prototyping, including updated hardware boards and instructions Internet of Things A to Z: Technologies and Applications, Second Edition, is ideal for students interested in the Internet of Things, ICT researchers, industry professionals, and lifetime IT learners seeking a comprehensive and up-to-date reference that connects theory with real-world implementation.

cybersecurity topics for research: *Unsettled Topics Concerning the Impact of Quantum Technologies on Automotive Cybersecurity* Joachim Taiber, 2020-12-10 Quantum computing is considered the “next big thing” when it comes to solving computational problems impossible to tackle using conventional computers. However, a major concern is that quantum computers could be used to crack current cryptographic schemes designed to withstand traditional cyberattacks. This threat also impacts future automated vehicles as they become embedded in a vehicle-to-everything (V2X) ecosystem. In this scenario, encrypted data is transmitted between a complex network of cloud-based data servers, vehicle-based data servers, and vehicle sensors and controllers. While the vehicle hardware ages, the software enabling V2X interactions will be updated multiple times. It is essential to make the V2X ecosystem quantum-safe through use of “post-quantum cryptography” as well other applicable quantum technologies. This SAE EDGE™ Research Report considers the following three areas to be unsettled questions in the V2X ecosystem: How soon will quantum computing pose a threat to connected and automated vehicle technologies? What steps and measures are needed to make a V2X ecosystem “quantum-safe?” What standardization is needed to ensure that quantum technologies do not pose an unacceptable risk from an automotive cybersecurity perspective? Click here to access the full SAE EDGETM Research Report portfolio. <https://doi.org/10.4271/EPR2020026>

Related to cybersecurity topics for research

What is cybersecurity? - IBM What is cybersecurity? Cybersecurity is the practice of protecting people, systems and data from cyberattacks by using various technologies, processes and policies. At the enterprise level,

What is Cybersecurity? - CISA Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of

What is cybersecurity? - Cisco Cybersecurity is the convergence of people, processes, and technology that combine to protect organizations, individuals, or networks from digital attacks

What Is Cybersecurity | Types and Threats Defined - CompTIA Cybersecurity involves any activities, people, and technology your organization uses to avoid security incidents, data breaches, or loss of critical systems. It's how you protect

What is Cybersecurity? Key Concepts Explained | Microsoft Security Learn about cybersecurity and how to defend your people, data, and applications against today's growing number of cybersecurity threats. Cybersecurity is a set of processes, best practices,

What is Cybersecurity? Different types of Cybersecurity | Fortinet Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

What Is Cybersecurity? | Definition from TechTarget Cybersecurity is the practice of protecting systems, networks and data from digital threats. It involves strategies, tools and frameworks designed to safeguard sensitive

What Is Cybersecurity? A Comprehensive Guide - Purdue Global Cybersecurity is "the art of protecting networks, devices, and data from unauthorized access or criminal use." Cybersecurity has become especially relevant, with

What is Cyber Security? - GeeksforGeeks Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks." It involves a range of

What is cybersecurity? - IBM What is cybersecurity? Cybersecurity is the practice of protecting people, systems and data from cyberattacks by using various technologies, processes and policies. At the enterprise level,

What is Cybersecurity? - CISA Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of

What is cybersecurity? - Cisco Cybersecurity is the convergence of people, processes, and technology that combine to protect organizations, individuals, or networks from digital attacks

What Is Cybersecurity | Types and Threats Defined - CompTIA Cybersecurity involves any activities, people, and technology your organization uses to avoid security incidents, data breaches, or loss of critical systems. It's how you protect

What is Cybersecurity? Key Concepts Explained | Microsoft Security Learn about cybersecurity and how to defend your people, data, and applications against today's growing number of cybersecurity threats. Cybersecurity is a set of processes, best practices,

What is Cybersecurity? Different types of Cybersecurity | Fortinet Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

What Is Cybersecurity? | Definition from TechTarget Cybersecurity is the practice of protecting systems, networks and data from digital threats. It involves strategies, tools and frameworks designed to safeguard sensitive

What Is Cybersecurity? A Comprehensive Guide - Purdue Global Cybersecurity is "the art of protecting networks, devices, and data from unauthorized access or criminal use." Cybersecurity has become especially relevant, with

What is Cyber Security? - GeeksforGeeks Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks." It involves a range of

What is cybersecurity? - IBM What is cybersecurity? Cybersecurity is the practice of protecting people, systems and data from cyberattacks by using various technologies, processes and policies. At the enterprise level,

What is Cybersecurity? - CISA Cybersecurity is the art of protecting networks, devices, and data

from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of

What is cybersecurity? - Cisco Cybersecurity is the convergence of people, processes, and technology that combine to protect organizations, individuals, or networks from digital attacks

What Is Cybersecurity | Types and Threats Defined - CompTIA Cybersecurity involves any activities, people, and technology your organization uses to avoid security incidents, data breaches, or loss of critical systems. It's how you protect

What is Cybersecurity? Key Concepts Explained | Microsoft Security Learn about cybersecurity and how to defend your people, data, and applications against today's growing number of cybersecurity threats. Cybersecurity is a set of processes, best practices,

What is Cybersecurity? Different types of Cybersecurity | Fortinet Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

What Is Cybersecurity? | Definition from TechTarget Cybersecurity is the practice of protecting systems, networks and data from digital threats. It involves strategies, tools and frameworks designed to safeguard sensitive

What Is Cybersecurity? A Comprehensive Guide - Purdue Global Cybersecurity is "the art of protecting networks, devices, and data from unauthorized access or criminal use." Cybersecurity has become especially relevant, with

What is Cyber Security? - GeeksforGeeks Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks." It involves a range of

What is cybersecurity? - IBM What is cybersecurity? Cybersecurity is the practice of protecting people, systems and data from cyberattacks by using various technologies, processes and policies. At the enterprise level,

What is Cybersecurity? - CISA Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of

What is cybersecurity? - Cisco Cybersecurity is the convergence of people, processes, and technology that combine to protect organizations, individuals, or networks from digital attacks

What Is Cybersecurity | Types and Threats Defined - CompTIA Cybersecurity involves any activities, people, and technology your organization uses to avoid security incidents, data breaches, or loss of critical systems. It's how you protect

What is Cybersecurity? Key Concepts Explained | Microsoft Security Learn about cybersecurity and how to defend your people, data, and applications against today's growing number of cybersecurity threats. Cybersecurity is a set of processes, best practices,

What is Cybersecurity? Different types of Cybersecurity | Fortinet Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

What Is Cybersecurity? | Definition from TechTarget Cybersecurity is the practice of protecting systems, networks and data from digital threats. It involves strategies, tools and frameworks designed to safeguard sensitive

What Is Cybersecurity? A Comprehensive Guide - Purdue Global Cybersecurity is "the art of protecting networks, devices, and data from unauthorized access or criminal use." Cybersecurity has become especially relevant, with

What is Cyber Security? - GeeksforGeeks Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks." It involves a range of

Related to cybersecurity topics for research

Auburn Research Center to Expand AI and Cybersecurity Work (Government Technology6mon) Auburn University has launched a new research hub aimed at tackling complex challenges in cyber defense by staying on the cutting edge of cybersecurity and artificial intelligence technologies,

Auburn Research Center to Expand AI and Cybersecurity Work (Government Technology6mon) Auburn University has launched a new research hub aimed at tackling complex challenges in cyber defense by staying on the cutting edge of cybersecurity and artificial intelligence technologies,

Hackers are targeting U.S. farms and food companies. Lawmakers say it's time to act (KCUR4d) As food production and farming become increasingly computerized, cyberattacks are on the rise. Lawmakers and universities are

Hackers are targeting U.S. farms and food companies. Lawmakers say it's time to act (KCUR4d) As food production and farming become increasingly computerized, cyberattacks are on the rise. Lawmakers and universities are

UALR will get \$1M in settlement funds for cybersecurity research, education center (Arkansas Democrat-Gazette11mon) Arkansas Attorney General Tim Griffin announced \$1 million in funding from his office to the University of Arkansas at Little Rock On Thursday for a cybersecurity research and education center. "What

UALR will get \$1M in settlement funds for cybersecurity research, education center (Arkansas Democrat-Gazette11mon) Arkansas Attorney General Tim Griffin announced \$1 million in funding from his office to the University of Arkansas at Little Rock On Thursday for a cybersecurity research and education center. "What

Info-Tech Research Group Launches LEVEL-UP Series: New Regional Training Events to Accelerate IT Skills in AI, Cybersecurity, and Leadership (7d) Info-Tech Research Group has announced the launch of its LEVEL-UP Series, a new regional training initiative designed to

Info-Tech Research Group Launches LEVEL-UP Series: New Regional Training Events to Accelerate IT Skills in AI, Cybersecurity, and Leadership (7d) Info-Tech Research Group has announced the launch of its LEVEL-UP Series, a new regional training initiative designed to

BITS Pilani and CERT-In Conclude Inaugural Batch of Landmark Cybersecurity Professional Development Course, Strengthening National Security (Press Trust of India on MSN7d) BITS Pilani is an Institution of Eminence recognized for pioneering educational paradigms. Its Center for Research Excellence in National Security (CRENS) focuses on a multi-disciplinary approach to

BITS Pilani and CERT-In Conclude Inaugural Batch of Landmark Cybersecurity Professional Development Course, Strengthening National Security (Press Trust of India on MSN7d) BITS Pilani is an Institution of Eminence recognized for pioneering educational paradigms. Its Center for Research Excellence in National Security (CRENS) focuses on a multi-disciplinary approach to

Strengthening Hessen's cybersecurity research (EurekAlert!2y) FRANKFURT. Almost every company at one point or another falls victim to IT-based attacks. In addition, online attackers are becoming increasingly professional, Germany's digital association Bitkom,

Strengthening Hessen's cybersecurity research (EurekAlert!2y) FRANKFURT. Almost every company at one point or another falls victim to IT-based attacks. In addition, online attackers are becoming increasingly professional, Germany's digital association Bitkom,

Purdue hosts cybersecurity leaders, addresses challenges at CERIAS symposium (Purdue University5mon) Phil Venables, chief information security officer at Google Cloud. Purdue University

photo/Lena Kovalenko WEST LAFAYETTE, Ind. — Purdue University's innovation leaders in cybersecurity and their

Purdue hosts cybersecurity leaders, addresses challenges at CERIAS symposium (Purdue University5mon) Phil Venables, chief information security officer at Google Cloud. Purdue University photo/Lena Kovalenko WEST LAFAYETTE, Ind. — Purdue University's innovation leaders in cybersecurity and their

10 Topics Every Cybersecurity Awareness Training Program Should Cover

(TechRepublic7mon) Employee training starts with cybersecurity awareness programs, which teach employees how to recognize cyberattacks and prevent or mitigate cyber incidents. Boost Cybersecurity — The 10 logical topics

10 Topics Every Cybersecurity Awareness Training Program Should Cover

(TechRepublic7mon) Employee training starts with cybersecurity awareness programs, which teach employees how to recognize cyberattacks and prevent or mitigate cyber incidents. Boost Cybersecurity — The 10 logical topics

Back to Home: <https://staging.devenscommunity.com>