Computational Intelligence Cyber Security And Computational Models Proceedings Of Icc3 2015 Advances In Intelligent Systems And Computing

Advances and Innovations
2014 IEEE Symposium on Computational Intelligence in Cyber Security : Proceedings
Intelligent Distributed Computing VIII
Fundamentals, techniques and applications
Cyber Security Intelligence and Analytics
Artificial Intelligence Safety and Security
Nature-Inspired Cyber Security and Resiliency
Proceedings of the 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)
CICS 2014
Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation
16-19 April, 2013, Singapore
Third International Conference, ICC3 2017, Coimbatore, India, December 14-16, 2017, Proceedings
Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges
13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)
Computational Intelligence, Cyber Security and Computational Models
Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation
Artificial Immune System
Proceedings of ICC3 2015
Artificial Intelligence, Cybersecurity and Cyber Defence
2011 IEEE Symposium on Computational Intelligence in Cyber Security
Computational Intelligence in Cyber Security (CICS), 2013 IEEE Symposium on
Computational Intelligence, Cyber Security and Computational Models
Computational Intelligence in Cyber Security, CICS, IEEE Symposium on
Artificial Intelligence and Cybersecurity
Artificial Intelligence Tools for Cyber Attribution
AI in Cybersecurity
Computational Intelligence in Cyber Security (CICS), 2014 IEEE Symposium on
Proceedings of ICC3, 2013
Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies
Hands-On Artificial Intelligence for Cybersecurity
Implications of Artificial Intelligence for Cybersecurity
Cyber Security in Intelligent Computing and Communications
2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)
Proceedings of a Workshop
Artificial Intelligence in Cyber Security: Impact and Implications

Cyber Security: Issues and Current Trends
2021 International Conference on Cyber Security Intelligence and Analytics (CSIA2021), Volume 2
Implementing Computational Intelligence Techniques for Security Systems Design
Cyber Security, Artificial Intelligence, Data Protection & the Law

ESSENCE DASHAWN

Advances and Innovations Springer
This book presents the outcomes of the 2021 International Conference on Cyber Security Intelligence and Analytics (CSIA 2021), an international conference dedicated to promoting novel theoretical and applied research advances in the interdisciplinary field of cyber security, particularly focusing on threat intelligence, analytics, and countering cybercrime. The conference provides a forum for presenting and discussing innovative ideas, cutting-edge research findings and novel techniques, methods and applications on all aspects of cyber security intelligence and analytics. Due to COVID-19, Authors, Keynote Speakers and PC committees will attend the conference online.
2014 IEEE Symposium on Computational Intelligence in Cyber Security : Proceedings Computational Intelligence, Cyber Security and Computational ModelsProceedings of ICC3 2015
The book provides a valuable reference for cyber security experts, digital forensic practitioners and network security professionals. In recent years, AI has gained substantial attention from researchers in both academia and industry, and as a result AI's capabilities are constantly increasing at an extraordinary pace. AI is considered to be the Fourth Industrial Revolution or at least the next significant technological change after the evolution in mobile and cloud computing technologies. AI is a vehicle for improving the quality of our lives across every spectrum with a broad range of beneficial applications in various sectors. Notwithstanding its numerous beneficial use, AI simultaneously poses numerous legal, ethical, security and privacy challenges that are compounded by its malicious use by criminals. These challenges pose many risks to both our privacy and security at national, organisational and individual levels. In view of this, this book aims to help address some of these challenges focusing on the implication, impact and mitigations of the stated issues. The book provides a comprehensive coverage of not only the technical and ethical issues presented by the use of AI but also the adversarial application of AI and its associated implications. The authors recommend a number of novel approaches to assist in better detecting, thwarting and addressing AI challenges. The book also looks ahead and forecasts what attacks can be carried out in the future through the malicious use of the AI if sufficient defences are not implemented. The research contained in the book fits well into the larger body of work on various aspects of AI and cyber security. It is also aimed at researchers seeking to obtain a more profound knowledge of machine learning and deep learning in the context of cyber security, digital forensics and cybercrime. Furthermore, the book is an exceptional advanced text for Ph.D. and master's degree programmes in cyber security, digital forensics, network security, cyber terrorism and computer science. Each chapter contributed to the book is written by an internationally renowned expert who has extensive experience in law enforcement, industry or academia. Furthermore, this book blends advanced research findings with practice-based methods to provide the reader with advanced understanding and relevant skills.
Intelligent Distributed Computing VIII Springer Nature
The history of robotics and artificial intelligence in many ways is also the history of humanity's attempts to control such technologies. From the Golem of Prague to the military robots of modernity, the debate continues as to what degree of independence such entities should have and how to make sure that they do not turn on us, its inventors. Numerous recent advancements in all aspects of research, development and deployment of intelligent systems are well publicized but safety and security issues related to AI are rarely addressed. This book is proposed to mitigate this fundamental problem. It is comprised of chapters from leading AI Safety researchers addressing different aspects of the AI control problem as it relates to the development of safe and secure artificial intelligence. The book is the first edited volume dedicated to addressing challenges of constructing safe and secure advanced machine intelligence. The chapters vary in length and technical content from broad interest opinion essays to highly formalized algorithmic approaches to specific problems. All chapters are self-contained and could be read in any order or skipped without a loss of comprehension.
Fundamentals, techniques and applications John Wiley & Sons
Recently, cryptology problems, such as designing good cryptographic systems and analyzing them, have been challenging researchers. Many algorithms that take advantage of approaches based on computational intelligence techniques, such as genetic algorithms, genetic programming, and so on, have been proposed to solve these issues. Implementing Computational Intelligence Techniques for Security Systems Design is an essential research book that explores the application of computational intelligence and other advanced techniques in information security, which will contribute to a better understanding of the factors that influence successful security systems design. Featuring a range of topics such as encryption, self-healing systems, and cyber fraud, this book is ideal for security analysts, IT specialists, computer engineers, software developers, technologists, academicians, researchers, practitioners, and students.
Cyber Security Intelligence and Analytics IGI Global
This book presents the latest advances in machine intelligence and big data analytics to improve early warning of cyber-attacks, for cybersecurity intrusion detection and monitoring, and malware analysis. Cyber-attacks have posed real and wide-ranging threats for the information society. Detecting cyber-attacks becomes a challenge, not only because of the sophistication of attacks but also because of the large scale and complex nature of today's IT infrastructures. It discusses novel trends and achievements in machine intelligence and their role in the development of secure systems and identifies open and future research issues related to the application of machine intelligence in the cybersecurity field.

Bridging an important gap between machine intelligence, big data, and cybersecurity communities, it aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this area or those interested in grasping its diverse facets and exploring the latest advances on machine intelligence and big data analytics for cybersecurity applications.
Artificial Intelligence Safety and Security Springer Nature
This book presents state-of-the-art research on artificial intelligence and blockchain for future cybersecurity applications. The accepted book chapters covered many themes, including artificial intelligence and blockchain challenges, models and applications, cyber threats and intrusions analysis and detection, and many other applications for smart cyber ecosystems. It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this particular area or those interested in grasping its diverse facets and exploring the latest advances on artificial intelligence and blockchain for future cybersecurity applications.
Nature-Inspired Cyber Security and Resiliency IGI Global
This book presents various areas related to cybersecurity. Different techniques and tools used by cyberattackers to exploit a system are thoroughly discussed and analyzed in their respective chapters. The content of the book provides an intuition of various issues and challenges of cybersecurity that can help readers to understand and have awareness about it. It starts with a very basic introduction of security, its varied domains, and its implications in any working organization; moreover, it will talk about the risk factor of various attacks and threats. The concept of privacy and anonymity has been taken into consideration in consecutive chapters. Various topics including, The Onion Router (TOR) and other anonymous services, are precisely discussed with a practical approach. Further, chapters to learn the importance of preventive measures such as intrusion detection system (IDS) are also covered. Due to the existence of severe cyberattacks, digital forensics is a must for investigating the crime and to take precautionary measures for the future occurrence of such attacks. A detailed description of cyberinvestigation is covered in a chapter to get readers acquainted with the need and demands. This chapter deals with evidence collection from the victim's device and the system that has importance in the context of an investigation. Content covered in all chapters is foremost and reported in the current trends in several journals and cybertalks. The proposed book is helpful for any reader who is using a computer or any such electronic gadget in their daily routine. The content of the book is prepared to work as a resource to any undergraduate and graduate-level student to get aware about the concept of cybersecurity, various cyberattacks, and threats in the security. In addition to that, it aimed at assisting researchers and developers to build a strong foundation for security provisioning in any newer technology which they are developing.
Proceedings of the 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS) Springer Nature
The Cyber Ecosystem can be a replica of our natural ecosystem where different living and non-living things interact with each other to perform specific tasks. Similarly, the different entities of the cyber ecosystem collaborate digitally with each other to revolutionize our lifestyle by creating smart, intelligent, and automated systems/processes. The main actors of the cyber ecosystem, among others, are the Internet of Things (IoT), Artificial Intelligence (AI), and the mechanisms providing cybersecurity. This book documents how this blend of technologies is powering a digital sustainable socio-economic infrastructure which improves our life quality. It offers advanced automation methods fitted with amended business and audits models, universal authentication schemes, transparent governance, and inventive prediction analysis.
CICS 2014 CRC Press
This book looks at cyber security challenges with topical advancements in computational intelligence and communication technologies. This book includes invited peer-reviewed chapters on the emerging intelligent computing and communication technology research advancements, experimental outcomes, and cyber security practices, threats, and attacks with challenges. The book begins with a state-of-the-art survey and reviews of cyber security trends and issues. It further covers areas such as developments in intelligent computing and communication, smart healthcare, agriculture, transportation, online education, and many more real-life applications using IoT, big data, cloud computing, artificial intelligence, data science, and machine learning. This book is of interest to graduate/postgraduate students, researchers, and academicians. This book will be a valuable resource for practitioners and professionals working in smart city visualization through secure and intelligent application design, development, deployment to foster digital revolution, and reliable integration of advanced computing and communication technologies with global significance.
Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation Springer Nature
This book presents a collection of state-of-the-art AI approaches to cybersecurity and cyberthreat intelligence, offering strategic defense mechanisms for malware, addressing cybercrime, and assessing vulnerabilities to yield proactive rather than reactive countermeasures. The current variety and scope of cybersecurity threats far exceed the capabilities of even the most skilled security professionals. In addition, analyzing yesterday’s security incidents no longer enables experts to predict and prevent tomorrow’s attacks, which necessitates approaches that go far beyond identifying known threats. Nevertheless, there are promising avenues: complex behavior matching can isolate threats based on the actions taken, while machine learning can help detect anomalies, prevent malware infections, discover signs of illicit activities, and protect assets from hackers. In turn, knowledge representation enables automated reasoning over network data, helping achieve cybersituational awareness. Bringing together contributions by high-caliber experts, this book suggests new research directions in this critical and rapidly growing field.
16-19 April, 2013, Singapore IGI Global
Artificial intelligence and cybersecurity are two emerging fields that have made phenomenal contributions toward technological advancement. As cyber-attacks increase, there is a need to identify threats and thwart attacks. This book incorporates recent developments that artificial intelligence brings to the cybersecurity world. Artificial Intelligence and Cybersecurity: Advances and Innovations provides advanced system implementation for Smart Cities using artificial intelligence. It addresses the complete functional framework workflow and explores basic and high-level concepts. The book is based on the latest technologies covering major challenges, issues and advances, and discusses intelligent data management and automated systems. This edited book provides a premier interdisciplinary platform for researchers, practitioners and

educators. It presents and discusses the most recent innovations, trends and concerns as well as practical challenges and solutions adopted in the fields of artificial intelligence and cybersecurity.
Third International Conference, ICC3 2017, Coimbatore, India, December 14-16, 2017, Proceedings Springer
Computational Intelligence, Cyber Security and Computational ModelsProceedings of ICC3 2015Springer
Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges Springer
This book contains cutting-edge research material presented by researchers, engineers, developers, and practitioners from academia and industry at the International Conference on Computational Intelligence, Cyber Security and Computational Models (ICC3) organized by PSG College of Technology, Coimbatore, India during December 19–21, 2013. The materials in the book include theory and applications to provide design, analysis, and modeling of the key areas. The book will be useful material for students, researchers, professionals, as well academicians in understanding current research trends and findings and future scope of research in computational intelligence, cyber security, and computational models.
13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020) Springer
This book constitutes the proceedings of the Third International Conference on Computational Intelligence, Cyber Security, and Computational Models, ICC3 2017, which was held in Coimbatore, India, in December 2017. The 15 papers presented in this volume were carefully reviewed and selected from 63 submissions. They were organized in topical sections named: computational intelligence; cyber security; and computational models.
Computational Intelligence, Cyber Security and Computational Models Springer
This book highlights several gaps that have not been addressed in existing cyber security research. It first discusses the recent attack prediction techniques that utilize one or more aspects of information to create attack prediction models. The second part is dedicated to new trends on information fusion and their applicability to cyber security; in particular, graph data analytics for cyber security, unwanted traffic detection and control based on trust management software defined networks, security in wireless sensor networks & their applications, and emerging trends in security system design using the concept of social behavioral biometric. The book guides the design of new commercialized tools that can be introduced to improve the accuracy of existing attack prediction models. Furthermore, the book advances the use of Knowledge-based Intrusion Detection Systems (IDS) to complement existing IDS technologies. It is aimed towards cyber security researchers.
Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation Springer Nature
In recent years, interest and progress in the area of artificial intelligence (AI) and machine learning (ML) have boomed, with new applications vigorously pursued across many sectors. At the same time, the computing and communications technologies on which we have come to rely present serious security concerns: cyberattacks have escalated in number, frequency, and impact, drawing increased attention to the vulnerabilities of cyber systems and the need to increase their security. In the face of this changing landscape, there is significant concern and interest among policymakers, security practitioners, technologists, researchers, and the public about the potential implications of AI and ML for cybersecurity. The National Academies of Sciences, Engineering, and Medicine convened a workshop on March 12-13, 2019 to discuss and explore these concerns. This publication summarizes the presentations and discussions from the workshop.
Artificial Immune System Springer
The aim of the book is to analyse and understand the impacts of artificial intelligence in the fields of national security and defense; to identify the political, geopolitical, strategic issues of AI; to analyse its place in conflicts and cyberconflicts, and more generally in the various forms of violence; to explain the appropriation of artificial intelligence by military organizations, but also law enforcement agencies and the police; to discuss the questions that the development of artificial intelligence and its use raise in armies, police, intelligence agencies, at the tactical, operational and strategic levels.
Proceedings of ICC3 2015 CRC Press
"This book focuses on the technologies and applications of artificial immune systems in malware and spam detection proposed in recent years by the computation intelligence laboratory at Peking University, China. It offers a theoretical perspective and practical solutions to graduate students, practitioners, and researchers working in the area of artificial immune system, machine learning, pattern recognition, and computer security"--
Artificial Intelligence, Cybersecurity and Cyber Defence Springer
This book represents the combined peer-reviewed proceedings of the Eight International Symposium on Intelligent Distributed Computing - IDC'2014, of the Workshop on Cyber Security and Resilience of Large-Scale Systems - WSRL-2014, and of the Sixth International Workshop on Multi-Agent Systems Technology and Semantics- MASTS-2014. All the events were held in Madrid, Spain, during September 3-5, 2014. The 47 contributions published in this book address several topics related to theory and applications of the intelligent distributed computing and multi-agent systems, including: agent-based data processing, ambient intelligence, collaborative systems, cryptography and security, distributed algorithms, grid and cloud computing, information extraction, knowledge management, big data and ontologies, social networks, swarm intelligence or videogames amongst others.
2011 IEEE Symposium on Computational Intelligence in Cyber Security Packt Publishing Ltd
Cyber-physical systems (CPS) have emerged as a unifying name for systems where cyber parts (i.e., the computing and communication parts) and physical parts are tightly integrated, both in design and during operation. Such systems use computations and communication deeply embedded in and interacting with human physical processes as well as augmenting existing and adding new capabilities. As such, CPS is an integration of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. Artificial Intelligence Paradigms for Smart Cyber-Physical Systems focuses on the recent advances in Artificial intelligence-based approaches towards affecting secure cyber-physical systems. This book presents investigations on state-of-the-art research issues, applications, and achievements

in the field of computational intelligence paradigms for CPS. Covering topics that include autonomous systems, access control, machine learning, and intrusion detection and prevention systems, this book is ideally designed for engineers, industry professionals, practitioners, scientists, managers, students, academicians, and researchers seeking current research on artificial intelligence and cyber-physical systems.