360 Anomaly Based Unsupervised Intrusion Detection

Thank you for reading **360 Anomaly Based Unsupervised Intrusion Detection** . Maybe you have knowledge that, people have look numerous times for their favorite novels like this 360 Anomaly Based Unsupervised Intrusion Detection , but end up in harmful downloads.
Rather than enjoying a good book with a cup of tea in the afternoon, instead they cope with some infectious bugs inside their computer.

360 Anomaly Based Unsupervised Intrusion Detection is available in our book collection an online access to it is set as public so you can download it instantly.
Our book servers spans in multiple countries, allowing you to get the most less latency time to download any of our books like this one.
Kindly say, the 360 Anomaly Based Unsupervised Intrusion Detection is universally compatible with any devices to read

Cloud Computing for Geospatial Big Data Analytics - Himansu Das 2018-12-11
This book introduces the latest research findings in cloud, edge, fog, and mist computing and their applications in various fields using geospatial data. It solves a number of problems of cloud computing and big data, such as scheduling, security issues using different techniques, which researchers from industry and academia have been attempting to solve in virtual environments. Some of these problems are of an intractable nature and so efficient technologies like fog, edge and mist computing play an important role in addressing these issues. By exploring emerging advances in cloud computing and big data analytics and their engineering applications, the book enables researchers to understand the mechanisms needed to implement cloud, edge, fog, and mist computing in their own endeavours, and motivates them to examine their own research findings and developments.
Advances in Internet, Data and Web Technologies - Leonard Barolli 2019-02-05
This book presents original contributions on the theories and practices of emerging Internet, Data and Web technologies and their applications in businesses, engineering and academia. As a key feature, it addresses advances in the life-cycle exploitation of data generated by digital ecosystem technologies. The Internet has become the most proliferative platform for emerging large-scale computing paradigms. Among these, Data and Web technologies are two of the most prominent paradigms, manifesting in a variety of forms such as Data Centers, Cloud Computing, Mobile Cloud, Mobile Web Services, and so on. These technologies altogether create a digital ecosystem whose cornerstone is the data cycle, from capturing to processing, analysis and visualization. The need to investigate various research and development issues in this digital ecosystem has been made even more pressing by the ever-increasing demands of real-life applications, which are based on storing and processing large amounts of data. Given its scope, the book offers a valuable asset for all researchers, software developers, practitioners and students interested in the field of Data and Web technologies.
Outlier Analysis - Charu C. Aggarwal 2016-12-10
This book provides comprehensive coverage of the field of outlier analysis from a computer science point of view. It integrates methods from data mining, machine learning, and statistics within the computational framework and therefore appeals to multiple communities. The chapters of this book can be organized into three

categories: Basic algorithms: Chapters 1 through 7 discuss the fundamental algorithms for outlier analysis, including probabilistic and statistical methods, linear methods, proximity-based methods, high-dimensional (subspace) methods, ensemble methods, and supervised methods. Domain-specific methods: Chapters 8 through 12 discuss outlier detection algorithms for various domains of data, such as text, categorical data, time-series data, discrete sequence data, spatial data, and network data. Applications: Chapter 13 is devoted to various applications of outlier analysis. Some guidance is also provided for the practitioner. The second edition of this book is more detailed and is written to appeal to both researchers and practitioners. Significant new material has been added on topics such as kernel methods, one-class support-vector machines, matrix factorization, neural networks, outlier ensembles, time-series methods, and subspace methods. It is written as a textbook and can be used for classroom teaching.

Outlier Ensembles - Charu C. Aggarwal 2017-04-06

This book discusses a variety of methods for outlier ensembles and organizes them by the specific principles with which accuracy improvements are achieved. In addition, it covers the techniques with which such methods can be made more effective. A formal classification of these methods is provided, and the circumstances in which they work well are examined. The authors cover how outlier ensembles relate (both theoretically and practically) to the ensemble techniques used commonly for other data mining problems like classification. The similarities and (subtle) differences in the ensemble techniques for the classification and outlier detection problems are explored. These subtle differences do impact the design of ensemble algorithms for the latter problem. This book can be used for courses in data mining and related curricula. Many illustrative examples and exercises are provided in order to facilitate classroom teaching. A familiarity is assumed to the outlier detection problem and also to generic problem of ensemble analysis in classification. This is because many of the ensemble methods discussed in this book are adaptations from their counterparts in the classification domain. Some techniques explained in this book, such as wagging, randomized feature weighting, and geometric subsampling, provide new insights that are not available elsewhere. Also included is an analysis of the performance of various types of base detectors and their relative effectiveness. The book is valuable for researchers and practitioners for leveraging ensemble methods into optimal algorithmic design.

Machine Learning and Its Applications - Georgios Paliouras 2003-06-29

In recent years machine learning has made its way from artificial intelligence into areas of administration, commerce, and industry. Data mining is perhaps the most widely known demonstration of this migration, complemented by less publicized applications of machine learning like adaptive systems in industry, financial prediction, medical diagnosis and the construction of user profiles for Web browsers. This book presents the capabilities of machine learning methods and ideas on how these methods could be used to solve real-world problems. The first ten chapters assess the current state of the art of machine learning, from symbolic concept learning and conceptual clustering to case-based reasoning, neural networks, and genetic algorithms. The second part introduces the reader to innovative applications of ML techniques in fields such as data mining, knowledge discovery, human language technology, user modeling, data analysis, discovery science, agent technology, finance, etc.

Smart Log Data Analytics - Florian Skopik 2021-08-28

This book provides insights into smart ways of computer log data analysis, with the goal of spotting adversarial actions. It is organized into 3 major parts with a total of 8 chapters that include a detailed view on existing solutions, as well as novel techniques that go far beyond state of the art. The first part of this book motivates the entire topic and highlights major challenges, trends and design criteria for log data analysis approaches, and further surveys and compares the state of the art. The second part of this book introduces concepts that apply character-based, rather than token-based, approaches and thus work on a more fine-grained level. Furthermore, these solutions were designed for “online use”, not only forensic analysis, but also process new log lines as they arrive in an efficient single pass manner. An advanced method for

time series analysis aims at detecting changes in the overall behavior profile of an observed system and spotting trends and periodicities through log analysis. The third part of this book introduces the design of the AMiner, which is an advanced open source component for log data anomaly mining. The AMiner comes with several detectors to spot new events, new parameters, new correlations, new values and unknown value combinations and can run as stand-alone solution or as sensor with connection to a SIEM solution. More advanced detectors help to determines the characteristics of variable parts of log lines, specifically the properties of numerical and categorical fields. Detailed examples throughout this book allow the reader to better understand and apply the introduced techniques with open source software. Step-by-step instructions help to get familiar with the concepts and to better comprehend their inner mechanisms. A log test data set is available as free download and enables the reader to get the system up and running in no time. This book is designed for researchers working in the field of cyber security, and specifically system monitoring, anomaly detection and intrusion detection. The content of this book will be particularly useful for advanced-level students studying computer science, computer technology, and information systems. Forward-thinking practitioners, who would benefit from becoming familiar with the advanced anomaly detection methods, will also be interested in this book.

2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) - IEEE Staff 2019-07-06

The 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) aims to provide a forum that brings together International researchers from academia and practitioners in the industry to meet and exchange ideas and recent research work on all aspects of Information and Communication Technologies including Computing, communication, IOT, LiDAR, Image Analysis, wireless communication and other new technologies

Nature-Inspired Computing for Smart Application Design - Santosh Kumar Das 2021-03-17

This book focuses primarily on the nature-inspired approach for designing smart applications. It includes several implementation paradigms such as design and path planning of wireless network, security mechanism and implementation for dynamic as well as static nodes, learning method of cloud computing, data exploration and management, data analysis and optimization, decision taking in conflicting environment, etc. The book fundamentally highlights the recent research advancements in the field of engineering and science.

Proceedings of the Future Technologies Conference (FTC) 2021, Volume 3 - Kohei Arai 2022

This book provides the state-of-the-art intelligent methods and techniques for solving real world problems along with a vision of the future research. The sixth Future Technologies Conference 2021 was organized virtually and received a total of 531 submissions from academic pioneering researchers, scientists, industrial engineers, and students from all over the world. The submitted papers covered a wide range of important topics including but not limited to technology trends, computing, artificial intelligence, machine vision, communication, security, e-learning and ambient intelligence and their applications to the real world. After a double-blind peer-reviewed process, 191 submissions have been selected to be included in these proceedings. One of the meaningful and valuable dimensions of this conference is the way it brings together a large group of technology geniuses in one venue to not only present breakthrough research in future technologies but also to promote discussions and debate of relevant issues, challenges, opportunities, and research findings. We hope that readers find the volume interesting, exciting, and inspiring.

AI and Learning Systems - Konstantinos Kyprianidis 2021-02-17

Over the last few years, interest in the industrial applications of AI and learning systems has surged. This book covers the recent developments and provides a broad perspective of the key challenges that characterize the field of Industry 4.0 with a focus on applications of AI. The target audience for this book includes engineers involved in automation system design, operational planning, and decision support. Computer science practitioners and industrial automation platform developers will also

benefit from the timely and accurate information provided in this work. The book is organized into two main sections comprising 12 chapters overall: •Digital Platforms and Learning Systems •Industrial Applications of AI

Cognitive Radio Techniques - Kandeepan Sithamparanathan 2012
Providing an in-depth treatment of the core enablers of cognitive radio technology, this unique book places emphasis on critical areas that have not been sufficiently covered in existing literature. You find expert guidance in the key enablers with respect to communications and signal processing. The book presents fundamentals, basic solutions, detailed discussions of important enabler issues, and advanced algorithms to save you time with your projects in the field. For the first time in any book, you find an adequately detailed treatment of spectrum sensing that covers nearly every aspect of the subject. Moreover, this valuable resource provides you with thorough working knowledge of localization and interference mitigation as enablers of cognitive radio technology. The book includes all the necessary mathematics, statistical and probabilistic treatments, and performance analysis to give you a comprehensive understanding of the material.

Information and Software Technologies - Audrius Lopata 2022
This book constitutes the refereed proceedings of the 28th International Conference on Information and Software Technologies, ICIST 2022, held in Kaunas, Lithuania, in October 2022. The 23 full papers and 3 short papers presented were carefully reviewed and selected from 66 submissions. The papers discuss such topics as business intelligence for information and software systems, intelligent methods for data analysis and computer aided software engineering, information technology applications, smart e-learning technologies and applications, language technologies.

Cybersecurity of Digital Service Chains - Joanna Kołodziej 2022
This open access book presents the main scientific results from the H2020 GUARD project. The GUARD project aims at filling the current technological gap between software management paradigms and cybersecurity models, the latter still lacking orchestration and agility to effectively address the dynamicity of the former. This book provides a comprehensive review of the main concepts, architectures, algorithms, and non-technical aspects developed during three years of investigation; the description of the Smart Mobility use case developed at the end of the project gives a practical example of how the GUARD platform and related technologies can be deployed in practical scenarios. We expect the book to be interesting for the broad group of researchers, engineers, and professionals daily experiencing the inadequacy of outdated cybersecurity models for modern computing environments and cyber-physical systems.

Insider Computer Fraud - Kenneth Brancik 2007-12-06
An organization’s employees are often more intimate with its computer system than anyone else. Many also have access to sensitive information regarding the company and its customers. This makes employees prime candidates for sabotaging a system if they become disgruntled or for selling privileged information if they become greedy. Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks presents the methods, safeguards, and techniques that help protect an organization from insider computer fraud. Drawing from the author’s vast experience assessing the adequacy of IT security for the banking and securities industries, the book presents a practical framework for identifying, measuring, monitoring, and controlling the risks associated with insider threats. It not only provides an analysis of application or system-related risks, it demonstrates the interrelationships that exist between an application and the IT infrastructure components it uses to transmit, process, and store sensitive data. The author also examines the symbiotic relationship between the risks, controls, threats, and action plans that should be deployed to enhance the overall information security governance processes. Increasing the awareness and understanding necessary to effectively manage the risks and controls associated with an insider threat, this book is an invaluable resource for those interested in attaining sound and best practices over the risk management process.

Learning to Analyze what is Beyond the Visible Spectrum - Amanda

Berg 2019-11-13

Thermal cameras have historically been of interest mainly for military applications. Increasing image quality and resolution combined with decreasing camera price and size during recent years have, however, opened up new application areas. They are now widely used for civilian applications, e.g., within industry, to search for missing persons, in automotive safety, as well as for medical applications. Thermal cameras are useful as soon as there exists a measurable temperature difference. Compared to cameras operating in the visual spectrum, they are advantageous due to their ability to see in total darkness, robustness to illumination variations, and less intrusion on privacy. This thesis addresses the problem of automatic image analysis in thermal infrared images with a focus on machine learning methods. The main purpose of this thesis is to study the variations of processing required due to the thermal infrared data modality. In particular, three different problems are addressed: visual object tracking, anomaly detection, and modality transfer. All these are research areas that have been and currently are subject to extensive research. Furthermore, they are all highly relevant for a number of different real-world applications. The first addressed problem is visual object tracking, a problem for which no prior information other than the initial location of the object is given. The main contribution concerns benchmarking of short-term single-object (STSO) visual object tracking methods in thermal infrared images. The proposed dataset, LTIR (Linköping Thermal Infrared), was integrated in the VOT-TIR2015 challenge, introducing the first ever organized challenge on STSO tracking in thermal infrared video. Another contribution also related to benchmarking is a novel, recursive, method for semi-automatic annotation of multi-modal video sequences. Based on only a few initial annotations, a video object segmentation (VOS) method proposes segmentations for all remaining frames and difficult parts in need for additional manual annotation are automatically detected. The third contribution to the problem of visual object tracking is a template tracking method based on a non-parametric probability density model of the object's thermal radiation using channel representations. The second addressed problem is anomaly detection, i.e., detection of rare objects or events. The main contribution is a method for truly unsupervised anomaly detection based on Generative Adversarial Networks (GANs). The method employs joint training of the generator and an observation to latent space encoder, enabling stratification of the latent space and, thus, also separation of normal and anomalous samples. The second contribution is the previously unaddressed problem of obstacle detection in front of moving trains using a train-mounted thermal camera. Adaptive correlation filters are updated continuously and missed detections of background are treated as detections of anomalies, or obstacles. The third contribution to the problem of anomaly detection is a method for characterization and classification of automatically detected district heat leakages for the purpose of false alarm reduction. Finally, the thesis addresses the problem of modality transfer between thermal infrared and visual spectrum images, a previously unaddressed problem. The contribution is a method based on Convolutional Neural Networks (CNNs), enabling perceptually realistic transformations of thermal infrared to visual images. By careful design of the loss function the method becomes robust to image pair misalignments. The method exploits the lower acuity for color differences than for luminance possessed by the human visual system, separating the loss into a luminance and a chrominance part.

Network Intrusion Detection and Prevention - Ali A. Ghorbani 2009-10-10

Network Intrusion Detection and Prevention: Concepts and Techniques provides detailed and concise information on different types of attacks, theoretical foundation of attack detection approaches, implementation, data collection, evaluation, and intrusion response. Additionally, it provides an overview of some of the commercially/publicly available intrusion detection and response systems. On the topic of intrusion detection system it is impossible to include everything there is to say on all subjects. However, we have tried to cover the most important and common ones. Network Intrusion Detection and Prevention: Concepts and Techniques is designed for researchers and practitioners in industry.

This book is suitable for advanced-level students in computer science as a reference book as well.

Cloud Computing for Optimization: Foundations, Applications, and Challenges - Bhabani Shankar Prasad Mishra 2018-02-26

This book discusses harnessing the real power of cloud computing in optimization problems, presenting state-of-the-art computing paradigms, advances in applications, and challenges concerning both the theories and applications of cloud computing in optimization with a focus on diverse fields like the Internet of Things, fog-assisted cloud computing, and big data. In real life, many problems – ranging from social science to engineering sciences – can be identified as complex optimization problems. Very often these are intractable, and as a result researchers from industry as well as the academic community are concentrating their efforts on developing methods of addressing them. Further, the cloud computing paradigm plays a vital role in many areas of interest, like resource allocation, scheduling, energy management, virtualization, and security, and these areas are intertwined with many optimization problems. Using illustrations and figures, this book offers students and researchers a clear overview of the concepts and practices of cloud computing and its use in numerous complex optimization problems.

Anomaly detection using the correlational paraconsistent machine with digital signatures of network segment - Eduardo H.M. Pena

This study presents the correlational paraconsistent machine (CPM), a tool for anomaly detection that incorporates unsupervised models for traffic characterization and principles of paraconsistency, to inspect irregularities at the network traffic flow level.

Industrial Internet of Things - Anand Sharma 2022-04-06

This book focuses on the key technologies, challenges, and research directions of the Industrial Internet of Things (IIoT). It provides a basis for discussing open principles, methods, and research problems, and provides a systematic overview of the state-of-the-art research efforts, directions, and potential challenges associated with IIoT. Industrial Internet of Things: Technologies and Research Directions covers how industry automation is projected to be the largest and fastest-growing segment of the market. It explores the collaborative development of high-performance telecommunications, military, industrial, and general-purpose embedded computing applications, and offers a systematic overview of the state-of-the-art research efforts and new potential directions. Researchers, academicians, and professionals working in this inter-disciplinary area will be interested in this book.

Malware Detection - Mihai Christodorescu 2007-03-06

This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Emerging Technologies in Computer Engineering: Cognitive Computing and Intelligent IoT - Valentina E. Balas 2022-06-26

This book constitutes the refereed proceedings of the 5th International Conference on Emerging Technologies in Computer Engineering, ICETCE 2021, held in Jaipur, India, in February 2022. The 40 revised full papers along with 20 short papers presented were carefully reviewed and selected from 235 submissions. The papers are organized according to the following topical headings: cognitive computing; Internet of Things (IoT); machine learning and applications; soft computing; data science and big data analytics; blockchain and cyber security.

Machine Learning for Cyber Physical Systems - Jürgen Beyerer 2016-11-25

The work presents new approaches to Machine Learning for Cyber Physical Systems, experiences and visions. It contains some selected papers from the international Conference ML4CPS – Machine Learning for Cyber Physical Systems, which was held in Karlsruhe, September 29th, 2016. Cyber Physical Systems are characterized by their ability to adapt and to learn: They analyze their environment and, based on observations, they learn patterns, correlations and predictive models.

Typical applications are condition monitoring, predictive maintenance, image processing and diagnosis. Machine Learning is the key technology for these developments.

Network Intrusion Detection - Stephen Northcutt 2002

This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.

Computer and Network Security Essentials - Kevin Daimi 2017-08-12

This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book's website at Springer.com.

Global Security, Safety, and Sustainability - Hamid Jahankhani 2009-08-20

The Annual (ICGS) International Conference is an established platform in which se- rity, safety and sustainability issues can be examined from several global perspectives through dialogue between academics, students, government representatives, chief executives, security professionals, and research scientists from the United Kingdom and from around the globe. The 2009 two-day conference focused on the challenges of complexity, rapid pace of change and risk/opportunity issues associated with modern products, systems, s- cial events and infrastructures. The importance of adopting systematic and systemic approaches to the assurance of these systems was emphasized within a special stream focused on strategic frameworks, architectures and human factors. The conference provided an opportunity for systems scientists, assurance researchers, owners, ope- tors and maintainers of large, complex and advanced systems and infrastructures to update their knowledge with the state of best practice in these challenging domains while networking with the leading researchers and solution providers. ICGS3 2009 received paper submissions from more than 20 different countries around the world. Only 28 papers were selected and were presented as full papers. The program also included three keynote lectures by leading researchers, security professionals and government representatives. June 2009 Hamid Jahankhani Ali Hessami Feng Hsu

Intelligent Systems and Applications - Yaxin Bi 2019-08-23

The book presents a remarkable collection of chapters covering a wide range of topics in the areas of intelligent systems and artificial intelligence, and their real-world applications. It gathers the proceedings of the Intelligent Systems Conference 2019, which attracted a total of 546 submissions from pioneering researchers, scientists, industrial engineers, and students from all around the world. These submissions underwent a double-blind peer-review process, after which 190 were selected for inclusion in these proceedings. As intelligent systems continue to replace and sometimes outperform human intelligence in decision-making processes, they have made it possible to tackle a host of problems more effectively. This branching out of computational intelligence in several directions and use of intelligent systems in everyday applications have created the need for an international conference as a venue for reporting on the latest innovations and trends. This book collects both theory and application based chapters on virtually all aspects of artificial intelligence; presenting state-of-the-art intelligent methods and techniques for solving real-world problems, along with a vision for future research, it represents a unique and valuable asset.

Frontier Computing - Neil Y. Yen 2017-09-28

This volume contains the proceedings of the 5th International

Conference on Frontier Computing (FC 2016), Tokyo, Japan, July 13-15, 2016. This international meeting provided a forum for researchers to share current understanding of recent advances and emergence in information technology, science, and engineering, with themes in the scope of Communication Networks, Business Intelligence and Knowledge Management, Web Intelligence, and any related fields that further the development of information technology. The articles presented cover a wide spectrum of topics: database and data mining, networking and communications, web and internet of things, embedded system, soft computing, social network analysis, security and privacy, optics communication, and ubiquitous/pervasive computing. Many papers report results of great academic potential and value, and in addition, indicate promising directions of research in the focused realm of this conference series. Readers, including students, academic researchers, and professionals, will benefit from the results presented in this book. It also provides an overview of current research and can be used as a guidebook for those new to the field.

Handbook of Information and Communication Security - Peter Stavroulakis 2010-02-23

At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called “Y2K” issue. Te Y2K scare was the fear that c- puter networks and the systems that are controlled or operated by sofware would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several Computer Emergency Response Teams (CERTs) around the world that now work - operatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment. Te terrorist attacks of 11 September 2001 raised security concerns to a new level. Te - ternational community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about - tential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communi- tions conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security. Te ?rst editor was intimately involved with security for the Athens Olympic Games of 2004.

Foundations of Information Security - Jason Andress 2019-10-15

High-level overview of the information security field. Covers key concepts like confidentiality, integrity, and availability, then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. In this high-level survey of the information security field, best-selling author Jason Andress covers the basics of a wide variety of topics, from authentication and authorization to maintaining confidentiality and performing penetration testing. Using real-world security breaches as examples, Foundations of Information Security explores common applications of these concepts, such as operations security, network design, hardening and patching operating systems, securing mobile devices, as well as tools for assessing the security of hosts and applications. You'll also learn the basics of topics like: • Multifactor authentication and how biometrics and hardware tokens can be used to harden the authentication process • The principles behind modern cryptography, including symmetric and asymmetric algorithms, hashes, and certificates • The laws and regulations that protect systems and data • Anti-malware tools, firewalls, and intrusion detection systems • Vulnerabilities such as buffer overflows and race conditions A valuable resource for beginning security professionals, network systems administrators, or anyone new to the field, Foundations of Information Security is a great place to start your journey into the dynamic and rewarding field of information security.

Advances in Communication, Devices and Networking - Rabindranath Bera 2018-05-23

The book provides insights of International Conference in Communication, Devices and Networking (ICCDN 2017) organized by the

Department of Electronics and Communication Engineering, Sikkim Manipal Institute of Technology, Sikkim, India during 3 – 4 June, 2017. The book discusses latest research papers presented by researchers, engineers, academicians and industry professionals. It also assists both novice and experienced scientists and developers, to explore newer scopes, collect new ideas and establish new cooperation between research groups and exchange ideas, information, techniques and applications in the field of electronics, communication, devices and networking.

Detection of Intrusions and Malware, and Vulnerability Assessment - Clémentine Maurice 2020-07-07

This book constitutes the proceedings of the 17th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2020, held in Lisbon, Portugal, in June 2020.* The 13 full papers presented in this volume were carefully reviewed and selected from 45 submissions. The contributions were organized in topical sections named: vulnerability discovery and analysis; attacks; web security; and detection and containment. *The conference was held virtually due to the COVID-19 pandemic.

Botnets - Georgios Kambourakis 2019-09-26

This book provides solid, state-of-the-art contributions from both scientists and practitioners working on botnet detection and analysis, including botnet economics. It presents original theoretical and empirical chapters dealing with both offensive and defensive aspects in this field. Chapters address fundamental theory, current trends and techniques for evading detection, as well as practical experiences concerning detection and defensive strategies for the botnet ecosystem, and include surveys, simulations, practical results, and case studies.

Data Analytics and Decision Support for Cybersecurity - Iván Palomares Carrascosa 2017-08-01

The book illustrates the inter-relationship between several data management, analytics and decision support techniques and methods commonly adopted in Cybersecurity-oriented frameworks. The recent advent of Big Data paradigms and the use of data science methods, has resulted in a higher demand for effective data-driven models that support decision-making at a strategic level. This motivates the need for defining novel data analytics and decision support approaches in a myriad of real-life scenarios and problems, with Cybersecurity-related domains being no exception. This contributed volume comprises nine chapters, written by leading international researchers, covering a compilation of recent advances in Cybersecurity-related applications of data analytics and decision support approaches. In addition to theoretical studies and overviews of existing relevant literature, this book comprises a selection of application-oriented research contributions. The investigations undertaken across these chapters focus on diverse and critical Cybersecurity problems, such as Intrusion Detection, Insider Threats, Insider Threats, Collusion Detection, Run-Time Malware Detection, Intrusion Detection, E-Learning, Online Examinations, Cybersecurity noisy data removal, Secure Smart Power Systems, Security Visualization and Monitoring. Researchers and professionals alike will find the chapters an essential read for further research on the topic.

Cloud Computing – CLOUD 2019 - Dilma Da Silva 2019-06-18

This volume constitutes the proceedings of the 12th International Conference on Cloud Computing, CLOUD 2019, held as part of the Services Conference Federation, SCF 2019, in San Diego, CA, USA, in June 2019. The 24 full papers were carefully reviewed and selected from 53 submissions. CLOUD has been a prime international forum for both researchers and industry practitioners to exchange the latest fundamental advances in the state of the art and practice of cloud computing, to identify emerging research topics, and to define the future of cloud computing. All topics regarding cloud computing align with the theme of CLOUD.

Identification of Outliers - D. Hawkins 2013-04-17

The problem of outliers is one of the oldest in statistics, and during the last century and a half interest in it has waxed and waned several times. Currently it is once again an active research area after some years of relative neglect, and recent work has solved a number of old problems in outlier theory, and identified new ones. The major results are, however,

scattered amongst many journal articles, and for some time there has been a clear need to bring them together in one place. That was the original intention of this monograph: but during execution it became clear that the existing theory of outliers was deficient in several areas, and so the monograph also contains a number of new results and conjectures. In view of the enormous volume ofliterature on the outlier problem and its cousins, no attempt has been made to make the coverage exhaustive. The material is concerned almost entirely with the use of outlier tests that are known (or may reasonably be expected) to be optimal in some way. Such topics as robust estimation are largely ignored, being covered more adequately in other sources. The numerous ad hoc statistics proposed in the early work on the grounds of intuitive appeal or computational simplicity also are not discussed in any detail.

Network Anomaly Detection - Dhruba Kumar Bhattacharyya 2013-06-18

With the rapid rise in the ubiquity and sophistication of Internet technology and the accompanying growth in the number of network attacks, network intrusion detection has become increasingly important. Anomaly-based network intrusion detection refers to finding exceptional or nonconforming patterns in network traffic data compared to normal behavior. Finding these anomalies has extensive applications in areas such as cyber security, credit card and insurance fraud detection, and military surveillance for enemy activities. Network Anomaly Detection: A Machine Learning Perspective presents machine learning techniques in depth to help you more effectively detect and counter network intrusion. In this book, you'll learn about: Network anomalies and vulnerabilities at various layers The pros and cons of various machine learning techniques and algorithms A taxonomy of attacks based on their characteristics and behavior Feature selection algorithms How to assess the accuracy, performance, completeness, timeliness, stability, interoperability, reliability, and other dynamic aspects of a network anomaly detection system Practical tools for launching attacks, capturing packet or flow traffic, extracting features, detecting attacks, and evaluating detection performance Important unresolved issues and research challenges that need to be overcome to provide better protection for networks

Examining numerous attacks in detail, the authors look at the tools that intruders use and show how to use this knowledge to protect networks. The book also provides material for hands-on development, so that you can code on a testbed to implement detection methods toward the development of your own intrusion detection system. It offers a thorough introduction to the state of the art in network anomaly detection using machine learning approaches and systems.

Information Technology and Applied Mathematics - Peeyush Chandra 2018-05-08

This book discusses recent advances and contemporary research in the field of cryptography, security, mathematics and statistics, and their applications in computing and information technology. Mainly focusing on mathematics and applications of mathematics in computer science and information technology, it includes contributions from eminent international scientists, researchers, and scholars. The book helps researchers update their knowledge of cryptography, security, algebra, frame theory, optimizations, stochastic processes, compressive sensing, functional analysis, and complex variables.

Introduction to Data Mining - Pang-Ning Tan 2018

Mobile Hybrid Intrusion Detection - Álvaro Herrero 2011-01-28

This monograph comprises work on network-based Intrusion Detection (ID) that is grounded in visualisation and hybrid Artificial Intelligence (AI). It has led to the design of MOVICAB-IDS (MObile VIsualisation Connectionist Agent-Based IDS), a novel Intrusion Detection System (IDS), which is comprehensively described in this book. This novel IDS combines different AI paradigms to visualise network traffic for ID at packet level. It is based on a dynamic Multiagent System (MAS), which integrates an unsupervised neural projection model and the Case-Based Reasoning (CBR) paradigm through the use of deliberative agents that are capable of learning and evolving with the environment. The proposed novel hybrid IDS provides security personnel with a synthetic, intuitive snapshot of network traffic and protocol interactions. This visualisation interface supports the straightforward detection of anomalous situations

and their subsequent identification. The performance of MOVICAB-IDS was tested through a novel mutation-based testing method in different real domains which entailed several attacks and anomalous situations.

A GA-LR wrapper approach for feature selection in network intrusion detection - Chaouki Khammassi

Intrusions constitute one of the main issues in computer network security.Through malicious actions, hackers can have unauthorised access that compromises the integrity, the confidentiality,and the availability of resources or services.Intrusion detection systems (IDSs) have been developed to monitor and filter network activities by identifying attacks and alerting network administrators.