Intrusion Detection System Using Datamining Techniques

OCONNOR RIVERA

Artificial Intelligence and Data Mining Approaches in Security Frameworks Springer Science & Business Media
Many networked computer systems are far too vulnerable to cyber attacks that can inhibit their functioning, corrupt important data, or expose private information. Not surprisingly, the field of cyber-based systems is a fertile ground where many tasks can be formulated as learning problems and approached in terms of machine learning algorithms. This book contains original materials by leading researchers in the area and covers applications of different machine learning methods in the reliability, security, performance, and privacy issues of cyber space. It enables readers to discover what types of learning methods are at their disposal, summarizing the state-of-the-practice in this significant area, and giving a classification of existing work. Those working in the field of cyber-based systems, including industrial managers, researchers, engineers, and graduate and senior undergraduate students will find this an indispensable guide in creating systems resistant to and tolerant of cyber attacks.
Feature Selection for Intrusion Detection Systems Springer
Since 1998, RAID has established its reputation as the main event in research on intrusion detection, both in Europe and the United States. Every year, RAID gathers researchers, security vendors and security practitioners to listen to the most recent research results in the area as well as experiments and deployment issues. This year, RAID has grown one step further to establish itself as a well-known event in the security community, with the publication of hardcopy proceedings. RAID 2000 received 26 paper submissions from 10 countries and 3 continents. The program committee selected 14 papers for publication and examined 6 of them for presentation. In addition RAID 2000 received 30 extended abstracts proposals; 15 of these extended abstracts were accepted for presentation. - tended abstracts are available on the website of the RAID symposium series, http://www.raid-symposium.org/. We would like to thank the technical p- gram committee for the help we received in reviewing the papers, as well as all the authors for their participation and submissions, even for those rejected. As in previous RAID symposiums, the program alternates between fun-mental research issues, such as newtechnologies for intrusion detection, and more practical issues linked to the deployment and operation of intrusion det- tion systems in a real environment. Five sessions have been devoted to intrusion detection technology, including modeling, data mining and advanced techniques.
Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2006 Springer Science & Business Media
MACHINE LEARNING TECHNIQUES AND ANALYTICS FOR CLOUD SECURITY This book covers new methods, surveys, case studies, and policy with almost all machine learning techniques and analytics for cloud security solutions The aim of Machine Learning Techniques and Analytics for Cloud Security is to integrate machine learning approaches to meet various analytical issues in cloud security. Cloud security with ML has long-standing challenges that require methodological and theoretical handling. The conventional cryptography approach is less applied in resource-constrained devices. To solve these issues, the machine learning approach may be effectively used in providing security to the vast growing cloud environment. Machine learning algorithms can also be used to meet various cloud security issues, such as effective intrusion detection systems, zero-knowledge authentication systems, measures for passive attacks, protocols design, privacy system designs, applications, and many more. The book also contains case studies/projects outlining how to implement various security features using machine learning algorithms and analytics on existing cloud-based products in public, private and hybrid cloud respectively. Audience Research scholars and industry engineers in computer sciences, electrical and electronics engineering, machine learning, computer security, information technology, and cryptography.
MATLAB Springer
This book presents recent advances in intrusion detection systems (IDSs) using state-of-the-art deep learning methods. It also provides a systematic overview of classical machine learning and the latest developments in deep learning. In particular, it discusses deep learning applications in IDSs in different classes: generative, discriminative, and adversarial networks. Moreover, it compares various deep learning-based IDSs based on benchmarking datasets. The book also proposes two novel feature learning models: deep feature extraction and selection (D-FES) and fully unsupervised IDS. Further challenges and research directions are presented at the end of the book. Offering a comprehensive overview of deep learning-based IDS, the book is a valuable reerence resource for undergraduate and graduate students, as well as researchers and practitioners interested in deep learning and intrusion detection. Further, the comparison of various deep-learning applications helps readers gain a basic understanding of machine learning, and inspires applications in IDS and other related areas in cybersecurity.
Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics Springer Nature
Artificial intelligence (AI) and its applications have risen to prominence as one of the most active study areas in recent years. In recent years, a rising number of AI applications have been applied in a variety of areas. Agriculture, transportation, medicine, and health are all being transformed by AI technology. The Internet of Things (IoT) market is thriving, having a significant impact on a wide variety of industries and applications, including e-health care, smart cities, smart transportation, and industrial engineering. Recent breakthroughs in artificial intelligence and machine learning techniques have reshaped various aspects of artificial vision, considerably improving the state of the art for artificial vision systems across a broad range of high-level tasks. As a result, several innovations and studies are being conducted to improve the performance and productivity of IoT devices across multiple industries using machine learning and artificial intelligence. Security is a primary consideration when analyzing the next generation communication network due to the rapid advancement of technology. Additionally, data analytics, deep intelligence, deep learning, cloud computing, and intelligent solutions are being employed in medical, agricultural, industrial, and health care systems that are based on the Internet of Things. This book will look at cutting-edge Network Attacks and Security solutions that employ intelligent data processing and Machine Learning (ML) methods. This book: Covers emerging technologies of network attacks and management aspects Presents artificial intelligence techniques for networks and resource optimization, and toward network automation, and security Showcases recent industrial and technological aspects of next-generation networks Illustrates artificial intelligence techniques to mitigate cyber-attacks, authentication, and authorization challenges Explains smart, and real-time monitoring services, multimedia, cloud computing, and information processing methodologies in 5G networks It is primarily for senior undergraduates, graduate students and academic researchers in the fields of electrical engineering, electronics and communication engineering, computer engineering, and information technology
Machine Learning Techniques and Analytics for Cloud Security Springer
The book is a collection of high quality peer reviewed research papers presented in Seventh International Conference on Bio-Inspired Computing (BIC-TA 2012) held at ABV-IIITM Gwalior, India. These research papers provide the latest developments in the broad area of "Computational Intelligence". The book discusses wide variety of industrial, engineering and scientific applications of nature/bio-inspired computing and presents invited papers from the inventors/originators of novel computational techniques.
Advances in Network Security and Applications Infinite Study

ARTIFICIAL INTELLIGENCE AND DATA MINING IN SECURITY FRAMEWORKS Written and edited by a team of experts in the field, this outstanding new volume offers solutions to the problems of security, outlining the concepts behind allowing computers to learn from experience and understand the world in terms of a hierarchy of concepts, with each concept defined through its relation to simpler concepts. Artificial intelligence (AI) and data mining is the fastest growing field in computer science. AI and data mining algorithms and techniques are found to be useful in different areas like pattern recognition, automatic threat detection, automatic problem solving, visual recognition, fraud detection, detecting developmental delay in children, and many other applications. However, applying AI and data mining techniques or algorithms successfully in these areas needs a concerted effort, fostering integrative research between experts ranging from diverse disciplines from data science to artificial intelligence. Successful application of security frameworks to enable meaningful, cost effective, personalized security service is a primary aim of engineers and researchers today. However realizing this goal requires effective understanding, application and amalgamation of AI and data mining and several other computing technologies to deploy such a system in an effective manner. This book provides state of the art approaches of artificial intelligence and data mining in these areas. It includes areas of detection, prediction, as well as future framework identification, development, building service systems and analytical aspects. In all these topics, applications of AI and data mining, such as artificial neural networks, fuzzy logic, genetic algorithm and hybrid mechanisms, are explained and explored. This book is aimed at the modeling and performance prediction of efficient security framework systems, bringing to light a new dimension in the theory and practice. This groundbreaking new volume presents these topics and trends, bridging the research gap on AI and data mining to enable wide-scale implementation. Whether for the veteran engineer or the student, this is a must-have for any library. This groundbreaking new volume: Clarifies the understanding of certain key mechanisms of technology helpful in the use of artificial intelligence and data mining in security frameworks Covers practical approaches to the problems engineers face in working in this field, focusing on the applications used every day Contains numerous examples, offering critical solutions to engineers and scientists Presents these new applications of AI and data mining that are of prime importance to human civilization as a whole

Data Warehousing and Data Mining Techniques for Cyber Security World Scientific

Network security is a serious global concern. The increasing prevalence of malware and incidents of attacks hinders the utilization of the Internet to its greatest benefit and incur significant economic losses. The traditional approaches in securing systems against threats are designing mechanisms that create a protective shield, almost always with vulnerabilities. This has created Intrusion Detection Systems to be developed that complement traditional approaches. However, with the advancement of computer technology, the behavior of intrusions has become complex that makes the work of security experts hard to analyze and detect intrusions. In order to address these challenges, data mining techniques have become a possible solution. However, the performance of data mining algorithms is affected when no optimized features are provided. This is because, complex relationships can be seen as well between the features and intrusion classes contributing to high computational costs in processing tasks, subsequently leads to delays in identifying intrusions. Feature selection is thus important in detecting intrusions by allowing the data mining system to focus on what is really important.

Networks Attack Detection on 5G Networks using Data Mining Techniques Springer Science & Business Media

The Hasty intensification of Internet communication and accessibility of systems to infringe the network, network security has become requisite. This paper focuses on development of efficient IDS in MANET. The KDD cup 99 dataset is considered for this proposal.

Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security ... Butterworth-Heinemann

Although the use of data mining for security and malware detection is quickly on the rise, most books on the subject provide high-level theoretical discussions to the near exclusion of the practical aspects. Breaking the mold, Data Mining Tools for Malware Detection provides a step-by-step breakdown of how to develop data mining tools for malware d

Machine Learning in Intrusion Detection CRC Press

This review volume introduces the novel intelligent Web theory calledcomputational Web intelligence (CWI) based on computationalintelligence (CI) and Web technology (WT). It takes an in-depth lookat hybrid Web intelligence (HWI), which is based on artificialbiological and computational intelligence with Web technology and isused to build hybrid intelligent Web systems that serve wired andwireless users more efficiently.

Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2007 Springer Science & Business Media

The book focuses to foster new and original research ideas and results in three broad areas: computing, analytics, and networking with its prospective applications in the various interdisciplinary domains of engineering. This is an exciting and emerging interdisciplinary area in which a wide range of theory and methodologies are being investigated and developed to tackle complex and challenging real world problems. It also provides insights into the International Conference on Computing Analytics and Networking (ICCAN 2017) which is a premier international open forum for scientists, researchers and technocrats in academia as well as in industries from different parts of the world to present, interact, and exchange the state of art of concepts, prototypes, innovative research ideas in several diversified fields. The book includes invited keynote papers and paper presentations from both academia and industry to initiate and ignite our young minds in the meadow of momentous research and thereby enrich their existing knowledge. The book aims at postgraduate students and researchers working in the discipline of Computer Science & Engineering. It will be also useful for the researchers working in the domain of electronics as it contains some hardware technologies and forthcoming communication technologies.

Machine Learning for Computer and Cyber Security CRC Press

Data mining is becoming a pervasive technology in activities as diverse as using historical data to predict the success of a marketing campaign, looking for patterns in financial transactions to discover illegal activities or analyzing genome sequences. From this perspective, it was just a matter of time for the discipline to reach the important area of computer security. Applications Of Data Mining In Computer Security presents a collection of research efforts on the use of data mining in computer security. Applications Of Data Mining In Computer Security concentrates heavily on the use of data mining in the area of intrusion detection. The reason for this is twofold. First, the volume of data dealing with both network and host activity is so large that it makes it an ideal candidate for using data mining techniques. Second, intrusion detection is an extremely critical activity. This book also addresses the application of data mining to computer forensics. This is a crucial area that seeks to address the needs of law enforcement in analyzing the digital evidence.

Privacy, Security, and Trust in KDD Springer Science & Business Media

While Computer Security is a broader term which incorporates technologies, protocols, standards and policies to ensure the security of the computing systems including the computer hardware, software and the information stored in it, Cyber Security is a specific, growing field to protect computer networks (offline and online) from unauthorized access, botnets, phishing scams, etc. Machine learning is a branch of Computer Science which enables computing machines to adopt new behaviors on the basis of observable and verifiable data and information. It can be applied to ensure the security of the computers and the information by detecting anomalies using data mining and other such techniques. This book will be an invaluable resource to understand the importance of machine learning and data mining in establishing computer and cyber security. It emphasizes important security aspects associated with computer and cyber security along with the analysis of machine learning and data mining based solutions. The book also highlights the future research domains in which these solutions can be applied. Furthermore, it caters to the needs of IT professionals, researchers, faculty members, scientists, graduate students, research scholars and software developers who seek to carry out research and develop combating solutions in the area of cyber security using machine learning based approaches. It is an extensive source of information for the readers belonging to the field of Computer Science and Engineering, and Cyber Security professionals. Key Features: This book contains examples and illustrations to demonstrate the principles, algorithms, challenges and applications of machine learning and data mining for computer and cyber security. It showcases important security aspects and current trends in the field. It provides an insight of the future research directions in the field. Contents of this book help to prepare the students for exercising better defense in terms of understanding the motivation of the attackers and how to deal with and mitigate the situation using machine learning based approaches in better manner.

Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2006 CRC Press

"Machine Learning and Data Mining for Computer Security" provides an overview of the current state of research in machine learning and data mining as it applies to problems in computer security. This book has a strong focus on information processing and combines and extends results from computer security. The first part of the book surveys the data sources, the learning and mining methods, evaluation methodologies, and past work relevant for computer security. The second part of the book consists of articles written by the top researchers working in this area. These articles deals with topics of host-based intrusion detection through the analysis of audit trails, of command sequences and of system calls as well as network intrusion detection through the analysis of TCP packets and the detection of malicious executables. This book fills the great need for a book that collects and frames work on developing and applying methods from machine learning and data mining to problems in computer security.

Data Analytics and Decision Support for Cybersecurity Springer

This important book introduces the concept of intrusion detection, discusses various approaches for intrusion detection systems (IDS), and presents the architecture and implementation of IDS. It emphasizes on the prediction and learning algorithms for intrusion detection and highlights techniques for intrusion detection of wired computer networks and wireless sensor networks. The performance comparison of various IDS via simulation will also be included. Contents: Attacks and Countermeasures in Computer SecurityMachine Learning MethodsIntrusion Detection SystemTechniques for Intrusion DetectionAdaptive Automatically Tuning Intrusion Detection SystemSystem Prototype and Performance EvaluationAttacks Against Wireless Sensor NetworkIntrusion Detection System for Wireless Sensor NetworkConclusion and Future Research Readership: Academicians, researchers and graduate students in software engineering/programming; computer engineering, knowledge and system engineering. Keywords:Intrusion;Detection;Machine Learning;Computer Network;Sensor Network;Computer SecurityKey Features:Discusses attacks and countermeasures in computer securityPresents state-of-the-art intrusion detection researchDescribes adaptive automatically tuning intrusion detection for wired networks

Network Intrusion Detection using Deep Learning LAP Lambert Academic Publishing

With the rapid advancement of information discovery techniques, machine learning and data mining continue to play a significant role in cybersecurity. Although several conferences, workshops, and journals focus on the fragmented research topics in this area, there has been no single interdisciplinary resource on past and current works and possible

Machine Learning and Data Mining for Computer Security Springer Nature

This book presents state-of-the-art research on intrusion detection using reinforcement learning, fuzzy and rough set theories, and genetic algorithm. Reinforcement learning is employed to incrementally learn the computer network behavior, while rough and fuzzy sets are utilized to handle the uncertainty involved in the detection of traffic anomaly to secure data resources from possible attack. Genetic algorithms make it possible to optimally select the network traffic parameters to reduce the risk of network intrusion. The book is unique in terms of its content, organization, and writing style. Primarily intended for graduate electrical and computer engineering students, it is also useful for doctoral students pursuing research in intrusion detection and practitioners interested in network security and administration. The book covers a wide range of applications, from general computer security to server, network, and cloud security.

Data Management, Analytics and Innovation Springer

The book presents the latest, high-quality, technical contributions and research findings in the areas of data management and smart computing, big data management, artificial intelligence and data analytics, along with advances in network technologies. It discusses state-of-the-art topics as well as the challenges and solutions for future development. It includes original and previously unpublished international research work highlighting research domains from different perspectives. This book is mainly intended for researchers and practitioners in academia and industry.

Investigative Data Mining for Security and Criminal Detection World Scientific

This book constitutes the refereed proceedings of the International ECML/PKDD Workshop on Privacy and Security Issues in Data Mining and Machine Learning, PSDML 2010, held in Barcelona, Spain, in September 2010. The 11 revised full papers presented were carefully reviewed and selected from 21 submissions. The papers range from data privacy to security applications, focusing on detecting malicious behavior in computer systems.

Related with Intrusion Detection System Using Datamining Techniques:
• Example Of Positive Economic Statement : click here