Machine Learning Forensics For Law Enforcement Security And Intelligence

Impact and Challenges
Machine Learning Forensics for Law Enforcement, Security, and Intelligence
From Reactive to Proactive Process, Second Edition
Computer and Intrusion Forensics
14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers
Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions
Third International Conference, AIST 2021, Delhi, India, November 12–13, 2021, Revised Selected Papers
Digital Forensics and Investigations
Law Enforcement Techniques for Knowing Who You're Dating
First International Conference, ICIIA 2021, Ota, Nigeria, November 25-27, 2021 : Revised Selected Papers
Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges
Advances in Malware and Data-Driven Network Security
Critical Concepts, Standards, and Techniques in Cyber Forensics
Privacy, Security And Forensics in The Internet of Things (IoT)
Machine Learning for Authorship Attribution and Cyber Forensics
Implementing Digital Forensic Readiness
Emerging Challenges at the Frontiers of Counter-Terrorism
Data Analytics in Project Management
Proceedings of International Conference on Big Data, Machine Learning and their Applications
Machine Learning Forensics for Law Enforcement, Security, and Intelligence
Machine Learning Forensics for Law Enforcement, Security, and Intelligence
7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31 - February 2, 2011, Revised Selected Papers
Dark Web Pattern Recognition and Crime Analysis Using Machine Intelligence
Modern Principles, Practices, and Algorithms
Shades of Blue - 30 Years of (Un) Ethical Policing
2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)
Methods and Solutions
Advances in Digital Forensics VII
Modern Principles, Practices, and Algorithms
System Forensics, Investigation and Response
Counter-Terrorism, Ethics and Technology
Informatics and Intelligent Applications
Confluence of AI, Machine, and Deep Learning in Cyber Forensics
Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book
Technologies to Advance Automation in Forensic Science and Criminal Investigation
Information Security Management Handbook, Volume 5
“The” Three Brides
Artificial Intelligence in Cyber Security: Impact and Implications
Pattern Recognition and Information Forensics

TALAN ALANNAH

CRC Press
PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Completely revised and rewritten to keep pace with the fast-paced field of Computer Forensics! Computer crimes call for forensics specialists, people who know how to find and follow the evidence. System Forensics, Investigation, and Response, Second Edition begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. New and Key Features of the Second Edition: Examines the fundamentals of system forensics Discusses computer crimes and forensic methods Written in an accessible and engaging style Incorporates real-world examples and engaging cases Instructor Materials for System Forensics, Investigation, and Response include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts Instructor's Manual
Impact and Challenges IGI Global
Artificial intelligence and its various components are rapidly engulfing almost every professional industry. Specific features of AI that have proven to be vital solutions to numerous real-world issues are machine learning and deep learning. These intelligent agents unlock higher levels of performance and efficiency, creating a wide span of industrial applications. However, there is a lack of research on the specific uses of machine/deep learning in the professional realm. Machine Learning and Deep Learning in Real-Time Applications provides emerging research exploring the theoretical and practical aspects of machine learning and deep

learning and their implementations as well as their ability to solve real-world problems within several professional disciplines including healthcare, business, and computer science. Featuring coverage on a broad range of topics such as image processing, medical improvements, and smart grids, this book is ideally designed for researchers, academicians, scientists, industry experts, scholars, IT professionals, engineers, and students seeking current research on the multifaceted uses and implementations of machine learning and deep learning across the globe.

Machine Learning Forensics for Law Enforcement, Security, and Intelligence Information Science Reference

Implementing Digital Forensic Readiness: From Reactive to Proactive Process, Second Edition presents the optimal way for digital forensic and IT security professionals to implement a proactive approach to digital forensics. The book details how digital forensic processes can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and redusing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stances, a company’s preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

From Reactive to Proactive Process, Second Edition John Wiley & Sons

Increasingly, crimes and fraud are digital in nature, occurring at breakneck speed and encompassing large volumes of data. To combat this unlawful activity, knowledge about the use of machine learning technology and software is critical. Machine Learning Forensics for Law Enforcement, Security, and Intelligence integrates an assortment of deductive

Computer and Intrusion Forensics Artech House

Annotation A comprehensive and broad introduction to computer and intrusion forensics, covering the areas of law enforcement, national security and corporate fraud, this practical book helps professionals understand case studies from around the world, and treats key emerging areas such as stegoforensics, image identification, authorship categorization, and machine learning.

14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers IGI Global

"The reference book will show the depth of Darkweb Environment by highlighting the Attackers techniques, crawling of hidden contents, Intrusion detection using advance algorithms, TOR Network structure, Memex search engine indexing of anonymous contents at Online Social Network, and more"--

Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions Springer Nature

This book provides a critical reflection on automated science and addresses the question whether the computational tools we developed in last decades are changing the way we humans do science. More concretely: Can machines replace scientists in crucial aspects of scientific practice? The contributors to this book re-think and refine some of the main concepts by which science is understood, drawing a fascinating picture of the developments we expect over the next decades of human-machine co-evolution. The volume covers examples from various fields and areas, such as molecular biology, climate modeling, clinical medicine, and artificial intelligence. The explosion of technological tools and drivers for scientific research calls for a renewed understanding of the human character of science. This book aims precisely to contribute to such a renewed understanding of science.

Third International Conference, AIST 2021, Delhi, India, November 12–13, 2021, Revised Selected Papers IGI Global

Developing a knowledge model helps to formalize the difficult task of analyzing crime incidents in addition to preserving and presenting the digital evidence for legal processing. The use of data analytics techniques to collect evidence assists forensic investigators in following the standard set of forensic procedures, techniques, and methods used for evidence collection and extraction. Varieties of data sources and information can be uniquely identified, physically isolated from the crime scene, protected, stored, and transmitted for investigation using AI techniques. With such large volumes of forensic data being processed, different deep learning techniques may be employed. Confluence of AI, Machine, and Deep Learning in Cyber Forensics contains cutting-edge research on the latest AI techniques being used to design and build solutions that address prevailing issues in cyber forensics and that will support efficient and effective investigations. This book seeks to understand the value of the deep learning algorithm to handle evidence data as well as the usage of neural networks to analyze investigation data. Other themes that are explored include machine learning algorithms that allow machines to interact with the evidence, deep learning algorithms that can handle evidence acquisition and preservation, and techniques in both fields that allow for the analysis of huge amounts of data collected during a forensic investigation. This book is ideally intended for forensics experts, forensic investigators, cyber forensic practitioners, researchers, academicians, and students interested in cyber forensics, computer science and engineering, information technology, and electronics and communication.

Digital Forensics and Investigations Springer Nature

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics VII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Forensic Techniques, Fraud and Malware Investigations, Network Forensics, and Advanced Forensic Techniques. This book is the 7th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of 21 edited papers from the 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National Center for Forensic Science,

Orlando, Florida, USA in the spring of 2011. Advances in Digital Forensics VII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma, USA.

Law Enforcement Techniques for Knowing Who You're Dating CRC Press

"This book provides a media for advancing research and the development of theory and practice of digital crime prevention and forensics, embracing a broad range of digital crime and forensics disciplines"--Provided by publisher.

First International Conference, ICIIA 2021, Ota, Nigeria, November 25-27, 2021 : Revised Selected Papers CRC Press

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today’s organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders’ abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges Springer

Machine Learning Forensics for Law Enforcement, Security, and Intelligence.

Advances in Malware and Data-Driven Network Security Jones & Bartlett Learning

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.

Critical Concepts, Standards, and Techniques in Cyber Forensics CRC Press

Digital forensics has been a discipline of Information Security for decades now. Its principles, methodologies, and techniques have remained consistent despite the evolution of technology, and, ultimately, it and can be applied to any form of digital data. However, within a corporate environment, digital forensic

professionals are particularly challenged. They must maintain the legal admissibility and forensic viability of digital evidence in support of a broad range of different business functions that include incident response, electronic discovery (ediscovery), and ensuring the controls and accountability of such information across networks. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise provides the methodologies and strategies necessary for these key business functions to seamlessly integrate digital forensic capabilities to guarantee the admissibility and integrity of digital evidence. In many books, the focus on digital evidence is primarily in the technical, software, and investigative elements, of which there are numerous publications. What tends to get overlooked are the people and process elements within the organization. Taking a step back, the book outlines the importance of integrating and accounting for the people, process, and technology components of digital forensics. In essence, to establish a holistic paradigm—and best-practice procedure and policy approach—to defending the enterprise. This book serves as a roadmap for professionals to successfully integrate an organization's people, process, and technology with other key business functions in an enterprise's digital forensic capabilities.

Privacy, Security And Forensics in The Internet of Things (IoT) IGI Global

Did you ever wonder how you could tell the difference between the good guys and bad? Once you can, what do you do? Most importantly, what do you need to be to live the most satisfied and productive life, and to attract the right kind of guy (Prince) while avoiding the wrong (the Frog)? The author, along with countless women and law enforcement officers, offers a guide on the single girl who is singleminded in her search for Prince Charming. Christine Kerrick reveals stories and techniques used by professionals to get the most information from a date to make the most informed decision for your future.

Machine Learning for Authorship Attribution and Cyber Forensics Machine Learning Forensics for Law Enforcement, Security, and Intelligence

This volume is a collation of articles on counter forensics practices and digital investigative methods from the perspective of crime science. The book also shares alternative dialogue on information security techniques used to protect data from unauthorised access and manipulation. Scandals such as those at OPCW and Gatwick Airport have reinforced the importance of crime science and the need to take proactive measures rather than a wait and see approach currently used by many organisations. This book proposes a new approach in dealing with cybercrime and unsociable behavior involving remote technologies using a combination of evidence-based disciplines in order to enhance cybersecurity and authorised controls. It starts by providing a rationale for combining selected disciplines to enhance cybersecurity by discussing relevant theories and highlighting the features that strengthen privacy when mixed. The essence of a holistic model is brought about by the challenge facing digital forensic professionals within environments where tested investigative practices are unable to provide satisfactory evidence and security. This book will be of interest to students, digital forensic and cyber security practitioners and policy makers. It marks a new route in the study of combined disciplines to tackle cybercrime using digital investigations and crime science.

Implementing Digital Forensic Readiness Springer Nature

This volume constitutes selected papers presented at the Third International Conference on Artificial Intelligence and Speech Technology, AIST 2021, held in Delhi, India, in November 2021. The 36 full papers and 18 short papers presented were thoroughly reviewed and selected from the 178 submissions. They provide a discussion on application of Artificial Intelligence tools in speech analysis, representation and models, spoken language recognition and understanding, affective speech recognition, interpretation and synthesis, speech interface design and human factors engineering, speech emotion recognition technologies, audio-visual speech processing and several others.

Emerging Challenges at the Frontiers of Counter-Terrorism Walter de Gruyter GmbH & Co KG

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Data Analytics in Project Management IGI Global

This open access book brings together a range of contributions that seek to explore the ethical issues arising from the overlap between counter-terrorism, ethics, and technologies. Terrorism and our responses pose some of the most significant ethical challenges to states and people. At the same time, we are becoming increasingly aware of the ethical implications of new and emerging technologies. Whether it is the use of remote weapons like drones as part of counter-terrorism strategies, the application of surveillance technologies to monitor and respond to terrorist activities, or counterintelligence agencies use of machine learning to detect suspicious behavior and hacking computers to gain access to encrypted data, technologies play a significant role in modern counter-terrorism. However, each of these technologies carries with them a range of ethical issues and challenges. How we use these technologies and the policies that govern them have broader impact beyond just the identification and response to terrorist activities. As we are seeing with China, the need to respond to domestic terrorism is one of the justifications for their rollout of the "social credit system." Counter-terrorism technologies can easily succumb to mission creep, where a technology's exceptional application becomes normalized and rolled out to society more generally. This collection is not just timely but an important contribution to understand the ethics of counter-terrorism and technology and has far wider implications for societies and nations around the world.

Proceedings of International Conference on Big Data, Machine Learning and their Applications Springer Nature

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect

of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XVI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, filesystem forensics, cloud forensics, social media forensics, multimedia forensics, and novel applications. This book is the sixteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of sixteen edited papers from the Sixteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India, in the winter of 2020. Advances in Digital Forensics XVI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.