Machine Learning Based Malware Detection For Android Using Machine Learning Based Malware Detection For Android Using | 4772bc8bf28c61ffdfb9c804c7319c97

Security in Computing and Communications
Biometric-Based Physical and Cybersecurity Systems
Machine Learning for Cybersecurity Cookbook
On Concept Drift, Deployability, and Adversarial Selection in Machine Learning-based Malware Detection
Applications of Artificial Intelligence for Smart Technology
Proceedings of International Conference on Artificial Intelligence and Applications
Deep Learning Applications for Cyber Security 2019 IEEE ACM 41st International Conference on Software Engineering New Ideas and Emerging Results (ICSE NIER)
Recent Trends in Computer Networks and Distributed Systems Security
Machine Learning in Cognitive IoT
2019 International Conference on Cyber Security and Protection of Digital Services (CyberSecurity)
Deployable Machine Learning for Security Defense
Botnet Detection Security of Information and Networks
Handbook of Big Data Analytics and Forensics
Android Malware Detection using Machine Learning
Research Anthology on Artificial Intelligence
Applications in Security Information and Communication Technology for Sustainable Development
Malware Detection
Malware Data Science
Machine Learning Based Malware Detection
Machine Learning and Security
Mastering Machine Learning for Penetration Testing
Confluence of AI, Machine, and Deep Learning in Cyber Forensics
Android Malware Detection
Malware Analysis Using Artificial Intelligence and Deep Learning
2019 6th International Conference on Information Science and Control Engineering
(ICISCE) International Conference on Communication, Computing and Electronics Systems
International Symposium on Distributed Computing and Artificial Intelligence Design and Development of Efficient Energy Systems
Adaptive Rule-based Malware Detection Employing Learning Classifier Systems
International Joint Conference CISIS’12-ICEUTE ’12-SOCO ’12 Special Sessions
Progress in Computing, Analytics and Networking

Security in Computing and Communications

The International Symposium on Distributed Computing and Artificial Intelligence 2011 (DCAI 2011) is a stimulating and productive forum where the scientific community can work towards future cooperation on Distributed Computing and Artificial Intelligence areas. This conference is the forum in which to present application of innovative techniques to complex problems. Artificial intelligence is changing our society. Its application in distributed environments, such as internet, electronic commerce, environment monitoring, mobile communications, wireless devices, distributed computing, to cite some, is continuously increasing, becoming an element of high added value with social and economic potential, both industry, life quality and research. These technologies are changing constantly as a result of the large research and technical effort being undertaken in universities, companies. The exchange of ideas between scientists and technicians from both academic and industry is essential to facilitate the development of systems that meet the demands of today’s society. This edition of DCAI brings together past experience, current work and promising future trends associated with distributed computing, artificial intelligence and their application to provide efficient solutions to real problems. This symposium is organized by the Bioinformatics, Intelligent System and Educational Technology Research Group (http://bisite.usal.es/) of the University of Salamanca. The present edition has been held in Salamanca, Spain, from 6 to 8 April 2011.

Biometric-Based Physical and Cybersecurity Systems

This book presents the latest developments in biometrics technologies and reports on new approaches, methods, findings, and technologies developed or being developed by the research community and the industry. The book focuses on introducing fundamental principles and concepts of key enabling technologies for biometric systems applied for both physical and cyber security. The authors disseminate recent research and developing efforts in this area, investigate related trends and challenges, and present case studies and examples such as fingerprint, face, iris, retina, keystroke dynamics, and voice applications. The
authors also investigate the advances and future outcomes in research and development in biometric security systems. The book is applicable to students, instructors, researchers, industry practitioners, and related government agencies staff. Each chapter is accompanied by a set of PowerPoint slides for use by instructors.

**Machine Learning for Cybersecurity Cookbook**

This book constitutes the refereed proceedings of the 10th International Conference on Information Systems Security, ICISS 2014, held in Hyderabad, India, in December 2014. The 20 revised full papers and 5 short papers presented together with 3 invited papers were carefully reviewed and selected from 129 submissions. The papers address the following topics: security inferences; security policies; security user interfaces; security attacks; malware detection; forensics; and location based security services.

**On Concept Drift, Deployability, and Adversarial Selection in Machine Learning-based Malware Detection**


**Applications of Artificial Intelligence for Smart Technology**

"Efficient and accurate malware detection is increasingly becoming a necessity for society to operate. Existing malware detection systems have excellent performance in identifying known malware for which signatures are available, but poor performance in anomaly detection for zero day exploits for which signatures have not yet been made available or targeted attacks against a specific entity. The primary goal of this thesis is to provide evidence for the potential of learning classifier systems to improve the accuracy of malware detection. A customized system based on a state-of-the-art learning classifier system is presented for adaptive rule-based malware detection, which combines a rule-based expert system with evolutionary algorithm based reinforcement learning, thus creating a self-training adaptive malware detection system which dynamically evolves detection rules. This system is analyzed on a benchmark of malicious and non-malicious files. Experimental results show that the system can outperform C4.5, a well-known non-adaptive machine learning algorithm, under certain conditions. The results demonstrate the system's ability to learn effective rules from repeated presentations of a tagged training set and show the degree of generalization achieved on an independent test set. This thesis is an extension and expansion of the work published in the Security, Trust, and Privacy for Software Applications workshop in COMPSAC 2011 – the 35th Annual IEEE Signature Conference on Computer Software and Applications"—Abstract, leaf iii.

**Proceedings of International Conference on Artificial Intelligence and Applications**

This book gathers high-quality papers presented at the International Conference on Artificial Intelligence and Applications (ICAIA 2020), held at Maharaja Surajmal Institute of Technology, New Delhi, India, on 6–7 February 2020. The book covers areas such as artificial neural networks, fuzzy systems, computational optimization technologies and machine learning.

**Deep Learning Applications for Cyber Security**

Botnets have become the platform of choice for launching attacks and committing fraud on the Internet. A better understanding of Botnets will help to coordinate and develop new technologies to counter this serious security threat. Botnet Detection: Countering the Largest Security Threat consists of chapters contributed by world-class leaders in this field, from the June 2006 ARO workshop on Botnets. This edited volume represents the state-of-the-art in research on Botnets.

**2019 IEEE ACM 41st International Conference on Software Engineering New Ideas and Emerging Results (ICSE NIER)**

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.

**Recent Trends in Computer Networks and Distributed Systems Security**

The book proposes new technologies and discusses future solutions for design infrastructure for ICT. The book contains high quality submissions presented at Second International Conference on Information and Communication Technology for Sustainable Development (ICT4SD - 2016) held at Goa, India during 1 - 2 July, 2016. The conference stimulates the cutting-edge research discussions among many academic pioneering researchers, scientists, industrial engineers, and students from all around the world. The topics covered in this book also focus on innovative issues at international level by bringing together the experts from different countries.

**Machine Learning in Cognitive IoT**

This book is focused on the use of deep learning (DL) and artificial intelligence (AI) as tools to advance the fields of malware detection and analysis. The individual chapters of the book deal with a wide variety of state-of-the-art AI and DL techniques, which are applied to a number of challenging malware-related problems. DL and AI based approaches to malware detection and analysis are largely data driven and hence minimal expert domain knowledge of malware is needed. This book fills a gap between the emerging fields of DL/AI and malware analysis. It covers a broad range of modern and practical DL and AI techniques, including frameworks and development tools enabling the audience to innovate with cutting-edge research advancements in a multitude of malware (and closely related) use cases.

**2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)**

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.

**Deployable Machine Learning for Security Defense**

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's
important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

Botnet Detection

Mobile phones have become central computing and communication devices since they offer almost the same functionalities as personal computers. They are also becoming ubiquitous and it has been an increase in the number of mobile users who are relying on them to store and handle personal information. Among them, Android-based mobile phones had appeared lately and were widely used so that they became an ideal target for malware developers. Android phone users can get free applications by downloading from the websites of Android Application Markets. Unfortunately, this phenomenon draws attention to malicious applications developers to upload their malicious applications. Because the free downloaded applications are not certified by legitimate organizations, they contain malware applications that can steal users’ private information.

Security of Information and Networks

Information Systems Security


Handbook of Research on Machine and Deep Learning Applications for Cyber Security

This book constitutes the refereed proceedings of the International Symposium on Security in Computing and Communications, SSCC 2014, held in Delhi, India, in September 2013. The 36 revised full papers presented together with 12 work-in-progress papers were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on security and privacy in networked systems; authentication and access control systems; encryption and cryptography; system and network security; work-in-progress.

Handbook of Big Data Analytics and Forensics

"Current antivirus software is effective at detecting well known threats but cannot keep up with the rate at which new malware is authored nor modern antivirus avoidance techniques, such as using polymorphic code. Some studies have investigated augmenting current antivirus techniques with machine learning, which could potentially detect some previously unknown malware. However, previously proposed methods either do not detect malware with satisfactory performance, or they have only been tested on laboratory software databases that cannot suitably be projected into realistic performance. This work explores several aspects of machine learning based malware detection. First, we propose an approach to learn primarily from program metadata, particularly header data in the 32-bit Windows Portable Executable (PE32) file format. We identify learning methods that learn effectively from this metadata, explore which metadata features can be trivially modified and are not appropriate for malware detection, test it on approximately realistic datasets, and find that it performs favorably compared to Windows API imports, another category of file characteristic that shows promise for machine learning based malware detection. Additionally, we find and explore the drastic performance drop which occurs when using a
realistically low proportion of malware in test datasets instead of datasets split evenly between malware and benign software.” -- abstract.

Android Malware Detection using Machine Learning

2019 International Conference on Computing, Networking and Communications (ICNC)

As the advancement of technology continues, cyber security continues to play a significant role in today’s world. With society becoming more dependent on the internet, new opportunities for virtual attacks can lead to the exposure of critical information. Machine and deep learning techniques to prevent this exposure of information are being applied to address mounting concerns in computer security. The Handbook of Research on Machine and Deep Learning Applications for Cyber Security is a pivotal reference source that provides vital research on the application of machine learning techniques for network security research. While highlighting topics such as web security, malware detection, and secure information sharing, this publication explores recent research findings in the area of electronic security as well as challenges and countermeasures in cyber security research. It is ideally designed for software engineers, IT specialists, cybersecurity analysts, industrial experts, academicians, researchers, and post-graduate students.

2021 11th International Conference on Cloud Computing, Data Science and Engineering (Confluence)

Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself! With this practical guide, you'll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis. Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike. Learn how machine learning has contributed to the success of modern spam filters Quickly detect anomalies, including breaches, fraud, and impending system failure Conduct malware analysis by extracting useful information from computer binaries Uncover attackers within the network by finding patterns inside datasets Examine how attackers exploit consumer-facing websites and app functionality Translate your machine learning algorithms from the lab to production Understand the threat attackers pose to machine learning solutions

Automated Software Engineering: A Deep Learning-Based Approach

The authors develop a malware fingerprinting framework to cover accurate android malware detection and family attribution in this book. The authors emphasize the following: (1) the scalability over a large malware corpus; (2) the resiliency to common obfuscation techniques; (3) the portability over different platforms and architectures. First, the authors propose an approximate fingerprinting technique for android packaging that captures the underlying static structure of the android applications in the context of bulk and offline detection at the app-market level. This book proposes a malware clustering framework to perform malware clustering by building and partitioning the similarity network of malicious applications on top of this fingerprinting technique. Second, the authors propose an approximate fingerprinting technique that leverages dynamic analysis and natural language processing techniques to generate Android malware behavior reports. Based on this fingerprinting technique, the authors propose a portable malware detection framework employing machine learning classification. Third, the authors design an automatic framework to produce intelligence about the underlying malicious cyber-infrastructures of Android malware. The authors then leverage graph analysis techniques to generate relevant intelligence to identify the threat effects of malicious Internet activity associated with android malware. The authors elaborate on an effective android malware detection system, in the online detection context at the mobile device level. It is suitable for deployment on mobile devices, using machine learning classification on method call sequences. Also, it is resilient to common code obfuscation techniques and adaptive to operating systems and malware change overtime, using natural language processing and deep learning techniques. Researchers working in mobile and network security, machine learning and pattern recognition will find this book useful as a reference. Advanced-level students studying
Malware Data Science explains how to identify, analyze, and classify large-scale malware using machine learning and data visualization. Security has become a "big data" problem. The growth rate of malware has accelerated to tens of millions of new files per year while our networks generate an ever-larger flood of security-relevant data each day. In order to defend against these advanced attacks, you'll need to know how to think like a data scientist. In Malware Data Science, security data scientist Joshua Saxe introduces machine learning, statistics, social network analysis, and data visualization, and shows you how to apply these methods to malware detection and analysis. You'll learn how to: - Analyze malware using static analysis - Observe malware behavior using dynamic analysis - Identify adversary groups through shared code analysis - Catch 0-day vulnerabilities by building your own machine learning detector - Measure malware detector accuracy - Identify malware campaigns, trends, and relationships through data visualization Whether you're a malware analyst looking to add skills to your existing arsenal, or a data scientist interested in attack detection and threat intelligence, Malware Data Science will help you stay ahead of the curve.

Information and Communication Technology for Sustainable Development

ICSE is the premier forum for researchers to present and discuss the most recent innovations, trends, outcomes, experiences, and challenges in the field of software engineering. The scope is broad and includes all original and unpublished results of empirical, conceptual, experimental, and theoretical software engineering research.

Malware Detection


Malware Data Science

Theme Socio political impacts of cyber security in the face of BREXIT IEEE Technically Co Sponsored (TCS) International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019), an international refereed conference dedicated to the advancement of Cyber Security, information security, network security, application security and business transformation of digital services, and the protection of public digital services, especially high value bearing online services. The aim of the Cyber Security 2019 is to encourage participation and promotion of collaborative scientific, industrial and academic inter workings among individual researchers, practitioners, members of existing associations, academia, standardisation bodies, and including government departments and agencies. The purpose is to build bridges between academia and industry, and to encourage interplay of different cultures. Cyber Security 2019 invites researchers and industry practitioners to submit papers.

Machine Learning Based Malware Detection

This book constitutes the refereed proceedings of the Second International Conference on Security in Computer Networks and Distributed Systems, SNDS 2014, held in Trivandrum, India, in March 2014. The 32 revised full papers presented together with 9 short papers and 8 workshop papers were carefully reviewed and selected from 129 submissions. The papers are organized in topical sections on security and privacy in networked systems; multimedia security; cryptosystems, algorithms; primitives; system and network security; short papers.
Machine Learning and Security

As global communities are attempting to transform into more efficient and technologically-advanced metropolises, artificial intelligence (AI) has taken a firm grasp on various professional fields. Technology used in these industries is transforming by introducing intelligent techniques including machine learning, cognitive computing, and computer vision. This has raised significant attention among researchers and practitioners on the specific impact that these smart technologies have and what challenges remain. Applications of Artificial Intelligence for Smart Technology is a pivotal reference source that provides vital research on the implementation of advanced technological techniques in professional industries through the use of AI. While highlighting topics such as pattern recognition, computational imaging, and machine learning, this publication explores challenges that various fields currently face when applying these technologies and examines the future uses of AI. This book is ideally designed for researchers, developers, managers, academicians, analysts, students, and practitioners seeking current research on the involvement of AI in professional practices.

Mastering Machine Learning for Penetration Testing

Become a master at penetration testing using machine learning with Python Key Features
Identify ambiguities and breach intelligent security systems Perform unique cyber attacks to breach robust systems Learn to leverage machine learning algorithms Book Description Cyber security is crucial for both businesses and individuals. As systems are getting smarter, we now see machine learning interrupting computer security. With the adoption of machine learning in upcoming security products, it’s important for pentesters and security researchers to understand how these systems work, and to breach them for testing purposes. This book begins with the basics of machine learning and the algorithms used to build robust systems. Once you’ve gained a fair understanding of how security products leverage machine learning, you’ll dive into the core concepts of breaching such systems. Through practical use cases, you’ll see how to find loopholes and surpass a self-learning security system. As you make your way through the chapters, you’ll focus on topics such as network intrusion detection and AV and IDS evasion. We’ll also cover the best practices when identifying ambiguities, and extensive techniques to breach an intelligent system. By the end of this book, you will be well-versed with identifying loopholes in a self-learning security system and will be able to efficiently breach a machine learning system. What you will learn Take an in-depth look at machine learning Get to know natural language processing (NLP) Understand malware feature engineering Build generative adversarial networks using Python libraries Work on threat hunting with machine learning and the ELK stack Explore the best practices for machine learning Who this book is for This book is for pen testers and security professionals who are interested in learning techniques to break an intelligent security system. Basic knowledge of Python is needed, but no prior knowledge of machine learning is necessary.

Confluence of AI, Machine, and Deep Learning in Cyber Forensics

The 11th 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.

Machine Learning Based Android Malware Detection

This book includes high impact papers presented at the International Conference on Communication, Computing, and Electronics Systems 2019, held at the PPG Institute of Technology, Coimbatore, India, on 15–16 November, 2019. Discussing recent trends in cloud computing, mobile computing, and advancements of electronics systems, the book covers topics such as automation, VLSI, embedded systems, integrated device technology, satellite communication, optical communication, RF communication, microwave engineering, artificial intelligence, deep learning, pattern recognition, Internet of Things, precision models, bioinformatics, and healthcare informatics.
Malware Analysis Using Artificial Intelligence and Deep Learning


2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)

This volume of Advances in Intelligent and Soft Computing contains accepted papers presented at CISIS 2012 and ICEUTE 2012, both conferences held in the beautiful and historic city of Ostrava (Czech Republic), in September 2012. CISIS aims to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of Computational Intelligence, Information Security, and Data Mining. The need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event. After a thorough peer-review process, the CISIS 2012 International Program Committee selected 30 papers which are published in these conference proceedings achieving an acceptance rate of 40%. In the case of ICEUTE 2012, the International Program Committee selected 4 papers which are published in these conference proceedings. The selection of papers was extremely rigorous in order to maintain the high quality of the conference and we would like to thank the members of the Program Committees for their hard work in the reviewing process. This is a crucial process to the creation of a high standard conference and the CISIS and ICEUTE conferences would not exist without their help.

Neural Information Processing. Models and Applications

Cybercrime remains a growing challenge in terms of security and privacy practices. Working together, deep learning and cyber security experts have recently made significant advances in the fields of intrusion detection, malicious code analysis and forensic identification. This book addresses questions of how deep learning methods can be used to advance cyber security objectives, including detection, modeling, monitoring and analysis of as well as defense against various threats to sensitive data and security systems. Filling an important gap between deep learning and cyber security communities, it discusses topics covering a wide range of modern and practical deep learning techniques, frameworks and development tools to enable readers to engage with the cutting-edge research across various aspects of cyber security. The book focuses on mature and proven techniques, and provides ample examples to help readers grasp the key points.

2019 6th International Conference on Information Science and Control Engineering (ICISCE)

"This book focuses on new and original research ideas and findings in three broad areas: computing, analytics, and networking and their potential applications in the various domains of engineering – an emerging, interdisciplinary area in which a wide range of theories and methodologies are being investigated and developed to tackle complex and challenging real-world problems. The book also features keynote presentations and papers from the International Conference on Computing Analytics and Networking (ICCAN 2019), which offers an open forum for scientists, researchers and technocrats in academia and industry from around the globe to present and share state-of-the-art concepts, prototypes, and innovative research ideas in diverse fields. Providing inspiration for postgraduate students and young researchers working in the field of computer science & engineering, the book also discusses hardware technologies and future communication technologies, making it useful for those in the field of electronics." -- Prové de l'editor.

International Conference on Communication, Computing and Electronics Systems

There is not a single industry which will not be transformed by machine learning and Internet of Things (IoT). IoT and machine learning have altogether changed the technological scenario by letting the user monitor and control things based on the
prediction made by machine learning algorithms. There has been substantial progress in the usage of platforms, technologies and applications that are based on these technologies. These breakthrough technologies affect not just the software perspective of the industry, but they cut across areas like smart cities, smart healthcare, smart retail, smart monitoring, control, and others. Because of these “game changers,” governments, along with top companies around the world, are investing heavily in its research and development.

Keeping pace with the latest trends, endless research, and new developments is paramount to innovate systems that are not only user-friendly but also speak to the growing needs and demands of society. This volume is focused on saving energy at different levels of design and automation including the concept of machine learning automation and prediction modeling. It also deals with the design and analysis for IoT-enabled systems including energy saving aspects at different level of operation. The editors and contributors also cover the fundamental concepts of IoT and machine learning, including the latest research, technological developments, and practical applications. Valuable as a learning tool for beginners in this area as well as a daily reference for engineers and scientists working in the area of IoT and machine technology, this is a must-have for any library.

International Symposium on Distributed Computing and Artificial Intelligence

The two volume set LNCS 6443 and LNCS 6444 constitutes the proceedings of the 17th International Conference on Neural Information Processing, ICONIP 2010, held in Sydney, Australia, in November 2010. The 146 regular session papers presented were carefully reviewed and selected from 470 submissions. The papers of part I are organized in topical sections on neurodynamics, computational neuroscience and cognitive science, data and text processing, adaptive algorithms, bio-inspired algorithms, and hierarchical methods. The second volume is structured in topical sections on brain computer interface, kernel methods, computational advance in bioinformatics, self-organizing maps and their applications, machine learning applications to image analysis, and applications.

Design and Development of Efficient Energy Systems

This book discusses various open issues in software engineering, such as the efficiency of automated testing techniques, predictions for cost estimation, data processing, and automatic code generation. Many traditional techniques are available for addressing these problems. But, with the rapid changes in software development, they often prove to be outdated or incapable of handling the software’s complexity. Hence, many previously used methods are proving insufficient to solve the problems now arising in software development. The book highlights a number of unique problems and effective solutions that reflect the state-of-the-art in software engineering. Deep learning is the latest computing technique, and is now gaining popularity in various fields of software engineering. This book explores new trends and experiments that have yielded promising solutions to current challenges in software engineering. As such, it offers a valuable reference guide for a broad audience including systems analysts, software engineers, researchers, graduate students and professors engaged in teaching software engineering.

Adaptive Rule-based Malware Detection Employing Learning Classifier Systems

This book covers the different technologies of Internet, and machine learning capabilities involved in Cognitive Internet of Things (CIoT). Machine learning is explored by covering all the technical issues and various models used for data analytics during decision making at different steps. It initiates with IoT basics, its history, architecture and applications followed by capabilities of CIoT in real world and description of machine learning (ML) in data mining. Further, it explains various ML techniques and paradigms with different phases of data pre-processing and feature engineering. Each chapter includes sample questions to help understand concepts of ML used in different applications. Explains integration of Machine Learning in IoT for building an efficient decision support system. Covers IoT, CIoT, machine learning paradigms and models Includes implementation of machine learning models in R Help the analysts and developers to work efficiently with emerging technologies such as data analytics, data processing, Big Data, Robotics Includes programming codes in Python/Matlab/R alongwith practical examples, questions and multiple choice questions
Learn how to apply modern AI to create powerful cybersecurity solutions for malware, pentesting, social engineering, data privacy, and intrusion detection. Key Features Manage data of varying complexity to protect your system using the Python ecosystem. Apply ML to pentesting, malware, data privacy, intrusion detection system (IDS) and social engineering. Automate your daily workflow by addressing various security challenges using the recipes covered in the book. Description Organizations today face a major threat in terms of cybersecurity, from malicious URLs to credential reuse, and having robust security systems can make all the difference. With this book, you'll learn how to use Python libraries such as TensorFlow and scikit-learn to implement the latest artificial intelligence (AI) techniques and handle challenges faced by cybersecurity researchers. You'll begin by exploring various machine learning (ML) techniques and tips for setting up a secure lab environment. Next, you'll implement key ML algorithms such as clustering, gradient boosting, random forest, and XGBoost. The book will guide you through constructing classifiers and features for malware, which you'll train and test on real samples. As you progress, you'll build self-learning, reliant systems to handle cybersecurity tasks such as identifying malicious URLs, spam email detection, intrusion detection, network protection, and tracking user and process behavior. Later, you'll apply generative adversarial networks (GANs) and autoencoders to advanced security tasks. Finally, you'll delve into secure and private AI to protect the privacy rights of consumers using your ML models. By the end of this book, you'll have the skills you need to tackle real-world problems faced in the cybersecurity domain using a recipe-based approach. What you will learn Learn how to build malware classifiers to detect suspicious activities. Apply ML to generate custom malware to pentest your security. Use ML algorithms with complex datasets to implement cybersecurity concepts. Create neural networks to identify fake videos and images. Secure your organization from one of the most popular threats - insider threats. Defend against zero-day threats by constructing an anomaly detection system. Detect web vulnerabilities effectively by combining Metasploit and ML. Understand how to train a model without exposing the training data. Who this book is for This book is for cybersecurity professionals and security researchers who are looking to implement the latest machine learning techniques to boost computer security, and gain insights into securing an organization using red and blue team ML. This recipe-based book will also be useful for data scientists and machine learning developers who want to experiment with smart techniques in the cybersecurity domain. Working knowledge of Python programming and familiarity with cybersecurity fundamentals will help you get the most out of this book.