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


Deployable Machine Learning for Security Defense This book provides an overview of emerging topics in the field of hardware security, such as artificial intelligence and quantum computing, and highlights how these technologies can be leveraged to secure and protect security devices. The authors of the book are experts in emerging technologies, traditional hardware design, and hardware security and trust. The book will cover a comprehensive understanding of hardware security problems and how to overcome these through an efficient combination of conventional approaches and emerging technologies, enabling them to design secure, reliable, and trustworthy hardware. It offers a high-level introduction to current hardware security problems, providing an overview of a wide range of related topics and their applications to hardware security problems. It covers state-of-the-art techniques, as well as ongoing research efforts in emerging technologies in hardware security. Provides guidance and techniques to design and security engineers on their protection design using emerging technologies. Security Incidents & Response Against Cyber Attacks

Applications and Techniques in Information Security This book compiles the refereed proceedings of the 10th International Conference on Digital Forensics and Cyber Crime, DFCS2018, held in New Orleans, LA, USA, in September 2018. The 31 reviewed full papers and 1 short paper were selected from 35 submissions and are grouped in topical sections on current and data hiding and digital forensics, artifact correlation. Adaptive Role-based Malware Detection Deploying Learning Classifier System The proceedings contain the Special Issue on “Green, Efficient, Energy-efficient and Sustainable Networks” of the Sensors Journal. Seventeen high-quality papers published in the Special Issue have been collected and reproduced in this book, demonstrating significant achievements in the field. The book is divided into the following six chapters:

Adaptive Rule-based Malware Detection Deploying Learning Classifier System: The proceedings contain the Special Issue on “Green, Efficient, Energy-efficient and Sustainable Networks” of the Sensors Journal. Seventeen high-quality papers published in the Special Issue have been collected and reproduced in this book, demonstrating significant achievements in the field. The book is divided into the following six chapters:

1. A review of recent research in malware detection and analysis
2. An overview of recent advances in machine learning techniques for malware detection
3. A comparison of different machine learning approaches for malware detection
4. A survey of recent research in the use of machine learning for malware detection in different environments
5. A discussion of the challenges and opportunities in the field of malware detection and analysis
6. A summary of recent trends and future directions in the field of malware detection and analysis

The book provides a comprehensive overview of the state-of-the-art in malware detection and analysis, covering both theoretical and practical aspects of the field. It is intended for researchers, practitioners, and students in the field of cybersecurity, with a particular focus on machine learning and data mining techniques for malware detection. The book is suitable for graduate students, researchers, and practitioners in the field of cybersecurity.
fields including cryptography, database and storage security, human and societal aspects of security and privacy.

Proceedings of International Conference on Artificial Intelligence and Applications Machine Vision Inspection Systems (MVIS) is a multidisciplinary research field that emphasizes image processing, machine vision and pattern recognition for industrial inspection, and the applications of computer vision and machine learning gained significant importance. The main assessment of the inspection may fail and turn into false assessment due to a large number of examining while inspection process. This volume covers machine learning-based approaches in MVIS applications, and it can be employed to a wide diversity of problems in the domains of computer vision, pattern recognition, object detection, and even natural language processing, medical diagnosis, etc. This edited book is designed to address various aspects of recent methodologies, concepts, and research plans out to the readers for giving more depth insights for pursuing research on machine learning-based approaches.

Confidence of AI, Machine, and Deep Learning in Cyber Forensics 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 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 technology perspective that has been used for developing 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.

Enhanced Machine Learning Based Dynamic Detection of Evasive Android Malware This book addresses the key security challenges in the big data centric computing and network systems, and discusses how to tackle them using a mix of conventional and state-of-the-art computer science and advanced analytics such as Microsoft, Amazon, and Google. It provides a comprehensive overview of the emerging techniques and platforms for 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 changed the game and have simplified this complex task. This volume presents a much-needed exploration of the emerging technologies and techniques for securing the use of online networks as a safe and effective platform.

Security and Privacy in Communication Networks 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 phones and the mobile applications. However, even with the tremendous progress AI has made within the sphere of cyber security, it’s important to understand the impacts, implications, and critical issues and challenges of AI applications along with the emerging technologies and techniques to address and understanding of the AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security, providing insights into the development of AI technologies, and discussing the latest tools and techniques. Thus, the book sheds light on how conventional security techniques can be adapted to the security landscape in the big data era.

Handbook of Research on Machine and Deep Learning Applications for Cyber Security This book presents the results of the Third International Conference on Machine Learning for Cyber Security, MIACS 2020, held in Xi'an, China in October 2020. The 11 full papers and 40 short papers presented were carefully reviewed and selected from 360 submissions. The papers offer a wide range of the following subjects: Machine learning, security, privacy-preserving, cyber, adversarial machine learning, malware detection and analysis, data mining, and Artificial Intelligence.

Machine Vision Inspection Systems, Machine Learning-Based Approaches This book develops 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 resilience to common obfuscation techniques; (3) the portability over different platforms and architectures. First, the authors propose an approximate fingerprinting technique for android packaging hash code extraction. Then, they develop a novel malware clustering framework to perform malware clustering by building and partitioning the similarity network of malicious applications over top of this fingerprinting technique. Second, the authors propose an approximate fingerprinting technique that leverages dynamic and natural language processing techniques to generate Android malware behavior reports. Based on this fingerprinting technique, the authors plan to develop an analytical model detection system to generate relevant intelligence to identify the threat effects of malicious Android activity associated with 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 call sequences and system log data to change over time, using natural language processing and deep learning techniques. Researchers working in mobile and network security.

Large Scale Machine Learning for the Detection and Classification of Malware 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 changed the game and have simplified this complex task. This volume presents a much-needed exploration of the emerging technologies and techniques for securing the use of online networks as a safe and effective platform.

Malware Analysis Using Artificial Intelligence and Deep Learning This book constitutes the proceedings of the first International Symposium on Cyber Security Cryptography and Machine Learning, held in Beer-Sheva, Israel, in June 2017. The 17 full and 4 short papers presented include cyber security; secure software development methodologies, formal methods semantics and verification of secure systems; fault tolerance, reliability, availability of distributed secure systems; game-theoretic approaches to secure computing; automatic detection of self-stabilizing and self-organising systems; communication, authentication and identification security; cyber security for mobile and internet of things; cyber security of corporations; security and privacy for cloud, edge and fog computing; cryptography; cryptographic implementation analysis and construction; secure multi-party computation; privacy-enhancing technologies and anonymity; post-quantum cryptography and security; machine learning and big data; anomaly detection and malware identification; business intelligence and security; digital forensics; digital rights management; trust management and reputation systems; information retrieval; risk analysis, DoS.

Computer Security – ESORICS 2021 This book constitutes the refereed proceedings of the 7th International Symposium on Engineering Secure Software and Systems, ESSoS 2015, held in Milan, Italy, in March 2015. The 11 full papers presented together with 12 short papers presented were carefully reviewed and selected from 360 submissions. The papers offer a wide range of the following subjects: Machine learning, security, privacy-preserving, cyber, adversarial machine learning, malware detection and analysis, data mining, and Artificial Intelligence.
AI 2017: Advances in Artificial Intelligence This book constitutes the refereed proceedings of the 30th Australasian Joint Conference on Artificial Intelligence, AI 2017, held in Melbourne, VIC, Australia, in August 2017. The 29 full papers and 2 short papers presented in this volume cover 12 sessions in the areas of artificial intelligence ranging from machine learning, optimization to big data science and their practical applications.

Research Anthology on Artificial Intelligence Applications in Security This book provides use case scenarios of machine learning, artificial intelligence, and real-time domain to supplement cyber security operations and proactively predict attacks and preempt cyber incidents. The authors discuss cyber security incident planning, starting from a draft response plan, to assigning responsibilities, to use of external experts, to equipping organization to cease incidents, to preparing comprehensive incident response team. The book also discusses classification of the incident response team, how to conduct situational awareness, how to contain and eradicate incidents, and how to cleanup and recover. The book shares real-world experiences and knowledge from authors from academia and industry. Shares case studies on using ML and AI to predict and preempt cyber attacks; describes security attacks, trends, and scenarios along with attack vectors for various domains and industry sectors; includes detail on incident planning, detection methods, containing incidents, and clean up recovery.

Machine Learning for Cyber Security Efficient and 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 a learning system. This work focuses on the self-training 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 malware learning algorithm, under certain conditions. The results demonstrate the system’s ability to learn effective rules from repeated presentations of a tapped 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 COMSAC 2011 - the 35th Annual IEEE Signature Conference on Computer Software and Applications—Abstract, leaf 1.

Cryptography and Network Security This book presents recent advances in intrusion detection systems (IDS) 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 IDS 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 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 areas in cybersecurity.

Android Malware Detection using Machine Learning This book constitutes the refereed proceedings of the 8th International Conference on Applications and Techniques in Information Security, ATIS 2017, held in Auckland, New Zealand, in July 2017. The 14 revised full papers and 4 short papers presented together with two abstracts of invited talks were carefully reviewed and selected from 29 submissions. The papers are organized in topical sections on Keynote Speeches; Crypto Algorithms and Applications; Attacks; Malware and Malicious Events Detection; System and Network Security.

Green, Energy-Efficient and Sustainable Networks The two volume set LNCS 12974 and LNCS 12975 constitutes the proceedings of the 26th European Symposium on Research in Computer Security, ESORICS 2021, which took place during October 4-8, 2021. The conference was originally planned to take place in Darmstadt, Germany, but changed to an online event due to the COVID-19 pandemic. The 78 full papers presented in this book were carefully reviewed and selected from 351 submissions. They were organized in topical sections as follows: Part I: network security; attacks; fuzzing; malware; user behavior and underground economy; blockchain; machine learning; anomaly detection; Part II: encryption; cryptography; privacy; differential privacy; zero-knowledge; key exchange; multi-party computation.

Network Intrusion Detection using Deep Learning This book presents recent advances in artificial intelligence research and blockchain technologies for cybersecurity applications. The accepted book chapters covered many themes, including artificial intelligence and blockchain challenges, models and applications, cyber threats and intrusions analysis and detection, and many other applications for smart cyber ecosystems. It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this particular area or interested in grasping the latest advances on artificial intelligence and blockchain for future cybersecurity applications.

Machine Learning Based Malware Detection In the present work we describe medical techniques which malware and with unknown characteristics are clustered into an unknown group. The classifiers used in this research are k-nearest Neighbors (KNN), SVM, Decision Trees, and nearest-neighbor.

Decision Tree and k-nearest neighbors (KNN) were used to take place in Paris, France, but had to change to an online format due to the COVID-19 pandemic. The 14 full and 7 short papers included in this volume were carefully reviewed and selected from 44 submissions. In addition, the book contains one invited talk in full paper length. The papers were organized in topical sections named: vulnerabilities, attacks and intrusion detection; TLS, openness and security control; access control, risk assessment and security knowledge; risk analysis, security awareness, detection and protection, infrastructure protection, information security and safety, and system security assurance.

Malware Data Science This book gathers high-quality papers presented at the International Conference on Artificial Intelligence and Applications (ICAI2020), 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.

Dependability in Sensor, Cloud, and Big Data Systems and Applications “Current antiviruses software is effective at detecting well known threats but cannot keep up with the rate at which new malware is authored or modern antivirus software technology." In this view, many 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 be projected to detect real 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 the impact of metadata features that 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 dramatic 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.

Cyber Security Cryptography and Machine Learning – ICCANN 2021

Malware Detection Artificial Intelligence This work presents the refereed proceedings of the 5th International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications, DependSys, held in Guangzhou, China, in November 2019. The volume presents 39 full papers, which were carefully reviewed and selected from 112 submissions. The papers are organized in topical sections on Dependability and security fundamentals and technologies; dependable and secure systems; dependable and secure applications; dependability and security measures and assessments; explainable artificial intelligence for cyber space.

Applied Learning Algorithms for Intelligent IoT The 4-volume set LNCS 11632 until LNCS 11635 constitutes the refereed proceedings of the 5th International Conference on Artificial Intelligence and Security, ICAIS 2019, which was held in New York, USA, in July 2019. The conference was formerly named "International Conference on Cloud Computing and Security" with the acronym ICCCS. The total of 215 full papers presented in this 4-volume proceedings was carefully reviewed and selected from 1259 submissions. The papers were organized in topical sections as follows: Part I: cloud computing; Part II: artificial intelligence; big data; and cloud computing and security; Part III: cloud computing and security; information hiding; IoT security; multimedia forensic; and encryption and cybersecurity; Part IV: encryption and cybersecurity.

Copyright code: 4772cbbf82f41ff6ddbe054b4371b3a7

Access Free Machine Learning Based Malware Detection For Android Using Page 3/3