Scopus

Document details

< Back to results | 1 of 1

Export Download Print E-mail Save to PDF Add to List More... >

Full Text View at Publisher

Procedia Computer Science
Volume 62, 2015, Pages 221-227
2015 International Conference on Soft Computing and Software Engineering, SCSE 2015; University of California, Berkeley, Sutardja Dai HallBerkeley; United States; 5 March 2015 through 6 March 2015; Code 119560

A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems (Conference Paper)

Abubakar, A.I.[a], Chiroma, H.[bc], Muaz, S.A.[d], Ila, L.B.[e]

[a]International Islamic University Malaysia, Faculty of Information and Communication Technology, Kuala Lumpur, Malaysia
[b]Federal College of Education (Technical), Department of Computer Science, Gombe, Nigeria
[c]University of Malaya, Department of Artificial Intelligence, Kuala Lumpur, Malaysia

View additional affiliations

Abstract

View references (25)

Cybercrime has led to the loss of billions of dollars, the malfunctioning of computer systems, the destruction of critical information, the compromising of network integrity and confidentiality, etc. In view of these crimes committed on a daily basis, the security of the computer systems has become imperative to minimize and possibly avoid the impact of cybercrimes. In this paper, we review recent advances in the use of cyber security benchmark datasets for the evaluation of machine learning and data mining-based intrusion detection systems. It was found that the state-of-the-art cyber security benchmark datasets KDD and UNM are no longer reliable, because their datasets cannot meet the expectations of current advances in computer technology. As a result, a new ADFA Linux (ADFA-LD) cyber security benchmark dataset for the evaluation of machine learning and data mining-based intrusion detection systems was proposed in 2013 to meet the current significant advances in computer technology. ADFA-LD requires improvement in terms of full descriptions of its attributes. This review can be used by the research community as a basis for abandoning the previous state-of-the-art cyber security benchmark datasets and starting to use the newly introduced benchmark dataset for effective and robust evaluation of machine learning and data mining-based intrusion detection system.

Indexed keywords

Engineering controlled terms: Artificial intelligence Computer crime Computer operating systems Data mining Learning systems Mercury (metal) Network security Soft computing Software engineering

Metrics View all metrics >

3 Citations in Scopus
65th Percentile

1.95 Field-Weighted Citation Impact

PlumX Metrics

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 3 documents

Toward a reliable anomaly-based intrusion detection in real-world environments

Viegas, E.K. , Santin, A.O. , Oliveira, L.S.
(2017) Computer Networks

A multi-class classification MCLP model with particle swarm optimization for network intrusion detection

Viswa Bharathy, A.M. , Mahabub Basha, A.
(2017) Sadhana - Academy Proceedings in Engineering Sciences

How South African SMEs address cyber security: The case of web server logs and intrusion detection

Kent, C. , Tanner, M. , Kabanda, S.
(2016) 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies, EmergiTech 2016

View all 3 citing documents

Inform me when this document is cited in Scopus:

Set citation alert > Set citation feed >