



Evolutionary Computing Environments: Implementing Security Risks Management and Benchmarking

Vinita Malik ^a , Sukhdip Singh ^b

Show more 

 Outline |  Share  Cite

<https://doi.org/10.1016/j.procs.2020.03.430>

[Get rights and content](#)

Under a Creative Commons [license](#)

[Open access](#)

Abstract

This research makes a focus on evolutionary computing environments i.e. Pervasive, Internet of Things, Artificially Intelligent (AI) and Big Data risks management. The contribution of paper lies in identifying, managing risks in advanced computing paradigms, mitigating security risks and benchmarking smart softwares. As the security and privacy of big volume data is heated discussion these days due to several vulnerabilities in data posed by its pervasive nature so the paper has implemented the security risks mitigation in big data projects. In addition, the benchmarking of pervasive software is done with the help of an intelligent tool for detecting application frameworks and security vulnerabilities. The application is scanned, and the intelligent tool quantifies the severity levels to provide the possible solutions. This tool also collects application metrics to benchmark it against technology, application business drivers and properties to improve the quantitative Performance of the software. This research also puts an analytical foundation for various risks management concepts in evolutionary environments i.e. Pervasive, AI, Internet of Things and Big Data.

PDF

Help

 Previous

Next 

Keywords

Security Vulnerabilities; Pervasive Computing; Big Data; Internet of Things; Artificially Intelligent computing

PDF
Help



[Download full text in PDF](#)

[Special issue articles](#)

[Recommended articles](#)

References

- 1 Y. Ren, A. Boukerche, (2008), "Modeling and managing trust for wireless and mobile Adhoc networks", in: proceedings of IEEE conference On Communications (ICC), Beijing, pp. 2129-2133
[Google Scholar](#)
- 2 J.M. Seigneur
Trust, Security and Privacy in global computing, Trinity College Dublin (2005)
PhD Theses
[Google Scholar](#)
- 3 Stefan. A Weis, (2005), "Security parallels between people and pervasive devices", in: Proceedings of the 3rd IEEE International Conference on pervasive computing and communications workshop, pp. 105-109
[Google Scholar](#)
- 4 Bessam Abdulrazak, Yasir Malik
Review of challenges, Requirements and approaches of pervasive computing system Evaluation
IETE Technical Review, 29 (6) (2012), pp. 506-522
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)
- 5 Lorenz M. Hilty, Claudia Som, (2004), "Assessing the Human, Social and Environmental risks of pervasive computing, Human and Ecological Risk Assessment", (10):853-874
[Google Scholar](#)
- 6 Jaydip Sen., (2012), "Ubiquitous Computing: Applications, Challenges and future trends", Book chapter in Embedded Systems and Wireless Technology: Theory and practical applications, pp.1 -41
[Google Scholar](#)
- 7 Cristiano Andre Da Costa, (2008), "Towards a General software Infrastructure for ubiquitous Computing", Journal of Pervasive Computing, IEEE CS, pp. 64-73
[Google Scholar](#)
- 8 Robert Richardson
2010/2011 CSI Computer Crime and Security Survey, Computer security institute (2012), pp. 1-44
[CrossRef](#) [Google Scholar](#)
- 9 Insight Consulting, (2009), http://dtps.unipi.gr/files/notes/2009-2010/eksamino_5/politikes_kai_diaxeirish_asfaleias/egxeiridio_cramm.pdf
[Google Scholar](#)
- 10 Clusif, (2010), <http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf>

PDF

Help




[Google Scholar](#)

- 11 Carnegie Mellon University, (2009), <http://www.cert.org/octave/download/intro.html>
[Google Scholar](#)
- 12 Thomas Lederm, Nathan L. Clarke, (2011), "Risk assessment for Mobile devices",
Lecture notes in computer science, (6863):210-218
[Google Scholar](#)
- 13 Germanjit Singh Sandhu, Daljinder Singh Salaria, (2014), "A Bayesian Network Model
of the Particle Swarm Optimization for Software Effort Estimation", International
Journal of Computer Applications, 96(4):52-58
[Google Scholar](#)
- 14 Taghi. M. Khoshgoftaar, Yi Liu, (2007), "A Multi-Objective Software Quality
Classification Model Using Genetic Programming", in IEEE Transactions on
Reliability, 56 (2):237-245
[Google Scholar](#)
- 15 DM. Rodvold, (1999), "A software development process model for artificial neural
networks in critical applications", IJCNN'99. International Joint Conference on Neural
Networks. Proceedings (Cat. No.99CH36339), Washington, DC, USA, (5): 3317-3322
[Google Scholar](#)
- 16 Xiaoking Liu, G. Kane, M. Bambroo
**An Intelligent Early Warning System for Software Quality Improvement and Project
Management**
Journal of systems and software, 11 (79) (2006), pp. 1562-1564
[View Record in Scopus](#) [Google Scholar](#)
- 17 Wen Tao Guo, Van Nam Huynh, Yoshiteru Nakamori
**A Proportional 3- Tuple Fuzzy Linguistic Representation Model for screening New
product projects**
Journal of Syst.Sci. And Syst. Eng., 1 (25) (2016), pp. 1-25
[View Record in Scopus](#) [Google Scholar](#)
- 18 Ming Yuan Hsieh, Yu Chin Hsu, Ching Torng Lin
**Risk assessment in new software development projects at the front end: A fuzzy logic
approach**
Ambient Intell Human Comput, 2 (9) (2018), pp. 295-305
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)
- 19 Radek Dorskocil
An Evaluation of total project risk based on fuzzy logic
Verslas: Theorija IR PRAKTIKA/Business: Theory and Practice, 17 (1) (2016), pp. 23-31
Vinita Malik / Procedia Computer Science 00 (2019) 000–000

PDF


Help

[Google Scholar](#)

- 20 Anupma Kaushik, S. Verma
Software Cost optimization integrating fuzzy systems and COA-Cuckoo optimization Algorithm
International Journal of System Assurance Engineering and Management, 2 (8) (2017), pp. 1461-1471
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)
- 21 Muhammad Saiful Islam, Madhav Prasad Nepal, Martin Skitmore, Meghdad Attarzadeh
Current research trends & application areas of fuzzy and hybrid methods to the risk assessment of construction projects
Advanced Engineering Informatics, 33 (2017), pp. 112-131
[Article](#)  [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)
- 22 Animesh Kumar Paul, Pintu Chandra Shill, Rafiqul Islam Rabin Md., Kazuyuki Murase
Adaptive weighted fuzzy rule-based system for the risk level assessment of heart disease
Applied Intelligence, 7 (48) (2017), pp. 1739-1756
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)
- 23 M. Sasidharan, M.P.N. Burrow, G.S. Ghataora, M.E. Torbaghan, (2017), "A review of risk management applications for railways" in the 14th International conference of railway Engineering
[Google Scholar](#)
- 24 Alexander Guzman Urbina, Atsushi Aoyama, (2017), "Pipeline Risk Assessment Using Artificial Intelligence: A Case from the Colombian Oil Network" in Process safety Process, 10.1002/prs.11890
[Google Scholar](#)
- 25 Xishi Huang, Danny Ho
Improving the COCOMO model by Neuro Fuzzy approach
Applied soft computing, 7 (2007), pp. 29-40
[Article](#)  [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)
- 26 Sun Jen Huang, Nan Hsing Chiu, (2009), "Applying fuzzy neural network to estimate software development effort", Appl Intell., pp.:30-73
[Google Scholar](#)
- 27 A. Kolus, D. Imbeau
: Classifying work rate from heart rate measurements using an adaptive Neuro-fuzzy inference system
l, Applied ergonomics, 54 (2016), pp. 158-168
[Article](#)  [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

PDF

Help

- 27 Sharifa Rajab, Vinod Sharma
A review on the applications of Neuro-Fuzzy systems in business
Springer Science+ Business Media, Artif. Intell Rev, 4 (49) (2017), pp. 481-510
[Google Scholar](#)
- 28 Amr Ali-Eldin, Jan van den Berg, Hesham A. Ali
A risk evaluation approach for authorization decisions in social pervasive applications
Computers and Electrical Engineering, 55 (2016), pp. 59-72
[Article](#)  [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)
- 29 Yousif I. Alhosani, Constantine J. Katsanis, Sabah Alkass
Predicting Firm Performance and the Role of Top Management Team (TMT): A Fuzzy Inference Approach
IJIMT, 8 (2) (2017)
[Google Scholar](#)
- 30 J.I. Hong, J.A. Landay, (2004), Architecture for Privacy Sensitive Ubiquitous Computing”, MobiSys’04”, Boston, Massachusetts, USA June 6-9, pp. 177-189
[Google Scholar](#)
- 31 Joseph Bradley, Joel Barbier, D. Handler, (2013) “Embracing the Internet of Everything to Capture Your Share of \$14.4 Trillion: More Relevant, Valuable Connections will improve innovation, Productivity, Efficiency & Customer Experience CISCO Whitepaper.” White Paper, Cisco Systems, pp. 1-18
[Google Scholar](#)
- 32 Vinita Malik, Sukhdip Singh, (2019), “Internet of Things: Risk Management” in the conference proceedings of SSIC, 2019
[Google Scholar](#)
- 33 Gib Sorebo, (2015), “Managing the unmanageable: A risk model for the Internet of Things”, <https://www.rsaconference.com/writable/presentations/fileupload/grc-r01/managing-the-unmanageable-a-risk-model-for-the-internet-of-things.pdf>, 2015, 1-20
[Google Scholar](#)
- 34 Ioannis Andreas, (2015), “Internet of Things: Security Vulnerabilities and Challenges”, The 3rd IEEE ISCC International workshop on Smart City and Ubiquitous Computing Applications
[Google Scholar](#)
- 35 R. Roman, P. Najera, J. Lopez
Securing the internet of things
Computer, 9 (44) (2011), pp. 51-58
[Google Scholar](#)


PDF

Help

- 36 M. Langheinrich
Privacy by design principles of privacy-aware ubiquitous systems, in UbiComp
Ubiquitous Computing, Springer (2001), pp. 273-291
(2001) 2001
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)
- 37 P. Mahalle, S. Babar, N.R. Prasad, R. Prasad
Identity management framework towards internet of things (IoT): Roadmap and key challenges
Recent Trends in Network Security and Applications, Springer (2010), pp. 430-439
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)
- 38 A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, (2013), "A Systemic approach for IoT security, " in Distributed Computing in Sensor Systems (DCOSS), IEEE International Conference on. IEEE, pp.: 351–355
[Google Scholar](#)
- 39 J. Chauhan, (2013), "Top 5 big data vulnerability classes",
<https://www.cisoplatform.com/profiles/blogs/top-5-big-data-vulnerability-classes-1>
[Google Scholar](#)
- 40 X. Xiaorong, J. Shizhun, (2018), "The research on industrial big data information security risks", IEEE 3rd International conference on big data Analytics, pp. 19-23
[Google Scholar](#)
- 41 P. Bellini., M.D. Claudio, (2013), "Taxonomy and review of big data solutions navigation", Big data computing
[Google Scholar](#)
- 42 P. Goel, A. Dutta, (2017), "Application of big data analytics in process safety and risk management", IEEE conference on big data, pp. 1143-1152
[Google Scholar](#)
- 43 Y. Demchenko, P. Grosso, (2013), "Addressing Big data issues in scientific data infrastructure in collaboration technologies and systems", International conference on IEEE, pp.: 48-55
[Google Scholar](#)
- 44 Neetu Chaudhari, Satyajee Srivastava, (2016), "Big data security issues and challenges", International conference on computing, communication and automation
[Google Scholar](#)
- 45 Min Chen, Shiwen Mao
Big data: A survey", Mobile Networks and applications, Springer Science + Business Media, 2 (19) (2014), pp. 171-209
[CrossRef](#)

PDF

Help

- 46 D. Agarwal, U.S. Barbara, (2012), "Challenges and opportunities with big data", A community white paper developed by leading researchers across united states
[Google Scholar](#)
- 47 Frankel Konkel
Big data big hurdles: Federal Policy, SAS (2013)
<https://fcw.com/articles/2013/03/11/big-data-policy.aspx>
[Google Scholar](#)
- 48 Pradeep Adluru, Srikari Sindhoori Datla, Zhang Xiaowen, (2015), "Hadoop eco system for big data security and privacy", Systems, Applications and Technology Conference (LISAT), Long Island, Farmingdale, NY, pp.: 1 – 6
[Google Scholar](#)
- 49 B. Saraladevi, N. Pazhaniraja, P. Victor, Paul M.S., Saleem Basha, P. Dhavachelvan
Big Data and Hadoop-A Study in Security Perspective
Procedia Computer Science, 50 (2015), pp. 596-601
[Article](#)  [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)
- 50 A. Kumar, L. Honjas, R.P. Singh, (2012), Information Science and Service Science and Data Mining (ISSDM), pp.: 162 – 166
[Google Scholar](#)
- 51 H. Cheng, C. Rong, K. Hwang, W. Wang, Y. Li
Secure big data storage and sharing scheme for cloud tenants
Communications, China, 6 (12) (2015), pp. 106-115
[View Record in Scopus](#) [Google Scholar](#)
- 52 Samuel Marchal, Jiang Xiuyan, Radu State, Thomas Engel, (2014), "A Big Data Architecture for Large Scale Security Monitoring", Big Data (Big Data Congress), pp: 56– 63
[Google Scholar](#)
- 53 L. Liu, J. Lin, (2013), "Some Special Issues of Network Security Monitoring on Big Environments", Dependable, Autonomic and Secure Computing(DASC), pp.: 10 – 15
[Google Scholar](#)
- 54 S. Madan, (1997), "A benchmark for the artificial intelligence applications on parallel computers" – BEAP, Conference on Communications, Power and computing, WESCANEX 97 Proceedings; Winnipeg, MB; pp.: 82-87
[Google Scholar](#)
- 55 <https://codeload.github.com/Smartuni/SmartFarm/zip/master>, 2018
[Google Scholar](#)
- 56 <https://www.castsoftware.com/products/highlight>, 2018

PDF

Help

[Google Scholar](#)

57 <http://codeload.github.com/opencv/hpbigdata/zip>, 2018

[Google Scholar](#)

Cited by (4)

[Modeling the impact of jamming attacks in the internet of things](#)

2022, Indonesian Journal of Electrical Engineering and Computer Science

[Digitalization Tools: Big Data](#)

2022, Lecture Notes in Networks and Systems

[Simulation and Analysis of Jamming Attack in IoT Networks](#)

2021, Lecture Notes in Networks and Systems

[Analysis Jamming Attack Against the Protocol S-MAC in IoT Networks](#)

2021, Lecture Notes in Networks and Systems

© 2020 The Author(s). Published by Elsevier B.V.



Copyright © 2022 Elsevier B.V. or its licensors or contributors.
ScienceDirect® is a registered trademark of Elsevier B.V.



PDF

Help