Documents

AL-Aamri, A.S.[a] , Abdulghafor, R.[a b] , Turaev, S.[c] , Al-Shaikhli, I.[a] , Zeki, A.[a] , Talib, S.[a]

Machine Learning for APT Detection
(2023) *Sustainability (Switzerland)*, 15 (18), art. no. 13820, .

DOI: 10.3390/su151813820

[a] Department of Computer Science, Faculty of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, 53100, Malaysia
[b] Faculty of Computer Studies (FCS), Arab Open University-Oman, P.O. Box 1596, Muscat, Oman
[c] Department of Computer Science and Software Engineering, College of Information Technology, United Arab Emirates University, Al Ain, 15551, United Arab Emirates

Abstract
Nowadays, countries face a multitude of electronic threats that have permeated almost all business sectors, be it private corporations or public institutions. Among these threats, advanced persistent threats (APTs) stand out as a well-known example. APTs are highly sophisticated and stealthy computer network attacks meticulously designed to gain unauthorized access and persist undetected threats within targeted networks for extended periods. They represent a formidable cybersecurity challenge for governments, corporations, and individuals alike. Recognizing the gravity of APTs as one of the most critical cybersecurity threats, this study aims to reach a deeper understanding of their nature and propose a multi-stage framework for automated APT detection leveraging time series data. Unlike previous models, the proposed approach has the capability to detect real-time attacks based on stored attack scenarios. This study conducts an extensive review of existing research, identifying its strengths, weaknesses, and opportunities for improvement. Furthermore, standardized techniques have been enhanced to enhance their effectiveness in detecting APT attacks. The learning process relies on datasets sourced from various channels, including journal logs, traceability audits, and systems monitoring statistics. Subsequently, an efficient APT detection and prevention system, known as the composition-based decision tree (CDT), has been developed to operate in complex environments. The obtained results demonstrate that the proposed approach consistently outperforms existing algorithms in terms of detection accuracy and effectiveess. © 2023 by the authors.

Author Keywords
APT; artificial intelligence; attacks; CDT

Index Keywords
artificial intelligence, detection method, Internet, security threat, time series

Funding details
12T034, G00003715
Center for Big Data Analytics, University of Texas at AustinCBDA
United Arab Emirates UniversityUAEU12R136, G00003676
Funding details
This research was funded by the United Arab Emirates University, UAEU Strategic Research Grant G00003676 (Fund No.: 12R136) through Big Data Analytics Center.
Funding details
The authors would like to thank United Arab Emirates University for funding this work under UAEU-ZU Joint Research Grant G00003715 (12T034) through Emirates Center for Mobility Research. Also, the authors would like to thank the Arab Open University, Oman.

References

- Czum, J.M.
  Dive into Deep Learning
  (2020) *J. Am. Coll. Radiol*, 17, pp. 637-638.

- Ahmad, W., Rasool, A., Javed, A.R., Baker, T., Jalil, Z.
  Cyber security in IoT-based cloud computing: A comprehensive survey
  (2022) *Electronics*, 11.

- Groenendaal, J., Helsloot, I., Reuter, C.
  Towards More Insight into Cyber Incident Response Decision Making and its Implications for Cyber Crisis Management
  Proceedings of the ISCRAM 2022 Conference Proceedings–19th International Conference

on Information Systems for Crisis Response and Management,
Tarbes, France, 22–25 May 2022

- Bajao, N.A., Sarucam, J.-A.
  Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units
  (2023) *Mesopotamian J. Cybersecur*, 2023, pp. 22-29.

- Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., Al-Shahwani, H.
  The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment
  (2023) *Mesopotamian J. Cybersecur*, 2023, pp. 1-6.

- Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., Disso, J.
  Cyber-attack modeling analysis techniques: An overview
  Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 69-76.
  Vienna, Austria, 22–24 August 2016

- Alshamrani, A., Myneni, S., Chowdhary, A., Huang, D.
  A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities
  (2019) *IEEE Commun. Surv. Tutor*, 21, pp. 1851-1877.

- Al-Matarneh, E.M.
  Advanced Persistent Threats and Its Role in Network Security Vulnerabilities
  (2020) *Int. J. Adv. Res. Comput. Sci*, 11, pp. 11-20.

- Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., Pavlova, G.
  Cyber Security: Threats and Challenges
  Proceedings of the 2020 International Conference Automatics and Informatics (ICAI),
  Varna, Bulgaria, 1–3 October 2020, Available online

- Sharma, A., Gupta, B.B., Singh, A.K., Saraswat, V.
  Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense
  (2022) *Comput. Secur*, 115, p. 102627.

- Hakonen, P.
  (2022) *Detecting Insider Threats Using User and Entity Behavior Analytics*,
  Available online

- Ashrafuzzaman, M., Chakhchoukh, Y., Jillepalli, A.A., Tosic, P.T., de Leon, D.C., Sheldon, F.T., Johnson, B.K.
  Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning
  Proceedings of the 2018 14th International Wireless Communications and Mobile Computing Conference (IWCMC 2018), pp. 219-225.
  Limassol, Cyprus, 25–29 June 2018

- Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J., Choudrie, J.
  Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce
  (2021) *Comput. Hum. Behav*, 114, p. 106531.

- Chamola, V., Kotesh, P., Agarwal, A., Naren, Gupta, N., Guizani, M.
  A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques
  (2021) *Ad Hoc Netw*, 111, p. 102324.

- Scherr, C.L., Aufox, S., Ross, A.A., Ramesh, S., Wicklund, C.A., Smith, M.
  What people want to know about their genes: A critical review of the literature on

large-scale genome sequencing studies
(2018) *Healthcare*, 6.

- Rohe, K., Chatterjee, S., Yu, B.
Spectral clustering and the high-dimensional stochastic blockmodel
(2011) *Ann. Statist*, 39, pp. 1878-1915.

- Brogi, G.
Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models to Cite This Version: HAL Id: Tel-01793752 Real-Time Detection of Advanced Per- Sistent Threats Using Information Flow Tracking and Hidden Markov 2018,
Available online

- Zhao, M.J., Driscoll, A.R., Sengupta, S., Fricker, R.D., Spitzner, D.J., Woodall, W.H.
Performance evaluation of social network anomaly detection using a moving window-based scan method
(2018) *Qual. Reliab. Eng. Int*, 34, pp. 1699-1716.

- Gu, J., Kong, R., Sun, H., Zhuang, H., Pan, F., Lin, Z.
A novel detection technique based on benign samples and one-class algorithm for malicious PDF documents containing JavaScript
Proceedings of the International Conference on Computer Application and Information Security (ICCAIS 2021), p. 62.
Riyadh, Saudi Arabia, 18–20 March 2021

- Horng, S.-J., Su, M.-Y., Chen, Y.-H., Kao, T.-W., Chen, R.-J., Lai, J.-L., Perkasa, C.D.
A novel intrusion detection system based on hierarchical clustering and support vector machines
(2011) *Expert Syst. Appl*, 38, pp. 306-313.

- Salama, M.A., Eid, H.F., Ramadan, R.A., Darwish, A., Hassanien, A.E.
Hybrid Intelligent Intrusion Detection Scheme
(2011) *Soft Computing in Industrial Applications*, pp. 293-303.
Springer, Berlin/Heidelberg, Germany

- Hasan, A.M., Nasser, M., Ahmad, S., Molla, K.I.
Feature Selection for Intrusion Detection Using Random Forest
(2016) *J. Inf. Secur*, 7, pp. 129-140.

- Gupta, M., Shrivastava, S.K.
Intrusion Detection System based on SVM and Bee Colony
(2015) *Int. J. Comput. Appl*, 111, pp. 27-32.

- Al-Yaseen, W.L., Othman, Z.A., Nazri, M.Z.A.
Real-time multi-agent system for an adaptive intrusion detection system
(2017) *Pattern Recognit. Lett*, 85, pp. 56-64.

- Kaveh, A., Dadras, A.
Structural damage identification using an enhanced thermal exchange optimization algorithm
(2018) *Eng. Optim*, 50, pp. 430-451.

- Joshi, J., Rinal, D., Patel, J.
Diagnosis and Prognosis Breast Cancer Using
(2014) *Int. J. Eng. Res. Gen. Sci*, 2, pp. 315-323.
Available online

- Yilmaz, A.A.
Intrusion Detection in Computer Networks using Optimized Machine Learning Algorithms

Proceedings of the 2022 3rd International Informatics and Software Engineering Conference (IISEC),
Ankara, Turkey, 15–16 December 2022

- Rakha, T., Gorodetsky, A.
Review of Unmanned Aerial System (UAS) applications in the built environment: Towards automated building inspection procedures using drones
(2018) *Autom. Constr*, 93, pp. 252-264.

- Aziz, A.S.A., Hassanien, A.E., Hanaf, S.E.-O., Tolba, M.
Multi-layer hybrid machine learning techniques for anomalies detection and classification approach
Proceedings of the 2013 13th International Conference on Hybrid Intelligent Systems (HIS 2013), pp. 215-220.
Gammarth, Tunisia, 4–6 December 2013

- Ingre, B., Yadav, A.
Performance analysis of NSL-KDD dataset using ANN
Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 92-96.
Guntur, India, 2–3 January 2015

- Jajoo, A.
A Study on the Morris Worm
(2021) *arXiv*,
2112.07647, Available online

- Marchetti, M., Pierazzi, F., Guido, A., Colajanni, M.
Countering Advanced Persistent Threats through security intelligence and big data analytics
Proceedings of the International Conference on Cyber Conflict, CYCON, 2016, pp. 243-261.
Washington, DC, USA, 21–23 October 2016

- Of, I.J.
Research in Computer Applications and Robotics
(2014) *Crit. Rev. Cryptogr*, 2, pp. 113-118.

- Trifonov, R., Manolov, S., Yoshinov, R., Tsochev, G., Pavlova, G.
Artificial Intelligence Methods for Cyber Threats Intelligence
(2017) *Int. J. Comput*, 2, pp. 129-135.
Available online

- Li, X., Jiang, H.
Artificial intelligence technology & engineering applications
(2017) *Appl. Comput. Electromagn. Soc. J*, 32, pp. 381-388.

- Poola, I.
The Best of the Machine Learning Algorithms Used in Artificial Intelligence
(2017) *Int. J. Adv. Res. Comput. Commun. Eng*, 6, pp. 187-194.

- Adams, C., Tambay, A.A., Bissessar, D., Brien, R., Fan, J., Hezaveh, M., Zahed, J.
Using Machine Learning to Detect APTs on a User Workstation
(2019) *Int. J. Sens. Netw. Data Commun*, 8, p. 3.

- Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., Aparicio-Navarro, F.J.
Detection of advanced persistent threat using machine-learning correlation analysis
(2018) *Future Gener. Comput. Syst*, 89, pp. 349-359.

- Abdullah, T.A., Ali, W., Abdulghafor, R.
  Empirical study on intelligent android malware detection based on supervised machine learning
  (2020) *Int. J. Adv. Comput. Sci. Appl*, 11, p. 215.

- Berrada, G., Cheney, J., Benabderrahmane, S., Maxwell, W., Mookherjee, H., Theriault, A., Wright, R.
  A baseline for unsupervised advanced persistent threat detection in system-level provenance
  (2020) *Future Gener. Comput. Syst*, 108, pp. 401-413.

Correspondence Address
Abdulghafor R.; Department of Computer Science, Malaysia; email: rawad.a@aou.edu.om
Turaev S.; Department of Computer Science and Software Engineering, United Arab Emirates; email: sherzod@uaeu.ac.ae

Publisher: Multidisciplinary Digital Publishing Institute (MDPI)

ISSN: 20711050
Language of Original Document: English
Abbreviated Source Title: Sustainability
2-s2.0-85172933527
Document Type: Article
Publication Stage: Final
Source: Scopus