Scopus

Documents

Hilal, A.M.[a b] , Hashim, A.H.A.[a] , Mohamed, H.G.[c] , Nour, M.K.[d] , Asiri, M.M.[e] , Al-Sharafi, A.M.[f] , Othman, M.[g] , Motwakel, A.[b]

Malicious URL Classification Using Artificial Fish Swarm Optimization and Deep Learning

(2023) *Computers, Materials and Continua*, 74 (1), pp. 607-621.

DOI: 10.32604/cmc.2023.031371

[a] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, 53100, Malaysia

[b] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia

[c] Department of Electrical Engineering, College of Engineering, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia

[d] Department of Computer Sciences, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia

[e] Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia

[f] Department of Computer Science, College of Computers and Information Technology, University of Bisha, Saudi Arabia

[g] Department of Computer Science, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo, 11835, Egypt

Abstract

Cybersecurity-related solutions have become familiar since it ensures security and privacy against cyberattacks in this digital era. Malicious Uniform Resource Locators (URLs) can be embedded in email or Twitter and used to lure vulnerable internet users to implement malicious data in their systems. This may result in compromised security of the systems, scams, and other such cyberattacks. These attacks hijack huge quantities of the available data, incurring heavy financial loss. At the same time, Machine Learning (ML) and Deep Learning (DL) models paved the way for designing models that can detect malicious URLs accurately and classify them. With this motivation, the current article develops an Artificial Fish Swarm Algorithm (AFSA) with Deep Learning Enabled Malicious URL Detection and Classification (AFSADL-MURLC) model. The presented AFSADL-MURLC model intends to differentiate the malicious URLs from genuine URLs. To attain this, AFSADL-MURLC model initially carries out data preprocessing and makes use of glove-based word embedding technique. In addition, the created vector model is then passed onto Gated Recurrent Unit (GRU) classification to recognize the malicious URLs. Finally, AFSA is applied to the proposed model to enhance the efficiency of GRU model. The proposed AFSADL-MURLC technique was experimentally validated using benchmark dataset sourced from Kaggle repository. The simulation results confirmed the supremacy of the proposed AFSADL-MURLC model over recent approaches under distinct measures.

Author Keywords

cybersecurity; deep learning; gated recurrent unit; machine learning; Malicious URL; metaheuristics

Index Keywords

Deep learning, Embedded systems, Learning systems, Losses, Swarm intelligence; Artificial fishswarm algorithm(AFSA), Classification models, Cyber security, Cyber-attacks, Deep learning, Detection models, Gated recurrent unit, Machine-learning, Malicious uniform resource locator, Metaheuristic; Cybersecurity

References

- Johnson, C., Khadka, B., Basnet, R. B., Doleck, T.
  Towards detecting and classifying malicious URLs using deep learning
  (2020) *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 11 (4), pp. 31-48.
- Vinayakumar, R., Soman, K. P., Poornachandran, P.
  Evaluating deep learning approaches to characterize and classify malicious URL's
  (2018) *Journal of Intelligent & Fuzzy Systems*, 34 (3), pp. 1333-1343.
- Liang, Y., Wang, Q., Xiong, K., Zheng, X., Yu, Z.
  Robust detection of malicious Robust detection of malicious URLs with self-paced wide & deep learning
  (2021) *IEEE Transactions on Dependable and Secure Computing*, pp. 1-1.

- Wang, Y., Cai, W., Wei, P.
  A deep learning approach for detecting malicious JavaScript code: Using a deep learning approach to detect JavaScript-based attacks
  (2016) *Security and Communication Networks*, 9 (11), pp. 1520-1534.

- Birthriya, S. K., Jain, A. K.
  Analysis for malicious URLs using machine learning and deep learning approaches
  (2021) *Proc. of the Int. Conf. on Paradigms of Computing, Communication and Data Sciences*, pp. 797-807.

- Albraikan, A. A., Haj Hassine, S. B., Fati, S. M., Al-Wesabi, F. N., Hilal, A. M.
  Optimal deep learning-based cyberattack detection and classification technique on social networks
  (2022) *Computers, Materials & Continua*, 72 (1), pp. 907-923.

- Yuan, J., Liu, Y., Yu, L.
  A novel approach for malicious URL detection based on the joint model
  (2021) *Security and Communication Networks*, 2021, pp. 1-12.

- Qarafi, A. A., Alrowais, F., Alotaibi, S., Nemri, N., Al-Wesabi, F. N.
  Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment
  (2022) *Applied Sciences*, 12 (12), pp. 1-17.

- Liu, Y., Zhu, C., Wu, Y., Xu, H., Song, J.
  MMWD: An efficient mobile malicious webpage detection framework based on deep learning and edge cloud
  (2021) *Concurrency and Computation: Practice and Experience*, 33 (18), p. e6191.

- Alrowais, F., Almasoud, A. S., Marzouk, R., Al-Wesabi, F. N., Hilal, A. M.
  Artificial intelligence based data offloading technique for secure mec systems
  (2022) *Computers, Materials & Continua*, 72 (2), pp. 2783-2795.

- Bu, S. J., Kim, H. J.
  Optimized URL feature selection based on genetic-algorithm-embedded deep learning for phishing website detection
  (2022) *Electronics*, 11 (7), p. 1090.

- Hamza, M. A., Hassine, S. B. H., Abunadi, I., Al-Wesabi, F. N., Alsolai, H.
  Feature selection with optimal stacked sparse autoencoder for data mining
  (2022) *Computers, Materials & Continua*, 72 (2), pp. 2581-2596.

- Qiu, J., Zhang, J., Luo, W., Pan, L., Nepal, S.
  A survey of android malware detection with deep neural models
  (2021) *ACM Computing Surveys*, 53 (6), pp. 1-36.

- Aljofey, A., Jiang, Q., Qu, Q., Huang, M., Niyigena, J. P.
  An effective phishing detection model based on character level convolutional neural network from URL
  (2020) *Electronics*, 9 (9), p. 1514.

- Peng, Y., Tian, S., Yu, L., Lv, Y., Wang, R.
  Malicious URL recognition and detection using attention-based CNN-LSTM
  (2019) *KSII Transactions on Internet and Information Systems (TIIS)*, 13 (11), pp. 5580-5593.

- Arslan, R. S.
  AndroAnalyzer: Android malicious software detection based on deep learning
  (2021) *PeerJ Computer Science*, 7, p. e533.

- Afzal, S., Asim, M., Javed, A. R., Beg, M. O., Baker, T.
URLdeepDetect: A deep learning approach for detecting malicious URLs using semantic vector models
(2021) *Journal of Network and Systems Management*, 29 (3), p. 21.

- Srinivasan, S., Vinayakumar, R., Arunachalam, A., Alazab, M., Soman, K. P.
DURLD: Malicious URL detection using deep learning-based character level representations
(2021) *Malware Analysis Using Artificial Intelligence and Deep Learning*, pp. 535-554. Springer, Cham

- Mondal, D. K., Singh, B. C., Hu, H., Biswas, S., Alom, Z.
SeizeMaliciousURL: A novel learning approach to detect malicious URLs
(2021) *Journal of Information Security and Applications*, 62, p. 102967.

- Mohammed, S. M., Jacksi, K., Zeebaree, S. R. M.
Glove word embedding and DBSCAN algorithms for semantic document clustering
(2020) *2020 Int. Conf. on Advanced Science and Engineering (ICOASE)*, pp. 1-6. Duhok, Iraq

- Wang, Y., Liao, W., Chang, Y.
Gated recurrent unit network-based short-term photovoltaic forecasting
(2018) *Energies*, 11 (8), p. 2163.

- Pustokhin, D. A., Pustokhina, I. V., Rani, P., Kansal, V., Elhoseny, M.
Optimal deep learning approaches and healthcare big data analytics for mobile networks toward 5G
(2021) *Computers & Electrical Engineering*, 95, pp. 1-14.

- Nguyen, G. N., Viet, N. H. L., Elhoseny, M., Shankar, K., Gupta, B. B.
Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with ResNet model
(2021) *Journal of Parallel and Distributed Computing*, 153, pp. 150-160.

- Devaraj, A. F. S., Murugaboopathi, G., Elhoseny, M., Shankar, K., Min, K.
An efficient framework for secure image archival and retrieval system using multiple secret share creation scheme
(2020) *IEEE Access*, 8, pp. 144310-144320.

- Neshat, M., Sepidnam, G., Sargolzaei, M., Toosi, A. N.
Artificial fish swarm algorithm: A survey of the state-of-the-art, hybridization, combinatorial and indicative applications
(2014) *Artificial Intelligence Review*, 42 (4), pp. 965-997.

Correspondence Address
Hilal A.M.; Department of Electrical and Computer Engineering, Malaysia; email: A.hilal@psau.edu.sa

Publisher: Tech Science Press

ISSN: 15462218
Language of Original Document: English
Abbreviated Source Title: Comput. Mater. Continua
2-s2.0-85139031003
Document Type: Article
Publication Stage: Final
Source: Scopus