Documents

Export Date: 03 Aug 2020

1) Kwon, S., Yoo, H., Shon, T.
IEEE 1815.1-Based power system security with bidirectional RNN-Based network anomalous attack detection for cyber-physical system
(2020) IEEE Access, 8, art. no. 9076709, pp. 77572-77586. Cited 1 time.

1) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084795501&doi=10.1109%2fACCESS.2020.2989770&partnerID=40&r
DOI: 10.1109/ACCESS.2020.2989770

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

2) Meng, C., Jiang, X.S., Wei, X.M., Wei, T.
A Time Convolutional Network Based Outlier Detection for Multidimensional Time Series in Cyber-Physical-Social Systems
(2020) IEEE Access, 8, art. no. 9072131, pp. 74933-74942.

2) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084317667&doi=10.1109%2fACCESS.2020.2988797&partnerID=40&r
DOI: 10.1109/ACCESS.2020.2988797

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

3) Albahar, M.A., Al-Falluji, R.A., Binsawad, M.
An Empirical Comparison on Malicious Activity Detection Using Different Neural Network-Based Models
(2020) IEEE Access, 8, art. no. 9050472, pp. 61549-61564.

3) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083436052&doi=10.1109%2fACCESS.2020.2984157&partnerID=40&r
DOI: 10.1109/ACCESS.2020.2984157

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

4) Zandigohar, M., Han, M., Erdoğmuş, D., Schirner, G.

Towards Creating a Deployable Grasp Type Probability Estimator for a Prosthetic Hand

(2020) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11971 LNCS, pp. 44-58.

4) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081180314&doi=10.1007%2f978-3-030-41131-2_3&partnerID=40&md

DOI: 10.1007/978-3-030-41131-2_3

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

5) Neha, N., Priyanga, S., Seshan, S., Senthilnathan, R., Shankar Sriram, V.S.

SCO-RNN: A behavioral-based intrusion detection approach for cyber physical attacks in SCADA systems

(2020) Lecture Notes in Networks and Systems, 89, pp. 911-919.

5) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079277046&doi=10.1007%2f978-981-15-0146-3_88&partnerID=40&m

DOI: 10.1007/978-981-15-0146-3_88

Document Type: Book Chapter
Publication Stage: Final
Source: Scopus

6) Jahromi, A.N., Karimpour, H., Sakhnini, J., Dehghantanha, A.

A deep unsupervised representation learning approach for effective cyber-physical attack detection and identification on highly imbalanced data

(2020) CASCON 2019 Proceedings - Conference of the Centre for Advanced Studies on Collaborative Research - Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering, pp. 14-23. Cited 2 times.

6) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078971801&partnerID=40&md5=fc8771036bf921508f78a6363927df36

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

7) Min, K.W., Choi, Y.H., Al-Shamiri, A.K., Kim, J.H.

Application of Artificial Neural Network for Cyber-Attack Detection in Water Distribution Systems as Cyber Physical Systems

(2020) Advances in Intelligent Systems and Computing, 1063, pp. 82-88.

7) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076109537&doi=10.1007%2f978-3-030-31967-0_10&partnerID=40&m

DOI: 10.1007/978-3-030-31967-0_10

Document Type: Conference Paper

Publication Stage: Final
Source: Scopus

8) Veith, E.M.S.P., Fischer, L., Tröschel, M., Nieße, A.
Analyzing Cyber-Physical Systems from the Perspective of Artificial Intelligence
(2019) ACM International Conference Proceeding Series, pp. 85-95.

8) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85086182601&doi=10.1145%2f3388218.3388222&partnerID=40&md5=e
DOI: 10.1145/3388218.3388222

Document Type: Conference Paper
Publication Stage: Final
Access Type: Open Access
Source: Scopus

9) Jotikabukkana, P., Sornlertlamvanich, V.
The Holistic Framework of Using Machine Learning for an Effective Incoming Cyber Threats Detection
(2019) Frontiers in Artificial Intelligence and Applications, 321, pp. 363-380.

9) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082527000&doi=10.3233%2fFAIA200025&partnerID=40&md5=0b506
DOI: 10.3233/FAIA200025

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

10) Abeyrathna, D., Huang, P.-C., Zhong, X.
Anomaly proposal-based fire detection for cyber-physical systems
(2019) Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019, art. no. 9071185, pp. 1203-1207. Cited 1 time.

10) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084730964&doi=10.1109%2fCSCI49370.2019.00226&partnerID=40&r
DOI: 10.1109/CSCI49370.2019.00226

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

11) Ranjan, A., Misra, P., Vasan, A., Krishnakumar, S., Sivasubramaniam, A.
City scale monitoring of on-street parking violations with streethawk
(2019) BuildSys 2019 - Proceedings of the 6th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, pp. 31-40.

11)

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077292936&doi=10.1145%2f3360322.3360841&partnerID=40&md5=6

DOI: 10.1145/3360322.3360841

Document Type: Conference Paper
Publication Stage: Final
Access Type: Open Access
Source: Scopus

12) Li, X., Li, W., Yang, Q., Yan, W., Zomaya, A.Y.
Building an online defect detection system for large-scale photovoltaic plants
(2019) BuildSys 2019 - Proceedings of the 6th ACM International Conference on Systems for

Energy-Efficient Buildings, Cities, and Transportation, pp. 253-262.

12) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077286140&doi=10.1145%2f3360322.3360835&partnerID=40&md5=7

DOI: 10.1145/3360322.3360835

Document Type: Conference Paper
Publication Stage: Final
Access Type: Open Access
Source: Scopus

13) Bernieri, G., Conti, M., Turrin, F.
KingFisher: An industrial security framework based on variational autoencoders
(2019) SenSys-ML 2019 - Proceedings of the 1st Workshop on Machine Learning on Edge in Sensor

Systems, Part of SenSys 2019, pp. 7-12.

13) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076608684&doi=10.1145%2f3362743.3362961&partnerID=40&md5=1

DOI: 10.1145/3362743.3362961

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

14) Yoginath, S., Tansakul, V., Chinthavali, S., Taylor, C., Hambrick, J., Irminger, P., Perumalla, K.
On the effectiveness of recurrent neural networks for live modeling of cyber-physical systems
(2019) Proceedings - IEEE International Conference on Industrial Internet Cloud, ICII 2019, art. no.

9065023, pp. 309-317.

14) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085943263&doi=10.1109%2fICII.2019.00062&partnerID=40&md5=5d1

DOI: 10.1109/ICII.2019.00062

Document Type: Conference Paper
Publication Stage: Final

Source: Scopus

15) Perumalla, K., Yoginath, S., Lopez, J.
Detecting Sensors and Inferring their Relations at Level-0 in Industrial Cyber-Physical Systems
(2019) 2019 IEEE International Symposium on Technologies for Homeland Security, HST 2019, art.

no. 9032891, .

15) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082672057&doi=10.1109%2fHST47167.2019.9032891&partnerID=40&
DOI: 10.1109/HST47167.2019.9032891

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

16) Pan, J.
Physical integrity attack detection of surveillance camera with deep learning based video frame interpolation
(2019) Proceedings - 2019 IEEE International Conference on Internet of Things and Intelligence

System, IoTaIS 2019, art. no. 8980385, pp. 79-85.

16) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081103114&doi=10.1109%2fIoTaIS47347.2019.8980385&partnerID=4
DOI: 10.1109/IoTaIS47347.2019.8980385

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

17) Lakshminarayana, S., Karachiwala, J.S., Teng, T.Z., Tan, R., Yau, D.K.Y.
Performance and Resilience of Cyber-Physical Control Systems with Reactive Attack Mitigation
(2019) IEEE Transactions on Smart Grid, 10 (6), art. no. 8681420, pp. 6640-6654. Cited 1 time.

17) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077561588&doi=10.1109%2fTSG.2019.2909357&partnerID=40&md5=
DOI: 10.1109/TSG.2019.2909357

Document Type: Article
Publication Stage: Final
Source: Scopus

18) Huang, X., Dong, J.
Reliable control of cyber-physical systems under sensor and actuator attacks: An identifier-critic based integral sliding-mode control approach
(2019) Neurocomputing, 361, pp. 229-242.

18)

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069663370&doi=10.1016%2fj.neucom.2019.06.069&partnerID=40&mo
DOI: 10.1016/j.neucom.2019.06.069

Document Type: Article
Publication Stage: Final
Source: Scopus

19) Lou, X., Tran, C., Yau, D.K.Y., Tan, R., Ng, H., Fu, T.Z., Winslett, M.
Learning-based time delay attack characterization for cyber-physical systems
(2019) 2019 IEEE International Conference on Communications, Control, and Computing

Technologies for Smart Grids, SmartGridComm 2019, art. no. 8909732, .

19) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076391973&doi=10.1109%2fSmartGridComm.2019.8909732&partnerI
DOI: 10.1109/SmartGridComm.2019.8909732

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

20) Vamvoudakis, K.G., Kanellopoulos, A.
Non-Equilibrium Learning and Cyber-Physical Security
(2019) 2019 57th Annual Allerton Conference on Communication, Control, and Computing, Allerton

2019, art. no. 8919756, pp. 1-6.

20) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077790153&doi=10.1109%2fALLERTON.2019.8919756&partnerID=40
DOI: 10.1109/ALLERTON.2019.8919756

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

21) Ding, K., Ding, S., Morozov, A., Fabarisov, T., Janschek, K.
On-line error detection and mitigation for time-series data of cyber-physical systems using deep learning based methods
(2019) Proceedings - 2019 15th European Dependable Computing Conference, EDCC 2019, art. no.

8893390, pp. 7-14.

21) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075631608&doi=10.1109%2fEDCC.2019.00015&partnerID=40&md5=
DOI: 10.1109/EDCC.2019.00015

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

22) Stockman, M., Dwivedi, D., Gentz, R., Peisert, S.
Detecting control system misbehavior by fingerprinting programmable logic controller functionality
(2019) International Journal of Critical Infrastructure Protection, 26, art. no. 100306, . Cited 1 time.

22) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070316658&doi=10.1016%2fj.ijcip.2019.100306&partnerID=40&md5=
DOI: 10.1016/j.ijcip.2019.100306

Document Type: Article
Publication Stage: Final
Source: Scopus

23) Nardelli, P., Papadias, C., Kalalas, C., Alves, H., Christou, I.T., MacAluso, I., Marchetti, N., Palacios, R., Alonso-Zarate, J.
Framework for the identification of rare events via machine learning and IoT networks
(2019) Proceedings of the International Symposium on Wireless Communication Systems,

2019-August, art. no. 8877287, pp. 656-660.

23) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074627903&doi=10.1109%2fISWCS.2019.8877287&partnerID=40&m
DOI: 10.1109/ISWCS.2019.8877287

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

24) Calimbahin, C.M., Pancho-Festin, S., Pedrasa, J.R.
Mitigating Data Integrity Attacks in Building Automation Systems using Denoising Autoencoders
(2019) International Conference on Ubiquitous and Future Networks, ICUFN, 2019-July, art. no.

8806072, pp. 390-395.

24) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071858343&doi=10.1109%2fICUFN.2019.8806072&partnerID=40&md
DOI: 10.1109/ICUFN.2019.8806072

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

25) Chen, Y., Zhang, Y., Maharjan, S., Alam, M., Wu, T.
Deep Learning for Secure Mobile Edge Computing in Cyber-Physical Transportation Systems
(2019) IEEE Network, 33 (4), art. no. 8782874, pp. 36-41. Cited 11 times.

25) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070216649&doi=10.1109%2fMNET.2019.1800458&partnerID=40&md
DOI: 10.1109/MNET.2019.1800458

Document Type: Article

Publication Stage: Final
Source: Scopus

26) De Dinechin, B.D.
INVITED consolidating high-integrity, high-performance, and cyber-security functions on a manycore processor
(2019) Proceedings - Design Automation Conference, art. no. a154, .

26) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067789283&doi=10.1145%2f3316781.3323473&partnerID=40&md5=0
DOI: 10.1145/3316781.3323473

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

27) Giorgi, R., Oro, D., Ermini, S., Montefoschi, F., Rizzo, A.
Embedded Face Analysis for Smart Videosurveillance
(2019) 2019 8th Mediterranean Conference on Embedded Computing, MECO 2019 - Proceedings,

art. no. 8760200, .

27) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073885705&doi=10.1109%2fMECO.2019.8760200&partnerID=40&md
DOI: 10.1109/MECO.2019.8760200

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

28) Liu, X., Konstantinou, C.
Reinforcement learning for cyber-physical security assessment of power systems
(2019) 2019 IEEE Milan PowerTech, PowerTech 2019, art. no. 8810568, . Cited 2 times.

28) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072349092&doi=10.1109%2fPTC.2019.8810568&partnerID=40&md5=
DOI: 10.1109/PTC.2019.8810568

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

29) Li, F., Shi, Y., Shinde, A., Ye, J., Song, W.
Enhanced cyber-physical security in internet of things through energy auditing
(2019) IEEE Internet of Things Journal, 6 (3), art. no. 8642398, pp. 5224-5231. Cited 7 times.

29) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067843663&doi=10.1109%2fJIOT.2019.2899492&partnerID=40&md5=
DOI: 10.1109/JIOT.2019.2899492

Document Type: Article
Publication Stage: Final
Source: Scopus

30) Liu, T., Wen, W.
Poster: Deep-evasion: Turn deep neural network into evasive self-contained cyber-physical malware
(2019) WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and

Mobile Networks, pp. 320-321.

30) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85066736622&doi=10.1145%2f3317549.3326311&partnerID=40&md5=9
DOI: 10.1145/3317549.3326311

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

31) Khanapuri, E., Chintalapati, T., Sharma, R., Gerdes, R.
Learning-Based Adversarial Agent Detection and Identification in Cyber Physical Systems Applied to Autonomous Vehicular Platoon
(2019) Proceedings - 2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart

Cyber-Physical Systems, SEsCPS 2019, art. no. 8823728, pp. 39-45.

31) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072832399&doi=10.1109%2fSEsCPS.2019.00014&partnerID=40&md5
DOI: 10.1109/SEsCPS.2019.00014

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

32) Rao, S., Spanias, A., Tepedelenlioglu, C.
Solar array fault detection using neural networks
(2019) Proceedings - 2019 IEEE International Conference on Industrial Cyber Physical Systems,

ICPS 2019, art. no. 8780208, pp. 196-200. Cited 6 times.

32) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070921595&doi=10.1109%2fICPHYS.2019.8780208&partnerID=40&m
DOI: 10.1109/ICPHYS.2019.8780208

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

33) Dogaru, D.I., Dumitrache, I.

Cyber security of smart grids in the context of big data and machine learning

(2019) Proceedings - 2019 22nd International Conference on Control Systems and Computer

Science, CSCS 2019, art. no. 8745044, pp. 61-67. Cited 1 time.

33) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069147477&doi=10.1109%2fCSCS.2019.00018&partnerID=40&md5=

DOI: 10.1109/CSCS.2019.00018

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

34) Eiteneuer, B., Hranisavljevic, N., Niggemann, O.

Dimensionality reduction and anomaly detection for cpps data using autoencoder

(2019) Proceedings of the IEEE International Conference on Industrial Technology, 2019-February,

art. no. 8755116, pp. 1286-1292.

34) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069037854&doi=10.1109%2fICIT.2019.8755116&partnerID=40&md5=

DOI: 10.1109/ICIT.2019.8755116

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

35) Liang, F., Hatcher, W.G., Liao, W., Gao, W., Yu, W.

Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly

(2019) IEEE Access, 7, art. no. 8879591, pp. 158126-158147. Cited 3 times.

35) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078057564&doi=10.1109%2fACCESS.2019.2948912&partnerID=40&

DOI: 10.1109/ACCESS.2019.2948912

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

36) Gauthama Raman, M.R., Somu, N., Mathur, A.P.

Anomaly Detection in Critical Infrastructure Using Probabilistic Neural Network

(2019) Communications in Computer and Information Science, 1116 CCIS, pp. 129-141.

36) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076720437&doi=10.1007%2f978-981-15-0871-4_10&partnerID=40&m

DOI: 10.1007/978-981-15-0871-4_10

Document Type: Conference Paper
Publication Stage: Final

Source: Scopus

37) Scrugli, M.A., Loi, D., Raffo, L., Meloni, P.
Runtime-adaptive cognitive IoT nodes
(2019) CEUR Workshop Proceedings, 2457, .

37) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073259923&partnerID=40&md5=0e03d75fa00f6a5537b55413202f2cf1
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

38) Macas, M., Chunming, W.
Enhanced cyber-physical security through deep learning techniques
(2019) CEUR Workshop Proceedings, 2457, .

38) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073219382&partnerID=40&md5=cf005868853bf25be12510e51a4c5ee
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

39) Li, D., Chen, D., Jin, B., Shi, L., Goh, J., Ng, S.-K.
MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks
(2019) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11730 LNCS, pp. 703-716. Cited 9 times.

39) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072871136&doi=10.1007%2f978-3-030-30490-4_56&partnerID=40&m
DOI: 10.1007/978-3-030-30490-4_56

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

40) Raghav, R.S., Dhavachelvan, P.
Bigdata fog based cyber physical system for classifying, identifying and prevention of SARS disease
(2019) Journal of Intelligent and Fuzzy Systems, 36 (5), pp. 4361-4373. Cited 1 time.

40) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065841146&doi=10.3233%2fJIFS-169992&partnerID=40&md5=34b48
DOI: 10.3233/JIFS-169992

Document Type: Article
Publication Stage: Final
Source: Scopus

41) Ma, T., Ali, S., Yue, T., Elaasar, M.
Testing self-healing cyber-physical systems under uncertainty: a fragility-oriented approach
(2019) Software Quality Journal, . Cited 1 time.

41) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85063237133&doi=10.1007%2fs11219-018-9437-3&partnerID=40&md5=
DOI: 10.1007/s11219-018-9437-3

Document Type: Article
Publication Stage: Article in Press
Source: Scopus

42) Ferragut, E.M., Laska, J., Olama, M.M., Ozmen, O.
Real-Time Cyber-Physical False Data Attack Detection in Smart Grids Using Neural Networks
(2018) Proceedings - 2017 International Conference on Computational Science and Computational

Intelligence, CSCI 2017, art. no. 8560712, pp. 1-6. Cited 3 times.

42) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060660364&doi=10.1109%2fCSCI.2017.1&partnerID=40&md5=a8bcd
DOI: 10.1109/CSCI.2017.1

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

43) Wadhawan, Y., Neuman, C.
RL-BAGS: A tool for smart grid risk assessment
(2018) 2018 International Conference on Smart Grid and Clean Energy Technologies, ICSGCE 2018,

art. no. 8556775, pp. 7-14. Cited 3 times.

43) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056246620&doi=10.1109%2fICSGCE.2018.8556775&partnerID=40&m
DOI: 10.1109/ICSGCE.2018.8556775

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

44) Fink, G.A., McKenzie, P.
Helping IT and OT Defenders Collaborate
(2018) Proceedings - 2018 IEEE International Conference on Industrial Internet, ICII 2018, art. no.

8539125, pp. 188-194.

44) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059852737&doi=10.1109%2fICII.2018.00036&partnerID=40&md5=90
DOI: 10.1109/ICII.2018.00036

Document Type: Conference Paper

Publication Stage: Final
Source: Scopus

45) Yavuz, F.Y., Ünal, D., Gül, E.
Deep learning for detection of routing attacks in the internet of things
(2018) International Journal of Computational Intelligence Systems, 12 (1), pp. 39-58. Cited 12 times.

45) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062708145&doi=10.2991%2fijcis.2018.25905181&partnerID=40&md5=
DOI: 10.2991/ijcis.2018.25905181

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

46) Schneider, P., Böttinger, K.
High-performance unsupervised anomaly detection for cyber-physical system networks
(2018) Proceedings of the ACM Conference on Computer and Communications Security, pp. 1-12.

Cited 12 times.

46) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056721492&doi=10.1145%2f3264888.3264890&partnerID=40&md5=2
DOI: 10.1145/3264888.3264890

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

47) Shafique, M., Khalid, F., Rehman, S.
Intelligent security measures for smart cyber physical systems
(2018) Proceedings - 21st Euromicro Conference on Digital System Design, DSD 2018, art. no.

8491829, pp. 280-287. Cited 6 times.

47) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056484526&doi=10.1109%2fDSD.2018.00058&partnerID=40&md5=c5
DOI: 10.1109/DSD.2018.00058

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

48) Sundararajan, A., Khan, T., Aburub, H., Sarwat, A.I., Rahman, S.
A Tri-Modular Human-on-the-Loop Framework for Intelligent Smart Grid Cyber-Attack Visualization
(2018) Conference Proceedings - IEEE SOUTHEASTCON, 2018-April, art. no. 8479180, . Cited 7

times.

48) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055847350&doi=10.1109%2fSECON.2018.8479180&partnerID=40&m
DOI: 10.1109/SECON.2018.8479180

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

49) Bezzo, N.
Predicting Malicious Intention in CPS under Cyber-Attack
(2018) Proceedings - 9th ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS

2018, art. no. 8443756, pp. 351-352. Cited 1 time.

49) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85053515139&doi=10.1109%2fICCPS.2018.00049&partnerID=40&md5=
DOI: 10.1109/ICCPS.2018.00049

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

50) Kriebel, F., Rehman, S., Hanif, M.A., Khalid, F., Shafique, M.
Robustness for smart cyber physical systems and internet-of-Things: From adaptive robustness methods to reliability and security for machine learning
(2018) Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI, 2018-July, art.

no. 8429432, pp. 581-586. Cited 6 times.

50) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85052128895&doi=10.1109%2fISVLSI.2018.00111&partnerID=40&md5=
DOI: 10.1109/ISVLSI.2018.00111

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

51) Chen, Y., Chen, F., Wu, T., Hu, W., Xu, X.
A deep learning model for secure cyber-physical transportation systems
(2018) INFOCOM 2018 - IEEE Conference on Computer Communications Workshops, pp. 1-2. Cited

4 times.

51) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85050685652&doi=10.1109%2fINFCOMW.2018.8406824&partnerID=40
DOI: 10.1109/INFCOMW.2018.8406824

Document Type: Conference Paper
Publication Stage: Final

Source: Scopus

52) Huang, X., Zhai, D., Dong, J.
Adaptive integral sliding-mode control strategy of data-driven cyber-physical systems against a class of actuator attacks
(2018) IET Control Theory and Applications, 12 (10), art. no. IET-CTA.2017.1278, . Cited 11 times.

52) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048533141&doi=10.1049%2fiet-cta.2017.1278&partnerID=40&md5=88
DOI: 10.1049/iet-cta.2017.1278

Document Type: Article
Publication Stage: Final
Source: Scopus

53) Demidov, R., Pechenkin, A.
Vector representation of machine instructions for vulnerability assessment of digital infrastructure components
(2018) Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS 2018, pp. 835-840. Cited 3 times.

53) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85050133318&doi=10.1109%2fICPHYS.2018.8390815&partnerID=40&m
DOI: 10.1109/ICPHYS.2018.8390815

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

54) McKee, D.W., Clement, S.J., Almutairi, J., Xu, J.
Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems
(2018) CAAI Transactions on Intelligence Technology, 3 (2), pp. 75-82. Cited 15 times.

54) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055736534&doi=10.1049%2ftrit.2018.0010&partnerID=40&md5=2a524
DOI: 10.1049/trit.2018.0010

Document Type: Review
Publication Stage: Final
Access Type: Open Access
Source: Scopus

55) Majdani, F., Petrovski, A., Doolan, D.
Evolving ANN-based sensors for a context-aware cyber physical system of an offshore gas turbine
(2018) Evolving Systems, 9 (2), pp. 119-133.

55) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047944581&doi=10.1007%2fs12530-017-9206-8&partnerID=40&md5=

DOI: 10.1007/s12530-017-9206-8

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

56) Lin, Q., Verwer, S., Adepu, S., Mathur, A.
TABOR: A graphical model-based approach for anomaly detection in industrial control systems
(2018) ASIACCS 2018 - Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security, pp. 525-536. Cited 19 times.

56) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049167693&doi=10.1145%2f3196494.3196546&partnerID=40&md5=1
DOI: 10.1145/3196494.3196546

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

57) Qiu, H., Liu, X., Rallapalli, S., Bency, A.J., Chan, K., Urgaonkar, R., Manjunath, B.S., Govindan, R.
Kestrel: Video analytics for augmented multi-camera vehicle tracking
(2018) Proceedings - ACM/IEEE International Conference on Internet of Things Design and Implementation, IoTDI 2018, pp. 48-59. Cited 14 times.

57) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048509478&doi=10.1109%2fIoTDI.2018.00015&partnerID=40&md5=f0
DOI: 10.1109/IoTDI.2018.00015

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

58) Liu, X., Zhou, Y., Wang, Z., Chen, X.
A BP Neural Network-Based Communication Blind Signal Detection Method with Cyber-Physical-Social Systems
(2018) IEEE Access, 6, art. no. 8362612, pp. 43920-43935. Cited 3 times.

58) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047613969&doi=10.1109%2fACCESS.2018.2838123&partnerID=40&r
DOI: 10.1109/ACCESS.2018.2838123

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

59) Osia, S.A., Shamsabadi, A.S., Taheri, A., Rabiee, H.R., Haddadi, H.
Private and Scalable Personal Data Analytics Using Hybrid Edge-to-Cloud Deep Learning
(2018) Computer, 51 (5), pp. 42-49. Cited 11 times.

59) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047736427&doi=10.1109%2fMC.2018.2381113&partnerID=40&md5=e
DOI: 10.1109/MC.2018.2381113

Document Type: Article
Publication Stage: Final
Source: Scopus

60) Hatcher, W.G., Yu, W.
A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends
(2018) IEEE Access, 6, pp. 24411-24432. Cited 93 times.

60) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046378997&doi=10.1109%2fACCESS.2018.2830661&partnerID=40&r
DOI: 10.1109/ACCESS.2018.2830661

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

61) Ren, L., Sun, Y., Wang, H., Zhang, L.
Prediction of bearing remaining useful life with deep convolution neural network
(2018) IEEE Access, 6, pp. 13041-13049. Cited 47 times.

61) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85041803341&doi=10.1109%2fACCESS.2018.2804930&partnerID=40&r
DOI: 10.1109/ACCESS.2018.2804930

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

62) Kadar, M., Jardim-Goncalves, R., Covaciu, C., Bullon, S.
Intelligent defect management system for porcelain industry through cyber-physical systems
(2018) 2017 International Conference on Engineering, Technology and Innovation: Engineering,

Technology and Innovation Management Beyond 2020: New Challenges, New Approaches,

ICE/ITMC 2017 - Proceedings, 2018-January, pp. 1338-1343.

62) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047461666&doi=10.1109%2fICE.2017.8280036&partnerID=40&md5=3
DOI: 10.1109/ICE.2017.8280036

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

63) Feng, M., Xu, H.
Deep reinforecement learning based optimal defense for cyber-physical system in presence of unknown cyber-attack
(2018) 2017 IEEE Symposium Series on Computational Intelligence, SSCI 2017 - Proceedings,

2018-January, pp. 1-8. Cited 4 times.

63) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046108086&doi=10.1109%2fSSCI.2017.8285298&partnerID=40&md5
DOI: 10.1109/SSCI.2017.8285298

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

64) Shin, J., Baek, Y., Eun, Y., Son, S.H.
Intelligent sensor attack detection and identification for automotive cyber-physical systems
(2018) 2017 IEEE Symposium Series on Computational Intelligence, SSCI 2017 - Proceedings,

2018-January, pp. 1-8. Cited 4 times.

64) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046095781&doi=10.1109%2fSSCI.2017.8280915&partnerID=40&md5
DOI: 10.1109/SSCI.2017.8280915

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

65) Li, S., Bi, F., Chen, W., Miao, X., Liu, J., Tang, C.
An improved information security risk assessments method for cyber-physical-social computing and networking
(2018) IEEE Access, 6, pp. 10311-10319. Cited 13 times.

65) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85041395110&doi=10.1109%2fACCESS.2018.2800664&partnerID=40&r
DOI: 10.1109/ACCESS.2018.2800664

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

66) Eiteneuer, B., Niggemann, O.

LSTM for model-based Anomaly Detection in Cyber-Physical Systems

(2018) CEUR Workshop Proceedings, 2289, .

66) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059814769&partnerID=40&md5=83cdddd8ca7d6f4196fbeeef73cadf42

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

67) Yang, B., Chen, X., Zhang, T.

A multichannel convolutional neural network based forensics-aware scheme for cyber-physical-social systems

(2018) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11068 LNCS, pp. 243-254.

67) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054850605&doi=10.1007%2f978-3-030-00021-9_23&partnerID=40&m

DOI: 10.1007/978-3-030-00021-9_23

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

68) Alpano, P.V.S., Pedrasa, J.R.I., Atienza, R.

Multilayer perceptron with binary weights and activations for intrusion detection of Cyber-Physical systems

(2017) IEEE Region 10 Annual International Conference, Proceedings/TENCON, 2017-December, pp. 2825-2829. Cited 3 times.

68) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044239703&doi=10.1109%2fTENCON.2017.8228342&partnerID=40&r

DOI: 10.1109/TENCON.2017.8228342

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

69) Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D.

Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning

(2017) IEEE Access, 6, pp. 3491-3508. Cited 37 times.

69) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85038810363&doi=10.1109%2fACCESS.2017.2782159&partnerID=40&r

DOI: 10.1109/ACCESS.2017.2782159

Document Type: Article
Publication Stage: Final
Access Type: Open Access

Source: Scopus

70) Wang, Y., Amin, M.M., Fu, J., Moussa, H.B.
A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids
(2017) IEEE Access, 5, art. no. 8093999, pp. 26022-26033. Cited 29 times.

70) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85033384300&doi=10.1109%2fACCESS.2017.2769099&partnerID=40&r
DOI: 10.1109/ACCESS.2017.2769099

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

71) Hariri, M.E., Harmon, E., Habib, H.F., Youssef, T., Mohammed, O.A.
A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems
(2017) 2017 19th International Conference on Intelligent System Application to Power Systems, ISAP 2017, art. no. 8071363, . Cited 9 times.

71) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85039968153&doi=10.1109%2fISAP.2017.8071363&partnerID=40&md5=
DOI: 10.1109/ISAP.2017.8071363

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

72) Amrouch, H., Henkel, J., Krishnamurthy, P., Karri, R., Patel, N., Khorrami, F.
Special session: Emerging (un-)reliability based security threats and mitigations for embedded systems
(2017) Proceedings of the 2017 International Conference on Compilers, Architectures and Synthesis for Embedded Systems Companion, CASES 2017, art. no. 3125529, . Cited 4 times.

72) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85035317920&doi=10.1145%2f3125501.3125529&partnerID=40&md5=c
DOI: 10.1145/3125501.3125529

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

73) Raj, S., Jha, S.K., Ramanathan, A., Pullum, L.L.
Work-in-progress: Testing autonomous cyber-physical systems using fuzzing features from convolutional neural networks

(2017) Proceedings of the 13th ACM International Conference on Embedded Software 2017

Companion, EMSOFT 2017, art. no. 1, . Cited 1 time.

73) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034850699&doi=10.1145%2f3125503.3125568&partnerID=40&md5=d
DOI: 10.1145/3125503.3125568

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

74) Lang, X., Li, P., Li, Y., Ren, H.
Leak location of pipeline with multibranch based on a cyber-physical system
(2017) Information (Switzerland), 8 (4), art. no. 113, . Cited 5 times.

74) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85030457405&doi=10.3390%2finfo8040113&partnerID=40&md5=5bce91
DOI: 10.3390/info8040113

Document Type: Article
Publication Stage: Final
Access Type: Open Access
Source: Scopus

75) Fu, Y., Zhu, J., Gao, S.
CPS Information Security Risk Evaluation System Based on Petri Net
(2017) Proceedings - 2017 IEEE 2nd International Conference on Data Science in Cyberspace, DSC

2017, art. no. 8005529, pp. 541-548. Cited 6 times.

75) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034264941&doi=10.1109%2fDSC.2017.65&partnerID=40&md5=e5552
DOI: 10.1109/DSC.2017.65

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

76) Llewellynn, T., Milagro, M., Deniz, O., Fricker, S., Storkey, A., Pazos, N., Velikic, G., Leufgen, K., Dahyot, R., Koller, S., Goumas, G., Leitner, P., Dasika, G., Wang, L., Tutschku, K.
BONSEYES: Platform for open development of systems of artificial intelligence
(2017) ACM International Conference on Computing Frontiers 2017, CF 2017, pp. 299-304. Cited 9

times.

76) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020497834&doi=10.1145%2f3075564.3076259&partnerID=40&md5=b
DOI: 10.1145/3075564.3076259

Document Type: Conference Paper

Publication Stage: Final
Access Type: Open Access
Source: Scopus

77) Goh, J., Adepu, S., Tan, M., Lee, Z.S.
Anomaly detection in cyber physical systems using recurrent neural networks
(2017) Proceedings of IEEE International Symposium on High Assurance Systems Engineering, art.

no. 7911887, pp. 140-145. Cited 70 times.

77) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85019260937&doi=10.1109%2fHASE.2017.36&partnerID=40&md5=60da
DOI: 10.1109/HASE.2017.36

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

78) Lee, H.
Framework and development of fault detection classification using IoT device and cloud environment
(2017) Journal of Manufacturing Systems, 43, pp. 257-270. Cited 33 times.

78) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85014081409&doi=10.1016%2fj.jmsy.2017.02.007&partnerID=40&md5=
DOI: 10.1016/j.jmsy.2017.02.007

Document Type: Article
Publication Stage: Final
Source: Scopus

79) Sargolzaei, A., Crane, C.D., Abbaspour, A., Noei, S.
A machine learning approach for fault detection in vehicular cyber-physical systems
(2017) Proceedings - 2016 15th IEEE International Conference on Machine Learning and

Applications, ICMLA 2016, art. no. 7838216, pp. 636-640. Cited 15 times.

79) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015453313&doi=10.1109%2fICMLA.2016.18&partnerID=40&md5=678
DOI: 10.1109/ICMLA.2016.18

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

80) Martín-Martín, P., González-Briones, A., Villarrubia, G., De Paz, J.F.
Intelligent transport system through the recognition of elements in the environment
(2017) Communications in Computer and Information Science, 722, pp. 470-480. Cited 1 time.

80)

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85021219911&doi=10.1007%2f978-3-319-60285-1_40&partnerID=40&m
DOI: 10.1007/978-3-319-60285-1_40

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

81) Muhamedyev, R.I., Muhamedyeva, J., Amirgaliyev, Y.N., Khamitov, A.N., Abdilmanova, A.
Revelation of new ICT domains for upcoming kazakhstan's participation
(2015) ACM International Conference Proceeding Series, 2015-November, pp. 179-188. Cited 1 time.

81) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85045627965&doi=10.1145%2f2846012.2846051&partnerID=40&md5=e
DOI: 10.1145/2846012.2846051

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

Search: TITLE-ABS-KEY ("*neural network*" OR "deep learning" OR "reinforcement learning") AND TITLE-ABS-KEY ("security" OR "detection" OR "cyber physical attack*") AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (LANGUAGE,"English")) AND (LIMIT-TO (EXACTKEYWORD,"Cyber Physical System"))