A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compro

DOI: 10.1016/j.future.2019.02.013
Future Generation Computer Systems, 2019, 96, 227-242.

#	Paper	IF	Citations
62	Financial technology: a review of extant literature. *Studies in Economics and Finance*, **2019**, 37, 71-88	1.3	34
61	Extraction of Threat Actions from Threat-related Articles using Multi-Label Machine Learning Classification Method. **2019**,		2
60	Society 5.0: Feasibilities and challenges of the implementation of fintech in small and medium industries. *Journal of Physics: Conference Series*, **2019**, 1402, 077053	0.3	3
59	A systematic review of cyber-resilience assessment frameworks. *Computers and Security*, **2020**, 97, 101996	4.9	11
58	A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. *Future Internet*, **2020**, 12, 108	3.3	14
57	Security of Cyber-Physical Systems. **2020**,		5
56	MVFCC: A Multi-View Fuzzy Consensus Clustering Model for Malware Threat Attribution. *IEEE Access*, **2020**, 8, 139188-139198	3.5	16
55	Detecting Cyber Threat Event from Twitter Using IDCNN and BiLSTM. *Applied Sciences (Switzerland)* , **2020**, 10, 5922	2.6	5
54	A Novel Enhanced Naïve Bayes Posterior Probability (ENBPP) Using Machine Learning: Cyber Threat Analysis. *Neural Processing Letters*, **2021**, 53, 177-209	2.4	1
53	A review of threat modelling approaches for APT-style attacks. *Heliyon*, **2021**, 7, e05969	3.6	11
52	Internet of Things: Evolution, Concerns and Security Challenges. *Sensors*, **2021**, 21,	3.8	32
51	The Triangle Model for Cyber Threat Attribution. *Journal of Cyber Security Technology*, 1-18	1.3	1
50	FinTech and commercial banksTperformance in China: A leap forward or survival of the fittest?. *Technological Forecasting and Social Change*, **2021**, 166, 120645	9.5	17
49	Preemptive Prediction-Based Automated Cyberattack Framework Modeling. *Symmetry*, **2021**, 13, 793	2.7	3
48	Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, **2021**, 21,	3.8	7
47	Towards Automated Matching of Cyber Threat Intelligence Reports based on Cluster Analysis in an Internet-of-Vehicles Environment. **2021**,		0
46	Examining factors that boost intention and loyalty to use Fintech post-COVID-19 lockdown as a new normal behavior. *Heliyon*, **2021**, 7, e07821	3.6	8

45	DMAPT: Study of Data Mining and Machine Learning Techniques in Advanced Persistent Threat Attribution and Detection.		
44	Integrating Security Behavior into Attack Simulations. **2021**,		2
43	Multifractal detrended fluctuation analysis based detection for SYN flooding attack. *Computers and Security*, **2021**, 107, 102315	4.9	1
42	Malware: The Never-Ending Arm Race. **2021**, 1-25		0
41	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems. *IEEE Internet of Things Journal*, **2021**, 8, 13712-13722	10.7	14
40	Text Mining in Cybersecurity. *ACM Computing Surveys*, **2022**, 54, 1-36	13.4	4
39	Knowledge Processing Method with Calculated Functors. *Lecture Notes in Networks and Systems*, **2020**, 187-194	0.5	1
38	A Systematic Review of Artificial Intelligence and Machine Learning Techniques for Cyber Security. *Communications in Computer and Information Science*, **2020**, 584-593	0.3	2
37	Customer-oriented ranking of cyber threat intelligence service providers. *Electronic Commerce Research and Applications*, **2020**, 41, 100976	4.6	4
36	Automated Preemptive Forecasting Framework Model for Cyber Attacks. *The Journal of Korean Institute of Information Technology*, **2020**, 18, 107-116	0.2	
35	Cyber Threat Hunting Through Automated Hypothesis and Multi-Criteria Decision Making. **2020**,		0
34	A Bibliometric Analysis on the Application of Deep Learning in Cybersecurity. **2020**, 203-221		1
33	Key Technologies of Threat Intelligence for Satellite Communication Network. *Software Engineering and Applications*, **2020**, 09, 403-411	0.1	
32	Mapping CKC Model Through NLP Modelling for APT Groups Reports. **2022**, 239-252		
31	A Survey of Machine Learning Techniques for IoT Security. *Communications in Computer and Information Science*, **2021**, 139-157	0.3	
30	A tree-based stacking ensemble technique with feature selection for network intrusion detection. *Applied Intelligence*, 1	4.9	6
29	Deep Learning for Threat Actor Attribution from Threat Reports. **2020**,		1
28	A Literature Review on Mining Cyberthreat Intelligence from Unstructured Texts. **2020**,		1

27	A Data Mining Framework to Predict Cyber Attack for Cyber Security. **2020**,		2
26	A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. *International Journal of Applied Engineering and Management Letters*, 149-159		
25	Identifikation der Urheber von Cyberattacken mithilfe künstlicher Intelligenz. *Wirtschaftsinformatik & Management*, 1	0.2	0
24	Cyber Threat Analysis And Prediction Using Machine Learning. **2021**,		
23	Construction of TTPS From APT Reports Using Bert. **2021**,		0
22	An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA). **2022**,		
21	An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems. *Journal of Advanced Transportation*, **2022**, 2022, 1-17	1.9	6
20	Focusing on the Weakest Link: A Similarity Analysis on Phishing Campaigns Based on the ATT&CK Matrix. *Security and Communication Networks*, **2022**, 2022, 1-12	1.9	
19	FinTech and Commercial BanksTPerformance in China: A Leap Forward or Survival of the Fittest?. *SSRN Electronic Journal*,	1	
18	Predicting future community intrusions using a novel type and encryption mechanism architecture for attack node mitigation. **2022**, 49, 174-182		
17	Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. *Computer Communications*, **2022**,	5.1	
16	CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution. **2022**, 1-15		1
15	Advanced Persistent Threat intelligent profiling technique: A survey. **2022**, 103, 108261		1
14	Artificial Intelligence for Digital Finance, Axes and Techniques. **2022**, 203, 633-638		1
13	Predicting Future Community Intrusions Using a Novel Type and Encryption Mechanism Architecture for Attack Node Mitigation.		0
12	CAVeCTIR: Matching Cyber Threat Intelligence Reports on Connected and Autonomous Vehicles Using Machine Learning. **2022**, 12, 11631		0
11	Cross-site Scripting Threat Intelligence Detection Based on Deep Learning. **2022**, 89-104		0
10	Taxonomy of Cyber Threat Intelligence Framework. **2022**,		0

9	What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey.	0
8	A Review of Cyber Threat (Artificial) Intelligence in Security Management. **2023**, 29-45	0
7	Cyber threat attribution using unstructured reports in cyber threat intelligence. **2022**,	0
6	SDOT: Secure Hash, Semantic Keyword Extraction, and Dynamic Operator Pattern-Based Three-Tier Forensic Classification Framework. **2023**, 11, 3291-3306	0
5	Development of WEB-based Automatic Detection Tool for Web Attack Traceability. **2022**,	0
4	Investigating Variables that Increase the Desire and Loyalty to Utilize Fintech After the COVID-19 Lockdown: A New Normal Behavior. **2023**, 267-293	0
3	Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. **2023**, 7, 1-33	0
2	Analysis of financial technology acceptance of peer to peer lending (P2P lending) using extended technology acceptance model (TAM). **2023**, 9, 100027	0
1	Fintech and financial sector performance in Saudi Arabia: An empirical study. **2023**, 12, 43-65	0