Paper Title	Authors	Paper
Adversarial Machine Learning		
Automated Adversary Emulation for Cyber-Physical Systems via Reinforcement Learning	Arnab Bhattacharya, Thiagarajan Ramachandran, Sandeep Banik, Chase Dowling and Shaunak Bopardikar	**68**
Detecting Cyber-Adversarial Videos in Traditional Social media	Bingyan Du, Pranay Singhal, Victor Benjamin and Weifeng Li	**55**
Evaluating Effectiveness of Adversarial Examples on state of art License Plate Recognition Models	Kanishk Rana and Rahul Madaan	**5**
Assessing GAN-based approaches for generative modeling of crime text reports	Samira Khorshidi, George Mohler and Jeremy Carter	**37**
COVID-19's Impact on Cybersecurity		
Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses	Mir Mehedi Ahsan Pritom, Kristin Schweitzer, Raymond Bateman, Min Xu and Shouhuai Xu	**56**
Data-Driven Characterization and Detection of COVID-19 Themed Malicious Websites	Mir Mehedi Ahsan Pritom, Kristin Schweitzer, Raymond Bateman, Min Xu and Shouhuai Xu	**60**
Analyzing the Evolutionary Characteristics of the Cluster of COVID-19 under Anti-contagion Policies	Pu Miao, Hu Tian, Xingwei Zhang, Saike He, Xiaolong Zheng, Daniel Zeng and Wu Desheng Dash	**48**
The Four-Stages Strategies on Social Media to Cope with "Infodemic" and Repair Public Trust: Covid-19 Disinformation and Effectiveness of Government Intervention in China	Yonghan Zhu and Yuqiao Jiang	**11**
Cyber Threat Intelligence		
Malware Family Fingerprinting Through Behavioral Analysis	Aaron Walker and Shamik Sengupta	**19**
Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior	Aritran Piplai, Sudip Mittal, Mahmoud Abdelsalam, Maanak Gupta, Anupam Joshi and Tim Finin	**34**
Multi-Dimensional Anomalous Entity Detection via Poisson Tensor Factorization	Maksim Eren, Juston Moore and Boian Alexandrov	**39**
Detection of Malicious Domains Using Passive DNS with XGBoost	Marcos Rogério Silveira, Adriano Mauro Cansian and Hugo Koji Kobayashi	**33**
Cybersecurity Threat Intelligence Augmentation and Embedding Improvement - A Healthcare Usecase	Matthew Sills, Priyanka Ranade and Sudip Mittal	**18**
Scalable Malware Clustering using Multi-Stage Tree Parallelization	Muqeet Ali, Josiah Hagen and Jonathan Oliver	**42**
A KG-based Enhancement Framework for Fact Checking Using Category Information	Shuai Wang, Lei Wang and Wenji Mao	**17**
XGBoosted Misuse Detection in LAN-Internal Traffic Dataset	Zhiqing Zhang, Pawissakan Chirupphapa, Hiroshi Esaki and Hideya Ochiai	**20**

Paper Title	Authors	Paper
Cybersecurity for Cyberinfrastructure		
Identifying Vulnerable GitHub Repositories and Users in Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach	Ben Lazarine, Sagar Samtani, Mark Patton, Hongyi Zhu, Steven Ullman, Benjamin Ampel and Hsinchun Chen	24
APIN: Automatic Attack Path Identification in Computer Networks	Eric Ficke and Shouhuai Xu	59
Fraud Prevention Within the Brazilian Governmental Public-Key Infrastructure	Fernanda Oliveira Gomes, Bruno Machado Agostinho and Jean Everson Martina	52
Adaptive and Predictive SDN Control During DDoS Attacks	Jagannadh Vempati, Ram Dantu, Syed Badruddoja and Mark Thompson	57
Efficient and Secure Implementation of BLS Multisignature Scheme on TPM	Mustapha Hedabou and Yunusa Simpa Abdulsalam	14
Performance Analysis of Secure Real-time Transport Protocol Using Elliptic Curves	Nilanjan Sen, Ram Dantu and Mark Thompson	61
A Comparative Study on Contemporary Intrusion Detection Datasets for Machine Learning Research	Smirti Dwibedi, Medha Pujari and Weiqing Sun	54
Effective Voice Fuzzing Method for Finding Vulnerabilities in AI Speech Recognition Devices	So-Hyun Park and Il-Gu Lee	31
Smart Vulnerability Assessment for Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach	Steven Ullman, Sagar Samtani, Ben Lazarine, Hongyi Zhu, Benjamin Ampel, Mark Patton and Hsinchun Chen	23
Discerning User Activity in Extended Reality Through Side-Channel Accelerometer Observations	Tiago Martins Andrade, Max Smith-Creasey and Jonathan Francis Roscoe	12
Dark Web Analytics		
Labeling Hacker Exploits for Proactive Cyber Threat Intelligence: A Deep Transfer Learning Approach	Benjamin Ampel, Sagar Samtani, Hongyi Zhu, Steven Ullman and Hsinchun Chen	13
An Expert System for Classifying Harmful Content on the Dark Web	Hanae Kobayashi, Masashi Kadoguchi, Shota Hayashi, Akira Otsuka and Masaki Hashimoto	15
Identifying Proficient Cybercriminals Through Text and Network Analysis	Jan William Johnsen and Katrin Franke	28
Deep Self-Supervised Clustering of the Dark Web for Cyber Threat Intelligence	Masashi Kadoguchi, Hanae Kobayashi, Shota Hayashi, Akira Otsuka and Masaki Hashimoto	26
A Generative Adversarial Learning Framework for Breaking Text-Based CAPTCHA in the Dark Web	Ning Zhang, Mohammadreza Ebrahimi, Weifeng Li and Hsinchun Chen	9
Improving the Data Quality for Credit Card Fraud Detection	Rongrong Jing, Hu Tian, Yidi Li, Xingwei Zhang, Xiaolong Zheng, zhu zhang and Daniel Zeng	50
Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web	Yizhi Liu, Fang Yu Lin, Zara Ahmad-Post, Mohammadreza Ebrahimi, Ning Zhang, James Lee Hu, Jingyu Xu, Weifeng Li and Hsinchun Chen	43

Paper Title	Authors	Paper
Deep Learning Applications for Cybersecurity		
Sentimental LIAR: Extended Corpus and Deep Learning Models for Fake Claim Classification	Bibek Upadhayay and Vahid Behzadan	67
Political Fake Statement Detection via Multistage Feature-assisted Neural Modeling	Fuad Mire Hassan and Mark Lee	40
DeepGuard: Deep Generative User-behavior Analytics for Ransomware Detection	Gaddisa Olani Ganfure, Chun-Feng Wu, Yuan-Hao Chang and Wei-Kuan Shih	25
A virtual simulation environment using deep learning for autonomous vehicles obstacle avoidance	Leila Haj Meftah and Rafik Braham	51
From Word Embedding to Cyber-Phrase Embedding: Comparison of Processing Cybersecurity Texts	Moumita Das Purba, Bill Chu and Ehab Al-Shaer	53
Weaponizing Unicodes with Deep Learning - Identifying Homoglyphs with Weakly Labeled Data	Perry Deng, Cooper Linsky and Matthew Wright	65
Phishcasting: Deep Learning for Time Series Forecasting of Phishing Attacks	Syed Hasan Amin Mahmood, Syed Mustafa Ali Abbasi, Ahmed Abbasi and Fareed Zaffar	21
Socio-technical Perspectives of Cybersecurity		
Is the user identity perception influenced by the blockchain technology?	Andreea-Elena Panait	32
Conceptual Models for Counter-Terrorism and Intelligence Knowledge Bases	Antonio Badia	35
An Ordinal Approach to Modeling and Visualizing Phishing Susceptibility	David G. Dobolyi, Ahmed Abbasi, F. Mariam Zahedi and Anthony Vance	49
A Bootstrapped Model to Detect Abuse and Intent in White Supremacist Corpora	David Skillicorn and Benjemin Simons	30
A Proxy-Based Encrypted Online Social Network With Fine-Grained Access	Fabian Schillinger and Christian Schindelhauer	6
A Survey of Real-Time Social-Based Traffic Detection	Hashim Abu-Gellban	8
Twitter Bot Detection with Reduced Feature Set	Jefferson Abreu, Célia Ralha and João Gondim	29
Towards a Story Scheme Ontology of Terrorist MOs	Joeri Peters and Floris Bex	38
A Human-Network-Security-Interface for an Average Joe	Rajasekhar Ganduri, Ram Dantu, Mark Thompson, Samuel Evans and Logan Widick	36
Heuristic Phishing Detection and URL Checking Methodology Based on Scraping and Web Crawling	Rômulo Almeida and Carla Westphall	58
Social Emotion Cause Extraction from Online Texts	Xinglin Xiao, Lei Wang, Qingchao Kong and Wenji Mao	64