Frederick T Sheldon

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7775174/publications.pdf

Version: 2024-02-01

87 papers	1,028 citations	686830 13 h-index	580395 25 g-index
90 all docs	90 docs citations	90 times ranked	645 citing authors

#	Article	IF	Citations
1	Quantifying security threats and their potential impacts: a case study. Innovations in Systems and Software Engineering, 2010, 6, 269-281.	1.6	104
2	Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship, 2017, 11, 286-300.	1.6	82
3	Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. Computers and Security, 2020, 97, 101994.	4.0	66
4	IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method. Applied Sciences (Switzerland), 2022, 12, 5015.	1.3	57
5	Metrics for maintainability of class inheritance hierarchies. Journal of Software: Evolution and Process, 2002, 14, 147-160.	1.1	51
6	Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning. , 2018, , .		40
7	The Insecurity of Wireless Networks. IEEE Security and Privacy, 2012, 10, 54-61.	1.5	36
8	Reliability measurement: from theory to practice. IEEE Software, 1992, 9, 13-20.	2.1	30
9	IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors, 2021, 21, 6432.	2.1	30
10	A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. Sensors, 2022, 22, 1837.	2.1	29
11	A data integrity verification scheme in mobile cloud computing. Journal of Network and Computer Applications, 2017, 77, 146-151.	5.8	26
12	Access Control in Fog Computing: Challenges and Research Agenda. IEEE Access, 2020, 8, 83986-83999.	2.6	26
13	A Methodology to Evaluate Agent Oriented Software Engineering Techniques. , 2007, , .		25
14	ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed. , 2019, , .		22
15	Risk Assessment Methodology Based on the NISTIR 7628 Guidelines. , 2013, , .		19
16	Network Intrusion Detection and Comparative Analysis Using Ensemble Machine Learning and Feature Selection. IEEE Transactions on Network and Service Management, 2022, 19, 4821-4833.	3.2	18
17	Security management of cyber physical control systems using NIST SP 800-82r2. , 2017, , .		17
18	Risk Assessment For Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC). Journal of Artificial Intelligence and Soft Computing Research, 2015, 5, 205-220.	3.5	16

#	Article	IF	Citations
19	Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value. , 2008, , .		15
20	Defining and computing a value based cyber-security measure. Information Systems and E-Business Management, 2012, 10, 433-453.	2.2	15
21	Managing complex IT security processes with value based measures. , 2009, , .		14
22	On quantum authentication protocols. , 2005, , .		13
23	Evaluating security controls based on key performance indicators and stakeholder mission. , 2008, , .		13
24	Moving Toward Trustworthy Systems: R&amp;D Essentials. Computer, 2010, 43, 31-40.	1.2	13
25	Measuring the complexity of class diagrams in reverse engineering. Journal of Software: Evolution and Process, 2006, 18, 333-350.	1.1	11
26	Modeling stakeholder/value dependency through mean failure cost. , 2010, , .		9
27	Elliptic Envelope Based Detection of Stealthy False Data Injection Attacks in Smart Grid Control Systems. , 2020, , .		9
28	Specification, safety and reliability analysis using stochastic Petri net models. , 0, , .		8
29	Measuring Reliability as a Mean Failure Cost. , 2007, , .		8
30	An outline of the three-layer survivability analysis architecture for strategic information warfare research. , 2009, , .		8
31	Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation. , 2014, , .		8
32	HERMES: A high-level policy language for high-granularity enterprise-wide secure browser configuration management. , 2016, , .		8
33	CSSR: Cloud Services Security Recommender. , 2016, , .		8
34	Novel Security Models for IoTâ€"Fogâ€"Cloud Architectures in a Real-World Environment. Applied Sciences (Switzerland), 2022, 12, 4837.	1.3	8
35	Reliability analysis of CSP specifications - A new method using Petri nets. , 1995, , .		7
36	Using a knowledge-based security orchestration tool to reduce the risk of browser compromise. , 2016, , .		7

#	Article	IF	Citations
37	A case study: validation of guidance control software requirements for completeness, consistency and fault tolerance. , 0, , .		6
38	Assessment of High Integrity Software Components for Completeness, Consistency, Fault-Tolerance, and Reliability. Lecture Notes in Computer Science, 2003, , 259-286.	1.0	6
39	Testing Software Requirements with Z and Statecharts Applied to an Embedded Control Systemt0t1. Software Quality Journal, 2004, 12, 231-264.	1.4	6
40	Security Analysis of Smart Grid Cyber Physical Infrastructures Using Game Theoretic Simulation. , 2015, , .		6
41	A virtual testbed for security management of industrial control systems. , 2017, , .		6
42	HESTIA: Adversarial Modeling and Risk Assessment for CPCS. , 2018, , .		6
43	An ontology-based software agent system case study. , 0, , .		5
44	A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance - Applying Cyber Security Econometrics System (CSES) to Mission Assurance Analysis Protocol (MAAP). , 2010, , .		5
45	Addressing the need for independence in the CSE model. , 2011, , .		5
46	Failure impact analysis of key management in AMI using cybernomic situational assessment (CSA). , 2013, , .		5
47	Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment. , 2013, , 133-147.		5
48	METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security. , 2018, , .		5
49	Attack Scenario-based Validation of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC). , 2019, , .		5
50	Key Factors Influencing the Rise of Current Ransomware Attacks on Industrial Control Systems. , 2021, , .		5
51	Title is missing!. Annals of Software Engineering, 1999, 8, 239-287.	0.5	4
52	Evaluating Security and Privacy in Cloud Services. , 2016, , .		4
53	An architecture for HESTIA: high-level and extensible system for training and infrastructure risk assessment. International Journal of Internet of Things and Cyber-Assurance, 2018, 1, 173.	0.7	4
54	Case study: B2B e-commerce system specification and implementation employing use-case diagrams, digital signatures and XML. , 0, , .		3

#	Article	IF	Citations
55	Recoverability preservation: a measure of last resort. Innovations in Systems and Software Engineering, 2005, 1, 54-62.	1.6	3
56	NISp1-10: Bank Transfer over Quantum Channel with Digital Checks. IEEE Global Telecommunications Conference (GLOBECOM), 2006, , .	0.0	3
57	Quantifying security threats and their impact. , 2009, , .		3
58	Anomaly detection in multiple scale for insider threat analysis. , 2011, , .		3
59	Has the cyber warfare threat been overstated?. , 2011, , .		3
60	Designing and operating through compromise. , 2013, , .		3
61	Improving Cyber Resiliency of Cloud Application Services by Applying Software Behavior Encryption (SBE). Procedia Computer Science, 2014, 28, 62-70.	1.2	3
62	Examining the Performance of Fog-Aided, Cloud-Centered IoT in a Real-World Environment. Sensors, 2021, 21, 6950.	2.1	3
63	SPECIFICATION AND ANALYSIS OF REAL-TIME SYSTEMS USING CSP AND PETRI NETS. International Journal of Software Engineering and Knowledge Engineering, 1996, 06, 229-248.	0.6	2
64	Modeling security as a dependability attribute: a refinement-based approach. Innovations in Systems and Software Engineering, 2006, 2, 39-48.	1.6	2
65	The handicap principle, strategic information warfare and the paradox of asymmetry. , 2010, , .		2
66	Defining and computing a value based cyber-security measure. , 2011, , .		2
67	Secure cryptographic key management system (CKMS) considerations for smart grid devices. , 2011, , .		2
68	Quantifying the impact of unavailability in cyber-physical environments. , 2014, , .		2
69	Quantifying availability in SCADA environments using the cyber security metric MFC. , 2014, , .		2
70	Risk and Vulnerability Assessment Using Cybernomic Computational Models. , 2015, , .		2
71	G-Model: A Novel Approach to Privacy-Preserving 1:M Microdata Publication. , 2020, , .		2
72	Validation of VANET message dissemination algorithms otherwise vulnerable to broadcast storms in urban contexts. Transactions on Emerging Telecommunications Technologies, 2021, 32, e4312.	2.6	2

#	ARTICLE	IF	CITATIONS
73	Authoring Adaptive Digital Computational Thinking Lessons Using vTutor for Web-Based Learning. Lecture Notes in Computer Science, 2018, , 125-131.	1.0	2
74	An Alert System: Using Fuzzy Logic for Controlling Crowd Movement by Detecting Critical Density Spots. , 2020, , .		2
75	Towards an Engineering Discipline of Computational Society. , 2007, , .		1
76	Software requirements for a system to compute mean failure cost. , 2010, , .		1
77	Validating Cyber Security Requirements: A Case Study. , 2011, , .		1
78	Toward Scalable Trustworthy Computing Using the Human-Physiology-Immunity Metaphor. IEEE Security and Privacy, 2011, 9, 14-23.	1.5	1
79	Intrinsically resilient energy control systems. , 2013, , .		1
80	A Best-Effort Damage Mitigation Model for Cyber-Attacks on Smart Grids. , 2018, , .		1
81	CloudMonitor: Data Flow Filtering as a Service. , 2019, , .		1
82	Performance Analysis of Two Cloud-Based IoT Implementations: Empirical Study. , 2020, , .		1
83	Model-based autonomic security management for cyber-physical infrastructures. International Journal of Critical Infrastructures, 2016, 12, 273.	0.1	1
84	Disrupting the Cooperative Nature of Intelligent Transportation Systems. , 2022, , .		1
85	Secure VM for monitoring industrial process controllers. , 2011, , .		0
86	Introduction to the special issue on cyber security and management. Information Systems and E-Business Management, 2012, 10, 429-431.	2.2	0
87	Formalizing an Automated, Adversary-aware Risk Assessment Process for Critical Infrastructure. , 2019, , .		0