

Javier Lopez

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/1469428/publications.pdf>

Version: 2024-02-01

216
papers

6,660
citations

147801

31
h-index

76900

74
g-index

239
all docs

239
docs citations

239
times ranked

5952
citing authors

#	ARTICLE	IF	CITATIONS
1	Personal IoT Privacy Control at the Edge. IEEE Security and Privacy, 2022, 20, 23-32.	1.2	2
2	Digital Twin: A Comprehensive Survey of Security Threats. IEEE Communications Surveys and Tutorials, 2022, 24, 1475-1503.	39.4	63
3	Real-time Crowd Counting based on Wearable Ephemeral IDs. , 2022, , .		1
4	Information Security and Privacy â€œ Challenges and Outlook. IFIP Advances in Information and Communication Technology, 2021, , 383-401.	0.7	1
5	A Blockchain Approach for Decentralized V2X (D-V2X). IEEE Transactions on Vehicular Technology, 2021, 70, 4001-4010.	6.3	15
6	Stakeholder perspectives and requirements on cybersecurity in Europe. Journal of Information Security and Applications, 2021, 61, 102916.	2.5	10
7	A model-driven approach to ensure trust in the IoT. Human-centric Computing and Information Sciences, 2020, 10, .	6.1	6
8	Blockchain-assisted access for federated Smart Grid domains: Coupling and features. Journal of Parallel and Distributed Computing, 2020, 144, 124-135.	4.1	29
9	Integration of a Threat Traceability Solution in the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2020, 16, 6575-6583.	11.3	16
10	Secure Interoperability in Cyber-Physical Systems. , 2020, , 521-542.		4
11	SealedGRID: A Secure Interconnection of Technologies for Smart Grid Applications. Lecture Notes in Computer Science, 2020, , 169-175.	1.3	0
12	Game Theory-Based Approach for Defense Against APTs. Lecture Notes in Computer Science, 2020, , 297-320.	1.3	5
13	Distributed Detection of APTs: Consensus vs. Clustering. Lecture Notes in Computer Science, 2020, , 174-192.	1.3	3
14	Detection of Node Capture Attack in Wireless Sensor Networks. IEEE Systems Journal, 2019, 13, 238-247.	4.6	29
15	Current cyber-defense trends in industrial control systems. Computers and Security, 2019, 87, 101561.	6.0	69
16	Escrowed decryption protocols for lawful interception of encrypted data. IET Information Security, 2019, 13, 498-507.	1.7	2
17	Covert Channels-Based Stealth Attacks in Industry 4.0. IEEE Systems Journal, 2019, 13, 3980-3988.	4.6	24
18	Edge-Assisted Vehicular Networks Security. IEEE Internet of Things Journal, 2019, 6, 8038-8045.	8.7	30

#	ARTICLE	IF	CITATIONS
19	Mobile Edge Computing for Vehicular Networks [From the Guest Editors]. IEEE Vehicular Technology Magazine, 2019, 14, 27-108.	3.4	9
20	Immune System for the Internet of Things Using Edge Technologies. IEEE Internet of Things Journal, 2019, 6, 4774-4781.	8.7	23
21	Enhancing Security and Dependability of Industrial Networks with Opinion Dynamics. Lecture Notes in Computer Science, 2019, , 263-280.	1.3	6
22	A Resilient Architecture for the Smart Grid. IEEE Transactions on Industrial Informatics, 2018, 14, 3745-3753.	11.3	36
23	A Trust-by-Design Framework for the Internet of Things. , 2018, , .		16
24	Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks. , 2018, , .		24
25	Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 2018, 78, 680-698.	7.5	914
26	A Cyber-Physical Systems-Based Checkpoint Model for Structural Controllability. IEEE Systems Journal, 2018, 12, 3543-3554.	4.6	8
27	Analyzing Cross-Platform Attacks: Towards a Three-Actor Approach. , 2018, , .		0
28	Capture the RAT: Proximity-Based Attacks in 5G Using the Routine Activity Theory. , 2018, , .		1
29	Evolution and Trends in IoT Security. Computer, 2018, 51, 16-25.	1.1	55
30	IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations. Sensors, 2018, 18, 492.	3.8	62
31	A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. IEEE Communications Surveys and Tutorials, 2018, 20, 3453-3495.	39.4	261
32	A Comprehensive Methodology for Deploying IoT Honeypots. Lecture Notes in Computer Science, 2018, , 229-243.	1.3	4
33	Cyber Stealth Attacks in Critical Information Infrastructures. IEEE Systems Journal, 2018, 12, 1778-1792.	4.6	44
34	Dynamic Knowledge-Based Analysis in Nonsecure 5G Green Environments Using Contextual Data. IEEE Systems Journal, 2017, 11, 2479-2489.	4.6	2
35	OCPP Protocol: Security Threats and Challenges. IEEE Transactions on Smart Grid, 2017, 8, 2452-2459.	9.0	89
36	Modelling trust dynamics in the Internet of Things. Information Sciences, 2017, 396, 72-82.	6.9	72

#	ARTICLE	IF	CITATIONS
37	Evolving privacy: From sensors to the Internet of Things. Future Generation Computer Systems, 2017, 75, 46-57.	7.5	115
38	From SMOG to Fog: A security perspective. , 2017, , .		19
39	Recommender system for privacy-preserving solutions in smart metering. Pervasive and Mobile Computing, 2017, 41, 205-218.	3.3	31
40	Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation. Journal of Network and Computer Applications, 2017, 87, 193-209.	9.1	53
41	Resilient interconnection in cyber-physical control systems. Computers and Security, 2017, 71, 2-14.	6.0	19
42	Digital Witness and Privacy in IoT: Anonymous Witnessing Approach. , 2017, , .		14
43	Cybersecurity of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method. , 2017, , .		9
44	Preventing Advanced Persistent Threats in Complex Control Networks. Lecture Notes in Computer Science, 2017, , 402-418.	1.3	15
45	Selecting Privacy Solutions to Prioritise Control in Smart Metering Systems. Lecture Notes in Computer Science, 2017, , 176-188.	1.3	2
46	Analysis of Intrusion Detection Systems in Industrial Ecosystems. , 2017, , .		33
47	On the application of generic CCAâ€secure transformations to proxy reâ€encryption. Security and Communication Networks, 2016, 9, 1769-1785.	1.5	5
48	A model-driven approach for engineering trust and reputation into software services. Journal of Network and Computer Applications, 2016, 69, 134-151.	9.1	9
49	Policy enforcement system for secure interoperable control in distributed Smart Grid systems. Journal of Network and Computer Applications, 2016, 59, 301-314.	9.1	35
50	Safeguarding Structural Controllability in Cyber-Physical Control Systems. Lecture Notes in Computer Science, 2016, , 471-489.	1.3	6
51	Probabilistic receiver-location privacy protection in wireless sensor networks. Information Sciences, 2015, 321, 205-223.	6.9	26
52	Relay selection for secure 5G green communications. Telecommunication Systems, 2015, 59, 169-187.	2.5	68
53	A three-stage analysis of IDS for critical infrastructures. Computers and Security, 2015, 55, 235-250.	6.0	7
54	A Parametric Family of Attack Models for Proxy Re-encryption. , 2015, , .		8

#	ARTICLE	IF	CITATIONS
55	Awareness and reaction strategies for critical infrastructure protection. Computers and Electrical Engineering, 2015, 47, 299-317.	4.8	1
56	Contextualising heterogeneous information in unified communications with security restrictions. Computer Communications, 2015, 68, 33-46.	5.1	0
57	A Context-based Parametric Relationship Model (CPRM) to measure the Security and QoS tradeoff in configurable environments. , 2014, , .		8
58	Preserving Receiver-Location Privacy in Wireless Sensor Networks. Lecture Notes in Computer Science, 2014, , 15-27.	1.3	1
59	A practical solution for sealed bid and multi-currency auctions. Computers and Security, 2014, 45, 186-198.	6.0	7
60	Delegated Access for Hadoop Clusters in the Cloud. , 2014, , .		3
61	WASAM: A dynamic wide-area situational awareness model for critical domains in Smart Grids. Future Generation Computer Systems, 2014, 30, 146-154.	7.5	30
62	A Model for the Analysis of QoS and Security Tradeoff in Mobile Platforms. Mobile Networks and Applications, 2014, 19, 64-78.	3.3	3
63	Diagnosis mechanism for accurate monitoring in critical infrastructure protection. Computer Standards and Interfaces, 2014, 36, 501-512.	5.4	14
64	Building trust from context similarity measures. Computer Standards and Interfaces, 2014, 36, 792-800.	5.4	16
65	Guest editorial to the Special Issue on Component-Based Software Engineering and Software Architecture. Science of Computer Programming, 2014, 90, 67-70.	1.9	0
66	Analysis and taxonomy of security/QoS tradeoff solutions for the future internet. Security and Communication Networks, 2014, 7, 2778-2803.	1.5	16
67	Location Privacy in WSNs: Solutions, Challenges, and Future Trends. Lecture Notes in Computer Science, 2014, , 244-282.	1.3	5
68	Engineering Trust-Awareness and Self-adaptability in Services and Systems. Lecture Notes in Computer Science, 2014, , 180-209.	1.3	1
69	A framework for enabling trust requirements in social cloud applications. Requirements Engineering, 2013, 18, 321-341.	3.1	18
70	Towards Trust-Aware and Self-adaptive Systems. IFIP Advances in Information and Communication Technology, 2013, , 255-262.	0.7	3
71	Wide-Area Situational Awareness for Critical Infrastructure Protection. Computer, 2013, 46, 30-37.	1.1	50
72	A privacy-aware continuous authentication scheme for proximity-based access control. Computers and Security, 2013, 39, 117-126.	6.0	10

#	ARTICLE	IF	CITATIONS
73	Secure sealed-bid online auctions using discreet cryptographic proofs. Mathematical and Computer Modelling, 2013, 57, 2583-2595.	2.0	13
74	Covert communications through network configuration messages. Computers and Security, 2013, 39, 34-46.	6.0	14
75	Security of industrial sensor network-based remote substations in the context of the Internet of Things. Ad Hoc Networks, 2013, 11, 1091-1104.	5.5	48
76	On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 2013, 57, 2266-2279.	5.1	992
77	Smart control of operational threats in control substations. Computers and Security, 2013, 38, 14-27.	6.0	27
78	(Un)Suitability of Anonymous Communication Systems to WSN. IEEE Systems Journal, 2013, 7, 298-310.	4.6	6
79	User-centric secure integration of personal RFID tags and sensor networks. Security and Communication Networks, 2013, 6, 1177-1197.	1.5	1
80	Towards Automatic Critical Infrastructure Protection through Machine Learning. Lecture Notes in Computer Science, 2013, , 197-203.	1.3	10
81	Building Trust and Reputation In: A Development Framework for Trust Models Implementation. Lecture Notes in Computer Science, 2013, , 113-128.	1.3	4
82	Trust, Privacy, and Security in Digital Business. Lecture Notes in Computer Science, 2013, , .	1.3	0
83	Critical Information Infrastructures Security. Lecture Notes in Computer Science, 2013, , .	1.3	0
84	Towards Engineering Trust-Aware Future Internet Systems. Lecture Notes in Computer Science, 2013, , 490-501.	1.3	3
85	A Novel Key Update Protocol in Mobile Sensor Networks. Lecture Notes in Computer Science, 2012, , 194-207.	1.3	8
86	Selecting key management schemes for WSN applications. Computers and Security, 2012, 31, 956-966.	6.0	36
87	Overview of Critical Information Infrastructure Protection. Lecture Notes in Computer Science, 2012, , 1-14.	1.3	6
88	Security and QoS Tradeoffs: Towards a FI Perspective. , 2012, , .		3
89	Traffic Classifier for Heterogeneous and Cooperative Routing through Wireless Sensor Networks. , 2012, , .		4
90	Accountability for cloud and other future Internet services. , 2012, , .		42

#	ARTICLE	IF	CITATIONS
91	Trust & security RTD in the internet of things. , 2012, , .		9
92	Analysis of requirements for critical control systems. International Journal of Critical Infrastructure Protection, 2012, 5, 137-145.	4.6	35
93	Secure Architecture for the Integration of RFID and Sensors in Personal Networks. Lecture Notes in Computer Science, 2012, , 207-222.	1.3	1
94	Integrating OpenID with proxy re-encryption to enhance privacy in cloud-based identity services. , 2012, , .		27
95	A Conceptual Framework for Trust Models. Lecture Notes in Computer Science, 2012, , 93-104.	1.3	32
96	Security in the Distributed Internet of Things. Lecture Notes in Computer Science, 2012, , 65-66.	1.3	6
97	On the energy cost of authenticated key agreement in wireless sensor networks. Wireless Communications and Mobile Computing, 2012, 12, 133-143.	1.2	14
98	Advanced secure multimedia services for digital homes. Information Systems Frontiers, 2012, 14, 527-540.	6.4	2
99	A Task Ordering Approach for Automatic Trust Establishment. Lecture Notes in Computer Science, 2012, , 75-88.	1.3	3
100	HIDE_DHCP: Covert Communications through Network Configuration Messages. International Federation for Information Processing, 2012, , 162-173.	0.4	9
101	Robust Probabilistic Fake Packet Injection for Receiver-Location Privacy in WSN. Lecture Notes in Computer Science, 2012, , 163-180.	1.3	5
102	Addressing Situational Awareness in Critical Domains of a Smart Grid. Lecture Notes in Computer Science, 2012, , 58-71.	1.3	2
103	Security and QoS relationships in Mobile Platforms. Lecture Notes in Electrical Engineering, 2012, , 13-21.	0.4	2
104	Managing Incidents in Smart Grids à la Cloud. , 2011, , .		24
105	Analysis of location privacy solutions in wireless sensor networks. IET Communications, 2011, 5, 2518-2532.	2.2	29
106	Towards a UML Extension of Reusable Secure Use Cases for Mobile Grid Systems. IEICE Transactions on Information and Systems, 2011, E94-D, 243-254.	0.7	2
107	Guest Editorial Advances in Digital Forensics for Communications and Networking. IEEE Journal on Selected Areas in Communications, 2011, 29, 1345-1348.	14.0	0
108	Securing the Internet of Things. Computer, 2011, 44, 51-58.	1.1	554

#	ARTICLE	IF	CITATIONS
109	An Early Warning System Based on Reputation for Energy Control Systems. IEEE Transactions on Smart Grid, 2011, 2, 827-834.	9.0	24
110	A methodology for security assurance-driven system development. Requirements Engineering, 2011, 16, 55-73.	3.1	15
111	Systematic design of secure Mobile Grid systems. Journal of Network and Computer Applications, 2011, 34, 1168-1183.	9.1	9
112	A cross-layer approach for integrating security mechanisms in sensor networks architectures. Wireless Communications and Mobile Computing, 2011, 11, 267-276.	1.2	8
113	Secure SCADA framework for the protection of energy control systems. Concurrency Computation Practice and Experience, 2011, 23, 1431-1442.	2.2	20
114	Key management systems for sensor networks in the context of the Internet of Things. Computers and Electrical Engineering, 2011, 37, 147-159.	4.8	243
115	Real-time location and inpatient care systems based on passive RFID. Journal of Network and Computer Applications, 2011, 34, 980-989.	9.1	96
116	Security services architecture for Secure Mobile Grid Systems. Journal of Systems Architecture, 2011, 57, 240-258.	4.3	11
117	Exploiting Context-Awareness to Enhance Source-Location Privacy in Wireless Sensor Networks. Computer Journal, 2011, 54, 1603-1615.	2.4	21
118	Early Warning System for Cascading Effect Control in Energy Control Systems. Lecture Notes in Computer Science, 2011, , 55-66.	1.3	3
119	SenseKey – Simplifying the Selection of Key Management Schemes for Sensor Networks. , 2011, , .		6
120	Engineering Secure Future Internet Services. Lecture Notes in Computer Science, 2011, , 177-191.	1.3	0
121	Certified electronic mail: Properties revisited. Computers and Security, 2010, 29, 167-179.	6.0	25
122	A security framework for a workflow-based grid development platform. Computer Standards and Interfaces, 2010, 32, 230-245.	5.4	2
123	Trust management systems for wireless sensor networks: Best practices. Computer Communications, 2010, 33, 1086-1093.	5.1	192
124	Pervasive authentication and authorization infrastructures for mobile users. Computers and Security, 2010, 29, 501-514.	6.0	11
125	A scale based trust model for multi-context environments. Computers and Mathematics With Applications, 2010, 60, 209-216.	2.7	11
126	Analysis of Secure Mobile Grid Systems: A systematic approach. Information and Software Technology, 2010, 52, 517-536.	4.4	21

#	ARTICLE	IF	CITATIONS
127	JCS special issue on EU-funded ICT research on Trust and Security. Journal of Computer Security, 2010, 18, 1-5.	0.8	1
128	A Multidimensional Reputation Scheme for Identity Federations. Lecture Notes in Computer Science, 2010, , 225-238.	1.3	0
129	Editorial ESORICS 2007. ACM Transactions on Information and System Security, 2010, 13, 1-2.	4.5	0
130	A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems. IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, 2010, 40, 419-428.	2.9	94
131	Authentication and Key Establishment in Dynamic Wireless Sensor Networks. Sensors, 2010, 10, 3718-3731.	3.8	31
132	Multiparty nonrepudiation. ACM Computing Surveys, 2009, 41, 1-43.	23.0	24
133	Concurrent access control for multi-user and multi-processor systems based on trust relationships. Concurrency Computation Practice and Experience, 2009, 21, 1389-1403.	2.2	0
134	Next generation wireless communications and mobile computing/networking technologies. Wireless Communications and Mobile Computing, 2009, 9, 441-443.	1.2	0
135	An Evolutionary Trust and Distrust Model. Electronic Notes in Theoretical Computer Science, 2009, 244, 3-12.	0.9	4
136	Secure multiparty payment with an intermediary entity. Computers and Security, 2009, 28, 289-300.	6.0	10
137	Integrating wireless sensor networks and the internet: a security analysis. Internet Research, 2009, 19, 246-259.	4.9	92
138	Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks. Lecture Notes in Computer Science, 2009, , 289-338.	1.3	68
139	Reusable security use cases for mobile grid environments. , 2009, , .		13
140	Security assurance during the software development cycle. Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing, 2009, , .	0.0	7
141	Delegating Privileges over Finite Resources: A Quota Based Delegation Approach. Lecture Notes in Computer Science, 2009, , 302-315.	1.3	1
142	Applying a UML Extension to Build Use Cases Diagrams in a Secure Mobile Grid Application. Lecture Notes in Computer Science, 2009, , 126-136.	1.3	6
143	Obtaining Security Requirements for a Mobile Grid System. International Journal of Grid and High Performance Computing, 2009, 1, 1-17.	0.9	8
144	Enabling Attribute Delegation in Ubiquitous Environments. Mobile Networks and Applications, 2008, 13, 398.	3.3	4

#	ARTICLE	IF	CITATIONS
145	Anonymity analysis in credentials-based systems: A formal framework. Computer Standards and Interfaces, 2008, 30, 253-261.	5.4	2
146	Situation awareness mechanisms for wireless sensor networks. , 2008, 46, 102-107.		35
147	KeyLED - transmitting sensitive data over out-of-band channels in wireless sensor networks. , 2008, , .		7
148	PSecGCM: Process for the Development of Secure Grid Computing based Systems with Mobile Devices. , 2008, , .		11
149	Fair Traceable Multi-Group Signatures. Lecture Notes in Computer Science, 2008, , 231-246.	1.3	19
150	An Asynchronous Node Replication Attack in Wireless Sensor Networks. International Federation for Information Processing, 2008, , 125-139.	0.4	3
151	A Workflow-Based Approach for Creating Complex Web Wrappers. Lecture Notes in Computer Science, 2008, , 396-409.	1.3	1
152	A Model for Trust Metrics Analysis. Lecture Notes in Computer Science, 2008, , 28-37.	1.3	17
153	A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks. Lecture Notes in Computer Science, 2008, , 120-132.	1.3	19
154	VI Conference on Telematics Engineering. IEEE Latin America Transactions, 2007, 5, 385-385.	1.6	0
155	A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks. , 2007, , .		42
156	International Cooperation to Fight Transnational Cybercrime. , 2007, , .		7
157	A versatile low-cost car plate recognition system. , 2007, , .		5
158	The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protection. Information Security Technical Report, 2007, 12, 24-31.	1.3	32
159	An effective multi-layered defense framework against spam. Information Security Technical Report, 2007, 12, 179-185.	1.3	6
160	On the deployment of a real scalable delegation service. Information Security Technical Report, 2007, 12, 139-146.	1.3	2
161	A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes. Mobile Networks and Applications, 2007, 12, 231-244.	3.3	85
162	Integration of non-repudiation services in mobile DRM scenarios. Telecommunication Systems, 2007, 35, 161-176.	2.5	4

#	ARTICLE	IF	CITATIONS
163	On the Protection and Technologies of Critical Information Infrastructures. Lecture Notes in Computer Science, 2007, , 160-182.	1.3	3
164	Anonymity 2.0 â€“ X.509 Extensions Supporting Privacy-Friendly Authentication. , 2007, , 265-281.		18
165	Featuring Trust and Reputation Management Systems for Constrained Hardware Devices. , 2007, , .		6
166	Delegation Services. , 2007, , 149-168.		0
167	Unleashing public-key cryptography in wireless sensor networks. Journal of Computer Security, 2006, 14, 469-482.	0.8	32
168	An anti-spam scheme using pre-challenges. Computer Communications, 2006, 29, 2739-2749.	5.1	16
169	Specification of a framework for the anonymous use of privileges. Telematics and Informatics, 2006, 23, 179-195.	5.8	14
170	Anonymous attribute certificates based on traceable signatures. Internet Research, 2006, 16, 120-139.	4.9	10
171	Graphical Representation of Authorization Policies for Weighted Credentials. Lecture Notes in Computer Science, 2006, , 383-394.	1.3	1
172	Attribute Delegation Based on Ontologies and Context Information. Lecture Notes in Computer Science, 2006, , 54-66.	1.3	1
173	A Synchronous Multi-Party Contract Signing Protocol Improving Lower Bound of Steps. , 2006, , 221-232.		5
174	Optimized multi-party certified email protocols. Information Management and Computer Security, 2005, 13, 350-366.	1.2	13
175	Specification and design of advanced authentication and authorization services. Computer Standards and Interfaces, 2005, 27, 467-478.	5.4	19
176	Security protocols analysis: A SDL-based approach. Computer Standards and Interfaces, 2005, 27, 489-499.	5.4	2
177	Protection Against Spam Using Pre-Challenges. IFIP Advances in Information and Communication Technology, 2005, , 281-293.	0.7	8
178	Why have public key infrastructures failed so far?. Internet Research, 2005, 15, 544-556.	4.9	40
179	A metadata-based access control model for web services. Internet Research, 2005, 15, 99-116.	4.9	15
180	Classifying Public Key Certificates. Lecture Notes in Computer Science, 2005, , 135-143.	1.3	5

#	ARTICLE	IF	CITATIONS
181	A Representation Model of Trust Relationships with Delegation Extensions. Lecture Notes in Computer Science, 2005, , 116-130.	1.3	11
182	A Novel Method to Maintain Privacy in Mobile Agent Applications. Lecture Notes in Computer Science, 2005, , 247-260.	1.3	2
183	Attacking an Asynchronous Multi-party Contract Signing Protocol. Lecture Notes in Computer Science, 2005, , 311-321.	1.3	3
184	Sorting out sorting through concretization with robotics. , 2004, , .		1
185	Agent-mediated non-repudiation protocols. Electronic Commerce Research and Applications, 2004, 3, 152-162.	5.0	10
186	PKI design based on the use of on-line certification authorities. International Journal of Information Security, 2004, 2, 91-102.	3.4	3
187	A framework for secure execution of software. International Journal of Information Security, 2004, 3, 99-112.	3.4	19
188	Non-repudiation protocols for multiple entities. Computer Communications, 2004, 27, 1608-1616.	5.1	13
189	Authentication and authorization infrastructures (AAs): a comparative survey. Computers and Security, 2004, 23, 578-590.	6.0	89
190	Nerve growth factor protects R2 cells against neurotoxicity induced by methamphetamine. Toxicology Letters, 2004, 150, 221-227.	0.8	3
191	A First Approach to Provide Anonymity in Attribute Certificates. Lecture Notes in Computer Science, 2004, , 402-415.	1.3	27
192	Analysis of e-commerce protocols: Adapting a traditional technique. International Journal of Information Security, 2003, 2, 21-36.	3.4	2
193	Integrating PMI services in CORBA applications. Computer Standards and Interfaces, 2003, 25, 391-409.	5.4	12
194	Virtual certificates and synthetic certificates: new paradigms for improving public key validation. Computer Communications, 2003, 26, 1826-1838.	5.1	8
195	BAAI: biometric authentication and authorization infrastructure. , 2003, , .		3
196	Towards a Business Process-Driven Framework for Security Engineering with the UML. Lecture Notes in Computer Science, 2003, , 381-395.	1.3	15
197	A secure solution for commercial digital libraries. Online Information Review, 2003, 27, 147-159.	3.2	7
198	A Multi-Party Non-Repudiation Protocol for Exchange of Different Messages. , 2003, , 37-48.		9

#	ARTICLE	IF	CITATIONS
199	Practical Service Charge for P2P Content Distribution. Lecture Notes in Computer Science, 2003, , 112-123.	1.3	5
200	How to Specify Security Services: A Practical Approach. Lecture Notes in Computer Science, 2003, , 158-171.	1.3	0
201	Security and Privacy in the Age of Uncertainty. , 2003, , .		2
202	Applying SDL to Formal Analysis of Security Systems. Lecture Notes in Computer Science, 2003, , 300-316.	1.3	0
203	Access Control Infrastructure for Digital Objects. Lecture Notes in Computer Science, 2002, , 399-410.	1.3	8
204	Secure Content Distribution for Digital Libraries. Lecture Notes in Computer Science, 2002, , 483-494.	1.3	3
205	XML-Based Distributed Access Control System. Lecture Notes in Computer Science, 2002, , 203-213.	1.3	10
206	A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI. Lecture Notes in Computer Science, 2002, , 136-149.	1.3	4
207	Design of a VPN Software Solution Integrating TCP and UDP Services. Lecture Notes in Computer Science, 2002, , 325-337.	1.3	0
208	Implementation of Virtual Private Networks at the Transport Layer. Lecture Notes in Computer Science, 1999, , 85-102.	1.3	1
209	Extending an OMA-based DRM Framework with Non-Repudiation Services. , 0, , .		1
210	On Secure Profiling. , 0, , .		1
211	Applying intrusion detection systems to wireless sensor networks. , 0, , .		136
212	Service-Oriented Security Architecture for CII based on Sensor Networks. , 0, , .		8
213	Secure Interoperability in Cyber-Physical Systems. Advances in Information Security, Privacy, and Ethics Book Series, 0, , 137-158.	0.5	8
214	PRoFIT: Modelo forense-IoT con integraci3n de requisitos de privacidad. , 0, , .		0
215	Identifying Secure Mobile Grid Use Cases. , 0, , 180-207.		0
216	Obtaining Security Requirements for a Mobile Grid System. , 0, , 247-260.		0