1.

Record Nr.	UNISA996466212103316
Titolo	Artificial Intelligence and Security [[electronic resource]] : 5th International Conference, ICAIS 2019, New York, NY, USA, July 26–28, 2019, Proceedings, Part IV / / edited by Xingming Sun, Zhaoqing Pan, Elisa Bertino
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-24268-4
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XVII, 651 p. 252 illus., 134 illus. in color.)
Collana	Security and Cryptology ; ; 11635
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer communication systems Application software Software engineering Computers Law and legislation Systems and Data Security Cryptology Computer Communication Networks Information Systems Applications (incl. Internet) Software Engineering Legal Aspects of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Encryption and Cybersecurity -- A Gray-Box Vulnerability Discovery Model based on Path Coverage -- Quantum Network Coding Based on Entanglement Distribution -- Moving Target Defense in Preventing SQL Injection -- Design and Security Analysis of Certificateless Aggregate Signature Scheme -- SuperEye: a Distributed Port Scanning System -- An Improved Multi-classification Algorithm for Imbalanced Online Public Opinion Data -- NCGs: Building A Trustworthy Environment to

Identify Abnormal Events Based on Network Connection Behavior Analysis -- Short Text Topic Recognition and Optimization Method for University Online Community -- A Survey on Network Traffic Identification -- A Survey of Network Security Situational Awareness Technology -- Multi-function Quantum Cryptography Protocol Based On Bell State -- The Attack Case of ECDSA on Blockchain based on Improved Simple Power Analysis -- A Weight-Based Channel Estimation Implementation Algorithm -- Multi-Party Quantum Communication Complexity on Composite Boolean-Valued Function -- BlockZone: A Blockchain-based DNS Storage and Retrieval Scheme -- Robust Analysis of Grid System Based on Complex Network Attack Mode -- A Secure Data Aggregation Protocol in VANETs based on Multi-key FHE -- Research on SQL Injection and Defense Technology -- A Review of the Factorization Problem of Large Integers -- A Comparison of Machine Learning Algorithms for Detecting XSS Attacks -- A Survey of Privacy-Preserving Techniques for Blockchain -- A Survey of Software Reverse Engineering Applications -- A Fast IP Matching Algorithm under Large Traffic -- An Effective Load Balance using Link Bandwidth for SDN-based Data Centers -- Zero-Day Vulnerability Risk Assessment and Attack Path Analysis Using Security Metric -- Research on Content Extraction of Rich Text Web Pages -- Network Protocol Analysis base on WeChat PC Version -- Bitcoin Network Size Estimation Based on Coupon Collection Model -- A Survey of the Software Vulnerability Discovery using Machine Learning Techniques -- A Distributed Cryptanalysis Framework based on Mobile Phones -- A Novel Threshold Signature Scheme Based on Elliptic Curve with designated verifier -- A Congestion Control Methodology with Probability Routing based on MNL for Datacenter Network -- Fast Failover for Link Failures in Software Defined Networks -- Steady-state Topology Discovery of Target Networks based on Statistics Method -- A Novel Method for Weighted Throughput Fairness in Contention-based WLANs with Multiple Priority Levels -- Bitcoin Node Discovery: Large-scale Empirical Evaluation of Network Churn -- DDoS Attack Situation Information Fusion Method Based on Dempster-Shafer Evidence Theory -- Webshell Detection Model based on Deep Learning -- A Security-Sensitive Function Mining Framework for Source Code -- Abstraction of Operations in Trusted Components Based on OR-transition Colored Petri Net -- Trusted Component Decomposition Based on OR-transition Colored Petri Net -- High-Speed File Transferring over Linux Bridge for QGA Enhancement in Cyber Range -- Playing First-Person-Shooter Games with A3C-Anticipator Network Based Agents using Reinforcement Learning -- Identify Influentials Based on User behavior Across Different Topics -- Taylor Series Localization Algorithm Based on Semi-definite Programming -- Research on Pedestrian Attribute Recognition Based on Semantic Segmentation in Natural Scene -- An evolving network model based on a triangular connecting mechanism for the Internet topology -- A new quantum private query protocol with better performance in resisting joint-measurement attack -- PPCSB:A Privacy-Preserving Electricity Consumption Statistics and Billing Scheme in Smart Grid -- Blockchain Private Key Storage Algorithm Based on Image Information Hiding -- Heuristic-Q: A Privacy Data Pricing Method Based on Heuristic Reinforcement Learning -- JPEGCNNA Transform Domain Steganalysis Model Based On Convolutional Neural Network -- Quantum algorithm for support vector machine with exponentially improved dependence on precision -- Reliability-based and QoS-aware Service Redundancy Backup Method in IoT-based Smart Grid -- A Privacy-Preserving Electricity Trading Scheme Based on Blockchain -- A Novel Facial Expression Recognition Scheme based on

Deep Neural Networks -- Active Defense System of Industrial Control System Based on Dynamic Behavior Analysis -- Research on Active Defense Technology of Smart Grid Control Terminal Based on Dynamic Trust.

Sommario/riassunto

The 4-volume set LNCS 11632 until LNCS 11635 constitutes the refereed proceedings of the 5th International Conference on Artificial Intelligence and Security, ICAIS 2019, which was held in New York, USA, in July 2019. The conference was formerly called “International Conference on Cloud Computing and Security” with the acronym ICCCS. The total of 230 full papers presented in this 4-volume proceedings was carefully reviewed and selected from 1529 submissions. The papers were organized in topical sections as follows: Part I: cloud computing; Part II: artificial intelligence; big data; and cloud computing and security; Part III: cloud computing and security; information hiding; IoT security; multimedia forensics; and encryption and cybersecurity; Part IV: encryption and cybersecurity.