1. Record Nr. UNINA9910580140303321

Titolo	Artificial Intelligence and Security : 8th International Conference, ICAIS 2022, Qinghai, China, July 15–20, 2022, Proceedings, Part III / / edited by Xingming Sun, Xiaorui Zhang, Zhihua Xia, Elisa Bertino
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-031-06791-6
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (744 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13340
Disciplina	006.3 005.8
Soggetti	Artificial intelligence Data protection Computer engineering Computer networks Artificial Intelligence Data and Information Security Computer Engineering and Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part III -- Encryption and Cybersecurity -- Research on Offense and Defense of DDos Based on Evolutionary Game Theory -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Hypothesis of the Evolutionary Game Model -- 3.2 Evolutionary Game Between Attackers and Defenders -- 3.3 Systematic Stability Analysis -- 4 System Simulation Analysis -- 5 Conclusion -- References -- A Method of Data Distribution and Traceability Based on Blockchain -- 1 Introduction -- 2 Relation -- 3 Risk Analysis, Workflow and Symbol Definition -- 3.1 Risk Analysis -- 3.2 Working Process -- 3.3 Symbol Definition -- 4 Blockchain Based Data Distribution Scheme -- 5 Data Tracing Schemes in Different Leak Scenarios -- 6 Total -- References -- Data Provenance in Large-Scale Distribution -- 1 Introduction -- 2 Related Work -- 3 Workflow and Notation -- 4 Provenance Model -- 4.1 Our Model -- 4.2 Fast

Method to Build Provenance Model -- 5 Implementation -- 5.1 Implementation on Electric Power System -- 5.2 Efficiency Analysis -- 6 Conclusions -- References -- A Vulnerability Detection Algorithm Based on Transformer Model -- 1 Introduction -- 2 Related Work -- 3 Method -- 3.1 Overall Structure -- 3.2 Node Set Generation -- 3.3 Data Dependence -- 3.4 Control Dependence -- 3.5 Feature Encode -- 3.6 Embedding Layer -- 3.7 Transformer -- 3.8 Attention Mechanism -- 3.9 Model Structure -- 4 Experiments -- 4.1 Dataset and Metrics -- 4.2 Experimental Results -- 5 Analysis of Valid Threads -- References -- Research on Video Falsity Detection Based on Publisher and Publishing Environment Features -- 1 Introduction -- 2 Related Work -- 2.1 Research on the Identification of False Information Publishers -- 2.2 Study of Disinformation Based on Environmental Characteristics -- 3 Methodology Model -- 3.1 Publisher Characteristics of the Video.
3.2 Environmental Characteristics of the Video -- 3.3 Model -- 4 Experiment and Analysis -- 4.1 Data Set -- 4.2 Video Falsity Test Based on Publisher Characteristics -- 4.3 Video Falsity Testing Based on Environmental Features -- 4.4 Experimental Results and Analysis -- 5 Conclusion -- References -- Intrusion Detection Model Based on KNN-AE-DNN -- 1 Introduction -- 2 Related Theory -- 2.1 Auto-encoder -- 2.2 Dense Neural Network -- 3 KNN-AE-DNN Model Design -- 3.1 Design Ideas and Overall Framework -- 3.2 Data Preprocessing -- 4 Experiment and Data Analysis -- 4.1 Experimental Data and Experimental Environment -- 4.2 Selection of Experimental Parameters -- 4.3 Experimental Result -- 5 Conclusion -- References -- A Framework for Unknown Traffic Identification Based on Neural Networks and Constraint Information -- 1 Introduction -- 2 Structure -- 3 Related Works -- 4 The Framework for Unknown Traffic Identification -- 4.1 Structure of the Framework -- 4.2 Deep Autoencoder for Features Extraction -- 4.3 GMM with Constraints -- 5 Experimental Methods and Results -- 5.1 Dataset -- 5.2 Dataset -- 5.3 A Subsection Sample -- 6 Conclusions -- References -- An Efficient Certificate-Based Encryption Scheme Without Random Oracles -- 1 Introduction -- 2 Preliminaries -- 2.1 Certificate-Based Encryption -- 2.2 One Time Authenticated Encryption -- 2.3 Bilinear Map and Hardness Assumption -- 3 Construction -- 4 Performance Comparison -- 5 Conclusion -- References -- A Rational Hierarchical Quantum State Sharing Protocol -- 1 Introduction -- 1.1 A Subsection Sample -- 2 Preliminaries -- 2.1 Quantum States and Quantum Operators -- 3 Rational Hierarchical Quantum State Sharing Protocol -- 3.1 Dealer's Protocol -- 3.2 Player's Protocol -- 4 Rubenstein Bargaining Model with Incomplete Information -- 4.1 Assumption -- 4.2 Solution -- 5 Analyses.
5.1 Utilities and Preferences -- 5.2 Security -- 5.3 Fairness -- 5.4 Correctness -- 5.5 Strict Nash Equilibrium -- 5.6 Comparison of Protocols -- 6 Conclusion -- References -- Blockchain-Based Efficient Incentive Mechanism in Crowdsensing -- 1 Introduction -- 2 Background -- 2.1 Blockchain -- 2.2 Crowdsensing System Model -- 2.3 Reverse Auction -- 3 Related Work -- 4 A Blockchain-Based Framework for Crowdsensing Incentives Mechanism -- 4.1 Posting Sensing Tasks -- 4.2 Select the Winning Bidder -- 4.3 Remuneration Allocation -- 5 System Analysis -- 5.1 Safety Analysis -- 5.2 Performance Analysis -- 5.3 Simulation Results and Analysis -- 6 Conclusion -- References -- BFAC-CS: A Blockchain-Based Fine-Grained Access Control Scheme for Complex Scenarios -- 1 Introduction -- 1.1 Contributions -- 1.2 Structure -- 2 Background -- 2.1 Blockchain -- 2.2 Access Control -- 3 Related Work -- 4 BFAC-CS

Scheme -- 4.1 System Model -- 4.2 Smart Contract -- 5 Security Analysis -- 5.1 Ultra Vires Attack Resistant -- 5.2 Collusion Attack Resistant -- 6 Implementation and Performance Analysis -- 7 Conclusion -- References -- Thoughts on the Application of Low-Interactive Honeypot Based on Raspberry Pi in Public Security Actual Combat, LIHRP -- 1 Opening Words -- 2 Introduction of Basic Information About Relevant Technologies -- 2.1 Raspberry Pi -- 2.2 Honeypot Technology -- 3 Environment Building -- 3.1 Build Pentbox Honey Pot -- 3.2 Build Hfish Honey Pot -- 3.3 Download the Docker -- 3.4 Pull the Mirror and Enter 'Docker Pull Imdevops/hfish' -- 4 Attack Demonstration and Log Analysis -- 4.1 Hfish Attack Demonstration and Log -- 4.2 Pentbox Attack Demonstration and Log -- 5 The Idea of Broadening the Data Collecting Range of Low Interaction Honeypot -- 5.1 Mixed Honeypot -- 5.2 Cloud Honeypot -- 5.3 Broadened Honeypot.
6 Thoughts on the Practical Application of Low Interaction Honeypot -- 6.1 Detecting Basic Network Attacks -- 6.2 Learning Network Defence Through Honeypot -- 6.3 Delay the Cyber Attack by Deploying a Large Number of Low-Interaction Honeypots -- 7 The End -- References -- Multi-objective Dual-Route Planning Algorithm for Grid Communication Network -- 1 Introduction -- 2 System Model and Problem Formulation -- 2.1 The Node Risk Model -- 2.2 The Link Risk Model -- 2.3 The Equilibrium Value of Network Risk -- 2.4 The End-to-End Delay -- 2.5 Constraints -- 3 Multi-objective Optimization Algorithm for Dual Routing Planning -- 3.1 Chromosome Encoding and Decoding -- 3.2 Selection, Crossover and Variation Operator -- 4 Simulation and Analysis -- 5 Conclusion -- References -- Blockchain Cross-Chain Research Based on Verifiable Ring Signatures -- 1 Introduction -- 2 Blockchain Cross-Chain Technology -- 2.1 Status of Cross-Chain Technology Research -- 2.2 Cross-Chain Technology Classification -- 3 Verifiable Ring Signature Cross-Chain Technology Model -- 3.1 Cross-Chain Model -- 3.2 Verifiable Ring Signature -- 3.3 Concurrent Signature -- 3.4 Cross-Chain Contract Deployment -- 3.5 Cross-Chain Chaincode Interface Design -- 3.6 Cross-Chain Transaction Process -- 3.7 Security Analysis -- 4 Analysis of Experimental Result -- 5 Conclusion -- References -- A Routing Algorithm for Node Protection in Wireless Sensor Network Based on Clustering Ant Colony Strategy -- 1 Introduction -- 2 Related Work -- 3 System Model and Problem Formulation -- 3.1 System Model -- 3.2 Energy Consumption Model -- 4 Routing Algorithm for Node protection in Wireless Sensor Network based on Clustering ant Colony Strategy -- 4.1 Cluster Head Selection -- 4.2 Node Protection Routing Between Clusters Based on Ant Colony Algorithm -- 5 Evaluation Analysis -- 6 Conclusion -- References.
Deep Learning Network Intrusion Detection Based on Network Traffic -- 1 Introduction -- 2 Background -- 2.1 Intrusion Detection Systems -- 2.2 Intrusion Detection Techniques -- 2.3 Neural Network Model -- 2.4 Related Works -- 3 Model Design -- 3.1 Introduction to the Dataset -- 3.2 Data Set Pre-processing -- 3.3 Intrusion Detection Model Design -- 4 Experimental Result -- 4.1 Simulation Experiments -- 4.2 Experimental Data -- 4.3 Experimental Results and Analysis -- 5 Conclusion -- References -- A Survey of Consensus Mechanism Based on Reputation Model -- 1 Introduction -- 1.1 Blockchain and Consensus Mechanism -- 1.2 Advantages of Reputation Consensus -- 2 Classification of Consensus Mechanisms Based on Reputation Models -- 2.1 Token Incentive -- 2.2 Concept Incentives -- 2.3 Double Incentive -- 2.4 No Incentive -- 3 Analysis of Evaluation Indicators of Reputation Consensus Performance -- 4 Security Analysis of Reputation Consensus -- 5 Conclusion -- References -- A Survey on Ethereum

Illicit Detection -- 1 Introduction -- 2 General Detection Technology for Illicit Transactions -- 2.1 Unsupervised Learning -- 2.2 Supervised Learning -- 3 Special Detection Technology for Illicit Transactions -- 3.1 Ponzi Scheme -- 3.2 Honeypot Contract -- 4 Trends and Challenges -- 4.1 Trends -- 4.2 Trends -- 5 Conclusion -- References -- Detect Adversarial Examples by Using Feature Autoencoder -- 1 Introduction -- 2 Proposed Approach -- 3 Experiments -- 3.1 Reconstruction Error Operations -- 3.2 Architectures -- 3.3 Generate Adversarial Examples -- 3.4 Detection Evaluation -- 4 Conclusion -- References -- Effect of Language Mixture on Speaker Verification: An Investigation with Amharic, English, and Mandarin Chinese -- 1 Introduction -- 2 The Yegna2021 Bilingual Speech Corpus -- 2.1 Building the Yegna2021 Bilingual Speech Corpus -- 3 Experiments and Findings.
3.1 Training Data Details.

Sommario/riassunto

This three-volume set LNCS 13338-13340 constitutes the thoroughly refereed proceedings of the 8th International Conference on Artificial Intelligence and Security, ICAIS 2022, which was held in Qinghai, China, in July 2022. The total of 166 papers included in the 3 volumes were carefully reviewed and selected from 1124 submissions. The papers present research, development, and applications in the fields of artificial intelligence and information security.