

| | |
|-------------------------|---|
| 1. Record Nr. | UNINA9910878050303321 |
| Autore | Huang De-Shuang |
| Titolo | Advanced Intelligent Computing Technology and Applications : 20th International Conference, ICIC 2024, Tianjin, China, August 5–8, 2024, Proceedings, Part IX // edited by De-Shuang Huang, Wei Chen, Jiayang Guo |
| Pubbl/distr/stampa | Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024 |
| ISBN | 981-9756-06-5 |
| Edizione | [1st ed. 2024.] |
| Descrizione fisica | 1 online resource (511 pages) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 14870 |
| Altri autori (Persone) | ChenWei GuoJiayang |
| Disciplina | 006.3 |
| Soggetti | Computational intelligence Machine learning Computer networks Application software Computational Intelligence Machine Learning Computer Communication Networks Computer and Information Systems Applications |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | Intro -- Preface -- Organization -- Contents - Part IX -- Information Security -- Non-targeted Adversarial Attacks on Object Detection Models -- 1 Introduction -- 2 Related Work -- 2.1 Adversarial Attacks Against Classification Models -- 2.2 Adversarial Attacks Against Object Detection Models -- 2.3 Targeted Attack and Non-targeted Attack -- 3 Generate Adversarial Examples -- 3.1 Overcoming the NMS Mechanism -- 3.2 UnTargeted Adversary -- 4 Experiment -- 4.1 Experiments Setup -- 4.2 Result on Object Detection Comparison with State-Of-The-Art Methods -- 4.3 The Denseness of Proposals -- 4.4 Perceptibility -- 5 Conclusion -- References -- Block Cipher Algorithms Identification Scheme Based on KFDA -- 1 Introduction -- 2 Related Work -- 3 Block Cipher Algorithm Identification Scheme -- 3.1 Block Cipher Algorithm Identification -- 3.2 Hamming Weight Based |

Ciphertext Feature Extraction Method -- 3.3 Data Mapping Based on Kernel Fisher Discriminant Analysis -- 4 Experimental Preparation -- 4.1 Data Mapping Based on Kernel Fisher Discriminant Analysis -- 4.2 Graded Result Evaluation Criteria -- 5 Evaluation and Comparison of Experimental Results -- 5.1 Experimental Results of Block Cipher with Fixed Keys -- 5.2 Experimental Results of Block Cipher with Random Keys -- 6 Conclusion -- References -- Network Traffic Intrusion Detection Strategy Based on E-GraphSAGE and LSTM -- 1 Introduction -- 2 Problem Description and Methodology -- 2.1 Problem Description -- 2.2 Framework -- 2.3 Data Processing -- 2.4 Traffic Graph Construction -- 2.5 E-GraphSAGE Layer -- 2.6 LSTM Layer -- 3 Experiments and Results Analysis -- 3.1 Dataset -- 3.2 Experimental Setup -- 3.3 Experimental Metrics -- 3.4 Analysis of Results -- 3.5 Ablation Experiments -- 4 Conclusion -- References -- A State of the Art Review on Artificial Intelligence-Enabled Cyber Security in Smart Grid. 1 Introduction -- 2 Related Works -- 2.1 Security Threats -- 2.2 Artificial Intelligence and Machine Learning -- 3 Network Security in Smart Grid -- 3.1 Security Countermeasures -- 3.2 Analyzing and Comparing -- 4 AI-Based Cyber Security -- 5 Conclusion -- References -- Reversible Data Hiding Based on Octree Partitioning and Arithmetic Coding in Encrypted Three-Dimensional Mesh Models -- 1 Introduction -- 2 Proposed Method -- 2.1 Pre-processing -- 2.2 Octree-Based Spatial Subdivision and Prediction Error Detection -- 2.3 Encryption -- 2.4 Data Embedding -- 2.5 Data Extraction and Mesh Recovery -- 3 Experimental Results and Analysis -- 3.1 Embedding Capacity Analysis -- 3.2 Performance Comparison -- 3.3 Model Restoration Quality Evaluation -- 4 Conclusion -- References -- A Differential Privacy Federated Learning Scheme with Improved Noise Perturbation -- 1 Introduction -- 2 Related Work -- 2.1 Federated Learning -- 2.2 Differential Privacy -- 3 Our Approach -- 3.1 Adjust Gradient Norm Clip Bound -- 3.2 Improved Noise Reduction -- 3.3 Privacy Cost Analysis -- 3.4 Improved Differential Privacy Federated Learning Algorithm -- 4 Experiment -- 4.1 Experiment Details -- 4.2 Private Cost -- 4.3 Accuracy -- 5 Conclusion -- References -- U-shaped Vertical Split Learning with Local Differential Privacy for Privacy Preserving -- 1 Introduction -- 2 System Design -- 2.1 Threat Model -- 2.2 System Model -- 3 Experiment -- 3.1 Experimental Settings -- 3.2 Experimental Results and Evaluation -- 4 Conclusion -- References -- An Intrusion Detection Method for Industrial Internet Fusing Multi-Scale TCN and Transformer Network -- 1 Introduction -- 2 Methodology -- 2.1 Overview of the Proposed Model -- 2.2 Improved Multi-scale Temporal Convolutional Network -- 2.3 Multiscale Patch Integrated Transformer -- 2.4 Parallel Branch Fusion -- 3 Results and Analysis. 3.1 Dataset Description -- 3.2 Evaluation Metrics -- 3.3 Implementation Details -- 3.4 Performance Comparison -- 3.5 Ablation Study -- 4 Conclusion -- References -- CSQF-BA: Efficient Container Query Technology for Cloud Security Query Framework with Bat Algorithm -- 1 Introduction -- 2 Related Work -- 2.1 Docker Applications and Docker Volume -- 2.2 Definition -- 3 Cloud Computing Security Query -- 4 Query Architecture with Docker Volume -- 5 Finding Algorithm in Volume -- 5.1 ACFA-BA, SFA-BA, and RFA-BA -- 5.2 Cloud Security Query Framework with Bat Algorithm (CSQF-BA) -- 6 Experiment -- 7 Conclusion -- References -- Full Database Reconstruction: Leakage-Abuse Attacks Based on Expected Distributions -- 1 Introduction -- 2 Model -- 2.1 Adversary Model -- 2.2 Reconstruction Attack -- 2.3 Edge Domain -- 3 Attack -- 3.1 Full

Ordering Reconstruction -- 3.2 Full Database Reconstruction -- 3.3 Adaptive Attack -- 4 Experiment -- 4.1 Full Ordering Reconstruction -- 4.2 Full Database Reconstruction -- 4.3 Adaptive Attack -- 5 Conclusion and Future Work -- References -- FedURL: A BERT-based Federated Malicious URL Detection Framework -- 1 Introduction -- 2 Methodology -- 2.1 Federated Learning -- 2.2 Parameter-Efficient Fine-Tuning -- 2.3 FedURL -- 3 Experiment -- 3.1 Dataset -- 3.2 Implementation and Setup -- 3.3 Model Performance -- 3.4 Performance and Network Traffic of Federated Learning with Different Training Parts -- 3.5 Performance Comparison with Varied Client Numbers -- 3.6 Analysis of Client Number Impact on Training strategy in Federated Learning -- 3.7 Performance Evaluation using Real-world Dataset -- 4 Results and Discussion -- References -- Show Criminals' True Color: Chinese Variant Toxic Text Restoration Based on Pointer-Generator Network -- 1 Introduction -- 2 Related Work -- 2.1 Variant Toxic Text Detection and Restoration. 2.2 Pointer Mechanism -- 3 Methodology -- 3.1 Sequence-To-Sequence Model -- 3.2 Pointer-Generator Networks -- 4 Experiments Settings -- 4.1 Datasets -- 4.2 Baselines -- 4.3 Evaluation Metric -- 5 Experiment Results and Analysis -- 5.1 Data Analysis and Variant Rules Extraction -- 5.2 Evaluation of Model Performance -- 5.3 Case Study -- 6 Conclusion -- References -- Adversarial Attacks on Network Intrusion Detection Systems Based on Federated Learning -- 1 Introduction -- 2 Adversarial Attack Scheme -- 2.1 Overview -- 2.2 Adversarial Sample Generation Method -- 2.3 Poisoning Attack Method -- 3 Experiment -- 3.1 Datasets and Evaluation Metrics -- 3.2 Experiment Results and Analysis -- 4 Conclusion -- References -- An EWMA-Based Mitigation Scheme Against Interest Flooding Attacks in Named Data Networks -- 1 Introduction -- 2 System Model -- 3 The Proposed EBMS -- 4 Performance Evaluation -- 4.1 Impacts of IFAs and bIFA on Network -- 4.2 Effectiveness of Attack Mitigation -- 5 Conclusions -- References. -- CAKGC: A Clustering Method of Cybercrime Assets Knowledge Graph Based on Feature Fusion -- 1 Introduction -- 2 Related Work -- 2.1 Detection Methods for Cybercrime Websites -- 2.2 Operation Chain of Cybercrime Underground Industry -- 2.3 Knowledge Graph Embedding -- 3 Methodology -- 3.1 Construction of Cybercrime Assets Knowledge Graph -- 3.2 Clustering of Cybercrime Assets Knowledge Graph -- 4 Experiment -- 4.1 Dataset -- 4.2 Evaluation Metrics -- 4.3 Comparison Algorithms -- 4.4 Experimental Results -- 5 Conclusion -- References -- Multi-texture Fusion Attack: A Robust Adversarial Camouflage in Physical World -- 1 Introduction -- 2 Related Work -- 2.1 Physical Camouflage Attack -- 3 Method -- 3.1 The Definition of Problem -- 3.2 Framework Overview -- 3.3 Generate Adversarial Camouflage -- 3.4 Expectation Over Transformation. 3.5 Physical Transformation -- 4 Experiment -- 4.1 Experimental Setting -- 4.2 Adversarial Attack in the Digital Space -- 4.3 Adversarial Attack in the Physical Space -- 4.4 Ablation Studies -- 5 Conclusion -- References -- When Blockchain Meets Asynchronous Federated Learning -- 1 Introduction -- 2 Categorization Based on Blockchain Extensions -- 2.1 Blockchain Based on Directed Acyclic Graph -- 2.2 Traditional Blockchain -- 3 Categorization Based on Coupling Approaches -- 3.1 Fully Coupled BCFL -- 3.2 Flexibly Coupled BCFL -- 3.3 Loosely Coupled BCFL -- 4 Challenges and Future Directions -- 5 Conclusion -- References -- A High-Dimensional Data Trust Publishing Method Based on Attention Mechanism and Differential Privacy -- 1 Introduction -- 2 Preliminaries -- 2.1 Differential Privacy -- 2.2 Attention Mechanism -- 3 AMPriv Method -- 3.1 ACHD -- 3.2 NAS --

3.3 NMEGreedybayes -- 3.4 NMENoisyConditionals -- 3.5 Sampling --
4 Experiments -- 4.1 Experimental Environment and Setup -- 4.2
Method Performance Analysis -- 4.3 Data Availability Analysis -- 5
Conclusion -- References -- PTGroup: An Automated Penetration
Testing Framework Using LLMs and Multiple Prompt Chains -- 1
Introduction -- 2 Related Work -- 2.1 Penetration Testing -- 2.2
Autonomous Agents -- 3 Methodology -- 3.1 Thought-Act-Observe
Loop -- 3.2 Multi-agent Framework -- 3.3 Multiple Prompt Chains -- 4
Experiments -- 4.1 Experimental Environment -- 4.2 Results
and Discussion -- 5 Conclusion -- References -- Spammer Group
Detection Approach Based on Deep Reinforcement Learning -- 1
Introduction -- 2 Related Work -- 2.1 Group Behavior-Based
Approaches -- 2.2 Graph-Based Approaches -- 3 The Proposed
Detection Method DRL-AE -- 3.1 Obtaining the Initial User Node
Embeddings -- 3.2 Generating the Candidate Groups -- 3.3 Detecting
Spammer Groups -- 4 Experiments -- 4.1 Experiments Datasets.
4.2 Evaluation Metrics.

Sommario/riassunto

This 13-volume set LNCS 14862-14874 constitutes - in conjunction with the 6-volume set LNAI 14875-14880 and the two-volume set LNBI 14881-14882 - the refereed proceedings of the 20th International Conference on Intelligent Computing, ICIC 2024, held in Tianjin, China, during August 5-8, 2024. The total of 863 regular papers were carefully reviewed and selected from 2189 submissions. This year, the conference concentrated mainly on the theories and methodologies as well as the emerging applications of intelligent computing. Its aim was to unify the picture of contemporary intelligent computing techniques as an integral concept that highlights the trends in advanced computational intelligence and bridges theoretical research with applications. Therefore, the theme for this conference was "Advanced Intelligent Computing Technology and Applications". Papers that focused on this theme were solicited, addressing theories, methodologies, and applications in science and technology. .
