1. Security Analysis of a Certificateless Provable Data Possession Scheme in Cloud
   Year: 2019 | Volume: 7 | Journal Article | Publisher: IEEE

2. Research on Intelligence Computing Models of Fine-Grained Opinion Mining in Online Reviews
   Published in: IEEE Access (Volume: 7)

3. Secure and energy efficient data aggregation method – MSACCESS DATABASE
   IEEE Access | Year: 2019 | Volume: 7

4. Input Feature Selection Method Based on Feature Set Equivalence and Mutual Information Gain Maximization
   IEEE Access 17 October 2019

5. Data hiding for ensuring the quality of the host image and the security of the message

6. Locating multiple license plates using scale, rotation, and colour-independent clustering and filtering techniques– DOTNET VS2013
   IET Image Processing year: 17 October 2019

7. An Evaluation of Bitcoin Address Classification based on Transaction History Summarization

8. Training Back Propagation Neural Networks in Map-Reduce on High-Dimensional Big Datasets with Global Evolution

9. Real-Time Detection of Apple Leaf Diseases Using Deep Learning Approach Based on Improved Convolutional Neural Network
   IEEE Access year: 06 may 2019

10. Challenges and Recommended Solutions in Multi-Source and Multi-Domain Sentiment Analysis IEEE access 03 oct 2019

11. Customer Reviews Analysis with Deep Neural Networks for E-Commerce Recommender Systems
12. A Data-Driven Approach for Accurate Rainfall Prediction - IEEE Access
10 July 2017


14. Commutative Encryption and Data Hiding in HEVC Video Compression
Published in: IEEE Access (Volume: 7), 2019

15. A SQL Injection Detection Method Based on Adaptive Deep Forest
Published in: IEEE Access (Volume: 7), 2019

Published in: IEEE Access (Volume: 7), 2019

17. Survey on Prediction of Smartphone Virality Using Twitter Analytics


19. Challenges and Recommended Solutions in Multi-Source and Multi-Domain Sentiment Analysis.

CLOUD COMPUTING

1. V-Matrix-Based Scalable Data Aggregation Scheme in WSN.

2. Dynamic Demand Prediction and Allocation in Cloud Service Brokerage.

3. Towards AI-Powered Multiple Cloud Management.


5. A New Encrypted Data Switching Protocol: Bridging IBE and ABE Without Loss of Data Confidentiality

6. An Attribute-Based Controlled Collaborative Access Control Scheme for Public Cloud Storage
7. CHARON: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data
8. Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud
10. Fast Boolean Queries With Minimized Leakage for Encrypted Databases in Cloud Computing
11. FS-PEKS: Lattice-based Forward Secure Public-key Encryption with Keyword Search for Cloud-assisted Industrial Internet of Things.
13. The Soft Underbelly of Cloud Security
14. Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage

15. Delegated Authorization Framework for HER Services using Attribute Based Encryption
17. Data Integrity Auditing without Private Key Storage for Secure Cloud Storage
18. Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage
19. Privacy-Preserving Multi-keyword Top-k Similarity Search Over Encrypted Data
20. Provably Secure Fine-Grained Data Access Control over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications
21. Revocable Identity-Based Broadcast Proxy Re-encryption for Data Sharing in Clouds
22. Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT
23. Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification
27. A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services
28. Hybrid Keyword-Field Search with Efficient Key Management for Industrial Internet of Things
29. An Attribute-based Controlled Collaborative Access Control Scheme for Public Cloud Storage
30. Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud
31. Delegated Authorization Framework for HER Services using Attribute Based Encryption
32. Dynamic Multi-Keyword Ranked Search Based on Bloom Filter Over Encrypted Cloud Data
33. Enabling Authorized Encrypted Search for Multi-Authority Medical Databases
34. Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage
35. Enabling Verifiable and Dynamic Ranked Search Over Outsourced Data
36. Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems
37. Hidden Ciphertext Policy Attribute-Based Encryption With Fast Decryption for Personal Health Record System
38. P-MOD: Secure Privilege-Based Multilevel Organizational Data Sharing in Cloud Computing
39. Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting
40. Privacy-Preserving Multi-keyword Top-k Similarity Search Over Encrypted Data
41. Profit Maximization for Cloud Brokers in Cloud Computing
42. Provable Data Possession with Outsourced Data Transfer
43. Provably Secure Fine-Grained Data Access Control over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications
44. Revocable Identity-Based Broadcast Proxy Re-encryption for Data Sharing in Clouds
45. Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing
46. Privacy Preserving Searchable Encryption with Fine-grained Access Control
47. Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT
48. Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification.
50. Enabling Authorized Encrypted Search for Multi-Authority Medical Databases.

51. Privacy-Preserving Attribute-Based Keyword Search in Shared Multiowner.

52. Privacy-Preserving Multi-keyword Top-k Similarity Search Over Encrypted Data.

DATA MINING

1. A Novel Load Image Profile-Based Electricity Load Clustering Methodology.

2. Predicting the Impact of Android Malicious Samples via Machine Learning.

3. Network Representation Learning Enhanced Recommendation Algorithm

4. DCCR: Deep Collaborative Conjunctive Recommender for Rating Prediction

5. Motion Based Inference of Social Circles via Self-Attention and Contextualized Embedding.

6. Composition Context-Based Web Services Similarity Measure.

7. Neural Binary Representation Learning for Large-Scale Collaborative Filtering.

8. Clustering-Based Collaborative Filtering Using an Incentivized/Penalized User Model.


12. BD2K Training Coordinating Center's ERuDItc: the Educational Resource Discovery Index.
13. A Particle Swarm Optimized Learning Model of Fault Classification in Web-Apps
14. Mining Users Trust From E-Commerce Reviews Based on Sentiment Similarity Analysis.
15. Old and Young Users’ White Space Preferences for Online News Web Pages.
17. Analysis and Accurate Prediction of User’s Response Behavior in Incentive-Based Demand.

**DATA MINING**

20. Hierarchical Multi-Clue Modelling for POI Popularity Prediction with Heterogeneous Tourist Information.
21. Peer Prediction Based Trustworthiness Evaluation and Trustworthy Service Rating in Social Networks
22. Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation
23. Predicting Consumption Patterns with Repeated and Novel Events
24. Trust Relationship Prediction in Alibaba E-Commerce Platform
25. Achieving Data Truthfulness and Privacy Preservation in Data Markets
26. Active Online Learning for Social Media Analysis to Support Crisis Management
27. An Efficient Method for High Quality and Cohesive Topical Phrase Mining
28. Ant Colony Stream Clustering: A Fast Density Clustering Algorithm for Dynamic Data Streams
29. Collaboratively Tracking Interests for User Clustering in Streams of Short Texts
30. Detecting Pickpocket Suspects from Large-Scale Public Transit Records
31. Finding Optimal Skyline Product Combinations under Price Promotion
32. Heterogeneous Information Network Embedding for Recommendation
33. Hierarchical Multi-Clue Modelling for POI Popularity Prediction with Heterogeneous Tourist Information
34. Learning Customer Behaviors for Effective Load Forecasting
35. 1-Injection: Toward Effective Collaborative Filtering Using Uninteresting Items
36. Multi-Party High-Dimensional Data Publishing under Differential Privacy
37. Normalization of Duplicate Records from Multiple Sources
38. Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation
39. Secure and Efficient Skyline Queries on Encrypted Data

MACHINE LEARNING
42. Competitive Bike: Competitive Analysis and Popularity Prediction of Bike-Sharing Apps Using Multi-Source Data
43. Discovering the Type 2 Diabetes in Electronic Health Records using the Sparse Balanced Support Vector Machine
44. Location Inference for Non-geotagged Tweets in User Timelines
45. Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation
46. SentiDiff: Combining Textual Information and Sentiment Diffusion Patterns for Twitter Sentiment Analysis
47. Sentiment Classification using N-gram IDF and Automated Machine Learning
48. Serendipity—A Machine-Learning Application for Mining Serendipitous Drug Usage from Social Media
49. Spammer Detection and Fake User Identification on Social Networks
50. Crop Yield Prediction and Efficient use of Fertilizers
51. Mining Users Trust From E-Commerce Reviews Based on Sentiment Similarity Analysis

**SECURE COMPUTING**

1. Traffic Analysis Attack for Identifying Users’ Online Activities.
2. Coverless Information Hiding Method Based on Web Text.
4. A Lightweight Privacy-Preserving CNN Feature Extraction Framework for Mobile Sensing
5. LBOA: Location-Based Secure Outsourced Aggregation in IoT.

**SECURE COMPUTING**

9. A Probabilistic Source Location Privacy Protection Scheme in Wireless Sensor Networks
10. Achieving Data Truthfulness and Privacy Preservation in Data Markets
11. Collusion Defender: Preserving Subscribers’ Privacy in Publish and Subscribe Systems
12. Dating with Scambots: Understanding the Ecosystem of Fraudulent Dating Applications
13. Efficient and Privacy-preserving Online Fingerprint Authentication Scheme Over Outsourced Data
14. Scalable Access Control For Privacy-Aware Media Sharing
15. Searchable Symmetric Encryption with Forward Search Privacy
16. Secure Channel Free Certificate-Based Searchable Encryption Withstanding Outside and Inside Keyword Guessing Attacks
17. Sensitive Label Privacy Preservation with Anatomization for DataPublishing
18. Enabling Efficient and Geometric Range Query with Access Control over Encrypted Spatial Data.
20. Dating with Scambots: Understanding the Ecosystem of Fraudulent Dating Applications
22. Authenticated Medical Documents Releasing with Privacy Protection and Release Control
23. Collusion Defender: Preserving Subscribers’ Privacy in Publish and Subscribe Systems
24. Dating with Scambots: Understanding the Ecosystem of Fraudulent Dating Applications
25. Detecting Malicious Social Bots Based on Clickstream Sequences
26. Privacy-Preserving Aggregate Queries for Optimal Location Selection
27. Sensitive Label Privacy Preservation with Anatomization for DataPublishing

MOBILE COMPUTING

1. ooDNet: Toward an Optimized Food Delivery Network based on Spatial Crowdsourcing.

**BLOCKCHAIN TECHNOLOGY**

1. PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Towards Mass Storage Management.
2. Blockchain for AI: Review and Open Research Challenges.
3. Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors.

**PATTERN ANALYSIS AND MACHINE INTELLIGENCE**

4. End-to-end Active Object Tracking and Its Real-world Deployment via Reinforcement Learning.

**BIG DATA**

2. Effective and Efficient Content Redundancy Detection of Web Videos.
3. Incorporating Data Context to Cost-Effectively Automate End-to-End Data Wrangling.
4. Sentiment Analysis of Comment Texts Based on BiLSTM.
5. Data Interpolation and Reconstruction.

**SOCIAL NETWORK, IMAGE PROCESSING**

2. Social Network Rumor Diffusion Predication Based on Equal Responsibility Game Model.
3. Fundamental Visual Concept Learning from Correlated Images and Text.

**SOCIAL NETWORK**

1. Credibility Evaluation of Twitter-Based Event Detection by a Mixing Analysis of Heterogeneous Data
2. Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges
3. Spammer Detection and Fake User Identification on Social Networks.
4. Trust-based Privacy-Preserving Photo Sharing in Online Social Networks.
5. Who You Should Not Follow: Extracting Word Embeddings from Tweets to Identify Groups of Interest and Hijackers in Demonstrations
6. Spammer Detection and Fake User Identification on Social Networks
7. A Fuzzy Approach to Text Classification With Two-Stage Training for Ambiguous Instances
8. Conversational Networks for Automatic Online Moderation
9. Credibility Evaluation of Twitter-Based Event Detection by a Mixing Analysis of Heterogeneous Data
10. Filtering Instagram hashtags through crowdtagging and the HITS Algorithm
11. Minimizing Influence of Rumors by Blockers on Social Networks: Algorithms and Analysis
12. Online Public Shaming on Twitter: Detection, Analysis, and Mitigation
13. PersoNet: Friend Recommendation System Based on Big-Five Personality Traits and Hybrid Filtering
14. Predicting Cyberbullying on Social Media in the Big Data Era
16. Spammer Detection and Fake User Identification on Social Networks
17. Trust-based Collaborative Privacy Management in Online Social Networks
18. Trust-based Privacy-Preserving Photo Sharing in Online Social Networks

**IMAGE PROCESSING**

19. New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams
20. Towards Robust Image Steganography

**SOFTWARE ENGINEERING, SERVICE COMPUTING**


**SERVICE COMPUTING**

1. Transactional Behavior Verification in Business Process as a Service Configuration
2. Building and Querying an Enterprise Knowledge Graph
3. Transactional Behavior Verification in Business Process as aService
   Configuration

**FUZZY SYSTEM, INDUSTRIAL INFORMATICS**

1. Epistasis Analysis Using an Improved Fuzzy C-means-based Entropy Approach
2. Intelligent Security Planning for Regional Distributed Energy Internet

**INFORMATION FORENSICS AND SECURITY**

1. Authentication by Encrypted Negative Password
2. Enabling Efficient and Geometric Range Query with AccessControl over Encrypted Spatial Data
4. Secure Key Agreement and Key Protection for Mobile Device User Authentication

**BIG DATA**

1. AccountTrade: Accountability Against Dishonest Big Data Buyers and Sellers
2. Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques
3. Leveraging Product Characteristics for Online Collusive Detection in Big Data Transactions
4. A Survey on Geographically Distributed Big-Data Processing using MapReduce
5. A Systematic Approach Toward Description and Classification of Cybercrime Incidents
6. Deadline-aware MapReduce Job Scheduling with Dynamic Resource Availability
7. Hadoop MapReduce for Mobile Clouds
8. Handling Big Data Using a Data-Aware HDFS and Evolutionary Clustering Technique
9. Hierarchical Density-Based Clustering using MapReduce
11. On Scalable and Robust Truth Discovery in Big Data Social Media Sensing Applications
12. PISCES: Optimizing Multi-job Application Execution in MapReduce
13. Practical Privacy-Preserving MapReduce Based K-means Clustering over Large-scale Dataset
14. Robust Big Data Analytics for Electricity Price Forecasting in the Smart Grid
15. A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era
16. AccountTrade: Accountability Against Dishonest Big Data Buyers and Sellers
17. Fast Communication-efficient Spectral Clustering Over Distributed Data

1. Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques
2. A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things
3. Toward a Lightweight Intrusion Detection System for the Internet of Things
4. Secure Cloud Storage Service Using Bloom Filters for the Internet of Things
5. A Scalable Blockchain Framework for Secure Transactions in IoT

ARTIFICIAL INTELLIGENCE

1. Collaborative Filtering-based Electricity Plan Recommender System

NETWORKING

1. Secure and energy aware load balancing framework for cloud data centre networks.