# Table of Contents

| Message from the TrustCom 2014 General Chairs | xvii |
| Message from the TrustCom 2014 Program Chairs | xviii |
| Message from the TrustCom 2014 Steering Chairs | xix |
| Message from the TrustCom 2014 Workshop/Symposium Chairs | xx |
| Message from the BDSE 2014 Chairs | xxi |
| Message from the EFINS 2014 Workshop Chairs | xxii |
| Message from the SpaIoT 2014 Symposium Chairs | xxiii |
| Message from the NOPE 2014 Workshop Chairs | xxiv |
| Message from the UbiSafe 2014 Symposium Chairs | xxv |
| Message from the TSCloud 2014 Symposium Chairs | xxvi |
| Message from the SPMBB 2014 Workshop Chairs | xxvii |
| TrustCom 2014 Organizing and Program Committees | xxviii |
Privacy in Mobile & Wireless Networks

A Clustering-Based Privacy-Preserving Method for Uncertain Trajectory Data ........................................... 1
   Zhou-Fu Cai, He-Xing Yang, Wang Shuang, Xu Jian, Wang-Ming Wei, and Wu-Li Na

A Lightweight Anonymous Mobile Shopping Scheme Based on DAA for Trusted Mobile Platform .................................................. 9
   Bo Yang, Dengguo Feng, and Yu Qin

Automated User Profiling in Location-Based Mobile Messaging Applications ............................................... 18
   Yao Cheng, Chang Xu, Yi Yang, Lingyun Ying, Purui Su, and Dengguo Feng

PrivateDroid: Private Browsing Mode for Android ........................................................................... 27
   Su Mon Kywe, Christopher Landis, Yutong Pei, Justin Satterfield, Yuan Tian, and Patrick Tague

TTPCookie: Flexible Third-Party Cookie Management for Increasing Online Privacy ........................................... 37
   Ashar Javed, Christian Merz, and Joerg Schwenk
Privacy and Trust in Social Networks

Adaptive Sharing for Online Social Networks: A Trade-off Between Privacy Risk and Social Benefit .................................................................45
Mu Yang, Yijun Yu, Arosha K. Bandara, and Bashar Nuseibeh

Garbling in Reverse Order .................................................................53
Tommi Meskanen, Valtteri Niemi, and Noora Nieminen

Private Outsourcing of Polynomial Functions .....................................61
Peili Li, Haixia Xu, and Jiaqi Hong

A Machine Learning Based Trust Evaluation Framework for Online Social Networks .................................................................................69
Kang Zhao and Li Pan

Multi-dimensions of Developer Trustworthiness Assessment in OSS Community ...............................................................................................75
Yu Bai, Gang Yin, and Huaimin Wang

Security Algorithms

A Novel Feature Selection Approach for Intrusion Detection Data Classification ........................................82
Mohammed A. Ambusaidi, Xiangjian He, Zhiyuan Tan, Priyadarsi Nanda, Liang Fu Lu, and Upasana T. Nagar

An On-Line Anomaly Detection Method Based on a New Stationary Metric - Entropy-Ratio .................................................................90
Ziyu Wang, Jiahai Yang, and Fuliang Li

Reaching Agreement in Security Policy Negotiation ................................98
Yanhuang Li, Nora Cuppens-Boulahia, Jean-Michel Crom, Frédéric Cuppens, and Vincent Frey

Remembrance of Local Information Status for Enforcing Robustness of Policy-Exchanged Strategies for Trust Negotiation ..........................106
Yunxi Zhang and Darren Mundy

Secure and Privacy-Friendly Public Key Generation and Certification .........................................................................................114
Fábio Borges, Leonardo A. Martucci, Filipe Beato, and Max Mühlhäuser

Security Applications

A Stateful Mechanism for the Tree-Rule Firewall ........................................122
Thawatchai Chomsiri, Xiangjian He, Priyadarsi Nanda, and Zhiyuan Tan

CAFS: A Framework for Context-Aware Federated Services ..........................130
Md. Sadek Ferdous and Ron Poet
Encrypted Keyword Search Mechanism Based on Bitmap Index for Personal Storage Services .................................................................140
   Yong Ho Hwang, Jae Woo Seo, and Il Joo Kim

High Performance FPGA Implementation of Elliptic Curve Cryptography over Binary Fields ........................................................................148
   Shuai Liu, Lei Ju, Xiaojun Cai, Zhiping Jia, and Zhiyong Zhang

A High-Performance Distributed Certificate Revocation Scheme for Mobile Ad Hoc Networks .................................................................156
   Chongxian Guo, Huaqiang Xu, Lei Ju, Zhiping Jia, and Jihai Xu

**Security Systems**

SIMS: A Comprehensive Approach for a Secure Instant Messaging Sifter ............................................................................................164
   Günter Fahrnberger

Towards Designing an Email Classification System Using Multi-view Based Semi-supervised Learning ................................................................174
   Wenjuan Li, Weizhi Meng, Zhiyuan Tan, and Yang Xiang

Ultra High-Speed SM2 ASIC Implementation .................................................................................................................................182
   Zhenwei Zhao and Guoqiang Bai

Visual Similarity Based Anti-phishing with the Combination of Local and Global Features ........................................................................189
   Yu Zhou, Yongzheng Zhang, Jun Xiao, Yipeng Wang, and Weiyao Lin

A Practically Optimized Implementation of Attribute Based Cryptosystems .............................................................................................197
   Chunqiang Hu, Fan Zhang, Tao Xiang, Hongjuan Li, Xiao Xiao, and Guilin Huang

**Authentication**

A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment ..................................................................205
   Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Zhiyuan Tan, and Ren Ping Liu

Bargaining-Based Dynamic Decision for Cooperative Authentication in MANETs ...................................................................................212
   Liu Licai, Yin Lihua, Guo Yunchuan, and Fang Bingxing

Multiplicative Attributes Graph Approach for Persistent Authentication in Single-Sign-On Mobile Systems ................................................221
   Uthpala Subodhani Premarathne and Ibrahim Khalil

ToAuth: Towards Automatic Near Field Authentication for Smartphones ...............................................................................................229
   Weixi Gu, Zheng Yang, Longfei Shangguan, Xiaoyu Ji, and Yiyang Zhao

One Kind of Cross-Domain DAA Scheme from Bilinear Mapping ........................................................................................................237
   Xiaoming Wang, Heyou Cheng, and Ruihua Zhang
Attack & Defense

Long Term Tracking and Characterization of P2P Botnet .................................................................244
   Jia Yan, Lingyun Ying, Yi Yang, Purui Su, and Dengguo Feng

A Survey of Security Network Coding toward Various Attacks .................................................................252
   Shixiong Yao, Jing Chen, Ruiying Du, Lan Deng, and Chiheng Wang

   Xuerui Pan, Yibing Zhongyang, Zhi Xin, Bing Mao, and Hao Huang

Public-Key Encryption Resilient against Linear Related-Key Attacks Revisited ......................................268
   Hui Cui, Yi Mu, and Man Ho Au

The Micro-architectural Support Countermeasures against the Branch Prediction Analysis Attack .................................................................276
   Ya Tan, Jizeng Wei, and Wei Guo

Security and Trust in Cloud Computing (1)

AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security .................................................................284
   Ahmed Taha, Ruben Trapero, Jesus Luna, and Neeraj Suri

Efficiently Attribute-Based Access Control for Mobile Cloud Storage System ........................................292
   Zhiquan Lv, Jialin Chi, Min Zhang, and Dengguo Feng

EqualVisor: Providing Memory Protection in an Untrusted Commodity Hypervisor .................................................................300
   Liang Deng, Qingkai Zeng, Weiguang Wang, and Yao Liu

FEACS: A Flexible and Efficient Access Control Scheme for Cloud Computing ........................................310
   Yu Zhang, Jing Chen, Ruiying Du, Lan Deng, Yang Xiang, and Qing Zhou

ONHelp: Components in Building Secure Cloud Based on OpenNebula .........................................................320
   Kao Zhao, Hai Jin, Deqing Zou, and Weiqi Dai

Security and Trust in Cloud Computing (2)

Proofs of Ownership and Retrievability in Cloud Storage .................................................................328
   Ruiying Du, Lan Deng, Jing Chen, Kun He, and Minghui Zheng

Temporal Access Control with User Revocation for Cloud Data .................................................................336
   Nihal Balani and Sushmita Ruj

Trust Enhanced Cloud Security for Healthcare Services .................................................................344
   Udaya Tupakula and Vijay Varadharajan

Trusted Geolocation-Aware Data Placement in Infrastructure Clouds .................................................................352
   Nicolae Paladi, Mudassar Aslam, and Christian Gehrmann
Trust-Enhanced Multicast Routing Protocol Based on Node's Behavior
Assessment for MANETs ...............................................................................................................................................473
Hui Xia, Jia Yu, Zhi-Yong Zhang, Xiang-Guo Cheng, and Zhen-Kuan Pan

BIBRM: A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks .................................................................481
Guanghao Wang and Yue Wu

Trust Modeling and Algorithms
Convergence of True Cooperations in Bayesian Reputation Game .................................................................487
Jooyoung Lee and Jae C. Oh

Practical Assessment of Biba Integrity for TCG-Enabled Platforms ..................................................................495
Roberto Sassu, Gianluca Ramunno, and Antonio Lioy

SigmoRep: A Robust Reputation Model for Open Collaborative Environments ........................................505
Ahmad A. Kardan, Reza Salarmehr, and Azade Farshad

Towards Robust and Effective Trust Management for Security: A Survey ......................................................511
Dongxia Wang, Tim Muller, Yang Liu, and Jie Zhang

Trust Mechanism for Enforcing Compliance to Secondary Data Use Contracts ...........................................519
Zeinab Noorian, Johnson Iyilade, Mohsen Mohkami, and Julita Vassileva

Trust Applications and Systems
An Effective Path Load Balancing Mechanism Based on SDN ..................................................................527
Jun Li, Xiangqing Chang, Yongmao Ren, Zexin Zhang, and Guodong Wang

Integrity Levels: A New Paradigm for Protecting Computing Systems ..........................................................534
Christopher Jenkins and Lyndon Pierson

Integrity Verification and Secure Loading of Remote Binaries
for Microkernel-Based Runtime Environments ..................................................................................................544
Michael Weiß, Steffen Wagner, Roland Hellman, and Sascha Wessel

Overhead-Free In-Place Recovery Scheme for XOR-Based Storage Codes ................................................552
Ximing Fu, Zhiqing Xiao, and Shenghao Yang

Untrusted User Detection in Microblogs ...........................................................................................................558
Zidan Yu and Huiqun Yu

Identity Management Systems and Mechanism
A Privacy-Enhanced Access Log Management Mechanism in SSO Systems
from Nominative Signatures ...............................................................................................................................565
Sanami Nakagawa, Keita Emura, Goichiro Hanaoka, Akihisa Kodate, Takashi Nishide, Eiji Okamoto, and Yusuke Sakai

Anonymous Proxy Signature with Restricted Traceability .......................................................................................575
Jiannan Wei, Guomin Yang, and Yi Mu
Efficient Traceable Attribute-Based Signature .................................................................582
   Shenglong Ding, Yiming Zhao, and Yuyang Liu

Computation Integrity Measurement Based on Branch Transfer ........................................590
   Jianming Fu, Yan Lin, Xu Zhang, and Pengwei Li

Emergency Key Rollover in DNSSEC ..................................................................................598
   Zheng Wang and Liyuan Xiao

Social Networking with Big Data
Crowd Sensing of Urban Emergency Events Based on Social Media Big Data .......................605
   Zheng Xu, Hui Zhang, Yunhuai Liu, and Lin Mei

SocAware: A Middleware for Social Applications in Online Social Networks .........................611
   Liang Chen, Kan Chen, Chengcheng Shao, and Peidong Zhu

Secure Multimedia Big Data Sharing in Social Networks Using Fingerprinting and Encryption in the JPEG2000 Compressed Domain .........................................................616
   Conghuan Ye, Zenggang Xiong, Yaoming Ding, Jiping Li, Guangwei Wang,
   Xuemin Zhang, and Kaibing Zhang

A Proposal for a Reference Architecture for Long-Term Archiving, Preservation, and Retrieval of Big Data ..............................................................................................................622
   Phillip Viana and Liria Sato

Big Data Analyses for Collective Opinion Elicitation in Social Networks .........................630
   Yingxu Wang and Victor J. Wiebe

Big Data Storage
An Improved Image File Storage Method Using Data Deduplication ........................................638
   Zhou Lei, Zhaoxin Li, Yu Lei, Yanling Bi, Luokai Hu, and Wenfeng Shen

HBaseSpatial: A Scalable Spatial Data Storage Based on HBase ........................................644
   Ningyu Zhang, Guozhou Zheng, Huajun Chen, Jiaoyan Chen, and Xi Chen

On the Application and Performance of MongoDB for Climate Satellite Data .....................652
   Parinaz Ameri, Udo Grabowski, Jörg Meyer, and Achim Streit

Research of Provenance Storage in Cloud Computing Environment ........................................660
   Zhangxuan Luo and Guoyan Xu

Data Interface All-in-A-Place (DIANA) for Big Data .............................................................665
   Frank Zhigang Wang, Theo Dimitrakos, Na Helian, Sining Wu, Yuhui Deng,
   Ling Li, and Rodric Yates
Big Data Processing
Performance Evaluation of the SSD-Based Swap System for Big Data Processing .................................................................673
Jaehun Lee, Sungmin Park, Minsoo Ryu, and Sooyong Kang
A Study on Recursive Neural Network Based Sentiment Classification of Sina Weibo ........................................................................................................................................................................681
Chen Fu, Bai Xue, and Zhan Shaobin
VALID: A Web Framework for Visual Analytics of Large Streaming Data ..................................................................................686
Chenhui Li and George Baciu
A High Speed Lossless Compression Algorithm Based on CPU and GPU Hybrid Platform ..................................................................................................................693
Bin Zhou, Hai Jin, and Ran Zheng
Picky Partial Least Squares for Feature Selection from Alzheimer's Data ..................................................................................699
Torbjorn Wasterlid and Li Bai

Big Data Application
Improved 2DLDA Algorithm and Its Application in Face Recognition ..................................................................................707
Dong Wang and Shunfang Wang
The Evaluation of Emulab as an Environment for Bio-Informatics Research ..................................................................................714
Kyungwoo Kang, Yunhee Kang, and Sungjin Sul
A Evaluation Method for Web Service with Large Numbers of Historical Records ........................................................................................................................................................................721
Lianyong Qi, Jiancheng Ni, Xiaona Xia, Chao Yan, Hua Wang, and Wanli Huang
BIG DATA: Preconditions to Productivity ........................................................................................................................................727
Steve Hallman, Jasur Rakhimov, Michel Plaisent, and Prosper Bernard
Data Mining Application of Decision Trees for Student Profiling at the Open University of China ........................................................................................................................................................................732

MapReduce for Big Data
Aeromancer: A Workflow Manager for Large-Scale MapReduce-Based Scientific Workflows ........................................................................................................................................................................739
Nabeel Mohamed, Nabanita Maji, Jing Zhang, Nataliya Timoshevskaia, and Wu-Chun Feng
MapReduce for Large-Scale Monitor Data Analyses ........................................................................................................................................747
Jianwei Ding, Yingbo Liu, Li Zhang, and Jianmin Wang
FedLoop: Looping on Federated MapReduce .................................................................755
   Chun-Yu Wang, Tzu-Li Tai, Kuan-Chieh Huang, Tse-En Liu, Jyh-Blau Chang, and Ce-Kuen Shieh

In-Map/In-Reduce: Concurrent Job Execution in MapReduce ........................................763
   Muhammad Idris, Shujaat Hussain, and Sungyoung Lee

**Big Data & Optimization**

Towards Policy Retrieval for Provenance Based Access Control Model ........................................769
   Jisheng Pei and Xiaojun Ye

SARAH - Statistical Analysis for Resource Allocation in Hadoop ........................................777
   Bruce Martin

Privacy Aware Non-linear Support Vector Machine for Multi-source Big Data ...............................783
   Yunmei Lu, Piyaphol Phoungphol, and Yanqing Zhang

Modeling of Data Provenance on Space and Time Based on OPM ................................................790
   Kang Jiehua and Xu Guoyan

Threshold-Based Secure and Privacy-Preserving Message Verification in VANETs ............................795
   Wei Gao, Mingzhong Wang, Liehuang Zhu, and Xiaoping Zhang

**Future Internet and Network Security**

A Semantic Knowledge Base Construction Method for Information Security ...............................803
   Yuanhang Yao, Xiaoyu Ma, Hui Liu, Jin Yi, Xianghui Zhao, and Lin Liu

Adding Privacy to Multicast DNS Service Discovery ................................................................809
   Daniel Kaiser and Marcel Waldvogel

Encrypted Program Execution ......................................................................................................817
   Dmytro Zhuravlev, Ihor Samoilovych, Roman Orlovskyi, Ievgen Bondarenko, and Yaroslav Lavre

Network Traffic Anomaly Detection Using Adaptive Density-Based Fuzzy Clustering ....................823
   Duo Liu, Chung-Horng Lung, Nabil Seddigh, and Biswajit Nandy

Unified Model for Data Security - A Position Paper ..................................................................831
   Raja Naeem Akram and Ryan K.L. Ko

A Secure Authentication Protocol for IP-Based Wireless Sensor Communications Using the Location/ID Split Protocol (LISP) ..........................................................840
   Ali Raheem, Aboubaker Lasebae, and Jonathan Loo
Network Optimization and Performance Evaluation

A Compact Hardware Implementation of SM3 Hash Function .................................................................846
   Tianyong Ao, Zhangqing He, Jinli Rao, Kui Dai, and Xuecheng Zou

A Load Balancing Strategy of SDN Controller Based on Distributed Decision ........................................851
   Yuanhao Zhou, Mingfa Zhu, Limin Xiao, Li Ruan, Wenbo Duan, Deguo Li, Rui Liu, and Mingming Zhu

Modeling Degrees of Fairness for Collaborations .....................................................................................857
   Florian Volk, Maria Pelevina, Sheikh Mahbub Habib, Sascha Hauke, and Max Mühlhäuser

Performance Analysis on M2M Communication Network Based on Stochastic Network Calculus ..................................................865
   Zhou Tao, Wang Quan, and Wang Gao-Cai

Mining Specification of Insecure Browser Extension Behavior .................................................................871
   Hongbin Pei, Xiaohong Li, Guangquan Xu, and Zhiyong Feng

Security, Privacy, and Anonymity in Internet of Things

Detection of Android Malicious Apps Based on the Sensitive Behaviors ....................................................877
   Daiyong Quan, Lidong Zhai, Fan Yang, and Peng Wang

Digital Trust - Trusted Computing and Beyond: A Position Paper ..........................................................884
   Raja Naeem Akram and Ryan K.L. Ko

Identifying P2P Network Activities on Encrypted Traffic ........................................................................893
   Xiaolei Wang, Jie He, and Yuexiang Yang

Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters .....................900
   Sufian Hameed, Bilal Hameed, Syed Atyab Hussain, and Waqas Khalid

Survey of Integrity Detection Methods in Internet of Things ....................................................................906
   Chaoliang Li, Qin Li, and Guojun Wang

TEEI - A Mobile Security Infrastructure for TEE Integration ...................................................................914
   Hongfeng Chai, Zhijun Lu, Qingyang Meng, Jun Wang, Xiubang Zhang, and Zhijian Zhang

Cloud Computing

Continuous Certification of Non-repudiation in Cloud Storage Services ...................................................921
   Maria Krotsiani and George Spanoudakis

JVM-Based Dynamic Attestation in Cloud Computing ..............................................................................929
   Haihe Ba, Zhiying Wang, Jiangchun Ren, and Huaizhe Zhou
Remote Programmatic vCloud Forensics: A Six-Step Collection Process and a Proof of Concept .............................................................935
  Ben Martini and Kim-Kwang Raymond Choo

vPatcher: VMI-Based Transparent Data Patching to Secure Software in the Cloud .................................................................943
  Hao Zhang, Lei Zhao, Lai Xu, Lina Wang, and Deming Wu

Enforcing File System Permissions on Android External Storage: Android File System Permissions (AFP) Prototype and ownCloud ........................................949
  Quang Do, Ben Martini, and Kim-Kwang Raymond Choo

**UbiSafe Computing**

A Novel Public Key Encryption Scheme for Large Image .................................................................955
  Lingjiao Chen, Xinji Chen, and Zhigang Peng

Analysis of the Count-Min Sketch Based Anomaly Detection Scheme in WSN ........................................961
  Guorui Li, Ying Liu, and Ying Wang

Attacks on Physically-Embedded Data Encryption for Embedded Devices ................................................967
  Chaohui Du and Guoqiang Bai

Challenge Set Designs and User Guidelines for Usable and Secured Recognition-Based Graphical Passwords .................................................................973
  Hani Moaiteq Aljahdali and Ron Poet

Escrow: A Large-Scale Web Vulnerability Assessment Tool .................................................................983
  Baden Delamore and Ryan K.L. Ko

Personal Data Access Based on Trust Assessment in Mobile Social Networking ..................................................989
  Zheng Yan, Xueyun Li, and Raimo Kantola

**Author Index** .........................................................................................................................995