

Table of Contents

Security and Privacy in Networked Systems

Collaborative Approach for Data Integrity Verification in Cloud Computing	1
<i>Rajat Saxena and Somnath Dey</i>	
EESOR: Energy Efficient Selective Opportunistic Routing in Wireless Sensor Networks	16
<i>C.R. Yamuna Devi, B. Shivaraj, S.H. Manjula, K.R. Venugopal, and Lalit M. Patnaik</i>	
A Security Framework for Multi-authority Based e-Sealed Bid Auction System	32
<i>Sourav Sinha and Mamata Jenamani</i>	
Analysis of Semantic Attacks in Online Social Networks.....	45
<i>K.P. Krishna Kumar and G. Geethakumari</i>	
Enhanced Security of PHR System in Cloud Using Prioritized Level Based Encryption	57
<i>D. Sangeetha, Vaidehi Vijayakumar, Valliammai Thirunavukkarasu, and Aiswarya Ramesh</i>	
MM-SOAR: Modified SOAR Protocol Using Multiple Metrics for Wireless Mesh Network	70
<i>Anuradha Jadiya and Deepak C. Karia</i>	
Clustering Based Routing Strategies for Energy Management in Ad-Hoc Networks.....	79
<i>Deepak C. Karia and Shravanee Shinde</i>	
Virtual Machine Isolation: A Survey on the Security of Virtual Machines	91
<i>R. Jithin and Priya Chandran</i>	
Trust Based VM Consolidation in Cloud Data Centers.....	103
<i>T.R. Venugopal Anandharajan and Marcharla Anjaneyulu Bhagyaveni</i>	
A Trust Model for Directory-Based Service Discovery in Mobile Ad Hoc Networks	115
<i>R. Deepa and S. Swamynathan</i>	

Chain Routing for Convergecast Small Scale Wireless Sensor Networks 127
C.R. Yamuna Devi, Deepak Sunder, S.H. Manjula, K.R. Venugopal, and Lalit M. Patnaik

A Genetic Algorithm for Scheduling Workflow Applications in Unreliable Cloud Environment 139
Lovejit Singh and Sarbjeet Singh

Autonomic SLA Management in Cloud Computing Services 151
S. Anithakumari and K. Chandra Sekaran

Multimedia Security

A Novel Audio Watermark Embedding and Extraction Method Based on Compressive Sensing, Sinusoidal Coding, Reduced SVD, over Complete Dictionary and L1 Optimization 160
G. Jyothish Lal and V.K. Veena

Compressive Sensing Based Audio Scrambling Using Arnold Transform 172
Nishanth Augustine, Sudhish N. George, and P.P. Deepthi

Cryptanalysis of Two Authentication Scheme for DRM System 184
Dheerendra Mishra and Sourav Mukhopadhyay

Improving Test Conformance of Smart Cards versus EMV-Specification by Using on the Fly Temporal Property Verification 192
Germain Jolly, Sylvain Vernois, and Jean-Luc Lambert

Palm Print Recognition Using Fusion of 2D-Gabor and 2D Log-Gabor Features 202
Munaga V.N.K. Prasad, Ilaiyah Kavati, and B. Adinarayana

Cryptosystems, Algorithms, Primitives

A New Variant of Algebraic Attack 211
Dibyendu Roy, Pratish Datta, and Sourav Mukhopadhyay

A Novel Design of Chaos Based S-Box Using Difference Distribution Table (CD S-Box) 223
Muhammad Asif Khan and Varun Jeoti

On the Extensions of $(k, n)^*$ -Visual Cryptographic Schemes 231
Kanakkath Praveen, K. Rajeev, and M. Sethumadhavan

A Graph Data Model for Attack Graph Generation and Analysis 239
Mridul Sankar Barik and Chandan Mazumdar

Computationally Perfect Secret Sharing Scheme Based on Error-Correcting Codes	251
<i>Appala Naidu Tentu, Prabal Paul, and V.Ch. Venkaiah</i>	
Warfare Message Communication in Tactical WMN Using HWMP	263
<i>Jayalakshmi G. Naragund and R.M. Banakar</i>	
Metadata Attribute Based Cipher-Key Generation System in Cloud	275
<i>Ramalingam Anitha and Saswati Mukherjee</i>	
Cryptanalysis of Yang et al.'s Digital Rights Management Authentication Scheme Based on Smart Card.....	288
<i>Dheerendra Mishra and Sourav Mukhopadhyay</i>	

System and Network Security

Automatic Evaluation and Signature Generation Technique for Thwarting Zero-Day Attacks	298
<i>Ratinder Kaur and Maninder Singh</i>	
A Theoretical Study on Access Control Model in Federated Systems	310
<i>Anant V. Nimkar and Soumya K. Ghosh</i>	
CASSHH – Case Adaptive SSH Honey-pot	322
<i>Adrian Pauna and Victor Valeriu Patriciu</i>	
Improved Detection of P2P Botnets through Network Behavior Analysis	334
<i>Shree Garg, Anil K. Sarje, and Sateesh Kumar Peddoju</i>	
SLASS: Secure Login against Shoulder Surfing	346
<i>Nilesh Chakraborty and Samrat Mondal</i>	
Differential Execution Analysis for Obfuscation Reduction	358
<i>R. Reno Robert</i>	

Short Papers

Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs	370
<i>Monika Darji and Bhushan H. Trivedi</i>	
Index Page Based EDoS Attacks in Infrastructure Cloud	382
<i>Bhavna Saini and Gaurav Somani</i>	
Privacy Preserving Ranked Keyword Search over Encrypted Cloud Data	396
<i>Dinesh Nepolean, I. Karthik, Mu. Preethi, Rahul Goyal, and M. Kathirvel Vanethi</i>	

Combining the X.509 and the SAML Federated Identity Management Systems	404
<i>Marcus Hardt, Arsen Hayrapetyan, Paul Mullar, and Shiraz Memon</i>	
Analysis of Electronic Voting Protocol Using Strand Space Model	416
<i>Venkatasamy Sureshkumar and Ramalingam Anitha</i>	
Seamless Handoff of Ping-Pong Calls in Mobile Wimax Networks	428
<i>Balu Sridevi, G.V. Shirley Julia, and S. Rajaram</i>	
Static Malware Analysis Using Machine Learning Methods	440
<i>Hiran V. Nath and Babu M. Mehtre</i>	
Making an Application Provenance-Aware through UML – A General Scheme	451
<i>P. Badharudheen, Anu Mary Chacko, and S.D. Madhu Kumar</i>	
Enhancing E-Payment Security through Biometric Based Personal Authentication Using Steganography Scheme – B-PASS	461
<i>Balasubramanian Chelliah and S. Geetha</i>	

Second International Workshop on Security in Self-Organising Networks (SelfNet 2014)

A Novel Cloud Based NIDPS for Smartphones	473
<i>Vijay Anand Pandian and T. Gireesh Kumar</i>	
Preserving Database Privacy in Cloud Computing	485
<i>Saed Alrabaee, Khaled Khateeb, and Fawaz A. Khasawneh</i>	
A Survey on Wi-Fi Protocols: WPA and WPA2	496
<i>Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaiby, and Anwar Althubayani</i>	

Workshop on Multidisciplinary Perspectives in Cryptology and Information Security (CIS 2014)

On the k-error Joint Linear Complexity and Error Multisequence over $F_q(\text{char } F_q = p, \text{ prime})$	512
<i>M. Sindhu and M. Sethumadhavan</i>	
Implementation of an Elliptic Curve Based Message Authentication Code for Constrained Environments	520
<i>P. Jilna and P.P. Deepthi</i>	
A Hybrid Encryption Technique for Securing Biometric Image Data Based on Feistel Network and RGB Pixel Displacement	530
<i>Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo Moses Eghan, and Nii Narku Quaynnor</i>	

A Simple and Efficient Key-Dependent S-Box Design Using Fisher-Yates Shuffle Technique	540
<i>Musheer Ahmad, Parvez Mahmood Khan, and Mohd Zeeshan Ansari</i>	

Second International Workshop on Trust and Privacy in Cyberspace (CyberTrust 2014)

Experimental Analysis on Access Control Using Trust Parameter for Social Network	551
<i>Saumya Omanakuttan and Madhumita Chatterjee</i>	

Author Index	563
---------------------------	------------