## Contents

### Attacks and Mitigation

An Attack Possibility on Time Synchronization Protocols Secured with TESLA-Like Mechanisms .......................... 3  
*Kristof Teichel, Dieter Sibold, and Stefan Milius*

Practical DoS Attacks on Embedded Networks in Commercial Vehicles ....... 23  
*Subhojeet Mukherjee, Hossein Shirazi, Indrakshi Ray, Jeremy Daily, and Rose Gamble*

### Authentication

Secure Lightweight User Authentication and Key Agreement Scheme for Wireless Sensor Networks Tailored for the Internet of Things Environment .... 45  
*Srinivas Jangirala, Dheerendra Mishra, and Sourav Mukhopadhyay*

SPOSS: Secure Pin-Based-Authentication Obviating Shoulder Surfing ....... 66  
*Ankit Maheshwari and Samrat Mondal*

### Authorization and Information Flow Control

Building a Fair System Using Access Rights .................................................. 89  
*Nada Essaouini, Frédéric Cuppens, and Nora Cuppens-Boulahia*

Collaborative Access Decisions: Why Has My Decision Not Been Enforced? .................................................. 109  
*Jerry den Hartog and Nicola Zannone*

Data Loss Prevention Based on Text Classification in Controlled Environments .................................................. 131  
*Kyrre Wahl Kongsgård, Nils Agne Nordbotten, Federico Mancini, and Paal E. Engelstad*

Defining Abstract Semantics for Static Dependence Analysis of Relational Database Applications .................................................. 151  
*Angshuman Jana and Raju Halder*

### Cryptosystem and Protocols

An Efficient Certificateless Signature Scheme in the Standard Model ....... 175  
*Sébastien Canard and Viet Cuong Trinh*
Constant-Size Ciphertext Attribute-Based Encryption from Multi-channel Broadcast Encryption ......................................................... 193  
  Sébastien Canard and Viet Cuong Trinh

Enhanced Modulo Based Multi Secret Image Sharing Scheme .................. 212  
  Maroti Deshmukh, Neeta Nain, and Mushtaq Ahmed

Performance Evaluation of Modified Henon Map in Image Encryption ........ 225  
  S.J. Sheela, K.V. Suresh, and Deepaknath Tandur

Network Security and Intrusion Detection

Network Counter-Attack Strategy by Topology Map Analysis .................. 243  
  Hidema Tanaka

Network Vulnerability Analysis Using a Constrained Graph Data Model ........ 263  
  Mridul Sankar Barik, Chandan Mazumdar, and Amarnath Gupta

Secured Dynamic Scheduling Algorithm for Real-Time Applications on Grid .................. 283  
  Surendra Singh, Sachin Tripathi, and Suvadip Batabyal

Privacy

A Framework for Analyzing Associativity and Anonymity in Conventional and Electronic Summative Examinations .............................................. 303  
  Kissan Gauns Dessai and Venkatesh Kamat

On the Security of “Verifiable Privacy-Preserving Monitoring for Cloud-Assisted mHealth Systems” .............................................................. 324  
  Hardik Gajera, Shruti Naik, and Manik Lal Das

Privacy Preserving Network Analysis of Distributed Social Networks .......... 336  
  Varsha Bhat Kukkala, Jaspal Singh Saini, and S.R.S. Iyengar

Software Security

Exploiting Block-Chain Data Structure for Auditorless Auditing on Cloud Data .................................................. 359  
  Sanat Ghoshal and Goutam Paul

Risk Evaluation of X.509 Certificates – A Machine Learning Application ...... 372  
  Varsharani Hawanna, Vrushali Kulkarni, Rashmi Rane, and Pooja Joshi
Wireless, Mobile and IoT Security

A Secure Routing Scheme for Wireless Mesh Networks ............... 393
   Ashish Nanda, Priyadarsi Nanda, Xiangjian He, and Aruna Jamdagni

Digital Forensic Source Camera Identification with Efficient Feature
Selection Using Filter, Wrapper and Hybrid Approaches ............ 409
   Venkata Udaya Sameer, S. Sugumaran, and Ruchira Naskar

Formal Verification of a Cross-Layer, Trustful Space-Time Protocol
for Wireless Sensor Networks. ........................................ 426
   Douglas Simões Silva, Davi Resner, Rick Lopes de Souza,
   and Jean Everson Martina

JITWORM: Jitter Monitoring Based Wormhole Attack Detection
in MANET. ................. 444
   Sudhir Bagade and Vijay Raisinghani

Short Papers

A Solution to Detect Phishing in Android Devices ............... 461
   Sharvari Prakash Chorghe and Narendra Shekokar

Feature Selection for Effective Botnet Detection Based on Periodicity
of Traffic ........................................ 471
   T. Harsha, S. Asha, and B. Soniya

Honeypot Deployment in Broadband Networks .................. 479
   Saurabh Chamotra, Rakesh Kumar Sehgal, Sanjeev Ror,
   and Bhupendra Singh

Generic Construction of Certificateless Signcryption Scheme ........ 489
   Jayaprakash Kar and Kshirasagar Naik

Reed-Muller Code Based Symmetric Key Fully Homomorphic
Encryption Scheme ........................................ 499
   RatnaKumari Challa and VijayaKumari Gunta

Towards Useful Anomaly Detection for Back Office Networks .... 509
   Ömer Yüksel, Jerry den Hartog, and Sandro Etalle

Detection of SQLite Database Vulnerabilities in Android Apps .... 521
   Vineeta Jain, M.S. Gaur, Vijay Laxmi, and Mohamed Mosbah

Discovering Vulnerable Functions by Extrapolation: A Control-Flow Graph
Similarity Based Approach ........................................ 532
   Lokesh Jain, Aditya Chandran, Sanjay Rawat, and Kannan Srinathan

Author Index ........................................ 543