Contents

Cryptosystems, Algorithms, Primitives

Computing Mod with a Variable Lookup Table . . . . . . . . . . . . . . . 3
  Mark A. Will and Ryan K.L. Ko

Mutual Authentication Based on HECC for RFID Implant Systems . . . 18
  Asha Liza John and Sabu M. Thampi

On the Use of Asynchronous Cellular Automata in Symmetric-Key
Cryptography . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 30
  Biswanath Sethi and Sukanta Das

A Random Key Generation Scheme Using Primitive Polynomials
over GF(2) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42
  Inderjeet Singh and Alwyn R. Pais

Multi-factor Authentication Using Recursive XOR-Based Visual
Cryptography in Online Voting System . . . . . . . . . . . . . . . . . . . . . . . . . . 52
  P. Sanyasi Naidu and Reena Kharat

Enhanced Image Based Authentication with Secure Key Exchange
Mechanism Using ECC in Cloud . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 63
  Anurag Singh Tomar, Shashi Kant Shankar, Manmohan Sharma,
  and Aditya Bakshi

Differential Fault Analysis on Tiaoxin and AEGIS Family of Ciphers . . 74
  Prakash Dey, Raghvendra Singh Rohit, Santanu Sarkar,
  and Avishek Adhikari

A Comparison of Diffusion Properties of Salsa, ChaCha, and MCC Core. . 87
  Rajeev Sobti and G. Geetha

A Secure Keyword Ordered Multiuser Searchable Encryption Framework . . 99
  Kulvaibhav Kaushik and Vijayaraghavan Varadharajan

Cryptographic Assessment of SSL/TLS Servers Popular in India . . . . . 112
  Prakhar Jain and K.K. Shukla

Key Identifications Using Hebbian Learning . . . . . . . . . . . . . . . . . . . . . . 124
  Bhavya Ishaan Murmu, Anu Kumari, Manu Malkani, and Sanjeet Kumar
Security and Privacy in Networked Systems

An Automated Methodology for Secured User Allocation in Cloud
Srijita Basu, Anirban Sengupta, and Chandan Mazumdar

Provenance-Aware NoSQL Databases
Anu Mary Chacko, Munavar Fairooz, and S.D. Madhu Kumar

Efficient Key Management in IoT Using Mobile Aggregator
Sumit Saurabh, Alwyn R. Pais, and Sumanta Chatterjee

Cloud Resources Optimization for Air Pollution Monitoring Devices and Avoiding Post Pillar Problem
Parampreet Singh and Pankaj Deep Kaur

Credibility Assessment of Public Pages over Facebook
Himanshi Agrawal and Rishabh Kaushal

Elliptic Curve Based Secure Outsourced Computation in Multi-party Cloud Environment
V. Thangam and K. Chandrasekaran

Secure and Privacy Preserving Mobile Healthcare Data Exchange Using Cloud Service
Doyel Pal, Gobinda Senchury, and Praveenkumar Khethavath

Secure Certificateless Signature Scheme with Batch Verification from Bilinear Pairings
N.B. Gayathri and P. Vasudeva Reddy

System and Network Security

Security Requirements Elicitation and Modeling Authorizations
Rajat Goel, Mahesh Chandra Govil, and Girdhari Singh

Two Level Signature Based Authorization Model for Secure Data Warehouse
Anjana Gosain and Amar Arora

Nonlinear Tracking of Target Submarine Using Extended Kalman Filter (EKF)
S. Vikranth, P. Sudheesh, and M. Jayakumar

Tracking Inbound Enemy Missile for Interception from Target Aircraft Using Extended Kalman Filter
T.S. Gokkul Nath, P. Sudheesh, and M. Jayakumar
Steganography/Visual Cryptography/Image Forensics

A Secure One-Time Password Authentication Scheme Using Image Texture Features ........................................... 283
   Maitreya Maity, Dhiraj Manohar Dhane, Tushar Mungle, Rupak Chakraborty, Vasant Deokamble, and Chandan Chakraborty

Analyzing the Applicability of Bitsum Algorithm on LSB Steganography Technique ........................................... 295
   Bagga Amandeep and G. Geetha

Extreme Learning Machine for Semi-blind Grayscale Image Watermarking in DWT Domain ................................ 305
   Ankit Rajpal, Anurag Mishra, and Rajni Bala

A Passive Blind Approach for Image Splicing Detection Based on DWT and LBP Histograms ................................... 318
   Mandeep Kaur and Savita Gupta

An Image Forensic Technique for Detection of Copy-Move Forgery in Digital Image ........................................... 328
   Ashwini Malviya and Siddharth Ladhake

Secure Authentication in Online Voting System Using Multiple Image Secret Sharing ........................................... 336
   P. Sanyasi Naidu and Reena Kharat

Applications Security

Touch and Track: An Anti-theft and Data Protection Technique for Smartphones ........................................... 347
   Sohini Roy, Arvind Kumar Shah, and Uma Bhattacharya

Enhancement of Detecting Wicked Website Through Intelligent Methods ......................................................... 358
   Tarik A. Rashid and Salwa O. Mohamad

Prediction of Malicious Domains Using Smith Waterman Algorithm ........................................... 369
   B. Ashwini, Vijay Krishna Menon, and K.P. Soman

Outsource-Secured Calculation of Closest Pair of Points ........................................... 377
   Chandrasekhar Kuruba, Kethzi Gilbert, Prabhav Sidhaye, Gaurav Pareek, and Prurushothama Byrapura Rangappa

Discovering Vulnerable Functions: A Code Similarity Based Approach ........................................... 390
   Aditya Chandran, Lokesh Jain, Sanjay Rawat, and Kannan Srinathan
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analysis of Spectrum Sensing Algorithm Using Multiple</td>
<td>403</td>
</tr>
<tr>
<td>Antenna in Cognitive Radio</td>
<td></td>
</tr>
<tr>
<td><em>Komal Pawar and Tanuja Dhope</em></td>
<td></td>
</tr>
<tr>
<td>Diagnosis of Multiple Stuck-at Faults Using Fault Element Graph</td>
<td>414</td>
</tr>
<tr>
<td>with Reduced Power</td>
<td></td>
</tr>
<tr>
<td>*T.S. Gokkul Nath, E.R. Midhila, Ashwin Swaminathan, Binitaa Lekshmi,</td>
<td></td>
</tr>
<tr>
<td>and J.P. Anita</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection Using Improved Decision Tree Algorithm with Binary</td>
<td>427</td>
</tr>
<tr>
<td>and Quad Split</td>
<td></td>
</tr>
<tr>
<td><em>Shubha Puthran and Ketan Shah</em></td>
<td></td>
</tr>
<tr>
<td>MalJs: Lexical, Structural and Behavioral Analysis of Malicious</td>
<td>439</td>
</tr>
<tr>
<td>JavaScripts Using Ensemble Classifier</td>
<td></td>
</tr>
<tr>
<td><em>Surendran K., Prabaharan Poornachandran, Aravind Ashok Nair, Srinath</em></td>
<td></td>
</tr>
<tr>
<td><em>N., Ysudhir Kumar, and Hrudya P.</em></td>
<td></td>
</tr>
<tr>
<td>SocialBot: Behavioral Analysis and Detection</td>
<td>450</td>
</tr>
<tr>
<td><em>Madhuri Dewangan and Rishabh Kaushal</em></td>
<td></td>
</tr>
<tr>
<td>Vulnebdroid: Automated Vulnerability Score Calculator for Android</td>
<td>461</td>
</tr>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td><em>Sugandha Gupta and Rishabh Kaushal</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>473</td>
</tr>
</tbody>
</table>
Security in Computing and Communications
4th International Symposium, SSCC 2016, Jaipur, India,
September 21-24, 2016, Proceedings
Mueller, P.; Thampi, S.M.; Alam Bhuiyan, Z.; Ko, R.; Doss, R.; Alcaraz Calero, J.M. (Eds.)
2016, XXII, 474 p. 179 illus., Softcover
ISBN: 978-981-10-2737-6