

# Contents

## Cryptosystems, Algorithms, Primitives

Computing Mod with a Variable Lookup Table . . . . .	3
<i>Mark A. Will and Ryan K.L. Ko</i>	
Mutual Authentication Based on HECC for RFID Implant Systems. . . . .	18
<i>Asha Liza John and Sabu M. Thampi</i>	
On the Use of Asynchronous Cellular Automata in Symmetric-Key Cryptography . . . . .	30
<i>Biswanath Sethi and Sukanta Das</i>	
A Random Key Generation Scheme Using Primitive Polynomials over GF(2). . . . .	42
<i>Inderjeet Singh and Alwyn R. Pais</i>	
Multi-factor Authentication Using Recursive XOR-Based Visual Cryptography in Online Voting System . . . . .	52
<i>P. Sanyasi Naidu and Reena Kharat</i>	
Enhanced Image Based Authentication with Secure Key Exchange Mechanism Using ECC in Cloud . . . . .	63
<i>Anurag Singh Tomar, Shashi Kant Shankar, Manmohan Sharma, and Aditya Bakshi</i>	
Differential Fault Analysis on Tiaoxin and AEGIS Family of Ciphers . . . . .	74
<i>Prakash Dey, Raghvendra Singh Rohit, Santanu Sarkar, and Avishek Adhikari</i>	
A Comparison of Diffusion Properties of Salsa, ChaCha, and MCC Core. . . .	87
<i>Rajeev Sobti and G. Geetha</i>	
A Secure Keyword Ordered Multiuser Searchable Encryption Framework . . .	99
<i>Kulvaibhav Kaushik and Vijayaraghavan Varadharajan</i>	
Cryptographic Assessment of SSL/TLS Servers Popular in India. . . . .	112
<i>Prakhar Jain and K.K. Shukla</i>	
Key Identifications Using Hebbian Learning. . . . .	124
<i>Bhavya Ishaan Murmu, Anu Kumari, Manu Malkani, and Sanjeet Kumar</i>	

## Security and Privacy in Networked Systems

An Automated Methodology for Secured User Allocation in Cloud . . . . .	137
<i>Srijita Basu, Anirban Sengupta, and Chandan Mazumdar</i>	
Provenance-Aware NoSQL Databases . . . . .	152
<i>Anu Mary Chacko, Munavar Fairooz, and S.D. Madhu Kumar</i>	
Efficient Key Management in IoT Using Mobile Aggregator . . . . .	161
<i>Sumit Saurabh, Alwyn R. Pais, and Sumanta Chatterjee</i>	
Cloud Resources Optimization for Air Pollution Monitoring Devices and Avoiding Post Pillar Problem . . . . .	173
<i>Parampreet Singh and Pankaj Deep Kaur</i>	
Credibility Assessment of Public Pages over Facebook . . . . .	188
<i>Himanshi Agrawal and Rishabh Kaushal</i>	
Elliptic Curve Based Secure Outsourced Computation in Multi-party Cloud Environment . . . . .	199
<i>V. Thangam and K. Chandrasekaran</i>	
Secure and Privacy Preserving Mobile Healthcare Data Exchange Using Cloud Service . . . . .	213
<i>Doyel Pal, Gobinda Senchury, and Praveenkumar Khethavath</i>	
Secure Certificateless Signature Scheme with Batch Verification from Bilinear Pairings . . . . .	225
<i>N.B. Gayathri and P. Vasudeva Reddy</i>	

## System and Network Security

Security Requirements Elicitation and Modeling Authorizations . . . . .	239
<i>Rajat Goel, Mahesh Chandra Govil, and Girdhari Singh</i>	
Two Level Signature Based Authorization Model for Secure Data Warehouse . . . . .	251
<i>Anjana Gosain and Amar Arora</i>	
Nonlinear Tracking of Target Submarine Using Extended Kalman Filter (EKF) . . . . .	258
<i>S. Vikranth, P. Sudheesh, and M. Jayakumar</i>	
Tracking Inbound Enemy Missile for Interception from Target Aircraft Using Extended Kalman Filter . . . . .	269
<i>T.S. Gokkul Nath, P. Sudheesh, and M. Jayakumar</i>	

## **Steganography/Visual Cryptography/Image Forensics**

A Secure One-Time Password Authentication Scheme Using Image Texture Features . . . . .	283
<i>Maitreya Maity, Dhiraj Manohar Dhane, Tushar Mungle, Rupak Chakraborty, Vasant Deokamble, and Chandan Chakraborty</i>	
Analyzing the Applicability of Bitsum Algorithm on LSB Steganography Technique . . . . .	295
<i>Bagga Amandeep and G. Geetha</i>	
Extreme Learning Machine for Semi-blind Grayscale Image Watermarking in DWT Domain . . . . .	305
<i>Ankit Rajpal, Anurag Mishra, and Rajni Bala</i>	
A Passive Blind Approach for Image Splicing Detection Based on DWT and LBP Histograms . . . . .	318
<i>Mandeep Kaur and Savita Gupta</i>	
An Image Forensic Technique for Detection of Copy-Move Forgery in Digital Image . . . . .	328
<i>Ashwini Malviya and Siddharth Ladhake</i>	
Secure Authentication in Online Voting System Using Multiple Image Secret Sharing . . . . .	336
<i>P. Sanyasi Naidu and Reena Kharat</i>	

## **Applications Security**

Touch and Track: An Anti-theft and Data Protection Technique for Smartphones. . . . .	347
<i>Sohini Roy, Arvind Kumar Shah, and Uma Bhattacharya</i>	
Enhancement of Detecting Wicked Website Through Intelligent Methods. . . . .	358
<i>Tarik A. Rashid and Salwa O. Mohamad</i>	
Prediction of Malicious Domains Using Smith Waterman Algorithm . . . . .	369
<i>B. Ashwini, Vijay Krishna Menon, and K.P. Soman</i>	
Outsource-Secured Calculation of Closest Pair of Points . . . . .	377
<i>Chandrasekhar Kuruba, Kethzi Gilbert, Prabhav Sidhaye, Gaurav Pareek, and Purushothama Byrapura Rangappa</i>	
Discovering Vulnerable Functions: A Code Similarity Based Approach . . . . .	390
<i>Aditya Chandran, Lokesh Jain, Sanjay Rawat, and Kannan Srinathan</i>	

Performance Analysis of Spectrum Sensing Algorithm Using Multiple Antenna in Cognitive Radio . . . . .	403
<i>Komal Pawar and Tanuja Dhope</i>	
Diagnosis of Multiple Stuck-at Faults Using Fault Element Graph with Reduced Power . . . . .	414
<i>T.S. Gokkul Nath, E.R. Midhila, Ashwin Swaminathan, Binitaa Lekshmi, and J.P. Anita</i>	
Intrusion Detection Using Improved Decision Tree Algorithm with Binary and Quad Split . . . . .	427
<i>Shubha Puthran and Ketan Shah</i>	
MalJs: Lexical, Structural and Behavioral Analysis of Malicious JavaScripts Using Ensemble Classifier . . . . .	439
<i>Surendran K., Prabakaran Poornachandran, Aravind Ashok Nair, Srinath N., Ysudhir Kumar, and Hrudya P.</i>	
SocialBot: Behavioral Analysis and Detection. . . . .	450
<i>Madhuri Dewangan and Rishabh Kaushal</i>	
Vulnebdroid: Automated Vulnerability Score Calculator for Android Applications . . . . .	461
<i>Sugandha Gupta and Rishabh Kaushal</i>	
<b>Author Index . . . . .</b>	<b>473</b>

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