

# Table of Contents

## Regular Papers

A Novel Key Management Mechanism for Dynamic Hierarchical Access Control Based on Linear Polynomials . . . . .	1
<i>Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami</i>	
Publicly Auditable Provable Data Possession Scheme for Outsourced Data in the Public Cloud Using Polynomial Interpolation . . . . .	11
<i>B.R. Purushothama and B.B. Amberker</i>	
Performance Evaluation of the Fuzzy ARTMAP for Network Intrusion Detection . . . . .	23
<i>Nelcileno Araújo, Ruy de Oliveira, Ed' Wilson Tavares Ferreira, Valtemir Nascimento, Ailton Shinoda Akira, and Bharat Bhargava</i>	
ID-Based Threshold Signcryption and Group Unsigncryption . . . . .	35
<i>Prashant Kumar Mishra, Kunwar Singh, and Sudhanshu Baruntar</i>	
Protocol for Secure Submissions into Learning Management Systems ...	45
<i>Manjunath Mattam</i>	
Secure Leader Election Algorithm Optimized for Power Saving Using Mobile Agents for Intrusion Detection in MANET . . . . .	54
<i>Monika Darji and Bhushan Trivedi</i>	
WAKE: Authentication and Key Establishment for Wireless Mesh Network . . . . .	64
<i>Somanath Tripathy and Debasish Sahoo</i>	
Effective Implementation of DES Algorithm for Voice Scrambling . . . . .	75
<i>Jinu Elizabeth John, A.S. Remya Ajai, and Prabakaran Poornachandran</i>	
Towards Constructing a Trustworthy Internet: Privacy-Aware Transfer of Digital Identity Document in Content Centric Internetworking . . . . .	85
<i>Amine Abidi, Ghazi Ben Ayed, and Farouk Kamoun</i>	
Security Analysis of CAPTCHA . . . . .	97
<i>Anjali Avinash Chandavale and A. Sapkal</i>	
Imperceptible Image Indexing Using Digital Watermarking . . . . .	110
<i>Jobin Abraham and Varghese Paul</i>	

A New Deterministic Algorithm for Testing Primality Based on a New Property of Prime Numbers .....	117
<i>Srikumar Manghat</i>	
Multilingual Speaker Identification with the Constraint of Limited Data Using Multitaper MFCC .....	127
<i>B.G. Nagaraja and H.S. Jayanna</i>	
Secure Group Key Management Scheme for Simultaneous Multiple Groups with Overlapped Memberships Using Binomial Key Tree .....	135
<i>B.R. Purushothama, Kusuma Shirisha, and B.B. Amberker</i>	
An Analytical Approach to Position-Based Routing Protocol for Vehicular Ad Hoc Networks .....	147
<i>Ram Shringar Raw, Daya Krishan Lobiyal, and Sanjoy Das</i>	
Simulation and Evaluation of Different Mobility Models in Ad-Hoc Sensor Network over DSR Protocol Using Bonnmotion Tool .....	157
<i>V. Vasanthi and M. Hemalatha</i>	
Secure Authentication in Multimodal Biometric Systems Using Cryptographic Hash Functions .....	168
<i>Aravind Ashok, Prabakaran Poornachandran, and Krishnasree Achuthan</i>	
Data Protection and Privacy Preservation Using Searchable Encryption on Outsourced Databases .....	178
<i>Lucas Rodrigo Raso Mattos, Vijayaraghavan Varadharajan, and Rajarathnam Nallusamy</i>	
A Dynamic Syntax Interpretation for Java Based Smart Card to Mitigate Logical Attacks .....	185
<i>Tiana Razafindralambo, Guillaume Bouffard, Bhagyalekshmy N. Thampi, and Jean-Louis Lanet</i>	
Taxonomy of Slow DoS Attacks to Web Applications .....	195
<i>Enrico Cambiaso, Gianluca Papaleo, and Maurizio Aiello</i>	
Crypto-Precision: Testing Tool for Hash Function .....	205
<i>Harshvardhan Tiwari, Ankit Luthra, Himanshu Goel, Sambhav Sharma, and Krishna Asawa</i>	
Performance Analysis and Improvement Using LFSR in the Pipelined Key Scheduling Section of DES .....	215
<i>P.V. Sruthi, Prabakaran Poornachandran, and A.S. Remya Ajai</i>	
Towards Retrieving Live Forensic Artifacts in Offline Forensics .....	225
<i>S. Diya, T.R. Deepthi, C. Balan, and K.L. Thomas</i>	

Carving of Bitmap Files from Digital Evidences by Contiguous File Filtering .....	234
<i>Balan Chelliah, Divya S. Vidyadharan, P. Shabana, and K.L. Thomas</i>	
Lightweight Cryptographic Primitives for Mobile Ad Hoc Networks.....	240
<i>Adarsh Kumar and Alok Aggarwal</i>	
Intrusion Protection against SQL Injection and Cross Site Scripting Attacks Using a Reverse Proxy .....	252
<i>S. Fouzul Hidhaya and Angelina Geetha</i>	
Three-Way Handshake-Based OTP Using Random Host-Side Keys for Effective Key Transfer in Symmetric Cryptosystems .....	264
<i>P.R. Mahalingam</i>	
Identity Based Privacy Preserving Dynamic Broadcast Encryption for Multi-privileged Groups .....	272
<i>Angamuthu Muthulakshmi, Ramalingam Anitha, S. Rohini, and Krishnan Princy</i>	
A Virtualization-Level Future Internet Defense-in-Depth Architecture.....	283
<i>Jerzy Konorski, Piotr Pacyna, Grzegorz Kolaczek, Zbigniew Kotulski, Krzysztof Cabaj, and Pawel Szalachowski</i>	
Experimental DRM Model Using Mobile Code and White-Box Encryption .....	293
<i>Stefan-Vladimir Ghita, Victor-Valeriu Patriciu, and Ion Bica</i>	
Towards a Secure, Transparent and Privacy-Preserving DRM System ...	304
<i>Dheerendra Mishra and Sourav Mukhopadhyay</i>	
Time Based Constrained Object Identification in a Dynamic Social Network .....	314
<i>M.T. Chitra, R. Priya, and Elizabeth Sherly</i>	
A New Approach towards Segmentation for Breaking CAPTCHA .....	323
<i>Anjali Avinash Chandavale and A. Sapkal</i>	
A Similarity Model to Estimate Attack Strategy Based on Intentions Analysis for Network Forensics .....	336
<i>Aman Jantan, Mohammad Rasmi, Mohd Izham Ibrahim, and Azri H.A. Rahman</i>	

**International Workshop on Security  
in Self-Organising Networks (SelfNet’12)**

Stationary Wavelet Transformation Based Self-recovery of  
Blind-Watermark from Electrocardiogram Signal in Wireless  
Telecardiology ..... 347  
*Nilanjan Dey, Anamitra Bardhan Roy, Achintya Das, and  
Sheli Sinha Chaudhuri*

eCloudIDS – Design Roadmap for the Architecture of Next-Generation  
Hybrid Two-Tier Expert Engine-Based IDS for Cloud Computing  
Environment ..... 358  
*Madhan Kumar Srinivasan, K. Sarukesi, Ashima Keshava, and  
P. Revathy*

A Comparative Study on Wormhole Attack Prevention Schemes  
in Mobile Ad-Hoc Network ..... 372  
*Subhashis Banerjee and Koushik Majumder*

Management of Routed Wireless M-Bus Networks for Sparsely  
Populated Large-Scale Smart-Metering Installations ..... 385  
*Philipp Digeser, Marco Tubolino, Martin Klemm, and Axel Sikora*

A Survey of Blackhole Attacks and Countermeasures in Wireless Mobile  
Ad-hoc Networks ..... 396  
*Subhashis Banerjee and Koushik Majumder*

**International Workshop on Intelligence and Security  
Informatics for International Security (IIS’12)**

iReSign-Implementation of Next-Generation Two-Tier Identity  
Classifier-Based Traffic Sign Recognition System Architecture Using  
Hybrid Region-Based Shape Representation Techniques ..... 408  
*Keerthi Balasundaram, Madhan Kumar Srinivasan, and K. Sarukesi*

**Work-in-Progress**

Neural Synchronization by Mutual Learning Using Genetic Approach  
for Secure Key Generation ..... 422  
*S. Santhanalakshmi, T.S.B. Sudarshan, and Gopal K. Patra*

eCloudIDS Tier-1 uX-Engine Subsystem Design and Implementation  
Using Self-Organizing Map (SOM) for Secure Cloud Computing  
Environment ..... 432  
*Madhan Kumar Srinivasan, K. Sarukesi, Ashima Keshava, and  
P. Revathy*

Implementation of MD6 .....	444
<i>Ananya Chowdhury and Utpal Kumar Ray</i>	
Location Estimation of Mobile in GSM and CDMA Networks.....	456
<i>Adapa Tataram and Alwyn Roshan Pais</i>	
An Adaptive Distributed Intrusion Detection System for Cloud Computing Framework .....	466
<i>Deepa Krishnan and Madhumita Chatterjee</i>	
Biologically Inspired Computer Security System: The Way Ahead .....	474
<i>Praneet Saurabh, Bhupendra Verma, and Sanjeev Sharma</i>	
A Comparative Analysis of the Ant Based Systems for QoS Routing in MANET.....	485
<i>Debañit Sensarma and Koushik Majumder</i>	
Efficient Weighted Innovative Routing Protocol (EWiRP) to Balance Load in Mobile Ad Hoc Networks (MANETs): Simulation and Feasibility Analysis.....	497
<i>Nitin Goel, Shruti Sangwan, and Ajay Jangra</i>	
<b>Author Index</b> .....	507