Dr. Maniklal Das

Contact Information

2103, Faculty Block 2
DA-IICT
Gandhinagar - 382007
Gujarat, INDIA

Phone: +91-79-30510-617
E-mail: maniklal@gmail.com
Homepage: http://intranet.daiict.ac.in/~maniklal_das/
My Research Group: http://security.daiict.ac.in/

H-index: 19 ; Citations: 2000$^+$
ORCID: 0000-0002-1218-4041; ResearcherID: Q-3767-2018

Research Interests

Cyber Security; Internet of Things; Blockchain Technology.

Education

Ph.D. (Computer Science), **Indian Institute of Technology**, Bombay, India.

M.Tech. (Computer Science), **Indian School of Mines**, Dhanbad, India.

M.Sc. (Mathematics), **Vidyasagar University**, West Bengal, India.

Honors and Awards

Senior Member, *IEEE.*

Life Member, *Cryptology Research Society of India.*

Visiting Researcher, *Western Kentucky University, USA, 2007-2008.*

Visiting Researcher, *University of Malaga, Spain, 2013.*

Visiting Researcher, *University of Clermont, France, 2016.*

Editorial

Associate Editor: IEEE Transactions on Dependable and Secure Computing [2018 -].

Reviewer: IEEE Transactions on Services and Computing; IEEE Transactions on Dependable and Secure Computing; IEEE Internet of Things Journal; IEEE Systems Journal; IEEE Transactions on Cloud Computing; IEEE Transactions on Knowledge and Data Engineering; IEEE Transactions on Vehicular Technology; IEEE Transactions on Information Forensics and Security; ACM Transactions on Information and System Security; IEEE Transactions on Wireless Communications; IEEE Communications Letters; IET Information Security; Computer Communications- Elsevier; Computers & Security-Elsevier.

Conference TPC: ICISS; IEEE CICS; ICDCIT; ACM Compute; IEEE TenSymp; ISSP; SecIoT; ICISA; UASS; and many others.

Administration and Supervision

Administration: Held positions as Convenor-Board of Studies; Convenor-Curriculum Development Committee; Convener-Undergraduate Studies; Convenor-Postgraduate Studies; Convenor-Admissions Committee, Faculty Search Committee; Accreditation Coomiittee; Research Progress Committee.

Supervision: 5 PhD students (2 graduated and 3 students on-going); 25$^+$Master theses; 70$^+$ BTech projects, and 100$^+$ interns work supervised.

Professional Experience

Professor [September, 2016 - present]

Associate Professor [April, 2012 - August, 2016]

Assistant Professor [July, 2006 - March, 2012]

Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar, India.

Research Officer [August, 2001 - July, 2006]

Institute for Development and Research in Banking Technology
Hyderabad, India

Lecturer [October, 1998 - July, 2001]

Haldia Institute of Technology, West Bengal, India

Visiting Faculty [1994 - 1998]

Vidyasagar University, West Bengal, India.

Visiting Faculty [2014 - present]

Indian Institute of Information Technology, Vadodara, India.

Sponsored International (Bilateral) Projects

Study of Privacy, Accountability and Ownership in IoT
Department of Science and Technology, Govt. of India (CEFIPRA) under Indo-French Collaborative Research Programme under DST-INRIA-CNRS Targeted Programme.

Investigators: Manik Lal Das (PI, DA-IICT, India) and Lafourcade Pascal (PI, University of Clermont, France).

Security and Privacy Infrastructure for Internet Of Things scenarios and applications.
Department of Science and Technology, Govt. of India under Indo-Spanish joint Programme of cooperation in Science and Technology.

Investigators: Manik Lal Das (PI, DA-IICT, India) and Javier Lopez (PI, University of Malaga, Spain).

Security proofs and multidisciplinary evaluation for dynamic hierarchical key assignment schemes
Department of Science and Technology, Govt. of India under Indo-Japan cooperative Programme.

Investigators: Manik Lal Das (Co-PI, DA-IICT, India) and Kanta Matsuura (PI, University of Tokyo, Japan).

Publications

Book Chapters

Manik Lal Das. *Privacy and Accountability Concerns in the Age of Big Data.* In: Big Data: Storage, Sharing, and Security, CRC Press, 2016.

Rachit Mittal, Sarita Agrawal, and Manik Lal Das. *Secure Node Localization in Clustered Sensor Networks with Effective Key Revocation.* In: Emerging Innovations in Wireless Networks and Broadband Technologies, pp. 12-41, 2016.

Manik Lal Das and Siva C Muraharirao. *Digital Image Protection using Keyed Hash Function.* Computer Vision and Image Processing in Intelligent Systems and Multimedia Technologies, IGI Global, pp. 203-215, 2014.

Shefali Jain, Anish Mathuria, and Manik Lal Das. *Misbehavior Detection in VANET: A Survey.* Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, IGI Global, pp. 134-147, 2014.

Manik Lal Das and Aakash Joshi. *Dynamic Program Update in Wireless Sensor Networks.* Security in Ad-hoc and Sensor Networks, World Scientific Publisher, pp. 369-384, 2009.

V. L. Narasimhan and Manik Lal Das. *Security Requires Information Literacy: A Perspective on Information Security for Business, Human, Social and Systemic Security.* Issues in Information and Media Literacy: Education, Practice and Pedagogy, Informing Science Press, pp. 257-286, 2009.

Journals

Payal Chaudhari and Manik Lal Das. *Privacy Preserving Searchable Encryption with Fine-grained Access Control.* IEEE Transactions on Cloud Computing, 2019.

Sarita Agrawal, Manik Lal Das, and Javier Lopez. *Detection of Node Capture Attack in Wireless Sensor Networks.* IEEE Systems Journal, 2018.

Dhwani Patel and Manik Lal Das. *TIDE: tampered image detection using mutual information.* International Journal of Multimedia Intelligence and Security, Inderscience, 2018.

Ainish Dave, Hardik Gajera, and Manik Lal Das. *Privacy-preserving Targeted Online Advertising.* International Journal of Social Computing and Cyber-Physical Systems, Inderscience, 2018.

Rahul Saranjame and Manik Lal Das. *Securing Digital Image from Malicious Insider Attacks.* International Journal of Computer Vision and Image Processing, Vol.8, No.2, Pages 49-58, 2018.

Sarita Agrawal and Manik Lal Das. *Mutual Healing enabled Group-key Distribution Protocol in Wireless Sensor Networks.* Computer Communications, Elsevier, 112:131-140, 2017.

Manik Lal Das. *Key-escrow free Multi-signature Scheme using Bilinear Pairings.* Groups Complexity & Cryptology, 7(1):47-57, 2015.

Jaydeep Solanki, Aenik Shah, and Manik Lal Das. *Secure Patrol : Patrolling against buffer overflow exploits.* Information Security Journal: A Global Perspective, 23(3):107-117, 2014.

Anand Mudgerikar and Manik Lal Das. *Secure Multicast using IPsec and Multi-party Key Computation.* International Journal of Internet Technology and Secured Transactions, Inderscience, 5(2):149-162, 2014.

Manik Lal Das and Navkar Samdaria. *On the Security of SSL/TLS-enabled Applications.* Applied Computing and Informatics, Elsevier, 10:68-81, 2014.

Rachit Mittal and Manik Lal Das. *Secure Node Localization in Mobile Sensor Networks.* International Journal of Wireless Networks and Broadband Technologies, IGI Global, 3(1):18-33, 2014.

Chandrapal Chahar, Vishal S Chauhan and Manik Lal Das. *Code Analysis for Software and System Security using Open Source Tools.* Information Security Journal: A Global Perspective, Taylor and Francis, 21(6):346-352, 2012.

Siva C Muraharirao and Manik Lal Das. *Digital Image Protection using Keyed Hash Function.* International Journal of Computer Vision and Image Processing, IGI Global, 2(2):36-47, 2012.

Anshul Singhal and Manik Lal Das. *MPEG Video Security using Motion Vectors and Quadtrees.* Journal of Mobile, Embedded and Distributed Systems, 4(3):203-208, 2012.

Anil Mundra, Anish Mathuria and Manik Lal Das. *Detecting flaws in dynamic hierarchical key management schemes using specification animation.* CSI Journal of Computing, 1(2):73-80, 2012.

Manik Lal Das. *A Key Escrow-free Identity-based Signature Scheme without using Secure Channel.* Cryptologia, 35(1):58-72, 2011.

Manik Lal Das. *Two-factor User Authentication in Wireless Sensor Networks.* IEEE Transactions on Wireless Communications, 8(3):1086-1090, 2009.

P. B. Reddy and Manik Lal Das. *An Improved and Efficient Micro-payment Scheme.* Journal of Theoretical and Applied Electronic Commerce Research, 4(1):91-100, 2009.

V. L. Narasimhan, P. T. Parthasarathy, and Manik Lal Das. *Evaluation of a Suite of Metrics for Component Based Software Engineering.* Issues in Informing Science and Information Technology, 6:731-740, 2009.

Manik Lal Das, Ashutosh Saxena, and Deepak B Phatak. *Algorithms and Approches of Proxy Signatures: A Survey.* International Journal of Network Security, 9(3):264-284, 2009.

G. Thulasi, Manik Lal Das, and Ashutosh Saxena. *An Improved Bilinear Pairing based Remote User Authentication Scheme.* Computer Standards & Interfaces, Elsevier, 31:181-185, 2009.

V. L. Narasimhan and Manik Lal Das. *DIS: Data and Information Security for BS and MS Program - A Proposal.* ACM SIGCSE, 40(4):95-99, 2008.

Manik Lal Das and Aaksh Joshi. *Dynamic Program Update in Wireless Sensor Networks Using Orthogonality Principle.* IEEE Communications Letters, 12(6):471-473, 2008.

Vidhani Kumar and Manik Lal Das. *Securing Wireless Sensor Networks with Public Key Techniques.* Adhoc & Sensor Wireless Networks, 5:189-201, 2008.

Manik Lal Das. *Comments on "Improved Efficient Remote User Authentication Schemes".* International Journal of Network Security, 6(3):282-284, 2008.

Manik Lal Das, Ashutosh Saxena, and Deepak B Phatak. *Proxy Signature Scheme with Effective Revocation using Bilinear Pairings.* International Journal of Network Security, 4(3):312-317, 2007.

G. Raju, G. M. Choudary, Manik Lal Das, and Ashutosh Saxena. *Threshold Key Issuing in Identity Based Cryptosystems.* Computer Standards & Interfaces, Elsevier, 29(2):260-264, 2007.

G. Raju, G. M. Choudary, Manik Lal Das, and Ashutosh Saxena. *Identity based Multisignatures.* INFORMATICA, 17(2):177-186, 2006.

Manik Lal Das. *A Flexible and Secure Remote Systems Authentication Scheme Using Smart Cards.*

Transaction on Electronics, Computer and Communication, 1(2):78-82, 2006.

Manik Lal Das, Ashutosh Saxena, V. P. Gulati, and Deepak B Phatak. *A Novel Remote User Authentication Scheme using Bilinear Pairings.* Computers & Security, Elsevier, 25(3):184-189, 2006.

Manik Lal Das, Ashutosh Saxena, V. P. Gulati, and Deepak B Phatak. *Hierarchical Key Management Scheme Using Polynomial Interpolation.* ACM System Interest Group (Operating Systems Review), 39(1):40-47, 2005.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *An Efficient Proxy Signature Scheme with Revocation.* INFORMATICA, 15(4):455-464, 2004.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *A Dynamic ID-based Remote User Authentication Scheme.* IEEE Transactions on Consumer Electronics, 50(2):629-631, 2004.

Conferences

Jinita Patel, Manik Lal Das, and Sukumar Nandi. *On the Security of Remote Key Less Entry for Vehicle.* In Proc. of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS 2018), IEEE, India, 2018.

Hardik Gajera, Shruti Naik, and Manik Lal Das. *MedCop: Verifiable Computation for Mobile Healthcare System.* In Proc. of International Symposium on Security in Computing and Communications, Bangalore, India, 2018.

K. Hemantha, Nidhi Desai, and Manik Lal Das. *On Minimality Attack for Privacy-Preserving Data Publishing.* In Proc. of International Symposium on Security in Computing and Communications, Bangalore, India, 2018.

Vishal Maral, Nachiket Trivedi, and Manik Lal Das. *Auditing Access to Private Data on Android Platform.* In Proc. of International Conference on Distributed Computing and Internet Technologies (ICDCIT 2018), LNCS 10722, Springer, pp. 105-111, India, 2018.

Xavier Bultel, Manik Lal Das, Hardik Gajera, David Gerault, Matthieu Giraud, and Pascal Lafourcade. *Private Polynomial Evaluation.* In Proc. of International Conference on Provable Security (ProvSec 2017), LNCS 10592, Springer, pp. 487-506, China, 2017.

Payal Chaudhari, Manik Lal Das, and Dipankar Dasgupta. *Privacy-Preserving Proxy Re-encryption with Fine-grained Access Control.* In Proc. of the International Conference on Information Systems Security (ICISS 2017), LNCS 10717, Springer, pp. 88-103, India, 2017 (Best Paper).

Nachiket Trivedi and Manik Lal Das. *MalDetec: A Non-Root Approach for Dynamic Malware Detection in Android.* In Proc. of the International Conference on Information Systems Security (ICISS 2017), LNCS 10717, Springer, pp. 231-240, India, 2017.

Nandan Parikh and Manik Lal Das. *Privacy-preserving Services in VANET with Misbehavior Detection.* In Proc. of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS 2017), IEEE, India, 2017.

Komal Falodiya and Manik Lal Das. *Security Vulnerability Analysis using Ontology-based Attack Graphs.* In Proc. of the IEEE India Council International Conference (INDICON 2017), IEEE, India, 2017.

Pradip Tilala, Anil Roy and Manik Lal Das. *Home Access Control Through a Smart Digital Locking-Unlocking System.* In Proc. of the IEEE Region 10 Conference (TENCON 2017), IEEE, Singapore, 2017.

Payal Chaudhari and Manik Lal Das. *A2BSE: Anonymous Attribute Based Searchable Encryption.* In Proc. of ISEA Asia Security & Privacy Conference (ISEA Asia S & P 2017), India.

Ritu Sharma and Manik Lal Das. *On the Verification of Conjunctive Keyword Search Results using Authenticated Crawlers.* In Proc. of the International Conference on Communication, Systems and Networks (COMSNETS 2017), IEEE, India, 2017.

Payal Chaudhari and Manik Lal Das. *On the Security of a Searchable Anonymous Attribute Based Encryption.* In Proc. of International Conference on Mathematics and Computing (ICMC 2017), India.

Payal Chaudhari and Manik Lal Das. *Privacy Preserving Signcryption Scheme.* In Proc. of International Conference on Distributed Computing and Internet Technologies (ICDCIT 2017), LNCS 10109, Springer, pp. 196-209, India, 2017.

Arjun Londhey and Manik Lal Das. *Efficient Image Authentication Scheme using Genetic Algorithms.* In Proc. of International Conference on Distributed Computing and Internet Technologies (ICDCIT 2017), LNCS 10109, Springer, 172-180, India, 2017.

Hardik Gajera, Shruti Naik and Manik Lal Das. *On the security of "Verifiable Privacy-preserving Monitoring for Cloud-assisted mHealth Systems".* In Proc. of the International Conference on Information Systems Security (ICISS 2016), LNCS 10063, Springer, pp. 324-335, India, 2016.

Sarita Agrawal and Manik Lal Das. *Node Revocation and Key Update Protocol in Wireless Sensor Networks.* In Proc. of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS 2016), IEEE, India, 2016.

Sarita Agrawal, Jay Patel and Manik Lal Das. *Pairing Based Mutual Healing in Wireless Sensor Networks.* In Proc. of the International Conference on Communication, Systems and Networks (COMSNETS 2016), IEEE, pp. 1-8, India, 2016.

Jay Dave and Manik Lal Das. *Securing SQL with Access Control for Database as a Service Model.* In Proc. of the International Conference on Information and Communication Technology for Competitive Strategies (ICTCS 2016), ACM Press, Article No. 104, India, 2016.

Arun Krishnan and Manik Lal Das. *Medical Image Security with Cheater Identification Using Secret Sharing Scheme.* In Proc. of the International Conference on Signal, Networking, Computing, and Systems (ICSNCS-2016), LNEE 395, Springer, India, 2016.

Bhavya Bansal, Ronak Patel and Manik Lal Das. *CheckPDF: Check What is Inside Before Signing a PDF Document.* In Proc. of the International Conference on Signal, Networking, Computing, and Systems (ICSNCS-2016), LNEE 395, Springer, India, 2016.

Sarita Agrawal, Manik Lal Das, Anish Mathuria and Sanjay Srivastava. *Program Integrity Verification for Detecting Node Capture Attack in Wireless Sensor Network.* In Proc. of the International Conference on Information Systems Security (ICISS 2015), Kolkata, India, LNCS 9478, Springer, pp. 419-440, 2015.

Payal Chaudhari, Manik Lal Das, and Anish Mathuria. *On Anonymous Attribute Based Encryption.* In Proc. of the International Conference on Information Systems Security (ICISS 2015), Kolkata,

India, LNCS 9478, Springer, pp. 378-392, 2015.

Punit Mehta, Jigar Sharda, and Manik Lal Das. *SQLshield: Preventing SQL Injection Attacks by Modifying User Input Data.* In Proc. of the International Conference on Information Systems Security (ICISS 2015), Kolkata, India, LNCS 9478, Springer, pp. 192-206, 2015.

Naveen Kumar, Anish Mathuria, and Manik Lal Das. *Achieving Forward Secrecy and Unlinkability in Cloud-based Personal Health Record System.* In Proc. of IEEE International Symposium on Security, Privacy and Anonymity in Internet of Things (TrustCom/BigDataSE/ISPA 2015), Helsinki, Finland, IEEE, pp. 1249-1254, 2015.

Naveen Kumar, Anish Mathuria, and Manik Lal Das. *Comparing the Efficiency of Key Management Hierarchies for Access Control in Cloud.* In Proc. of International Symposium on Security in Computing and Communications, Kelara, India, Springer Volume 536 of Communications in Computer and Information Science, pp. 36-44, 2015.

Nidhi Desai and Manik Lal Das. *On the Security of RFID Authentication Protocols.* In Proc. of IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT 2015), IEEE, Bangalore, India, pp. 1-5, 2015.

Manik Lal Das. *Privacy and Security Challenges in Internet of Things.* In Proc. of the 11th International Conference on Distributed Computing and Internet Technologies (ICDCIT 2015), Springer, February, 2015. [invited paper]

Raghuvir Songhela and Manik Lal Das. *Yet Another Strong Privacy-Preserving RFID Mutual Authentication Protocol.* In Proc. of International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2014), LNCS 8804, Springer, pp. 171-182, 2014.

Naveen Kumar, Anish Mathuria, and Manik Lal Das. *An Efficient Time-Bound Hierarchical Key Assignment Scheme.* In Proc. of the International Conference on Information Systems Security (ICISS 2013), Springer, LNCS 8303, pp.191-198, 2013.

Manik Lal Das. *Strong Security and Privacy of RFID system for Internet of Things Infrastructure.* In Proc. of the International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2013), LNCS 8204, pp.56-69, Springer, 2013.

Naveen Kumar, Anish Mathuria, Manik Lal Das, and Kanta Matsuura. *Improving Security and Efficiency of Time-Bound Access to Outsourced Data.* In Proc. of ACM India Computing Convention, 9, 2013.

Sarita Agrawal, Rodrigo Roman, Manik Lal Das, Anish Mathuria, and Javier Lopez. *A Novel Key Update Protocol in Mobile Sensor Networks.* In Proc. of the International Conference on Information Systems Security (ICISS 2012), LNCS 7671, pp.194-207, Springer, 2012.

Renu Aggarwal and Manik Lal Das. *RFID Security in the context of Internet of Things.* In Proc. of the International Conference of Security of Internet of Things, ACM Press, India, pp.51-56, 2012.

Manik Lal Das. *Grids Security without Public Key Settings.* In Proc. of the 8th International Conference on Distributed Computing and Internet Technologies (ICDCIT 2012), LNCS 7154 Springer, pp.253-254, February, 2012.

C. Anudeep and Manik Lal Das. *An Improved Scheme for False Data Filtering in Wireless Sensor Networks.* In Proc. of the 8th International Conference on Distributed Computing and Internet Technologies (ICDCIT 2012), LNCS 7154 Springer, pp.62-70, February, 2012.

Anil Mundra, Anish Mathuria, and Manik Lal Das. *Detecting flaws in dynamic hierarchical key management schemes using specification animation.* In Proc. of the 8th International Conference on Distributed Computing and Internet Technologies (ICDCIT 2012), LNCS 7154 Springer, pp.166-176, 2012.

Sarita Agrawal and Manik Lal Das. *Internet Of Things - a paradigm shift for future Internet.* In Proc. of the Second International Conference on Current Trends in Technology (NUiCONE 2011), IEEE, Ahmedabad, India, 2012.

Naveen Kumar, Anish Mathuria, and Manik Lal Das. *On Classifying Indirect Key Assignment Schemes for Hierarchical Access Control.* In Proc. of National Workshop on Cryptology, Surat, India 2010.

Manik Lal Das. *Secure and Efficient Authentication Scheme for Remote Systems.* In Proc. of the International Conference of Information Technology (ICIT 2008), IEEE, Bhubaneswar, India, 2008.

Manik Lal Das. *Efficient User Authentication and Secure Data Transmission in Wireless Sensor Networks.* In Proc. of the IEEE International Conference on Networks (ICON 2008), IEEE, India, 2008.

Manik Lal Das and Ravi Mukkamala. *Revisiting Bluetooth Security.* In Proc. of the International Conference on Information Systems Security (ICISS 2008), Hyderabad, India, LNCS 5353, Springer, pp. 132-139, 2008.

Manik Lal Das and V L Narasimhan. *A Simple and Secure Authentication and Key Establishment Protocol.* In Proc. of the International Conference on Emerging Trends in Engineering and Technology, India, IEEE Press, 844 -849, India, 2008.

Manik Lal Das and V L Narasimhan. *Towards a Formal Verification of an Authentication Protocol Using Non-monotonic Logic.* In Proc. of the International Conference of Information Technology - New Generation, IEEE, pp.545-550, USA, 2008.

Manik Lal Das and V L Narasimhan. *EARS: Efficient Entity Authentication in Remote Systems.* In Proc. of the International Conference of Information Technology - New Generation, IEEE, pp.603-608, USA, 2008.

Manik Lal Das. *Authentication Techniques: An Overview.* In Proc. of National Workshop on Cryptology, Cryptology Research Society of India, 2006.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *Cryptanalysis and Improvement of a Multi-signature scheme.* In Proc. of International Workshop on Distributed Computing, LNCS 3741, Springer-Verlag, India, pp.398-403, 2005.

G. Thulasi, Manik Lal Das, and Ashutosh Saxena. *An Efficient Scheme for Digital Cash Using Bilinear Pairings.* In Proc. of Annual National Convention of the CSI, pp.349-357, India, 2005.

G. Raju, G. M. Choudary, Manik Lal Das, Ashutosh Saxena, and V P Gulati. *Cryptanalysis of ID-based Key issuing Protocols.* In Proc. of National Workshop on Cryptology, India, 2005.

Manik Lal Das and Ashutosh Saxena. *Secure Protocol for Authentication in Mobile-Communications.* In Proc. of IEEE International Conference on Mobile Business, IEEE, Australia, pp.23-27, 2005.

Ashutosh Saxena, Manik Lal Das, and Anurag Gupta. *MMPS: A Versatile Mobile-to-Mobile Payment System.* In Proc. of IEEE International Conference on Mobile Business, IEEE, pp.400-405,

2005.

G. M. Choudary, G. Raju, Manik Lal Das, and Ashutosh Saxena. *An Effective Certificateless Signature Scheme Based on Bilinear Pairings.* In Proc. of International Workshop on Security in Information Systems, USA, pp.31-39, 2005.

G. Raju, G. M. Choudary, Manik Lal Das, Ashutosh Saxena, and V P Gulati. *ID-based Serial Multisignature Scheme using Bilinear Pairings.* In Proc. of International Workshop on Security in Information Systems, USA, pp.40-47, 2005.

G. Raju, G. M. Choudary, Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *An Efficient Secure Key Issuing Protocol in ID-Based Cryptosystems.* In Proc. of IEEE International Conference on Information Technology, IEEE, pp.674-678, USA, 2005.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *A Security Framework for Mobile-to-Mobile Payment Network.* In Proc. of IEEE International Conference on Personal Wireless Computing, pp. 420-423, 2005.

Manik Lal Das. *Authentication Techniques Using Smart Cards.* Doctoral Research Symposium, India, 2004.

Ashutosh Saxena, Manik Lal Das, V. P. Gulati, and Deepak B Phatak. *Dynamic Remote User Authentication.* In Proc. of International Conference on Advanced Computing and Communications, India, pp.313-315, 2004.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *A Novel Remote User Authentication Scheme Through Dynamic Login Identity.* In Proc. of International Workshop on Distributed Computing, LNCS 3326, Springer-Verlag, pp.532, 2004.

Manik Lal Das, Ashutosh Saxena, and V P Gulati. *An Efficient Multisignature scheme for E-Services.* In Proc. of National Workshop on Cryptology, Cryptology Research Society of India, India, 2004.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *An Efficient Proxy Signature Scheme with Effective Revocation.* In Proc. of International Conference on Cybernetics and Information Technologies, Systems and Applications, pp.23-27, USA, 2004.

Manik Lal Das, Ashutosh Saxena, V. P. Gulati, and Deepak B Phatak. *A Key Management Scheme Based on Collision-resistant Hash Function and Polynomial Interpolations.* In Proc. of International Conference on Number Theory for Secure Communications, pp.164-166, India, 2003.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *Proxy Signatures Using Partial Delegation with Warrant.* In Proc. of International Conference on Number Theory for Secure Communications, pp.152-154, India, 2003.

Technical Reports

Payal Chaudhari and Manik Lal Das. *Privacy-preserving Attribute Based Searchable Encryption.* IACR ePrint Achieve, No. 2015/899, http://eprint.iacr.org/2015/899.

Sarita Agrawal, Jay Patel, and Manik Lal Das. *Pairing Based Mutual Healing in Wireless Sensor Networks.* IACR ePrint Achieve, No. 2015/538, http://eprint.iacr.org/2015/538.

Payal Chaudhari, Manik Lal Das, and Anish Mathuria. *Security Weaknesses of an "Anonymous Attribute Based Encryption" appeared in ASIACCS'13.* IACR ePrint Achieve, No. 2014/1028, http://eprint.iacr.org/2014/1028.

Raghuvir Songhela, and Manik Lal Das. *Wide-weak Privacy Preserving RFID Mutual Authentication Protocol.* IACR ePrint Achieve, No. 2013/787, http://eprint.iacr.org/2013/787

Harsh N. Thakker, Mayank Saha, and Manik Lal Das. *Reputation Algebra for Cloud-based Anonymous Data Storage Systems.* Computing Research Repository CORRabs/1304.4002(2013)

Manik Lal Das. *Comment- Practical Data Protection.* Computing Research Repository - CORR abs/0804.4628, 2008.

Manik Lal Das. *On the Security of "an efficient and complete remote user authentication scheme".* Computing Research Repository - CoRR abs/0802.2112, 2008.

Manik Lal Das. *Comments on "Improved Efficient Remote User Authentication Schemes".* Computing Research Repository - CoRR abs/0712.3037, 2007.

G. Thulasi, Manik Lal Das, and Ashutosh Saxena. *Cryptanalysis of a recent Remote User Authentication Scheme.* International Association for Cryptology Research, ePrint Report No. 2006/028, 2006.

Manik Lal Das, Ashutosh Saxena, and Deepak B. Phatak. *Algorithms and Approaches of Proxy Signature: A Survey.* Computing Research Repository - CoRR abs/cs/0612098, 2006.

Manik Lal Das, Ashutosh Saxena, and V. P. Gulati. *Security Analysis of Lal and Awasthi's Proxy Signature Schemes.* International Association for Cryptology Research, ePrint Report No. 2003/263, 2003.

Personal Information

Date of Birth: 19-February-1970

Nationality: Indian

Gender: Male

Spouse: Uma Das

Son: Sankha Das

******