Professor
Office: 2103, Faculty Block 2
DA-IICT, Gandhinagar
Gujarat-382007, INDIA.
Email: maniklal_das@daiict.ac.in
Phone(O): +91-79-30510617
(M): +91-9723760942
Homepage: http://intranet.daiict.ac.in/~maniklal_das/

Manik Lal Das

Educational Qualifications

Ph. D. (Information Technology), IIT Bombay, India.

M. Tech. (Computer Applications), ISM Dhanbad, India.

M. Sc. (Applied Mathematics), Vidyasagar University, India.

Career Summary

- Teaching/research/industrial experience: **19** years.
- Broad area of Teaching/Research: Information Technology.
- Research Area: Security & Privacy, Cyber Security.
- Funds managed for sponsored projects where I am (and was) involved in: INR **270** Lakhs (funded by DST, CEFIPRA, MCIT, Govt. of India)
- Research publications:
  Book Chapter : **6+**
  Journal : **27+**
  Conference / Workshop : **51+**
- Thesis/Project supervised: **4** PhD students (one student has submitted thesis and another student is ready for synopsis); **20**+ Master theses supervised; **60**+ BTech projects supervised and **80**+ interns worked under my supervision.
- Reviewer/Program committee member/Speaker/Organizer for many national and international forums.
- Held positions for several administrative responsibilities including Board of Studies Convener, Undergraduate Program Convener, Postgraduate Program Convener, Admissions Committee Convener, Curriculum Committee Convener.

Personal Particulars

Date of Birth : February 19, 1970

Nationality : Indian

Gender : Male

Academic Credentials

Examination	Year	Board/Institute	Specialization/Area
M. Sc. (Applied Mathematics)	1993	Vidyasagar University, West Bengal, India	*Specialization:* Operations Research
M. Tech. (Computer Applications)	1998	Indian School of Mines Dhanbad, India	*Dissertation:* Automation of Materials Management
Ph. D. (Information Technology)	2006	Indian Institute of Technology Bombay, India	*Thesis:* Design and Analysis of Authentication Techniques
Postdoctoral Research	2008	Western Kentucky University, USA	Design and Analysis of Security Protocols

Research Interest

- Security & Privacy
- Cyber Security
- Data Security

Honors and Awards

- Senior Member of IEEE
- Life Member of Cryptology Research Society of India
- Chair, IEEE Computer Society Chapter, Gujarat Section
- Vice-Chair, IEEE Gujarat Section

Research Grants

Project title: **Study of Privacy, Accountability and Ownership in IoT**

Funded by Department of Science and Technology, Govt. of India (CEFIPRA) under Indo-French Collaborative Research Programme under DST-INRIA-CNRS Targeted Programme.

Amount Awarded: INR 17.60 Lakh for India side.

Term: 2016-2019

Investigators: Manik Lal Das (PI) and A. Mathuria (Co-PI), India

Investigators: Lafourcade Pascal (PI) and Gerard Chalhoub (Co-PI), University Clermont Auvergne, France

Project title: **Enabling Technologies for Remote Health Monitoring**

Funded by: Gujarat Council on Science and Technology, Govt. of Gujarat.

Amount: 2.8 Lakhs

Term: 2014-2015

Investigators: Biswajit Mishra (PI) and Manik Lal Das (co-PI)

***Project title*: Security and Privacy Infrastructure for Internet Of Things** scenarios and applications.

Funded by Department of Science and Technology, Govt. of India under Indo-Spanish joint Programme of cooperation in Science and Technology.

Amount Awarded: INR 21.44 Lakh for India side.

Term: Completed

Investigators: Manik Lal Das (PI) and A. Mathuria (Co-PI), India

Investigators: J. Lopez (PI) and R. Roman (Co-PI), University of Malaga, Spain

***Project title*: Security proofs and multidisciplinary evaluation for dynamic hierarchical key assignment schemes**

Funded by Department of Science and Technology, Govt. of India under Indo-Japan cooperative Programme.

Amount Awarded: INR 29.36 Lakhs for India side.

Term: Completed

Investigators: A. Mathuria (PI) and Manik Lal Das (Co-PI), India

Investigators: K. Matsuura (PI) and T. Hosoi (Co-PI), University of Tokyo, Japan

***Project title*: Mobile Payment Systems**

Funded by Ministry of Comm. and Information Technology, Govt. of India.

Amount Awarded: INR 100.00 Lakhs.

Term: Completed

Investigators: D. B. Phatak, A. Saxena, V. P. Gulati and Manik Lal Das

***Project title*: Multi-application Smart card based Payment Systems**

Funded by Ministry of Comm. and Information Technology, Govt. of India

Amount Awarded: INR 80.00 Lakhs.

Term: Completed

Investigators: D. B. Phatak, V. P. Gulati, A. Saxena, and Manik Lal Das

Professional Experience

Professor *(September 2016 – present)*
DA-IICT, Gandhinagar, India

Associate Professor (April 2012 – August 2016)
DA-IICT, Gandhinagar, India

Assistant Professor (July 2006 – March 2012)
Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT), Gandhinagar, India

Postdoctoral Researcher (July 2007 – June 2008)
Western Kentucky University, USA

Research Officer (August 2001 - July 2006)
Institute for Development and Research in Banking Technology (IDRBT)
Hyderabad, India

Lecturer (October 1998 – July 2001)
Haldia Institute of Technology
West Bengal, India

Courses taught

Undergraduate Level	Postgraduate Level
- Discrete Mathematics	- System and Network Security
- Data Structures and Algorithms	- Algorithms
- Programming Languages	- Programming Paradigms
- Introduction to Cryptography	- Security Protocols
- Security Protocols	- Information Systems Security
- Computer Networks	- Computer Systems
- Optimization Techniques	- Operations Research

Students Supervised

Ph.D, M.Tech, B.Tech, M.Sc

Research Publications

Contributed Book Chapters (6)

- **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.

Refereed Journals (27)

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

Refereed Conferences (51)

- 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. [to appear]
- 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 & Networks (COMSNETS 2017)*, IEEE, India, 2017.[to appear]
- 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. [to appear]
- 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 & 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** 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)*, India, IEEE, 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)*, Bhubaneswar, India, IEEE Computer Society, 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)*, New Delhi, India, IEEE Computer Society, 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 & Technology*, India, IEEE Press, 844 - 849, 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*, Las Vegas, USA, IEEE Computer Society, pp.545-550, 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*, Las Vegas, USA, IEEE Computer Society pp.603-608, 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*, India, pp.349-357, 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 Computer Society, 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 Computer Society, 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 Computer Society, USA, pp.674-678, 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*, USA, pp.23-27, 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*, India, pp.164-166, 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*, India, pp.152-154, 2003.

Technical Reports (11)

- 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, **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**, 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, 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.

Software Systems Delivered

1) **GSM SIM-based Mobile Payment Systems**: The objective of this project was to develop a mobile payment system for banks. The payment system, named ***mChq***, was designed for mobile payment business. The pilot testing of the project was conducted by an Industry consortium, several banks in India, IIT Bomay and IDRBT-Hyderabad.

2) **Multi-application Smart cards based Payment Systems**: This was a pilot project sponsored by the MCIT, Govt. of India for exploring feasibility and viability of chip-card based payment system in India. I was one of the technical architects of this project. The pilot was tested and found suitable for its commercialization as and when the financial institutions willing to adopt this module.

3) **Key Management system using Hardware Security Module for Payment systems**: The system was designed for master key generation for card issuer and merchants, and personalization of cards at banks for smart card based payment scenarios.

4) **Public Key Certification Module for Certifying Authority**: The objective of the project was to develop the life cycle of the certification process aiming to use the module in Certifying Authority project. The module was designed, developed and tested using the real test cases.

Reviewer / Committee member / Invited Talks

Reviewer

- 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
- Journal of Systems and Software, Elsevier

Technical Program Committee Member / Chair

- *Technical Program Committee member*: International Conference on Next Generation Computing Technologies (NGCT-2017) during Oct, 2017, Dehradun, India.
- *Technical Program Committee member*: International Conference on

Intelligent Communication and Computational Techniques, Jaipur, India, 2017.

- *Technical Program Committee member*: International Conference on Smart Systems, Innovations and Computing, Jaipur, India, 2017.
- *Technical Program Committee member*: International Conference on Soft Computing and its Engineering Applications, Vadodara, India, 2017
- *PhD Conclave co-chair*: ISEA ASIA Security & Privacy Conference, Jan 28-Feb 1, 2017, Surat, India.
- *Technical Program Committee member* : IEEE International Conference on MOOCs, Innovation and Technology in Education (MITE 2016), December 9-10, , Madurai, India, 2016.
- *Technical Program Committee member*: International Conference on Mathematics and Computing (ICMC 2017) during January 17-21, 2017, Haldia, India.
- *Technical Program Committee member*: International Conference on Distributed Computing and Internet Technologies (ICDCIT 2017), January 13-18, Bhubaneswar, India, 2017.
- *Technical Program Committee member*: ACM Compute 2016, 21-13 October, Gandhinagar, 2016.
- *Technical Program Committee member*: International Conference on Information Systems Security (ICISS 2016), December 16-20, 2016, Jaipur, India
- *Technical Program Chair*: TENSYMP 2015, Gandhinagar, India, May 13-15, 2015.
- *Technical Program Committee member*: IEEE International Conference on Computing, Communication & Automation (ICCCA 2015), May 15-16, 2015
- *Technical Program Committee member*: International Conference on Distributed Computing and Internet Technologies (ICDCIT 2015), February 5-8, Bhubaneswar, India, 2015.
- *Technical Program Committee member*: International Conference on Computing and Communication Systems, April 9-10, 2014, India.
- *Technical Program Committee member*: International Conference on Mathematics and Computing (ICMC 2015) during January 05-10, 2015, Haldia, India.
- *Technical Program Committee member*: IEEE International Symposium on Signal Processing and Information Technology, 2014, India.
- *Technical Program Committee member*: International Conference on Contemporary Computing. August 7-9, 2014, Noida, India.
- *Technical Program Committee member*. International Workshop on Mobile Cloud Computing: Data, Management & Security, June 3-6 2013, Milan, Italy.
- *Technical Program Committee member*. Second International Workshop on Cloud Computing & Identity Management (CloudID 2013), Mysore, India, 22-25 August, 2013.

- *Technical Program Committee member*: International Conference on Distributed Computing and Internet Technologies (ICDCIT 2013), February 5-8, Bhubaneswar, India, 2013.
- *Technical Program Committee member*: International Conference on Intelligent Systems and Signal Processing (ISSP 2013), 1-2 March, 2013, Vallabh Vidyanagar, Gujarat, India.
- *Technical Program Committee member*: Third International Conference on Advances in Computing, Communication and Control (ICAC3 2013), January Mumbai, India, 2013.
- *Technical Program Committee member*: International Workshop on Cloud Computing and Identity Management (CloudID 2012), August 3-5, Chennai, India, 2012.
- *Technical Program Committee member*: Workshop on the Security of the Internet of Things (SecIoT 2011), Dalian (China), October 19, 2011.
- *Technical Program Committee member*: International Workshop on Identity, Security, Management and Applications, Kerala, India, 2011.
- *Technical Program Committee member*: International Workshop on Convergence Security in Pervasive Environments (IWCS 2011), Crete, Greece, 2011.
- *Technical Program Committee member*: International Conference on Computing, Communication, and Control, Mumbai, India, January 28-29, 2011.
- *Technical Program Committee member*: International Conference on Information Science and Applications (ICISA 2010), Seoul, Korea, April 21st - 23rd, 2010.
- *Finance Chair*: International Conference on Information System Security (ICISS 2010), December 15-19, 2010, Gandhinagar, India
- *Technical Program Committee member*: International Conference on Intelligent Systems and Data Processing, Ahmedabad, India, January 24-25, 2011.
- *Technical Program Committee member*: Workshop on the Security of the Internet of Things (SecIoT 2010), Tokyo, Japan, November 29 - December 1, 2010.
- *Technical Program Committee member*: National Conference on Mobile and Pervasive Computing (CoMPC 2010), Chennai, India, 2010.
- *Technical Program Committee member*: National Workshop on Cryptology, India, 2009.
- *Technical Program Committee member*: The Fourth International Symposium on Ubiquitous Applications & Security Services (UASS 2009), USA, 2009.
- *Technical Program Committee member*: International Conference on Emerging Trends in Computing (ICETiC 2009), India, Jan 08-10, 2009.
- *Technical Program Committee member*: IEEE International Conference on Emerging Trends in Computing, India, 2008.
- *Session Chair* - Information Security and Privacy Track: International Conference on Information Technology – New Generation, USA, 2008.

Invited Talks/Presentations

- Security and Privacy Challenges in the Internet of Things. Marwadi University, March 18, Rajkot, India, 2017. **[Invited Talk]**
- Cyber Security Issues and Challenges. State-level Workshop on Emerging Technologies, December 22, 2016, Ahmedabad, India. **[Invited Talk]**
- Security and Privacy Challenges in the Digital Age. State-level Seminar Series on Emerging Technologies, 17-18 April, Ahmedabad, India, 2015. **[Invited Talk]**
- Security and Privacy Challenges in the Digital Age. National Conference on Innovative and Emerging Technologies, 17-18 April, Ahmedabad, India, 2015. **[Keynote Talk]**
- Privacy and Security Challenges in Internet of Things. International Conference on Distributed Computing and Internet Technologies (ICDCIT 2015), February 5-8, Bhubaneswar, India, 2015. **[Invited Talk]**
- Internet of Things – Challenges and Opportunities. International Conference on Contemporary Issue in Engineering and Technology, March 19-21, 2014, Ahmedabad, India. **[Keynote Talk]**
- Security and Privacy Challenges in Internet of Things. SVNIT, Surat, India, December 2013. **[Invited Talk]**
- Security and Privacy Challenges in Internet of Things. Central University Rajasthan, India, December 2013. **[Invited Talk]**
- Elliptic Curves Cryptography. Central University Rajasthan, India, December 2013. **[Invited Talk]**
- Security in Wireless Networks. Haldia Institute of Technology, India, December 2012. **[Invited Talk]**
- Security and Privacy Challenges in Internet of Things. National Institute of Technology, Surat, India, May 2011. **[Invited Talk]**
- Identity-based Cryptography. National Institute of Technology, Surat, India, May 2010. **[Invited Talk]**
- Web Security. National Institute of Technology, Surat, India, January 2009. **[Invited Talk]**
- Dynamic Authentication. National Institute of Technology, Surat, India, January 2009. **[Invited Talk]**
- Identity-based Cryptosystems, Computer Science deptt., Western Kentucky University, USA, May 2008. **[Invited Talk]**
- Visited **National Institute of Standards and Technology (NIST)** in 2008 for attending the event on Federal Information Security Management Act implementation project.
- Authentication Techniques, Computer Science deptt., Western Kentucky University, USA, April 2008. **[Invited Talk]**
- Authentication Protocol, International Conference on Information Technology – New Generation, USA, January 2008.
- Certificateless Cryptosystems, National Institute of Technology, Surat, India, October 2006.
- Authentication Techniques – *from Password to Public key*. GHP Engineering College, Anand, India, November 2006.
- Design and Analysis of Authentication Techniques. K R School of Information Technology, Indian Institute of Technology Bombay, 2006.

- Proxy Signatures. Institute for Development and research in Banking Technology, India, 2005.
- Two-factor Authentication. International Conference on Distributed Computing, India, 2005.
- Smart cards security. Institute for Development and Research in Banking Technology, India, 2004.
- RSA-based Proxy Signatures. International Institute of Informatics and Systemics, USA, 2004.
- Security architecture for mobile payment. International Conference on Personal Wireless Computing, India, 2004.
- Authentication techniques using smart cards. Doctoral Symposium, India, 2004.
- Key Management Scheme. International Conference on Number Theory for Secure Communications, India, 2003.
- Cryptanalysis for stereotyped message. National Conference on Cryptology Research, India, 2003.

Programmes Organized

Involved in organizing many national/international conferences, workshops and short-term training programmes.