SIDDAGANGA INSTITUTE OF TECHNOLOGY
Tumkur, Karnataka, India
DEPARTMENT OF COMPUTER SCIENCE & ENGG.

Bio-data

1. NAME : Dr. N.R.SUNITHA

2. DATE OF BIRTH : 05-03-1969

3. NATIONALITY: INDIAN

4.OFFICIAL ADDRESS : Dr.N.R.Sunitha
Professor & Head
Department of Computer Science & Engg.
Siddaganga Institute of Technology,
Tumkur-572103, India.

5. RESIDENTIAL ADDRESS : Dr. N.R.Sunitha
"SiddaShree", 15th Cross
SIT Extension, Tumkur-572103, India.

6. CONTACT NO.: Off.: (0816) 2214005 Res.: (0816) 2274579
Mob. : 9986276851

7. E-MAIL ID : nrsunitha@sit.ac.in, nrsunithasit@gmail.com

8. EDUCATIONAL QUALIFICATION :

DEGREE	Year	UNIVERSITY	CLASS OBTAINED
B.E.(Electronics & Communication)	Dec. 1990	Gulbarga University	I Class
M.S.(Software Systems)	Dec. 1995	Birla Institute of Technology and Science , Pilani	I Class

Ph.D	April 2011	Visveswaraiah Technological University, Belguam	Thesis Title: New Signature Protocols and Applications in e-Banking. Worked under the guidance of Dr.B.B.Amberker, Professor, Dept. of CSE,NIT, Warangal, Andhra Pradesh, India.

9. Work Experience : 24 years

Industry/College	Designation	Period
Siddaganga Institute of Technology, Tumkur-3	Professor Dept. of CSE Head of the Department of CSE	Since 29-08-2011 Since 01/07/2014
Siddaganga Institute of Technology, Tumkur-3	Associate Professor Dept. of CSE	01-01-2011 to 28-08-2011
Siddaganga Institute of Technology, Tumkur-3	Assistant Professor Dept. of CSE	08-11-1998 to 31-12-2010
Siddaganga Institute of Technology, Tumkur-3	Lecturer Dept. of CSE	16-06-1996 to 07-11-1998
Siddaganga Institute of Technology, Tumkur-3	Programmer Dept. of CSE	07-09-1992 to 12-06-1996
Bharath Electronics, Bangalore	Graduate Trainee	01-11-1991 to 31-08-1992

10. Teaching :

Taught the following courses for B.E. / M.Tech./ MCA Degree Programmes :

Operating Systems , Simulation & Modeling, System Software, Finite Automata and Formal languages, Object Oriented Analysis and Design, Object Oriented Programming, Unix Shell programming, Multimedia Communication, Unix System Programming, Linux Internals, Database Management Systems, Storage Area Networks, Cryptography and Network Security, Problem solving using computers, Optical Networks, Advanced Operating Systems, Cyber Security, Big Data and Data Analytics, High performance Computing.

11. Research Contributions

- Refereed Journals : (published : 16 Nos. submitted: 03 Nos.)
- Book Chapters in Springer Verlag : 06 Nos.
- International Conferences : 42
  - IEEE : 15 Nos.

- Springer : 04 Nos.
- ACM : 07 Nos.
- Others (IACR, IAENG, CISTM, Elsevier…….) : 16 Nos.

- Completed the following Research projects:
  - Research Project titled "Device Cyber Security" with ABB GISL, Bangalore. (1.78 lakhs)
  - Research Project titled "Generic Key management Infrastructure (GKMI)" with ABB GISL, Bangalore . (7 lakhs)
  - AICTE sponsored project "Design and Performance Evaluation of Algorithms for Key Management and Security of Routing Protocols for Distributed Sensor Networks".
  - Research project titled " Techniques for Security on Adhoc Networks" funded by DRDO (9.614 lakhs).
  - Security Solutions to participatory Sensing: a citizen powered approach funded by KSCST, IISc., Bangalore.

- Presently executing the following Research projects:
  - Research project titled " Side-channel attacks infrastructure framework" funded by ABB GISL, Bangalore. (15 lakhs)
  - Smart Meter funded by ICT Skill Development Society, Department of IT, BT and S&T, Govt. of Karnataka (4 lakhs)

- Applied to SAG, DRDO for funding of the following Research:
  - Formal Verification of Security Protocols in Network Devices (22.31 lakhs)

- Six patents filed
  - Secure SCADA
  - DNS Security
  - Method, System and Apparatus for Personal Privacy of Medical Data Set
  - Method and Apparatus for Intra-Group and Inter-Group Key Management in Spontaneous Wireless Ad-Hoc Networks
  - A Layered Encryption Method for Critical Infrastructure Network
  - Secured Data Transmission Using Modified AES algorithm

- Reviewer for the journals Elsevier's Computers and Security and Intl. Journal of Network Security (IJNS).
- Chairperson in the International conferences CISTM 2007 (Conference on Information Sci. Tech. & Mgt.) CSNA 2010 (Conference on Network Security & Applications) , NCACA, National Conference on Advances in Computer Applications, International Conference on Advances in Computing, ICAdC 2012.
- Biodata included in Marquis Who's is Who in Science & Engineering 2010.
- IBM Mentor Award during 2014.

12 About Ph.D Work :

In this thesis, we focus on developing different digital signature protocols with application to various activities in an e-banking environment. A highlight of our results is given below:

- **Secure e-cheque clearance between Financial Institutions:** For an untrusted banking environment, a protocol is devised to perform secure inter FI (Financial Institution) e-cheque clearance operations. Also, a method is formulated in which one can verify that two signatures received from a signer indeed belongs to the same signer without the help of public key of the signer assuming the validity of the first signature. This method is applied for DSA and ElGamal Signatures.
- **Forward-Secure Signatures:** Forward-Secure Digital Signatures enable the signer to guarantee the security of messages signed in the past even if his secret key is exposed today. A solution is given to the two open problems stated in the Bellare-Miner paper on Forward-Secure signatures. A Forward-Secure like signature scheme is modeled which can be used for unbounded number of time periods. Further, Forward-Secure schemes for basic digital signatures like DSA and ElGamal are developed.
- **Forward-Secure Multi-signatures:** It is proposed to apply the concept of Forward-Security to multi-signatures. The basic signature schemes considered are ElGamal and DSA Signature schemes. Initially these signature schemes are made forward-secure and then multi-signatures are developed. These can be used to provide e-cheque facility for joint account holders with collective signing agreement and also be used to provide Transferable e-cheques.
- **Proxy Signatures:** A proxy signature scheme is proposed which can be used to control delegation of financial power to a proxy signer. Also, as digital signatures, proxy signatures are also vulnerable to leakage of proxy secret key. Therefore, the property of forward-security is applied to proxy signatures. Two Forward-secure proxy signature schemes are proposed, one based on DSA and the other based on popular Bellare-Miner scheme. In another scheme, a Forward-secure proxy signature scheme for a proxy signer with multiple original signers is proposed. All the schemes proposed are provided with proxy signer revocation.
- **Proxy Re-signatures:** A Multi-use unidirectional proxy resignature system and schemes which translates one type of signature scheme to another type are developed. A proxy resignature scheme for RSA is also proposed . All the schemes are provided with proxy signer revocation.
- **Aggregate Signatures:** Aggregate schemes for some Forward-Secure Signature Schemes are proposed. ElGamal, DSA and Bellare-Miner forward-secure signatures are considered for aggregation.

13. About Research Projects Executed:

i) Research project titled "**Device Cyber Security**" funded by ABB, GISL, Bangalore.

Following Research work was carried out

1) A survey on state of art in digital signature algorithms for Embedded Systems
2) Analysis of various algorithms for Complexity and Security Strength.
3) Tools and Techniques to evaluate Security Strength of the algorithms
4) Propose the best algorithm and provide a map for the infrastructure of Power Sectors.

ii) Research project titled "***Generic Key Management Infrastructure***" funded by ABB, GISL, Bangalore.:

Following Research work was carried out

(1) Study on various use cases w.r.t. key management in an industrial automation environment.
(2) Designing an architecture for GKMI, which includes all components of key management.
(3) Identification & implementation of methods/techniques.
(4) Feasibility study of GKMI in an industrial automation environment.
(5) Developing a prototype of GKMI.
(6) Conducting performance analysis.
(7) Generating performance reports.

iii) Research project titled "***Techniques for Security on Adhoc Networks" (completed)*** funded by DRDO, New Delhi :

Research on security of MANETs remains active, in spite of years of exploration, in both academia and industry. It is partially due to the fact that no mature solution is widely accepted and the growing availability of small, personalized mobile devices with peer to peer communication capability through wireless channels.

Cryptographic techniques used in MANETs can be classified into two categories, namely, Symmetric Key based and Asymmetric Key based. Identity-based cryptography (IBC) is a special form of public key cryptography. It is an approach to eliminate the requirement of a CA and PKCs. Since 2001, IBC has attracted more and more attention

from security researchers. Some properties of IBC make it especially suitable for MANETs.

It is proposed to develop Identity Based Cryptography (IBC) for **key management** and **secure routing** and **demonstrate** the solution on a test-bed.

iv) Research project titled **"*Side-channel attacks infrastructure framework*" (ongoing)** funded by ABB, GISL, Bangalore.

The proposal aims at:

i) Establishing security laboratory with selected devices and network to measure information leakage through side channels by various cryptographic devices.

ii) Survey of side channel attacks

iii) Comparative study of side channel attacks on widely used security algorithms like RSA,AES,DSS etc,

iv) Demonstration of side channel attacks on simple operations like EXOR logic.

v) Identification of side channel information that get exposed on cryptographic devices

vi) Design of methods for security implementations which are robust to side channel attacks

v) Research project titled ***"Algorithms for Key Management and Security of Routing Protocols for Distributed Sensor Networks"*** **funded by AICTE, New Delhi.**

We have addressed the security problems related to Key Distribution and Routing in Wireless Sensor Networks(WSN). Following are the salient features of this research work:

1) The concept of role based trust/reputation model is used to evaluate the trustworthiness of sensor nodes.

2) A neighbor based dynamic key distribution scheme is developed to provide authentication between the nodes for secure communication in a densely deployed WSN.

3) Role based Dynamic Trust model for route selection is proposed to establish secure, reliable path between sensor nodes & base station and also to deal with potential faulty sensors in WSN. In our proposed system we have considered certain roles of sensor nodes such as: Packet forwarding, Data Aggregation and Time synchronization.

4) A Key Management Infrastructure which supports various key management procedures in a resource constrained environment is proposed. Instead of securely

transmitting the secret keys, we propose to generate the secret keys in the communicating nodes using polynomial and matrix based approaches.

5) The concept of self-diagnosis which enables sensors in a network to diagnose themselves. Diagnosis tasks are executed which make the sensor nodes to join the diagnosis process and infer the root causes based on local evidences. The advantages of self-diagnosis are: They save a large amount of transmissions by applying local decision. They provide more real-time diagnosis results. Also, self diagnosis avoids information loss on the way to sink and thus improves the accuracy. In literature, self diagnosis is done to identify high retransmissions occurring across the wireless sensor networks. We have proposed self diagnosis techniques to identify errors in Data aggregation, Key synchronization and Forwarding of packets.

vi) Research project on **Smart Meter** funded by ICT Skill Development Society, Department of IT, BT and S&T, Govt. of Karnataka

vii) Research project on "Security Solutions to participatory Sensing: a citizen powered approach", funded by KSCST, IISc., Bangalore.

viii) Research project titled "***Formal Verification of Security Protocols in Network Devices" (ongoing)*** funded by DRDO (SAG), New Delhi .

12. List of Research publications :

2006

International Conference:

1.B.B.Amberker, P.Koulgi and N.R.Sunitha, Application of Forward Security to Mobile Computing, In: Third IEEE and IFIP International Conference on Wireless and Optical Communications Networks (WOCN), 2006.

National Conference:

1.N.R.Sunitha, B.B. Amberker and P. Koulgi, Forward Security for an ElGamal-like Signature Scheme, National conference on Mathematical Foundations of Coding, Complexity, Computation and Cryptography, IISc., Bangalore , June 2006.

2007

International Journals:

1.N.R.Sunitha, B.B.Amberker, P.Koulgi, Forward Secure Signatures for Unbounded Time Periods in Mobile Applications, International Journal of Computer Science and Network Security, Vol.7, No.5, May 2007, pp. 208-212.

2.N.R.Sunitha, B.B.Amberker, P.Koulgi, Controlled delegation in e-cheques using Proxy Signatures, Journal of Advanced computations, Vol 1, Issue 2, October 2007, pp. 74-78. **Impact Factor 0.423**

International Conferences:

1.B.B.Amberker, P.Koulgi and N.R.Sunitha, Forward Secure ElGamal like signatures, In: 6th International Security Conference, Lasvegas, USA, April 11-12, 2007.

2.N.R.Sunitha,, B.B. Amberker, P. Koulgi Repetitive Keys in Forward Secure Signatures with Forgery Detection, Fifth Annual Conference on Information Science Technology and Management (CISTM) 2007, Hyderabad, July 16-18, 2007.

3.N.R.Sunitha, B.B.Amberker, P.Koulgi, Siddharth P., Secure e-cheque clearance between Financial Institutions, In: Joint IEEE Conference on E-CommerceTechnology (CEC'07) and Enterprise Computing, E-Commerce and E-Services (EEE'07), Tokyo, Japan, July 24-26, 2007.

4.N.R.Sunitha, B.B.Amberker, P.Koulgi, Controlled delegation in e-cheques using Proxy Signatures, In: Eleventh IEEE International EDOC Conference (EDOC 2007) on Enterprise Computing, Annapolis, Maryland, U.S.A, October15-19, 2007.

5.N.R.Sunitha, B.B.Amberker, P.Koulgi, Transferable e-cheques using ForwardSecure Multi Signature Scheme, In: IAENG (International Association of Engineers) International Conference on Computer Science and Applications 2007 (ICCSA'07), San Francisco, USA, 24-26 October 2007.

2008

International Journals:

1.N.R.Sunitha and B.B.Amberker, Proxy Signatures for Controlled Delegation, International Journal of Information Assurance and Security, Vol 2, 2008 pp.159-174.

International Conferences:

1.N.R.Sunitha and B.B.Amberker, Secure Signature Protocols, ACM Compute 2008 Doctoral Consortium, Banglaore, India, Jan 18-20 2008.

2. N.R.Sunitha and B.B.Amberker, Forward-Secure Proxy Signature Scheme for Cellphone Service Providers, In: The fifth IEEE and IFIP International Conference on wireless and Optical communications Networks (WOCN 2008), Surabaya, East Java Indonesia, May 5-7, 2008.

3.N.R.Sunitha, B.B.Amberker, P.Koulgi, Secure e-cheques for Joint Account with collective signing using Forward-secure Multi-Signatures, In: 7th IEEE/ ACIS

conference on Computer and Information Science ICIS 2008, Marriot Portland City Center, Portland, Oregon, USA, May 14-16, 2008.

4.N.R.Sunitha and B.B.Amberker , Forward-Secure Proxy Signature and Revocation Scheme for a proxy signer with Multiple Original Signers, In: IACR (International Association of Cryptographic Research) International Conference on Security and Cryptography SECRYPT 2008, Porto Portugal, July 26-29, 2008.

5.N.R.Sunitha and B.B.Amberker, An Undisturbed Banking Environment : A Protocol to handle Managers Transfer, In: 6th Annual Conference on Information Science Technology and Management (CISTM), New Delhi, July 31- Aug. 2, 2008.

6.N.R.Sunitha and B.B.Amberker, Forward-Secure Proxy Signature Scheme with Proxy Revocation, In: The 4th IEEE International Conference on Information Assurance and Security (IAS 2008), Naples, Italy, 8-10 Sept. 2008.

7.N.R. Sunitha and B.B. Amberker, Proxy Re-Signature Scheme for RSA, 20th IASTED International Conference on Parallel and Distributed Computing and Systems, PDCS 2008, Nov. 16-18, 2008, New Brunswick, Canada.

8.N.R.Sunitha and B.B.Amberker, Some Aggregate Forward-Secure Signature Schemes, In: IEEE TENCON 2008, Hyderabad, India, Nov. 18-21, 2008.

9.N.R.Sunitha and B.B.Amberker, Forward-Secure Multi-Signatures, In: 5th International Conference on Distributed Computing and Internet Technologies (ICDCIT) 2008, LNCS 5375, Springer Verlag, pp. 89-99, New Delhi, India, December 10-13, 2008.

10.N.R.Sunitha and B.B.Amberker, A New Method of Verifying Digital Signatures, in e-cheque processing. In: 16th IEEE International Conference on Networks (ICON 2008) New Delhi, India, Dec.12-14, 2008.

11.N.R.Sunitha and B.B.Amberker, Proxy Re-signature Schemes In: IACR (International Association of Cryptographic Research) International Conference on Information Systems Security (ICISS 2008), LNCS 5352, Springer Verlag, pp. 156-157, Hyderabad, India, 16-20 December 2008.

Book Chapters:

1.N.R.Sunitha, B.B.Amberker, P.Koulgi, Transferable e-cheques: An application of Forward-Secure Serial Multisignatures, In Sio-long Ao, Burghard B. Rieger, Su-Shing Chen, Editors, Advances in Computational Algorithms and Data Analysis, ISBN: 978-1-4020-8918-3, Lecture Notes in Electrical Engineering (LNEE), Springer-Verlag, 2008, pp. 147-158.

2.N.R.Sunitha and B.B.Amberker, Forward-Secure Multi-Signatures, LNCS 5375, Springer Verlag, pp. 89-99, New Delhi, India, December 10-13, 2008.

3.N.R.Sunitha and B.B.Amberker, Proxy Re-signature Schemes, LNCS 5352, Springer Verlag, pp. 156-157, Hyderabad, India, 16-20 December 2008.

2009

International Journals:

1.N.R.Sunitha and B.B.Amberker, Some Aggregate Forward-Secure Signature Schemes, International Journal of Information Assurance and Security, Vol 3, Issue 4, 2009, pp 84-90.
2.N.R.Sunitha, B.B.Amberker, New Signature Derivation using Existing Signatures, Academy Publishers, Finland, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009, pp. 47-51.

International Conferences:
1. N.R.Sunitha and B.B.Amberker, Forward-Secure Proxy Signature Scheme for Multiple Proxy Signers using DSA with Proxy Revocation, In: IEEE International Advance Computing Conference IACC'09, Patiala, India, 6-7 March, 2009.

2.N.R. Sunitha, B.B. Amberker, Multi-use Unidirectional Forward-Secure Proxy Re-Signature scheme, IEEE Workshop on Collaborative Security Technologies (CoSec'09 2009), Bangalore, India, Dec.9, 2009.

2010

Book Chapter:

1. N.R. Sunitha, B.B. Amberker, *Proxy Re-signature Scheme that translates one type of Signature Scheme to another type of Signature Scheme*, Third International Conference on Network Security & Applications (CNSA-2010) Chennai, India, Communications in Computer and Information Science (CCIS) Series , Springer Verlag, JULY 23 ~ 25, 2010.

2011

International Journals:

1. Kavitha M. N.R.Sunitha, B.B.Amberker, *A Divisible and Transferable Digital Cash protocol*, International Journal of Computing , June 2011, Vol. 1, Issue 3, 407-413.

2. Shilpa S.G, N.R.Sunitha, B.B.Amberker, *A Trust Model for Secure and QoS Routing in MANETS*, International Journal of Innovative Technology and Creative Engineering, May 2011, Issue Vol.1 No.5,22-31. **Impact Factor 0.499**

3. N.R.Sunitha, B.B.Amberker, *Proxy Re-signature Schemes : Multi-use, Unidirectional & Translations,* Journal of Advances in Information Technology, Volume 2, Issue 3 of 2011.

Book Chapter:

4. Kavitha M. N.R.Sunitha, B.B.Amberker, *A New Transferable Digital Cash Protocol using Proxy re-signature Scheme*, International Conference on Computational Intelligence and Information Technology – CIIT 2011, Springer LNCS-CCIS**,** Nov 07-08, 2011 in Pune, India.

International Conference:

5. Shilpa S.G, N.R.Sunitha, B.B.Amberker, *A New Trust Model for QOS Routing in MANETS*, ICN-2011, International Conference on Communication, Computation, Management and Nanotechnology, REC Bhalki, Sept.23-25, 2011.

2012

International Journals:

1) Shamshekar Patil, N.R.Sunitha, " Security and Energy Efficiency in Wireless Sensor Networks, International Journal of Advanced and Innovative Research , August 2012**.** **Impact Factor 0.349,** SSN: 2278 - 7844

2) Alok G, N.R.Sunitha, "*MAZE Security Protocol for Self Securing S4 Storage Server", Special Issue.,* International Journal of Computer Applications (IJCA), 2012 ..

3) Thejaswini S , N R Sunitha, B B Amberker, *Trust Model for Secure Key Distribution and Routing in Mobile Wireless Sensor Networks,* International Journal of Information Processing . 6(4), 27 - 41. 2012

International Conference:

4) Thejaswini S , N R Sunitha, B B Amberker, *Role based Dynamic Trust Model for Routing in Mobile Wireless Sensor Networks*, The Sixth International Conference on Information processing (ICIP 2012), In proceedings of Springer Verlag, CCIS-Communications in Computer and Information Science, August 10-12,2012, Bangalore.

5) Alok G, N.R.Sunitha, "*MAZE Security protocol for S4 storage server*" ICNICT - 2012 Ghaziabad , 7-8 September 2012.

2013

International Conference:

1) Pramod T C, Pavan Kumar Bharampura Nanjundappa, B Sathish Babu, and N R Sunitha, "An Efficient Key-Distribution approach for SCADA Systems", IEEE International Conference on Research and Development Prospects on Engg. and Technology, (ICRDPET 2013, March 28th , 29th 2013, Nagapattanam, India

2) Alok G, N.R.Sunitha, "*Faker System*", IEEE International Conference on Research and Development Prospects on Engg. and Technology, (ICRDPET 2013), March 28th, 29th 2013, Nagapattanam, India

3) Pramod T.C. N.R.Sunitha "An Approach to Detect Malicious Activities in SCADA Systems", IEEE International Conference on Computing, Communications and Networking (ICCCNT 2013) , July 4-6 2013, Tiruchengode, Tamilnadu.
4) Mahesh Kumar and Sunitha N.R, *"A Novel Forward-Secure Symmetric Key Generation System" ,* International Conference On Emerging Computation and Information Technologies (ICECIT-2013), Nov. 22-23 2013, Tumkur, Karnataka, Inda

5) Pramod TC. N R Sunitha, *"An Efficient Key-Establishment Approach for SCADA Systems"*, International Conference On Emerging Computation and Information Technologies (ICECIT-2013), Nov. 22-23 2013, Tumkur, Karnataka, Inda
6) Shilpa M, Supriya N and Sunitha N.R, "*Extended Diffie-Hellman Key Exchange Algorithm for Position Based Cryptography"*, International Conference On Emerging Computation and Information Technologies (ICECIT-2013), Nov. 22-23 2013, Tumkur, Karnataka, Inda
7) Thejaswini S and Sunitha N R, "*Zero Coding for basic Security Requirements with Zero Trust Network Model"*, International Conference On Emerging Computation and Information Technologies (ICECIT-2013), Nov. 22-23 2013, Tumkur, Karnataka, Inda

International Journals:

1. Pramod TC. N R Sunitha *A Framework to Mitigate Attacks and Establish Secure Communications in SCADA Systems*., International Journal of Information Processing (IJIP) . 8(1), 73-91, 2014

2014

International Conference:

1. Radhakrishna Bhata, N R Sunitha, *OPTAR: Optional PIR Based Trusted Address Resolution for DNS*, South Asian Research Centre(SARC) International Conference on Electrical, Electronics and Computer Science (ICEECS-2014), May 4th 2014, Bangalore
2. Prema S, N.R.Sunitha, *Intra-Group and Inter-Group Key Management in Spontaneous Wireless Ad-Hoc Networks.* Eighth International MultiConference on Information Processing (IMCIP 2014) .
3. Shivaprakash Rangaa, N.R Sunitha, *SW-SDF Based Personal Privacy with QIDB-Anonymization using HadoopMapReduce on Medical Data Set.* Eighth International MultiConference on Information Processing (IMCIP 2014) .
4. Pramod T. C and N. R. Sunitha, *Self-Diagnosis Approach for Key Synchronization Problem in Symmetric Crypto Systems Used in SCADA*, 8th INDIACom; INDIACom-2014, International Conference on "Computing for Sustainable Global Development", 5th – 7th March, 2014, New Delhi.

International Journals:

5. Pramod T. C and N. R. Sunitha **,** *Solution to Key synchronization problem in SCADA crypto Systems : A Self-Diagnosis Approach,* JUET Research Journal of Science and Technology, Narosa Publishing House, New Delhi.

6. Radhakrishna Bhat, N R Sunitha, OPTAR: Optional PIR Based Trusted Address Resolution for DNS, International Journal of Advanced Computational Engineering and Networking, Impact Factor 2.25, Volume 2, Issue 8, Aug.- 2014.

2015

International Conference:

1. Pramod T. C and N. R. Sunitha , Matrix Based Key Pre-distributi on Schemes for WSN, Bilingual International Conference Information Technology-Yesterday, Today, and Tomorrow, DRDO, Feb 19-21 2015, New Delhi.
2. Pramod T. C and N. R. Sunitha , Key Management Issues for Industrial Automati on and Control Systems, Bilingual International Conference Information Technology-Yesterday, Today, and Tomorrow, Feb 19-21 2015, New Delhi.
3. Reethalakshmi M D and N R Sunitha, "Securing Publisher Subscriber System using Identity Based Encryption", International Conference on Recent Advances in Engineering Science & Management IACRAESM-2015, 30th August 2015, New Delhi.
4. Satish Chandra K R and N R Sunitha , "Cost Effective Streaming of videos from the cloud by using iCloudAccess". International Conference on Electrical, Electronics, Computer Science and Mechanical Engineering ICEECSME-2015, 16th August 2015, Pune.
5. Pramod T. C and N. R. Sunitha , *KMI for SCADA and WirelessHART in IACS*, ETFA 2015 - IEEE 20thInternational Conference on Emerging Technology & Factory Automation, Luxembourg, Europe, September 8 - 11, 2015. **IEEE IES Student travel grant award)**

International Journals

1. Pramod T.C and N.R.Sunitha, "Polynomial Based Scheme for Secure SCADA Operations", Elsevier Procedia Technology, Science Direct, Smart Grid Technologies, Vol.21, PP.474-481, 2015.

2. **S S Iyengar,** Pramod T.C and N.R.Sunitha **, "**Key Pre-distribution Scheme with Join Leave Support for Resource Constraint Networks", IEEE Journal on Emerging and Selected Topics in Circuits and Systems (under review).

2016

International Conference:

1. Mahesh Kumar K.M, Reema Mathew, Mallapur Veerayya, Chaitra Vijendra and Sunitha N.R , Secure Ad-hoc On-demand Distance Vector Routing using Identity

Based Symmetric Key Management, International Conference on IEEE International Onference on Wireless Communications, Signal Processing and Networking (WiSPNET 2016), Chennai, March 23-25, 2016.

2. Anusha K Udagatti, Sunitha N R, "Fault Tolerant Public Auditing Scheme in Cloud Environment", IEEE International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT-2016) , 21-23 July 2016, Bangalore
3. Mahesh Kumar K.M, Sunitha N.R, "Hybrid Cryptographically Secure Pseudo-Random Bit Generator" to IEEE International Conference on Contemporary Computing and Informatics, Noida (UP) India, 14-17, Dec 2016.

International Journals:

1. Pramod T.C and N.R.Sunitha, "Key pre-distribution schemes to support various architectural deployment models in WSN", **Inderscience International journal on information and computer security**, special Issue on Challenges and Solutions in Wireless Network Security , Volume 8, Issue 2 2016, DOI: 10.1504/IJICS.2016.078124
2. Pramod T.C and N.R.Sunitha, "Key management infrastructure design and novel techniques to establish secure communications in critical infrastructures". **Inderscience** International Journal of Critical Computer-Based Systems. Vol 6, 2016.

13. **Research Guidance:**

Guiding six candidates for Ph.D under Visvesvaraya Technological University, Belgaum.

14. **Membership of Professional Bodies**

- Association of Computing Machinery, USA (ACM)
- Indian Society for Technical Education, India (ISTE) – Life Member
- Computer Society of India (CSI)
- IAENG (International Association of Engineers)
- IEEE
- Institution of Engineers (FIE)

References :

1. Dr.M.N.Channabasappa
   Director,SIT,Tumkur

2. Dr.B.B.Amberker
   Professor,Dept.of CSE

NIT, Warangal, AP

(Sunitha.N.R.)