

## CURRICULUM-VITAE



### **VARUN SHUKLA**

Assistant Professor  
Department of Electronics & Communication  
Pranveer Singh Institute of Technology  
Kanpur-Agra-Delhi, National Highway-2  
Bhauti, Kanpur-209305, UP, India

Mo. +91-8896717681

Email: [varun.shuklaa@gmail.com](mailto:varun.shuklaa@gmail.com)

#### ➤ **Educational qualification:**

- M.Tech (HONS) in Electronics and Communication from Rajiv Gandhi Technical University (RGTU) (Awarded Silver Medal by Honorable President of India for scoring highest marks at the state level).
- PGDBA (M.B.A) in Marketing and Management from Symbiosis (SCDL), Pune.
- B.Tech in Electronics and Communication from Jaypee University of Information Technology.
- Intermediate and High School both are from UP Board.

#### ➤ **Areas of interest:**

- Cryptography and its applications
- Wireless Security
- Cyber Security
- Network security

- Data communication networks
- **Some Research publications:**
  - In journals and international conference proceedings
    - Tripartite Key Agreement Protocol using Conjugacy Problem in Braid Groups, International journal of computer applications (ISSN: 0975-8887), volume 31, number 1, October 2011.
    - A Secure Money Transaction Scheme (Identification Scheme) using Elliptic Curves, International journal of computer applications (ISSN: 0975-8887), volume 39, number 5, February 2012.
    - A Secure Wireless Communication Protocol using Diffie - Hellman Key Exchange, International Journal of Computer Applications (ISSN: 0975-8887) Volume 126 – No.5, September 2015.
    - A Secure Zero Knowledge Authentication Protocol for Wireless (Mobile) Ad-Hoc Networks, International Journal of Computer Applications (ISSN: 0975-8887) Volume 128 – No.2, October 2015.
    - A New Secure Authenticated Key Agreement Scheme for Wireless (Mobile) Communication in an EHR System using Cryptography, Communications on Applied Electronics (ISSN:2394-4714), Volume 3– No.3, October 2015.
    - Authenticated Wireless Information Display System Using GSM Module, Communications on Applied Electronics (ISSN: 2394-4714), Volume 5, number 3, June 2016.
    - Secure Wireless Communication Protocol: To Avoid Vulnerabilities in Shared Authentication, Communications on Applied Electronics (ISSN: 2394-4714), Volume 7 – number 6, September 2017.
    - A New Key Agreement Protocol Using BDP and CSP in Non Commutative Groups, Int. J. Advanced Networking and Applications Volume: 09 Issue: 03 Pages: 3428-3431
    - An Authenticated Key Agreement Protocol Using Artin's Braid Group, International Journal of Computer Sciences and Engineering (ISSN: 2347-2693), Vol.5, Issue.12, December 2017
    - A bit commitment signcryption protocol for wireless transport layer security (WTLS), 2016 IEEE Uttar Pradesh Section International Conference on

Electrical, Computer and Electronics Engineering (UPCON), December 2016,  
DOI: [10.1109/UPCON.2016.7894629](https://doi.org/10.1109/UPCON.2016.7894629)

- A Cryptographic Key Agreement Communication Protocol for Data Management System, IEEE International conference on advanced computing and software engineering (ICACSE), October 2016.
- Three Party Key Sharing Protocol using Polynomial Rings, IEEE International Conference-UPCON-18 (Scopus Indexed) held on 2-4 Nov, 2018 at MMMUC, Gorakhpur, Paper is available online at IEEE Xplore since February 2019, DOI: [10.1109/UPCON.2018.8596905](https://doi.org/10.1109/UPCON.2018.8596905) .
- A Secure Peer to Peer Entity Authentication Scheme using Lattice Cryptography in JARDCS (Scopus Indexed), volume 2018, issue 6, pp. 1874-1880.
- Nanotechnology and Cryptographic Protocols: Issues and Possible Solutions” in Nanomaterials and Energy (Scopus indexed), Volume 8, Issue 1, June, 2019, DOI: <https://doi.org/10.1680/jnaen.18.00006>
- Cryptocurrency: Characteristics & Future Perspectives” has been published in Everyman’s Science, Indian Science Congress (A government of India body), volume 53, number 2, pp. 77-80.

➤ (b) In national conferences

- An authenticated key agreement protocol for wireless communication using cryptography in TEQIP-II sponsored National conference on emerging trends in electrical & electronics engineering (NCETEE’16) at IET, Lucknow, August 2016.
- A two party communication protocol for financial transactions using discreet logarithm problem in TEQIP-II sponsored National conference on emerging trends in electrical & electronics engineering (NCETEE’16) at IET, Lucknow, August 2016.
- User authentication using elliptic curves in MCM, IBS Khandari campus, (Conducted by Vigayana Parishad), Agra, 24-26 May 2013.
- Secure wireless group communication protocol in 48<sup>th</sup> IETE midterm symposium, April 2017.
- Presented a paper entitled “A User Friendly Authentication Procedure for Peer to

Peer Communication” in National Conference on Mathematical Sciences and Development at Dr.B.R.A. University, Agra on 22-24 December 2018.

- Presented a paper entitled “Vulnerability of Routing Protocols: A Cryptographic Aspect” in National Conference on Mathematical Sciences and Development at Dr.B.R.A. University, Agra on 22-24 December 2018.
- Presented a paper entitled “A Lightweight Authentication Mechanism” in IEEE international conference ICETTA-2019 at REC Kannauj on 1-2 February 2019.
- Presented a paper entitled “On Security of Routing Protocols” in IEEE international conference ICETTA-2019 at REC Kannauj on 1-2 February 2019.
- Presented a paper entitled “Peer to Peer Authentication Method for Wireless Communication Using RSA Cryptosystem” in International conference on Engineering Science & Advance Research (ESAR-18) at Faculty of engineering and technology, RAMA University, Kanpur on 23-24 February 2018.

➤ **Books published:**

The books are in the field of management. There are three volumes under the project-outline series which targets all the three pillars of Indian economy, Government sector banks (SBI), Private sector banks (ICICI) and Life insurance corporation (LIC).

- Study with reference to reason of preference for ICICI prudential, LAP Lambert Academic Publishing, Germany, ISBN-13: 978-3-659-26443-6, ISBN-10: 3659264431, March 2014.
- SBI-The backbone of Indian banking system, LAP Lambert Academic Publishing, Germany, ISBN-13: 978-3-659-91170-5, ISBN-10: 3659911704, June 2016.
- Life insurance corporation (LIC) of India-Consumer aspect, LAP Lambert Academic Publishing, Germany, ISBN-13: 978-3-659-92701-0, ISBN-10: 3659927015, July 2016.

➤ **Membership of professional bodies:**

- Life member of Cryptology research society of India (CRSI) (Membership no. L0834).
- Life member of The Institution of Electronics and Telecommunication Engineers (IETE) (membership no. M501351)

- Life member of The Indian Society for Technical Education (ISTE) (membership no. LM120167)
- Life member of the Institution of Engineers (India) (IEI) (membership no. M1632129)
- Life member of Indian Science Congress (ISC) (Membership no. L33404).
- Life member of The Internet Society (Membership no. 150147).
- Life member of IANEG (Membership no. 162192).
- Life member of IRED (Membership no. AM10100056524).

➤ **FDPs/Workshops/seminars/conferences attended:**

- Participated as a coordinator in National Workshop on Cryptology & Network Security (NWCNS-19) on 11-13 January 2019 under the aegis of CRSI and DRDO at PSIT, Kanpur.
- Attended a five day FDP on Network security on 20-24 may 2019 organized by ICT academy, Ministry of Electronics and Information Technology (MeitY) and NIT Patna at PSIT, Kanpur
- Attended a five day FDP on VLSI Chip Design Hands-on Using Open Source EDA on 8-12 July 2019 organized by ICT academy, Ministry of Electronics and Information Technology (MeitY) and NIT Patna at PSIT, Kanpur
- One week FDP on Recent trends in wireless & mobile communication on 04-09 June 2018 conducted by Dr APJAKTU at PSIT, Kanpur
- Seven days workshop on Micro-controller and its application on 19 June 2017-24 June 2017 conducted by APJAKTU at PSIT, Kanpur.
- One day Faculty development program on Patents and Copyrights, 30 June 2016.
- One day seminar on R & D trends in technology and sustainable innovation, 30 July, 2016.
- Attended Quality Management Workshop by ISO and successfully cleared the exam.
- Attended two day workshop conducted by Ministry Of Human Resource Development, Government of India (MHRD).

- Two days workshop on Deployment & use of mini MOOCs under the research project entitled: Innovative research in pedagogy for mini-MOOCs blended with instruction strategies to enhance quality of higher education, sponsored by Royal academy of engineering, London and Thapar University, Patiala, 16-17 June 2017 at PSIT, Kanpur.
- One day workshop on virtual laboratories conducted by IIT, Kanpur, an initiative of Ministry of Human Resource Development (MHRD), Government of India via national Mission on Education through Information and Communication Technology (NMEICT) on 30 November 2016.
- One day faculty development program on NBA conducted by Equate-India.
- One day workshop on Brahaspati-The virtual classroom conducted by IIT-Kanpur.
- One week FDP on Microprocessors conducted by PSIT/PSITCoE, Kanpur.
- Attended a seven days workshop on Digital Signal Processing conducted by HBTI Professors at PSIT, Kanpur.

➤ **Online certification courses:**

- NPTEL course on Introduction to research conducted by IIT-Madras with a score of 67%.
- NPTEL course on Developing soft skills and personality conducted by IIT-Kanpur with a score of 83%.
- NPTEL course on Introduction to cryptology conducted by IIT-Roorkee with a score of 65%.
- NPTEL course on Enhancing soft skills and personality conducted by IIT-Kanpur with a score of 82%.
- NPTEL course on Internetwork security conducted by IIT-Kharagpur with a score of 80% (Holds a place in All India Toppers category).
- NPTEL course on Wireless ad hoc and sensor networks conducted by IIT-Kharagpur with a score of 57%.

➤ **Various academic and administrative duties:**

- IIT-Madras appointed me a part of NPTEL-Text to Translation project run by Ministry of Human Resource Development along with IITs and IISc. I have reviewed a course on Soft Skills conducted by IIT-Roorkee (Prof. Binod Mishra). I have reviewed the full course of 38 hours duration.
  - Flying squad team leader at UPTTI (college code: 044) appointed by Uttar Pradesh technical university in 2013-14 even semester examinations.
  - Flying squad team member at UPTTI (college code: 044) appointed by Uttar Pradesh technical university in 2013-14 odd semester examination.
  - Flying squad team member at PSITCoE (college code: 348) appointed by Uttar Pradesh technical university in 2014-15 even semester examination.
  - Question paper setter of Uttar Pradesh technical university of various subjects.
  - Question paper setter of Chandrashekhar Azad Agricultural University (CSA) (Faculty of Engineering and Technology) of various subjects.
  - External practical examiner of various subjects appointed by Uttar Pradesh Technical University.
  - Proctorial board member of the session 2016-17 at PSIT, Kanpur.
  - Advisory committee member of one week FDP on micro-controller & its applications conducted by APJ AKTU on 19-24 June 2017.
  - Publicity committee member of one week FDP on Recent trends in wireless & mobile communication conducted by Dr APJAKTU on 4-9 June 2018.
- **Reviewer/Editorial member:**
- Board member of International journal of engineering research and science (ISSN: 2395-6992).
  - Reviewer of Journal of Advances in Mathematics and Computer Science.
  - Reviewer of Journal of Basic and Applied Research international (International Knowledge Press).
  - Asian Journal of Current Research (International Knowledge Press).
  - Reviewer of Asian Journal of Mathematics and Computer Research.

- Reviewer of British journal of mathematics and computer science.
- Reviewer of International journal of network security.
- Reviewer of Athens Institute for Education and Research (ATINER).
- Reviewer of Asian Journal of Research in Computer Science

➤ **Awards and appreciations:**

- Received best paper award for presenting a paper entitled “Quantum cryptography with nanotechnology: Issues and future perspectives” in National conference on nanotechnology held at PSIT, Kanpur during 18-19 November, 2017.
- Honoured with Rashtriya Gaurav Award (An award of national repute) given by IIFS in December 2017.
- Copyrighted an algorithm entitled “A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography” with registration number L-70706/2017 awarded by copyright office, department of industrial policy & promotion under ministry of commerce and industry, government of India.
- Copyrighted an algorithm entitled “A secure stop and wait communication protocol for disturbed networks with registration number-73429/2018 awarded by copyright office, department of industrial policy & promotion under ministry of commerce and industry, government of India.
- Got feedback appraisal letter for scoring very high feedback (91.16%) in the teaching learning process in 2018-19 odd semester.
- Got feedback appraisal letter for scoring very high feedback (81.27%) in the teaching learning process in 2017-18 even semester.
- 
- Won University Silver Medal in M.Tech and Awarded by Mr. Pranab Mukherjee, Honorable President of India in June 2013.
- Faculty appreciation award by PSIT, Kanpur in the year 2017.
- Faculty appreciation award by PSIT, Kanpur in the year 2018.



- Faculty appreciation award by PSIT, Kanpur in the year 2019 for significant contribution in research.
- Letter of appreciation by training and placement department of PSIT, Kanpur for contributing significantly in the placement activities in the year 2016.
- Secured a place in all India topper categories in NPTEL course on Internetwork Security conducted by IIT-Khadagpur in the year 2017.
- Cleared Scholarship exam from ASNT in collaboration with University of Texas for Master of Science in the field of Information Security and Ethical Hacking, 2008-09 (Scholarship of INR 15000 per month was offered).

➤ **Personal details**

- Date of Birth : 19.12.1986
- Sex : Male
- Father's Name : Late. R. D. Shukla
- Nationality : Indian
- Marital status : Married
- Permanent Address : F-88, Panki, Kanpur-208020
- Correspondence Address : F-88, Panki Kanpur-208020