Ras Dwivedi

112, Old RA Hostel, IIT Kanpur, Kanpur, Uttar Pradesh 208016

+91 9416212814 dwivedi@cse.iitk.ac.in https://www.linkedin.com/in/ras-dwivedi/ github.com/Ras-Dwivedi

About Me

I am a Ph.D. candidate at the Indian Institute of Technology Kanpur, actively seeking postdoctoral opportunities in the realm of trusted computation and distributed systems. My extensive academic journey has fueled a profound interest in Blockchain, Cryptography, and the intricate domain of privacy-preserving data sharing.

Education

Ph.D. Candidate **Sep. 2017 – Present**
Indian Institute of Technology, Kanpur *CPI:8.7*
Advisors: Dr. Manindra Agarwal, Dr. Sandeep Shukla

Bachelor of Technology **Sep. 2007– 2011**
Indian Institute of Technology, Kanpur *CPI:7.9*

All India Senior School Certificate Examination **2006**
St. Paul's Senior Secondary School *88.8%*

All India School Certificate Examination **2004**
St. Paul's Senior Secondary School *90.00%*

Publications

Cross-Chain Atomic Swaps without Time Locks. **BCCA 2023**
Ras Dwivedi, Tushar Singla and Sandeep Shukla
5^{th} International Conference on Blockchain Computing and Applications

Pluggable Integrity layer for Property Registration **BCCA 2023**
Ras Dwivedi, Mukul Verma, Tanmay Yadav and Sandeep Shukla.
5^{th} International Conference on Blockchain Computing and Applications

Blockchain-Based Transferable Digital Rights of Land. **ICSF 2023**
Ras Dwivedi, Sumit Patel and Sandeep Shukla
8^{th} International Conference on Smart Finance

Preserving Patient's Privacy using Proxy Re-encryption in Permissioned Blockchain **IOTSMS 2019**
Devendra Meena, Ras Dwivedi and Sandeep Shukla
6^{th} International Conference on Internet of Things: Systems, Management and Security

Entangled Blockchains in Land registry Management **2019**
Ashwin Sekhari, Rishav Chatterjee, Ras Dwivedi, Rohit Negi, and Sandeep Shukla
3^{rd} Workshop on Blockchains and its Applications, IIT Bombay

Patents

Functional Flow Generator **2012**
Medical pump that generates variable fluid flow based on the required flow rate profile

Work Experience

IHUB NTIHAC FOUNDATION | *Sr. Research Engineer* **December 2022-Present**

- **Tokenization of Development Rights**
  - Presented a case for the tokenization of Development Rights against the tokenization of land.
  - Developed a portal for Kanpur Development Authority to identify the sending and receiving zones, tokenize development rights, trade tokens and utilize the development rights token

CRUBN Foundation | *CTO, CFO* **September 2020-December 2022**

- **Java Card Wallet for Hyperledger Fabric**
  - Designed a protocol for user authentication and authorization enabling integration of pluggable eKYC services and hardware wallets. Protocol ensures the replacement of the user's wallet if lost or compromised.
  - Developed a lightweight wallet applet inside a Java card, implementing ECDSA signature using secp-256-r1 curve. The wallet boasts a secure PIN lock and a robust key reset mechanism for enhanced user protection.
  - created customized ASN1 parser to verify CDAC's e-sign response.
- **Self-Sovereign Identity**
  - Formulated a comprehensive business plan for the development of immutable and easily shareable digital credentials, leveraging the Hyperledger Indy blockchain. Notably, the product was officially launched by the Prime Minister of India.
  - Engineered a robust protocol for dynamically modifying the pool genesis file post the blockchain launch, strategically preventing potential Denial of Service (DoS) attacks on the critical genesis nodes.

National Blockchain Project | *Sr. Student Research Associate* **July 2018-September 2020**

- **Privacy Preserving Patient Data Sharing**
  - Designed a patient data sharing framework using Proxy Re-Encryption on Hyperledger Fabric
  - Project builds on top of DEPA framework of Niti Aayog and provides a transparent consent manager
- **Atomic Swaps without Time locks**
  - Created a protocol to conduct an atomic swap between two independent blockchains without locking funds
  - The protocol is fast, deterministic, and does not use hash-time lock nor involve any third party.

NTPC Ltd | *Asst. Manager* **July 2011-January 2017**

- Handled major crisis during world's largest grid failure and took necessart actions to save major critical equipment and by synchronizing with the grid within 3 hours of grid restoration.
- Otimized design parameters for enhanced performance in the Ash Handling plant, successfully averting station shutdown, and finalized comprehensive strategy achieving 100% ash utilization for eco-friendly oeprations
- Led a cross functional team to optimize algorithm for superheater and re-heater temperature and spray control

Professional Services

Teaching Assistant **January 2017- June 2020**

- Introduction to Computing
- Abstract Algebra
- Human-Centered Computing
- Data Structures and Algorithm
- Modern Cryptology
- Blockchain Technology and Applications

Summer Internship Mentor

- Designing Secure File Access System using CL Accumulator and TEE
- Sorting encrypted data using Partially Homomorphic Encryption Schemes

Reviewer **2020-2023**

- IEEE Transactions on Information Forensics and Security, 2023
- Blockchain Technology and its Potential Applications, 2020

Instructor **2018**

- ACA Summer School on Blockchain and Software Security