Nikhil Vanjani

+91-7755057798 • nikhilvanjani61@gmail.com • nikhilvanjani.github.io

Research Interests

Cryptography, Cyber Security, Blockchains, Quantum Computing

Education

Year	Degree (Board)	Institute	Performance
2014-2018	B.Tech., Computer Science and Engg.	Indian Institute of Technology, Kanpur, India	7.8/10.0
2014	XII (CBSE)	Aklank Public School, Kota, India	89.2/100.0
2012	X (CBSE)	Welspun Vidya Mandir, Anjar, India	10.0/10.0

Scholastic Achievements

- **Red Hat Certified System Administrator (RHCSA)** *2017*
- Secured 1^{st} position in **Blockchain Hackathon** organised at Techkriti, IIT Kanpur *2017*
- Secured Rank **461** in **Codechef Snackdown** Final Round among **8500** total teams *2015*
- Secured **All India Rank 201** in **Joint Entrance Examination Advanced** among **1.5** lakh participants *2014*
- Secured **All India Rank 2981** in **Joint Entrance Examination Mains** among **1.4 million** participants *2014*
- Secured **Statewise Top 1 %** (Rajasthan State) in **National Standard Examination in Physics(NSEP)** held by **Indian Association of Physics Teachers**. *2014*

Research Experience

- **Blockchain based Voting Systems** Aug 2019 - Present
  Project Associate under Dr. Shweta Agrawal; IIT Madras (IITM)
  - Surveyed State of the Art E-Voting Protocols - **Pret A Voter, Scratch & Vote, Scantagreity, MarkPledge**
  - Surveyed recent blockchain based and internet based voting schemes and initiatives by various countries
  - Designed a blockchain based E-Voting scheme for **Election Commission of India**
- **Various notions of Obfuscation** Aug - Nov 2019
  Course project for Topics in Cryptography, taken by Dr. Shweta Agrawal; IITM
  - Studied the limitations of iO and explored alternate notions of obfuscation
  - Read and presented a paper by Canetti et. al. - **Obfuscation of Probabilistic Circuits and Applications**
- **Fully Homomorphic Encryption** Jan - Apr 2018
  Course project for Linear Algebra tools for TCS, taken by Dr. Rajat Mittal; IIT Kanpur (IITK) Report
  - Studied about challenges with secure computation and homomorphic encryption
  - Read and presented Craig Gentry's PhD thesis - **A fully homomorphic encryption scheme**
- **Post-Quantum Cryptography** Aug - Nov 2017
  Course project for Quantum Computing, taken by Dr. Rajat Mittal; IITK Report
  - Studied about integer factorisation problem, discrete logarithm problem, elliptic curve based discrete logarithm problem and how they can be easily solved using **Shor's algorithm**
  - Studied Oded Regev's course on *Lattices in Computer Science*
  - Read and presented Oded Regev's paper - **On Lattices, Learning with Errors, Random Linear Codes, and Cryptography**
- **Blockchain Technology** Aug - Nov 2017
  Under-Graduate Project, advised by Dr. Arnab Bhattacharya, Dr. Piyush Kurur; IITK Report
  - Studied Bitcoins and Cryptocurrency Technologies online course from Coursera
  - Explored challenges in blockchains such as - consensus, scalability, privacy
  - Studied Silvio Micali's proposed algorithm -**Algorand** for Scaling Byzantine Agreements for Cryptocurrencies
  - Studied **zk-SNARKs**, the Zero-Knowledge Proofs based protocol behind Zcash

- **Darknet Attacks Analysis** May 2016 - Apr 2017
  Under-Graduate Project, advised by Dr. Sandeep Shukla; IITK, Dr. Nasir Memon; New York University Report
  - Studied about trap-based monitoring systems, operation of darknet, taxonomy of darknet data, extraction of insights on suspicious activities and threats on the Internet
  - Performed **darknet profiling** and **visualized geographical distribution** of attack attempts and port scans
  - Detected **Mirai botnet** and its variants on the various ports they operated on in accordance with the global observations of zero days
  - Leveraged Collective Intelligence Framework on a **honeypot-like network** to gain **cyber threat intelligence**

Work Experience

- **Cohesity** | *Member of Technical Staff* *Jun 2018 - Jul 2019*
  Distriuted File System Team
  - Implemented **CHAP Authentication** protocol for iSCSI
  - Single-handedly created a light weight client for SnapFS - Cohesity's filesystem
  - Implemented **Source-Side Dedup** feature for reads, writes on SnapFS Client
  - Developed support for **SunRPC and gRPC Authentication and Authorization** in SnapFS Client and Server
  - Explored **erasure coding** based on Reed Solomon Codes and Locally Recoverable Codes

  Distributed Systems Team (Sub team: SAP)
  - Worked on **orchestration** of SAP HANA backups to SnapFS via Backint plugin
  - Migrated library dependencies of Backint plugin to **PowerPC** architecture in a **Linux From Scratch** way
  - Resolved **customer issues** by tracing and fixing real time threads utilization issues in asynchronous setup
- **Lucideus Inc.** | *Summer Intern* *May - July 2017*
  - Studied **CIS Benchmarks** for RHEL7, Cisco Switches
  - Articulated **security configuration controls** for **hardening** of Servers (HP - UX), Switches (Juniper, HP, 3COM), Firewalls & VPN (Fortigate), Databases (MySQL, MSSQL) to support automation of the company's enterprise product
  - Calculated CCSS scores for various attack vectors
- **IIT Kanpur New York Office** | *Summer Intern under Dr. Manindra Agarwal, IITK* *May - Jul 2016*
  - Developed an **online learning** collaborative filtering algorithm based on **matrix factorisation** for movie recommendation based on the users' ratings on other movies
  - Trained the model on **MovieLens 1M** dataset and optimized parameters
  - Designed a model incorporating collaborative filtering to generate news feed

Projects

- **Securing Zoobar Web Server** Jan-Apr 2017
  Course project for Computer Systems Security, taken by Dr. Sandeep Shukla; IITK
  - Studied the architecture of the zoobar web server - a model of **OKWS web server**, specialized for building fast and secure web services
  - Exploited security vulnerabilities using **Control Hijacking** techniques like buffer over-flow attacks, privilege escalation, broswer-based attacks like XSS, CSRF, SQL Injection, Side Channel Attacks, Phishing, Worms
  - **Improved security** using Stack Canaries, Privilege Separation and Server-Side Sandboxing
- **Cryptanalysis** Jan-Apr 2017
  Course project for Modern Cryptography, taken by Dr. Manindra Agrawal; IITK
  - Designed and implemented differential cryptanalysis attacks for various encryption schemes - 6-round DES, RSA with small public exponent using Coppersmith Algorithm, 4-round AES
- **Video Summarisation** Aug-Nov 2016
  Course project for Machine Learning & Techniques, taken by Dr. Piyush Rai; IITK Report
  - Surveyed various video summarisation techniques used in state of the art algorithms.
  - Implemented **VSUMM** algorithm and experiemnted with features obtained from SIFT, texture, color histograms
  - Implemented **Shot Boundary Detection** and **LSTM** based algorithms for generating video summary.

Selected Talks

- **Two case studies on advances in Blockchains: Algorand, Zcash** — Apr 2018
  Seminar Talk for National Blockchain Project being undertaken by C3I Center, IIT Kanpur — Slides
- **Convergence to Equilibria in Plurality Voting** — Apr 2018
  Course Project for Algorithmic Game Theory — Slides
- **Combinatorial Game Theory** — Nov 2015
  Course Project for Discrete Mathematics

Relevant Coursework

Theory		**Systems**	**Algorithms & ML**
Topics in Cryptography	Abstract Algebra	Computer System Security	Machine Learning Techniques
Modern Cryptology	Linear Algebra	Bitcoin & Cryptocurrencies	Advanced Algorithms
Quantum Computing	Discrete Mathematics	Computer Networks	Data Structures & Algorithms
Linear Algebra Tools for TCS	Probability & Statistics	Internet Technologies	
	Algortihmic Game Theory		

Co-curricular Activities

- **FSTTCS'17 Conference**: Attended Foundation of Software Technology and Theoretical Computer Science conference held at IIT Kanpur
- **Mentored 10 students** for project on Theory of Blockchains under Association of Computing Activities, IITK
- **Mentored 20 students** for a project on Overview of Cyber Security under Association of Computing Activities, IITK
- **Mentored 8 students** on a Blockchains based project for Medical Record keeping under Programming Club, IITK
- Reading Novels, playing Billiards, Table Tennis, Cricket, Swimming

Leadership

- **Overall Coordinator, Outreach Cell** | *IIT Kanpur* — *Mar 2017 - Mar 2018*
  - **Founded the Cell**, made its proposal and got it passed by the Students' Senate
  - **Prospective students:** Conducted **Info Sessions** at Delhi, Hyderabad, Kota and **Open House** at IIT Kanpur to help JEE Advanced 2017 Qualifiers and their parents make an informed choice for college
  - **Alumni:** Created and designed the special edition of the **Institute Alumni Newsletter**, helped Alumni Association to conduct **Alumni Reunions**
  - **Campus Students:** Reinstated **Tips From The Top**- Career Guidance Sessions by Alumni, started **Alumni Buddy Program**
  - **Branding:** Lead the Institute's online campaign for prospective students, assisted Dean of Resources and Alumni Office to modernize its online **fundraising** efforts