

# Manaar Alam

Secured Embedded Architecture Laboratory  
Department of Computer Science and Engineering  
Indian Institute of Technology Kharagpur, West Bengal, India.

+91 9073202113 • [alam.manaar@iitkgp.ac.in](mailto:alam.manaar@iitkgp.ac.in) • [manaaram.github.io](https://github.com/manaaram)  
[manaaram](#) • [manaar.alam](#)

## Current Position

### Indian Institute of Technology, Kharagpur

*Ph. D. in Computer Science and Engineering,*

I am working under the supervision of *Dr. Debdeep Mukhopadhyay* and *Dr. Sourangshu Bhattacharya*. My research interest mainly lies in the application of Machine Learning techniques in the field of security.

**Kharagpur**

*July 2016–Present*

## Education

### Indian Institute of Technology (Indian School of Mines), Dhanbad

*M. Tech. in Computer Science and Engineering, OGPA - 9.7/10*

Received M. Tech. with *Distinction* and secured 3<sup>rd</sup> place from the department.

**Dhanbad**

*July 2014–June 2016*

### Institute of Engineering and Management (under WBUT)

*B. Tech. in Computer Science and Engineering, DGPA - 8.88/10*

**Kolkata**

*August 2009–May 2013*

### Hindu School (under WBCHSE)

*Higher Secondary Examination (10+2), Overall - 92.6%*

Secured 13<sup>th</sup> place in all over West Bengal. Scored 100% in Mathematics.

**Kolkata**

*July 2007–May 2009*

### Modern School (under WBBSE)

*Secondary Examination (10), Overall - 89.37%*

**Kolkata**

*May 2007*

## Internship Experience

### Nanyang Technological University, Singapore.....

**Title:** *Lightweight Assessment of Malware for Embedded Architectures.*

**Supervisor:** Dr. Siew-Kei Lam.

**Description:** Worked in a team and developed a light-weight application to detect and prevent Malware for embedded platforms based on statistical  $t$  – *test*. The prototype of the application are implemented for both x86 and ARM processors.

**Duration:** August 2017 - January 2018.

## Academic Projects

### M. Tech. Thesis.....

**Title:** *A Novel Parallel Search Technique for Multi-Objective Optimization.*

**Supervisor:** Dr. Haider Banka.

**Description:** Developed a new Parallel Search Technique to deal with various Multi-Objective Optimization Problems. With binary encoding scheme this novel technique performs better than most of the existing multi-objective optimization algorithms like NSGA-II, and MOPS.

**Duration:** July 2015 - April 2016.

### B. Tech. Dissertation.....

**Title:** *Web Sentiment Analysis.*

**Supervisor:** Dr. Satyajit Chakraborty.

**Description:** Designed a web tool which allows visitors to assess the web sentiment on any subject. For each topic a pie chart expresses the current real-time sentiment along with a list of the latest news headlines associated with the subject. The pie chart and the headlines allow seeing what issues or events drive the sentiment in a positive or negative way.

**Duration:** August 2012 - July 2013.

## Other Projects

---

### Vocational Training.....

**Title:** *Online Job Portal using PHP and MySQL.*

**Organizer:** NIVT India.

**Description:** Designed an online job portal which helps both the job seekers and the recruiters to find the right organization and the employees respectively.

**Duration:** June 2012 - July 2012.

**Title:** *Online Photo Gallery using J2EE and MySQL*

**Organizer:** NIVT India.

**Description:** Developed an online photo gallery allowing every user to create online albums, organize digital photos and to share with other users.

**Duration:** December 2011 - January 2012.

## Competitions

---

### HOST: Hardware Demo

2018

*IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*

*Washington DC*

Designed a lightweight malware detection methodology for embedded platforms along with a fast ransomware detection techniques using Hardware Performance Counters. Reached Final round in the competition from all over the world.

### Cyber Security Awareness Week - Embedded Security Challenge in India

2016

*Indian Institute of Technology Kanpur*

*Kanpur*

Designed a novel hardware mitigation technique for memory corruption and control flow integrity attacks in embedded systems. Secured 2<sup>nd</sup> place in the competition from all over India.

### International Championship for Artificial Intelligence & Networking

2015

*Indian Institute of Technology Bombay*

*Mumbai*

Designed a cost effective prototype of a carom playing bot from scrap materials. Secured 2<sup>nd</sup> place in the competition from all over India. Demonstration can be found on the following link. ([https://www.youtube.com/watch?v=18lkxVzs\\_Zk](https://www.youtube.com/watch?v=18lkxVzs_Zk)).

### National Round of Indo-US Robo League

2015

*Indian Institute of Technology Bombay*

*Mumbai*

Reached Pre-Final round for designing a cost effective Line Follower Robot.

## Invited Talks

---

- Workshop on Advanced Side Channel Evaluation of Hardware Security (ASCEHS), Indian Institute of Technology Kharagpur, July 2018.
- ACM Summer School on Fundamentals for Cryptology Research, Indian Statistical Institute Kolkata, June 2018.

## Achievements and Professional Services

---

- Finalist of Qualcomm Innovation Fellowship India 2017.
- National Merit-cum-Means Scholarship awarded by WBMDFC from 2009 to 2013.
- Certificate of Excellence on ERP – Essentials from Research Software Solutions (P) Ltd. (Microsoft Gold Certified Partner), April 2010.
- National Merit Scholarship awarded by Govt. of India for securing position among Top 20 in Higher Secondary Board Examination in 2009.
- **Sub-Reviewer of Conferences:** *COSADE '18, DAC '18*
- **Sub-Reviewer of Workshops:** *TopinHES-18*

## Teaching Assistance

---

**Computer Programming Lab:** Autumn, 2015 and Spring, 2016

*IIT(ISM) Dhanbad*

**Data Structures Lab:** Autumn, 2015

*IIT(ISM) Dhanbad*

**Algorithm Design & Analysis Lab:** Spring, 2016

*IIT(ISM) Dhanbad*

**Programming and Data Structures Lab:** Spring, 2017

*IIT Kharagpur*

**Foundation of Algorithm Design and Machine Learning:** Spring, 2018

*IIT Kharagpur*

**Cryptography and Network Security:** Autumn, 2018

*IIT Kharagpur*

## Extra-Curricular Activities

---

- Awards and Positions in inter-school sit-and-draw competitions.
- Participated and secured 3<sup>rd</sup> Prize in a Mathematics Competition at FESTRONIX 2011 held at Institute of Engineering and Management, Kolkata, February 2011.

## Personal Details

---

**Date of Birth:** 11<sup>th</sup> February, 1991.

**Gender:** Male.

**Languages Known:** English, Bengali, Hindi.

**Nationality:** Indian.

## Journals

---

- [j1] Debapriya Basu Roy, **Manaar Alam**, Sarani Bhattacharya, Vidya Govindan, Francesco Regazzoni, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. Customized Instructions for Protection Against Memory Integrity Attacks. In *IEEE Embedded Systems Letters (ESL)*, Volume: 10, Issue: 3, September 2018, pages 91–94. DOI: 10.1109/LES.2018.2828506.

## Submitted Journals

---

- [sj4] Anirban Chakraborty, **Manaar Alam**, Vishal Dey, Anupam Chattopadhyay and Debdeep Mukhopadhyay. Adversarial Attacks and Defences: A Survey. In *ACM Computing Surveys (CSUR)*. [Under Review]
- [sj3] **Manaar Alam**, Sarani Bhattacharya, Sayan Sinha, Chester Rebeiro, and Debdeep Mukhopadhyay. IPA: An Instruction Profiling based Micro-Architectural Side-Channel Attack on Block Ciphers In *Journal of Hardware and Systems Security (HASS)*. [Under Review]
- [sj2] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Sourangshu Bhattacharya. Victims can be Saviors: A Machine Learning based detection for Micro-Architectural Side-Channel Attacks In *ACM Transactions on Privacy and Security (TOPS)*. [Under Review]
- [sj1] Sai Praveen Kadiyala, **Manaar Alam**, Yash Shrivastava, Sikhar Patranabis, Muhamed Fauzi Bin Abbas, Arnab Biswas, Debdeep Mukhopadhyay, Siew-Kei Lam, and Thambipillai Srikanthan. LAMBDA: Lightweight Assessment of Malware for emBeddeD Architectures. In *IEEE Transactions on Information Forensics and Security (TIFS)*. [Second Revision Submitted]

## Conferences

---

- [c6] Nimesh Kirit Shah, **Manaar Alam**, Durga Prasad Sahoo, Debdeep Mukhopadhyay and Arindam Basu. A 0.16pJ/bit Recurrent Neural Network Based PUF for Enhanced Machine Learning Attack Resistance. In *24th Asia and South Pacific Design Automation Conference, ASP-DAC 2019, Tokyo, Japan, January 21-24, 2019*. [Accepted]
- [c5] **Manaar Alam**, Sayan Sinha, Sarani Bhattacharya, Swastika Dutta, Debdeep Mukhopadhyay and Anupam Chattopadhyay. RAPPER: Ransomware Prevention via Performance Counters. In *Australian Workshop on Offensive Cryptography, Kangacrypt 2018, Adelaide, Australia, December 7–8, 2018*. [Accepted]
- [c4] **Manaar Alam**, Debdeep Mukhopadhyay, Sai Praveen Kadiyala, Siew-Kei Lam, and Thambipillai Srikanthan. Side-Channel Assisted Malware Classifier with Gradient Descent Correction for Embedded Platforms. In *7th International Workshop on Security Proofs for Embedded Systems, PROOFS@CHES 2018, Amsterdam, Netherlands, September 13, 2018*, pages 1–15. DOI: 10.29007/5sdj
- [c3] **Manaar Alam**, Sarani Bhattacharya, and Debdeep Mukhopadhyay. Tackling the Time-Defence: An Instruction Count Based Micro-architectural Side-Channel Attack on Block Ciphers. In *Security, Privacy, and Applied Cryptography Engineering - 7th International Conference, SPACE 2017, Goa, India, December 13-17, 2017*, pages 30–52. DOI: 10.1007/978-3-319-71501-8\_3.
- [c2] **Manaar Alam**, Debapriya Basu Roy, Sarani Bhattacharya, Vidya Govindan, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. SmashClean: A hardware level mitigation to stack smashing attacks in OpenRISC. In *ACM/IEEE International Conference on Formal Methods and Models for System Design, MEMOCODE 2016, Kanpur, India, November 18-20, 2016*, pages 1–4. DOI: 10.1109/MEMCOD.2016.7797764.
- [c1] **Manaar Alam**, Soumyajit Chatterjee, and Haider Banka. A novel parallel search technique for optimization. In *3rd International Conference on Recent Advances in Information Technology, RAIT 2016, Dhanbad, India, March 3-5, 2016*, pages 259–263. DOI: 10.1109/RAIT.2016.7507912.

## Patents Filed

---

- [pt1] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. RAPPER: Ransomware Prevention via Performance Counters. [Filed Indian Patent. ID: 21398]

## Poster Presentations

---

- [p3] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. Detecting Malware and Ransomware using Hardware Performance Counters. *POSTER: IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2018.
- [p2] Sai Praveen Kadiyala, Muhamed Fauzi Bin Abbas, Yash Shrivastava, Sikhar Patranabis, **Manaar Alam**, Debdeep Mukhopadhyay, Siew-Kei Lam, and Thambipillai Srikanthan. LAMBDA: Lightweight Assesment of Malware for emBeddeD Architectures. *POSTER: Singapore International Cyber Week (SICW)*, September 2017.
- [p1] **Manaar Alam**, Debapriya Basu Roy, Sarani Bhattacharya, Vidya Govindan, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. SmashClean: A Hardware level mitigation to stack smashing attacks in OpenRISC. *POSTER: Cyber Security Awareness Week (CSAW)*, November 2016.

## Archive Papers

---

- [w3] Anirban Chakraborty, **Manaar Alam**, Vishal Dey, Anupam Chattopadhyay and Debdeep Mukhopadhyay. Adversarial Attacks and Defences: A Survey. In *arXiv, CoRR, abs/1810.00069*, September 2018.
- [w2] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. RAPPER: Ransomware Prevention via Performance Counters. In *arXiv, CoRR, abs/1802.03909*, February 2018.
- [w1] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Sourangshu Bhattacharya. Performance Counters to Rescue: A Machine Learning based safeguard against Micro-architectural Side-Channel-Attacks. In *Cryptology ePrint Archive, Report 2017/564*, July 2017.

## References

---

- **Dr. Debdeep Mukhopadhyay**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, debdeep@cse.iitkgp.ernet.in
- **Dr. Sourangshu Bhattacharya**, Assistant Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, sourangshu@cse.iitkgp.ernet.in
- **Dr. Haider Banka**, Associate Professor, Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, banka.h.cse@ismdhanbad.ac.in