AS6-04-25
117416
Singapore
✉ *aashish7@comp.nus.edu.sg*
🖱 *ashgeek.github.io*
in *Aashish Kolluri*
Google Scholar

Aashish Kolluri

Education

2018–Ongoing **PhD**, *National University Of Singapore*, Singapore, *GPA: 4.67/5*.

2017 **Undergraduate**, *IIT Kanpur*, Kanpur.

2013 **Senior Secondary(12th)**, *Sri Chaitanya Narayana*, Hyderabad.

2011 **Secondary(10th)**, *Narayana Olympiad School*, Hyderabad.

Research Experience

Aug'17–Ongoing **NUS**, *Prof. Prateek Saxena*.
Verification of decentralized applications(DApps)

Stipulated checkable properties of DApps to ensure safety and fairness in the ecosystem. Designed novel techniques and built scalable tools to verify them.

2019 Verifying DApps to detect bugs arising from their inherent concurrent nature. **(ISSTA'19)**
- Event Ordering bugs are prevalent on blockchains but are understudied.
- It is a hard problem since verification using traditional dynamic analyses cannot scale and there is no source code for doing static analysis on blockchain.
- Redefined original Happens Before and used novel Partial order reduction techniques based on concolic execution. This, along with fuzzing events makes verification of DApps feasible.
- Implemented **EthRacer** which flagged over **8%**of **10,000** DApps as vulnerable.
- Popular ones which handled more than **1 million** transactions were found buggy.

2018 Efficiently detecting trace vulnerabilities that arise in stateful DApps. **(ACSAC'18)**
- Trace vulnerabilities occur over long traces of transactions made to a single/group of DApps.
- First work for specifying and reasoning about trace properties of DApps. We implemented **MAIAN** which does inter-procedural symbolic analysis and also simulates the found exploit.
- MAIAN is a highly scalable verifier which takes only **10** seconds on average, per DApp. It was very well received [1,2] in the community and industry.
- Evaluated a **million** contracts available on Ethereum blockchain.
- MAIAN finds exploits which led to losses of **200** million dollars from the Ethereum ecosystem!

Jan'17–Apr'17 **IIT Kanpur**, *Prof. Indranil Saha*.
Optimized Multi-Robot Path Planner

- Got acquainted with the state-of-the art motion planning algorithms.
- Designed a new algorithm with inspirations from the existing ones like IMPLAN for stationary initial and final points of the robots. Find the presentation **here**.

Publications

2019 Aashish Kolluri, Ivica Nikolic, Ilya Sergey, Aquinas Hobor, Prateek Saxena, Exploiting the laws of order in smart contracts: **ISSTA'19** (slides|artifact) *(20% acc.rate)*

2018 Ivica Nikolic, Aashish Kolluri, Ilya Sergey, Prateek Saxena, Aquinas Hobor, Finding The Greedy, Prodigal, and Suicidal Contracts at Scale: **ACSAC'18** (slides|artifact)*(20%)*

2018 Sourav Das, Aashish Kolluri, Prateek Saxena, Haifeng Yu (alphabetical order of last name), Invited Paper - on the Security of Blockchain Consensus Protocols: **ICISS'18**

Industry Experience

May'16–July'16 **Flipkart Internet Pvt. Ltd.**, *Vijayant Singh*.
Project JIRO-Anomaly Detection for Flipkart Cloud's Alerting Service

- Finding better algorithms for Anomaly Detection while reducing False Positives.
- Implemented unsupervised learning methods like clustering since the data was unlabelled.
- Implemented statistical methods such as AR, MA models, Twitter(SHESD).
- Developed an engine which compares existing algorithms. Find the presentation **here**.

Technical skills

Advanced	Python, Geth (Ethereum), Z3, KLEE
Intermediate	C, C++, MySQL, Php, GNUPlot, R, Solidity, Z3, SkLearn, Latex
Basic	Any online resource/library

Relevant Coursework

NUS Systems Security (CS5231), Advanced Topics in Program Analysis (CS6215), Big Data Analytics Technology (CS5344), Property Testing (Ongoing).

IITK Data Structures and Algorithms (CS210), Computer Organization (CS220), Operating Systems (CS330), Tools For Programming (CS251), Algorithms-II (CS345), Theory of Computation (CS340), Compilers(CS335), Machine Learning(CS771), Systems Security(CS628), DBMS(CS315), Computer Networks(CS425), Cyber Physical Systems(CS637).

Achievements

2018–2022 **Research Scholar Fellowship**, *National University Of Singapore*.

2011–2013 **Scholastic**.

- Achieved **ALL INDIA RANK 286 (99.998 percentile)** in **JEE-Advanced** and scored **414/450** in **BIT SAT**(Birla Institute of Technology and Science Aptitude Test) 2013.
- Awarded the K.V.P.Y(Kishore Vaigyanik Protsahan Yojana) scholarship. Secured **175th rank among 1.5 lakh candidates** all over the country.
- Secured **146 rank (99.95 percentile)** in EAMCET (Engineering, Medical and Agricultural Common Entrance Test in A.P) among over 3 lakh students in the year 2013.
- Secured **First Rank** in district level in **S.L.S.T.S.E**(State Level Science Talent Search Examination in 2011) conducted by UNIFIED COUNCIL.

Teaching

Spring 2019 **Introduction to Computer Security**, *CS 3235*, Prateek Saxena.

Fall 2019 **Systems Security**, *CS 5231*, Prateek Saxena.

Talks & Panels

August 2019 **Panel - Industry/Academics after PhD: prospects and challenges**, *@ Resarch Week, NUS*, Moderator.

August 2019 **Exploiting the Laws of Order in Smart Contracts**, *@ Resarch Week, NUS*, Invited talk.

July 2019 **Exploiting the Laws of Order in Smart Contracts**, *@ ISSTA'19*, Conference talk.

Dec 2018 **Finding the Greedy, Prodigal and Suicidal Contracts**, *@ ACSAC'18*, Conference talk.

June 2018 **Blockchain Fundamentals - Smart Contract Security**, *@ Zilliqa*, Invited talk.

May 2018 **Smart Contract Security: Hacking 34,200 Smart Contracts**, *@ Paypal Innovation Labs, Singapore*, Invited talk.

Major Course Projects

Aug'16– Nov'16 **Networks**, *Prof. Sandeep Shukla*.

- Implemented an HTTP server client model and established a connection between them using sockets which facilitated transfer of files from server to client.
- Implemented a real time Proxy Server, tested on Firefox browser and also implemented a simple Routing protocol using prefix matching for maximum match.
- Implemented a simple TCP which in its final configuration facilitated transfer of files of all formats between client and server, also implemented ARP.

Aug'16– Nov'16 **Buddy-CyberPhysical Systems**, *Prof. Indranil Saha*.

- Developed a **helper bot** which could sense opening of a door, go to the person entering into the room and ask him to command.
- Used a simple bot and Orange Pi board for all the processing and HTTP server client mechanism for detecting opening of the door.
- Used Python to code the HTTP server client mechanism and Amazon Alexa api for communication with buddy.

Jan'16– Apr'16 **Zoobar Application**, *Prof. Sandeep Shukla*.

- Zoobar, a web application posted by "Zoobar Foundation" , contains many vulnerabilities.
- Studied its source code and enhanced its security by changing the vulnerable code i.e., provided checks for Buffer Overflows and Integer overflows, privilege separated different components of the application, used RPC libs for communication, studied control flow of programs for detecting vulnerabilities and also provided security from vulnerabilities like SQL Injection and Format String attacks.Secured the web application to prevent Cross Site Scripting attacks.

Jan'16– Apr'16 **Vehicle Identification and Foreground Background Separation**, *Prof. Harish Karnick*.

- Separated foreground frames from background frames using Frame Differencing method.
- Extracted the features of training data using HOG(histogram of oriented gradients) and SIFT and used different algorithms like LinearSVC, Nearest Neighbours and Random Forests for training. The accuracy of the trained classifier was an impressive 92% after training with random forests.

Jan'16– Apr'16 **Blood-Bank**, *Prof. Sumit Ganguly*.

- Created an end to end three level website, online Blood bank using PHP, MySQL and PhpMyadmin for the back end, HTML, CSS, Bootstrap for the front end.
- Efficiently handled the intricate details like user access levels, donation and request of blood processes, usability, security and error handling.