# Akhilesh Siddhanti

www.akhilesh.tech | +1-470-775-1825 | akhilesh@gatech.edu | Linkedin: akhilesh-siddhanti | Github: akhileshsiddhanti

## Education

**Georgia Institute of Technology** Atlanta, USA
Master of Science in Computer Science, Machine Learning and Systems Specialization Aug. 2019 – Dec. 2020

**Birla Institute of Technology and Science, Pilani** Goa, India
B.E. (Hons) Computer Science Aug. 2014 – May. 2019
M.Sc. (Hons) Mathematics (Dual Degree Program)

## Technical Proficiency

**Languages**: C, C++, Java, Python, HTML/CSS, Javascript, D3.js, Bash, MATLAB

**Frameworks**: ElasticSearch, Tensorflow, SAGE, Latex, Hadoop, Tableau, Numpy, scikit-learn, unittest, Mockito, ASP.NET

**Tools**: Eclipse, PyCharm, VSCode, Vim, Git, Jenkins, Kubernetes, GCP, Linux, Photoshop

**Courses**: Advanced Operating Systems, Computer Vision, Data & Visual Analytics, Network Security, Machine Learning, Advanced Software Engineering, Cryptography, AI, Graph Theory, Combinatorial Maths, Number Theory, Optimization, OOP, DBMS, Graduate Algorithms.

## Experience

**Software Development Intern at CI Analytics team, Salesforce** May 2020 – Aug 2020

- Identified failure of existing inventory service for Test Prioritizing Algorithm at Salesforce and migrated it to a new inventory service with better reliability. (Code in production)
- Added a monitoring tool to dashboard to notify autobuild downtime.
- Modified Yoda Bugging service to accommodate for the new inventory service.
- Using Changelist Prediction algorithm to narrow down risky changelists to prioritize testing.
- Introduced new tests to improve code coverage from 40% to 80%.

**Graduate Thesis at Indian Statistical Institute, Kolkata, India** Aug 2018 – May 2019

- Analysing and developing a Physically Unclonable Function resilient to SAC property.
- Studied Cube and Integral attacks on stream ciphers.

**Intern, HESL, Nanyang Technological University, Singapore** May 2018 – July 2018

- Modelled an Arbiter-based hardware PUF using minimal parameters.
- Studied Pseudo-boolean constraints and ways to use existing SAT solvers to solve them.

**Intern, Indian Statistical Institute, Kolkata** May 2017 – July 2017

- Attacked stream cipher Lizard using TMDTO attacks.
- Developed a new technique of Algebraic TMDTO Attacks, demonstrating an attack on ACORN v3.

**Software Development Intern, ESSAR Group, India** May 2016 – July 2016

- Automated the form-filling process for the HR department of ESSAR Power Gujarat Limited.
- Technologies used: ASP.NET framework, HTML, CSS, Javascript, SQL.

## Projects

**Pinning Accents: Accent Classification using Machine Learning**
Classifying different dialects of English language using K-means, CNN and Bidirectional-LSTMs.

**Nailed it: Selecting the most relevant thumbnail for a video**
Based on features developed on aesthetics and relevance, clustering and random forests is implemented.

**FindMyAir: An Intelligent Trip Planning Algorithm**
Searching for an optimal Airbnb accomodation and travel plan for a given set of parameters.

**ANN-aided fault location identification for stream ciphers**
Implemented Artificial Neural Networks to find fault locations in a stream cipher (waiting for publication).

**Surfboard - Surf the web, only using your keyboard!**
Developed a web extension in Javascript to help differently-abled browse the web only using a keyboard.

## Publications

**A TMDTO Attack Against Lizard** **IEEE Transactions on Computers**

Cryptanalysis of the stream cipher with a time complexity faster than brute-force search. (Citations: 14)

**A Differential Fault Attack on Plantlet** **IEEE Transactions on Computers**

Demonstrating a Differential Fault Attack on Plantlet with minimum fault requirements. (Citations: 5)

**Strict Avalanche Criterion in variants of Arbiter based PUFs** **INDOCRYPT 2019**

Designed a novel key generating S-PUF construction for wearables and reduced bias to zero for the first time.

**Differential Fault Attack on SIMON with Very Few Faults** **INDOCRYPT 2018**

Showed how block ciphers can also be vulnerable to fault attacks, like stream ciphers.

**Certain Observations on ACORN v3 and Grain v1** **Journal of Hardware and Sys Sec**

An extended work of conditional TMDTO attack on ACORN v3 and Grain v1.

**Differential Fault Attack on Grain v1, ACORN v3 and Lizard** **SPACE 2017**

Mounted fault attacks on popular stream ciphers using numerous optimizations.

**Differential fault attack on hardware stream ciphers** **RICAM Special Sem, Austria**

A survey of various fault attack techniques employed to cryptanalyze stream ciphers.

## Achievements

- Awarded the DST-INSPIRE Scholarship for exceptional performance in 12th Board examinations.
- Invited to publish in Journal of Hardware and Systems Security for a special contribution.
- Finalist to TheBlockchainSPIRIT Hackathon organized at NTU Singapore.

## Positions of Responsibility

**Mentor, Quark Summer Time Project - Machine Learning Course** **April 2016 - July 2016**

Mentored 26 students on ”Introduction to Machine Learning”, which involved tasking, checking assignments and solving doubts, along with a final project titled ”Detecting Fake Currency Notes from UCI repository”.