

# Muhammad Sajidur Rahman

276 Corry Village, Gainesville, FL 32603

☎ (+1) 785-770-6212 | ✉ [sajidrahman25@gmail.com](mailto:sajidrahman25@gmail.com) | 🏠 [sajid-rahman.com](http://sajid-rahman.com) | 💻 [sajidrahman](#) | 🎓 [Google Scholar](#) | 🌐 [sajidrahman1](#)

## Profile Summary

- Proven skills in designing and carrying out research studies, analyzing results both qualitatively and quantitatively, scrutinizing output, and improving methods.
- 4+ years of industry experience as a Software Engineer in the **Fintech** industry, **SaaS** in general.
- Research areas: **Security & Privacy Engineering, Natural Language Processing, Human-centered Computing.**

## Education

### University of Florida

PHD STUDENT, DEPT. OF COMPUTER & INFORMATION SCIENCE & ENGINEERING

Gainesville, FL

2017 - August'22

### Kansas State University

M.S. IN COMPUTER SCIENCE

Manhattan, KS

2017

- **MS thesis:** An Empirical Case Study on Stack Overflow to Explore Developers' Security Challenges.

### Bangladesh University of Engineering and Technology (BUET)

B.S. IN COMPUTER SCIENCE AND ENGINEERING

Dhaka, Bangladesh

2011

- **Undergrad thesis:** Location aware fuzzy logic based decision making of vertical hand-off in heterogeneous wireless networks.

## Research and Professional Experience

### Florida Institute for Cybersecurity Research (FICS)

GRADUATE RESEARCH ASSISTANT

University of Florida, Gainesville

May 2017 - Present

- Take initiative and responsibility in each phase of a research study - from the idea generation to experiment design, data analysis, interpretation, and manuscript writing.
- Currently investigating: i) developer-driven privacy threat modeling for Android Apps and ii) analysis of private data collection and sharing behavior policy of Android third-party libraries.

### Avast, Inc.

RESEARCH INTERN, AVAST RESEARCH LAB

Emeryville, CA

May 2020 - August 2020

- Conducted a large-scale Android app privacy analysis to find inconsistencies in *declared* data privacy practice with *actual* app behavior of sensitive data collection and sharing.
- Devised a mapping between *dangerous* Android permissions and privacy policy.
- Proposed visual indicator to support end-users making informed decisions (e.g., installing/uninstalling/switching apps) about App privacy.

### FireEye, Inc.

RESEARCH INTERN, DATA SCIENCE TEAM

Reston, VA

May 2019 - Aug. 2019

- Researched into the tactics, techniques, and procedures being employed by adversaries over social media platforms to spread disinformation.
- Used transfer learning to fine-tune GPT-2 language model to generate synthetic disinformation data and to detect disinformation in social media posts.
- Featured on **WIRED** and **FireEye**.

### Cyber Security Lab

GRADUATE RESEARCH ASSISTANT

Kansas State University

Aug. 2014 - Dec. 2016

- Remodeled and optimized functionality on Firefox SSL extension launcher for data logging and proxy setting for SSL warning study.
- Conducted semi-structured interviews, synthesized survey responses, and interpreted interview transcripts to elicit consumer usage patterns and behavior of different payment methods.
- Applied quantitative and qualitative techniques on the Stack Overflow dataset to gauge software developers' security perception.

### Progoti Systems Limited (FinTech company)

SENIOR SOFTWARE ENGINEER

Dhaka, Bangladesh

Mar. 2012 - Feb. 2014

- Orchestrated the engineering and architecture of the core service engine for **SureCash** Mobile Financial Service as a SaaS model which provides money deposit, withdrawal, and P2P and B2B financial transactions with seamless user experience.
- Headed several major milestones and new product features including three large bank integration with SureCash payment service, implementing and operationalizing USSD based push-pull service to ensure secure and seamless money withdrawal service from either Human or ATM agents, rolling out third-party utility bill payment service, to name a few.

- Implemented automated ETL service to run at the end of daily business hours to fetch data from core-banking system's data archive and populate MIS database for business analytics.
- Designed and developed a centralized MIS web portal with secure, role-based access control for various bank divisions (e.g., corporate/retail banking/credit-card) to facilitate real-time financial report generation and analysis from the current and historical dataset. This system increases the efficiency of these divisions in decision-making and policy planning by over 50%.

## Skills

---

<b>Programming Languages</b>	Java, C/C++ (advanced); Python, C#, R (moderate)
<b>Frameworks</b>	Spring, Grails, JavaEE(Servlet/JSP), Hibernate (advanced)
<b>Web/Mobile Technologies</b>	REST/SOAP, AWS, Microservice Design (advanced to moderate); PHP, Node.js, Android (prior experience)
<b>Big Data Technologies</b>	Apache Hadoop, Apache Pig (moderate)
<b>Machine Learning Tools</b>	PyTorch, TensorFlow, Keras, Scikit-learn, Pandas (moderate)
<b>Pen-testing Tools</b>	Metasploit, Kali Linux, Windbg (prior experience)
<b>Database</b>	MySQL, MS-SQL (advanced); Oracle, PostgreSQL (prior experience)

## Academic Projects

---

### Security & Privacy Threat Modeling of Mobile App

FICS, UF

RESEARCH PROJECT

2020 - Current

- Analyze Android app source code and data flow information to annotate source code with security and privacy threats and mitigation strategies.
- Investigate Android app's private data collection and sharing behavior by developing a mapping between app's usage of dangerous permissions, third party libraries, and app's privacy policy.
- **Research artifact:** Published at **2021 IEEE ASE**, in-submission at **PETS'22**.

### Adversarial Attacks against Automaterd Speech Recognition Systems

FICS, UF

RESEARCH PROJECT

Sep. 2018 - August 2021

- Investigated multiple widely-used speech recognition systems and developed techniques to force erroneous transcription of human speech while minimizing disruption to human auditory comprehension.
- Responsible for creating a cellular network testbed to run perturbed audio samples over the cellular network, designing and performing a user study on Amazon MTurk to understand the performance of the adversarial algorithm we designed and its applicability for real-time telecommunication, among others.
- **Research artifact:** Published at **2021 IEEE Security & Privacy Conference, 2021 ACML**, in-submission at **2022 IEEE Security & Privacy Conference**.

### API Blindspots: Why Experienced Developers Write Vulnerable Code

FICS, UF

RESEARCH PROJECT

May 2017 - June 2018

- Spearheaded every phase of the online user study - from implementing and optimizing server back-end for conducting a user study to data collection, analysis and interpretation, literature review, and research manuscript writing.
- Redesigned and optimized audio data capture functionality of the online user study for enhanced data logging and exception handling, which reduced audio-data loss from 30% to nearly 0%.
- **Research artifact:** Published at **2018 USENIX SOUPS** conference.

### Mining Stack Overflow to Explore Developers' Security Challenges

CS, K-State

M.S. PROJECT

Aug. 2016 - Dec. 2016

- Applied topic-modeling on Stack Overflow dataset to explore and analyze challenges, misconceptions, and deterrents among developers while they try to design and build security features during various phases of the software development life cycle.
- Defined and implemented metrics to identify software security-relevant key discussion topics and overlapping areas.
- Analyzed the nature and trends of *security-related* posts in Stack Overflow both quantitatively and qualitatively.
- **Research artifact:** Masters report available at [here http://tiny.cc/msreport](http://tiny.cc/msreport).

## Publications

---

- "SO{U}RCERER: Developer-Driven Security Testing Framework for Android Apps." In *Proceedings of the 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW'21)*.
- "Beyond  $L_p$  clipping: Equalization based Psychoacoustic Attacks against ASRs." In *2021 Asian Conference on Machine Learning (ACML'21)*.
- "Hear 'No Evil', See 'Kenansville': Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems." In *Proceedings of the 2021 IEEE Symposium on Security and Privacy (S&P'21)*.
- "Combating Social Media Information Operations with Neural Language Models." In *2020 USENIX Security and AI Networking Summit*.
- "Of Ulti, 'hajano', and 'Matachetar otanetak datam': Exploring Local Practices of Exchanging Confidential and Sensitive Information in Urban Bangladesh." In *Proceedings of the 22nd ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW'19)*.
- "API Blindspots: Why Experienced Developers Write Vulnerable Code." In *Proceedings of the 2018 USENIX SOUPS'18*.
- "Smart Blood Query: A Novel Mobile Phone-Based Privacy-Aware Blood Donor Recruitment and Management System for Developing Regions." In *Proceedings of 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications*.