Muhammad Sajidur **Rahman**

327 University Village South, Gainesville, FL 32603

(+1) 785-770-6212 | sajidrahman25@gmail.com | 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 interests: **Security & Privacy Engineering, Deep Learning, Human-centered Computing**.

Education

University of Florida — *Gainesville, FL*

PhD Student, Dept. of Computer & Information Science & Engineering — *2017 - May 2022*

Kansas State University — *Manhattan, KS*

M.S. in Computer Science — *2017*

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

Bangladesh University of Engineering and Technology (BUET) — *Dhaka, Bangladesh*

B.S. in Computer Science and Engineering — *2011*

- **Undergrad Thesis:** Location aware fuzzy logic based decision making of vertical handoff in heterogeneous wireless networks.

Research and Professional Experience

Florida Institute for Cybersecurity Research (FICS) — *University of Florida, Gainesville*

Graduate Research Assistant — *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. — *Emeryville, CA*

Research Intern, Avast Research Lab — *May 2020 - August 2020*

- Conducted a large-scale Android app privacy analysis to find gaps in *declared* privacy policy with *actual* app behavior of private 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. — *Reston, VA*

Research Intern, Data Science Team — *May 2019 - Aug. 2019*

- Researched into the tactics, techniques, and procedures being employed by adversaries over social media platforms to spread disinformation.
- Demonstrated transfer learning on language model by fine-tuning GPT-2 to generate synthetic disinformation data for simulation and then detect disinformation social media posts.
- The project was featured on WIRED and FireEye Blog.

Cyber Security Lab — *Kansas State University*

Graduate Research Assistant — *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 topic modeling on the Stack Overflow dataset to gauge software developers' security perception.

Progoti Systems Limited (FinTech company) — *Dhaka, Bangladesh*

Senior Software Engineer — *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.

Prime Bank Limited *Dhaka, Bangladesh*

Information Technology Engineer *Feb. 2011 - Feb. 2012*

- 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

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

Academic Projects

Security & Privacy Threat Modeling *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.
- Goal: Develop a lightweight threat modeling framework for developers to detect and mitigate mobile app privacy and security threats at the early phase of development.

Adversarial Speech Sample Generation against Automated Speech-to-Text Systems *FICS, UF*

Research Project *Sep. 2018 - May 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.
- Published in **2021 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%.
- Published in **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.

Publications

- "Beyond L_p clipping: Equalization based Psychoacoustic Attacks against ASRs" In *2021 Asian Conference on Machine Learning (ACML'21).*
- "So{u}rcerer : A Lightweight Security Testing Framework for Android App Developers" Under Review.
- "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.
- "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 14th Symposium on Usable Privacy and Security (SOUPS'18).*
- "An Exploratory Study of User Perceptions of Payment Methods in the UK and the US." In *Proceedings of the 10th NDSS Workshop on Usable Security (USEC'16).*
- "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.*