

SAZZADUR RAHAMAN

Assistant Professor, University of Arizona

✉ sazz@cs.arizona.edu · 📞 · 🌐 www.sazzadur.com

⚙️ RESEARCH INTEREST

I work towards making security research more democratized and affordable. I am broadly interested in building robust systems and methodologies by using program analysis, applied cryptography, formal verification, internet measurement and machine learning-based techniques. I emphasize on transitioning my work into practice. My strength is building rigorous methodologies and deployable systems.

🎓 EDUCATION

Ph.D. in Computer Science,

Virginia Tech, USA

Aug. 2015 – Aug. 2020

Thesis: “From Theory to Practice: Deployment-grade Tools and Methodologies for Security Compliance Measurements”, **Advisor:** Dr. Danfeng (Daphne) Yao, Professor.

B.Sc. in Computer Science and Engineering,

Bangladesh University of Engineering and Technology (BUET), Bangladesh

2006 – 2012

🐾 PROFESSIONAL APPOINTMENTS

University of Arizona, Tucson, AZ, USA

Aug. '20 – Present

Assistant Professor, Computer Science

Data Security Technologies, LLC, Dallas, TX, USA

May '19 – Aug. '19

Software Engineering Intern, SecureDL Team

Data Security Technologies, LLC, Dallas, TX, USA

May. '17 – Aug. '17

Software Engineering Intern, SecureDL Team

Kona Software Lab Ltd, Dhaka, Bangladesh

Mar. '14 – Jul. '15

Software Engineer and Team Lead, Kona Pay Team

Therap Services, LLC, Dhaka, Bangladesh

Apr. '12 – Feb. '14

Software Engineer, System Team

☆ HONORS AND AWARDS

- **Pratt Fellowship,** Fall 2019 and Spring 2020 2019
- **Bitshare Fellowship,** Fall 2018 and Spring 2019 2018
- **Champion in .Net platform,** Inter University System Design Competition-2011, BUET 2011
- **Dean's List Award,** BUET Session 2009-10

📖 PUBLICATIONS

Journal Papers

- **[TDSC'20]** Sazzadur Rahaman, Haipeng Cai, Omar Chowdhury and Danfeng (Daphne) Yao. “From Theory to Code: Identifying Logical Flaws in Cryptographic Implementations.” IEEE Transactions on Dependable and Secure Computing (TDSC). 2020. **(Impact Factor: 6.404)**

Conference Papers

- [SecDev'20] Mazharul Islam, [Sazzadur Rahaman](#), Na Meng, Behnaz Hassanshahi, Padmanabhan Krishnan and Danfeng (Daphne) Yao. “*Coding Practices and Recommendations of Spring Security for Enterprise Applications.*” IEEE Secure Development Conference. Atlanta, GA, September 2020.
- [CCS'19] [Sazzadur Rahaman](#), Gang Wang, Danfeng (Daphne) Yao. “*Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations.*” ACM Conference on Computer and Communications Security (CCS'19). London, United Kingdom. November 2019.
(Acceptance Rate: 16%)
Sources: <https://github.com/sazzad114/{pci-checker, buggycart}>
- [CCS'19] [Sazzadur Rahaman](#), Ya Xiao, Sharmin Afrose, Fahad Shaon, Ke Tian, Miles Frantz, Murat Kantarcioglu, Danfeng (Daphne) Yao. “*CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects.*” ACM Conference on Computer and Communications Security (CCS'19). London, United Kingdom. November 2019.
(Acceptance Rate: 16%, Adopted by Oracle)
Source: <https://github.com/CryptoGuardOSS/cryptoguard>
- [SecDev'19] Sharmin Afrose, [Sazzadur Rahaman](#), Danfeng (Daphne) Yao. “*CryptoAPI-Bench: A Comprehensive Benchmark on Java Cryptographic API Misuses.*” 2019 IEEE Secure Development Conference (SecDev'19). McLean, VA. September 2019.
(Acceptance Rate: 36%, Used by multiple research groups)
Source: <https://github.com/CryptoGuardOSS/cryptoapi-bench>
- [PETS'17] [Sazzadur Rahaman](#), Long Cheng, Danfeng (Daphne) Yao, He Li, and Jung-Min (Jerry) Park. “*Provably Secure Anonymous-yet-Accountable Crowdsensing with Scalable Sublinear Revocation.*” 17th Privacy Enhancing Technologies Symposium (PETS'17). Minneapolis, MN, USA. July, 2017.
(Acceptance Rate: 21.7%)
- [SecDev'17] [Sazzadur Rahaman](#), Danfeng (Daphne) Yao. “*Program Analysis of Cryptography Implementations for Security.*” 2017 IEEE Secure Development Conference (SecDev'17). Cambridge, MA, USA. September, 2017.
- [ICIEV'14] [Sazzadur Rahaman](#), Tousif Ahmed Eshan, Sad Al Abdullah, and Md. Saidur Rahman. “*Antibandwidth Problem for Itchy Caterpillars.*” IEEE International Conference on Informatics, Electronics & Vision (ICIEV'14). Dhaka, Bangladesh. May, 2014.
- [ISMS'13] Mohammad Raihanul Islam, [Sazzadur Rahaman](#), Rakibul Hasan, Ridwan Rashid Noel, Asif Salekin, and Hasan Shahid Ferdous. “*A Novel Approach for Constructing Emulator for Microsoft Kinect XBOX 360 Sensor in the .NET Platform.*” IEEE International Conference on Intelligent Systems Modelling & Simulation (ISMS'13). Bangkok, Thailand. January, 2013.

Tutorials

- [SecDev'20] Ya Xiao, Miles Frantz, Sharmin Afrose, [Sazzadur Rahaman](#) and Danfeng (Daphne) Yao. “*Tutorial: Principles and Practices of Secure Cryptographic Coding in Java*” (90 minutes Tutorial). 2020 IEEE Secure Development Conference (SecDev'20). September, 2020.
- [SecDev'18] [Sazzadur Rahaman](#), Na Meng and Danfeng (Daphne) Yao. “*Tutorial: Principles and Practices of Secure Crypto Coding In Java*” (90 minutes Tutorial). 2018 IEEE Secure Development Conference (SecDev'18). Cambridge, MA, USA. September, 2018.

Patents

- Fahad Shaon, [Sazzadur Rahaman](#). “*Systems and methods for proactive and reactive data security*”. U.S. Patent Application No: 16/698,328. (filed).

Posters

- [S&P'19] [Sazzadur Rahaman](#), Ya Xiao, Sharmin Afrose, Ke Tian, Miles Frantz, Danfeng (Daphne) Yao, Na Meng, Barton P. Miller, Fahad Shaon, Murat Kantarcioglu. “*Poster: Deployment-quality and Accessible Solutions for Cryptography Code Development.*” 2019 IEEE Symposium on Security and Privacy (IEEE S&P'19). San Francisco, CA, USA. May, 2019.
- [CCS'19] [Sazzadur Rahaman](#), Ya Xiao, Sharmin Afrose, Ke Tian, Miles Frantz, Danfeng (Daphne) Yao, Na Meng, Barton P. Miller, Fahad Shaon, Murat Kantarcioglu. “*POSTER: Deployment-quality and Accessible Solutions for Cryptography Code Development.*” 2019 ACM Conference on Computer and Communications Security (ACM CCS'19). London, United Kingdom. November 2019.
- [SecDev'19] Sharmin Afrose, [Sazzadur Rahaman](#), Danfeng (Daphne) Yao. “*A Comprehensive Benchmark on Java Cryptographic API Misuses.*” 2019 IEEE Secure Development Conference (SecDev'19). McLean, VA. September 2019.

- [SecDev'17] Sazzadur Rahaman, Long Cheng, Danfeng (Daphne) Yao, He Li, and Jung-Min (Jerry) Park. “Enabling Large-scale Anonymous-yet-Accountable Crowdsensing” (Poster). 2017 IEEE Secure Development Conference (SecDev'17). Cambridge, MA, USA. September, 2017.
- [USENIX SEC'16] Sazzadur Rahaman, Long Cheng, He Li, Danfeng (Daphne) Yao and Jung-Min (Jerry) Park. “GroupSense: Scalable Crowdsensing with Privacy and Accountability.” (Poster). 2016 USENIX Security (USENIX SEC'16). Austin, TX. August, 2016.

⚖️ SELECTED PROFESSIONAL SERVICES

- **Technical Program Committee:** NDSS '21.
- **Journal Reviewer:** IEEE TDSC, IEEE IoT Journal.
- **External Reviewer:** ACSAC '20, PETS '18 '19 '20, SecDev '18
- **Sub Reviewer:** CCS '17 '18 '19, S&P '18 '19 '20, NDSS '19, WWW '19, AsiaCCS '17 '18, DSN '17
- **Student Volunteer:** CCS 2017

🎤 SELECTED TALKS

- *From Theory to Practice: Deployment-grade Tools and Methodologies for Software Security*
Department of Computer Science, University of Arizona, Tucson, AZ. (March, 2020)
- *From Theory to Practice: Deployment-grade Tools and Methodologies for Software Security*
Department of Computer Science, Wayne State University, Detroit, MI. (March, 2020)
- *From Theory to Practice: Deployment-grade Tools and Methodologies for Software Security*
Department of Computer Science, University of Central Florida, Orlando, FL. (February, 2020)
- *CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects*
In ACM Conference on Computer and Communications Security (CCS'19), London, UK. (November, 2019)
- *Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations*
In ACM Conference on Computer and Communications Security (CCS'19), London, UK. (November, 2019)
- *Research on the dangers of copy/pasting code*
In *Snyk.io* Podcast with James Davis. (November, 2019)
- *Understanding and Minimizing The Gap Between Secure Coding Theory and Practice*
Invited Talk, The University of Wisconsin-Madison, Madison, WI. (**Hosted by Prof. Barton Miller**)
- *Principles and Practices of Secure Crypto Coding In Java*
Tutorial, IEEE Secure Development Conference (SecDev'18), Cambridge, MA. (September, 2018)
- *Program Analysis of Cryptography Implementations for Security*
In IEEE Secure Development Conference (SecDev'17), Cambridge, MA. (September, 2017)
- *Enabling Large-scale Anonymous-yet-Accountable Crowdsensing*
In 17th Privacy Enhancing Technologies Symposium (PETS'17), Minneapolis, MN. (July, 2017)
- *Smart Card to the Cloud for Convenient, Secured NFC Payment*
Invited talk, JavaOne'15, San Francisco, CA. (2015)
- *Languages in JVM Ecosystem and The future of JVM*
Invited talk, JUG, BD (Meetup 5.0), Dhaka, BD. (2015)
- *Java 8: Lambda expression and Stream API*
Invited talk, JUG, BD (Meetup 3.0), Dhaka, BD. (2015)
- *Antibandwidth problem for itchy caterpillar*
In IEEE International Conference on Informatics, Electronics & Vision (ICIEV'14), Dhaka, BD. (May, 2014)

👤 MENTORING EXPERIENCE

- **PhD Students:** Sharmin Afrose, Ya Xiao, Mazharul Islam
- **MS Students:** Miles Frantz, Hannah Roth (2017)

❤️ MISCELLANEOUS

- **Founding member and initiator**, Java User Group, Bangladesh (JUGBD).
- **Top 7% of StackOverflow users**, 200+ posts with 6000+ Reputation.
- **Qualifier Q/A panelist '17 '18**, Computer Science, Virginia Tech.