

# Mohammad Ishtiaq Ashiq Khan

☎ (540) 449-8267 @ iashiq5@vt.edu 📍 Blacksburg, VA 🏠 [Homepage](#) [in LinkedIn](#) [GitHub](#) [Google Scholar](#)

## Education

---

**Blacksburg, VA** **Jan 2021 - Dec 2025 (Expected)**

- Ph.D. in Computer Science and Applications at **Virginia Tech**; Available for internship during May '24 to Aug '24

**Blacksburg, VA** **Jan 2021 - Dec 2023**

- M.Sc. in Computer Science and Applications at **Virginia Tech**

**Dhaka, Bangladesh** **Jul 2014 - Oct 2018**

- B.Sc. in Computer Science at **Bangladesh University of Engineering and Technology (BUET)**, CGPA: 3.83

## Experience

---

**Graduate Research Assistant** **Virginia Tech** **Jan 2021 - Present**

- Conducting data-driven research aimed at enhancing management and security of **Email**, **DNS**, and **PKI**.
- Stack: Apache Spark, MongoDB, PostgreSQL, Node.js, Docker, Django Rest, Redis, AWS, etc.

**Lecturer** **United International University** **Jul 2019 - Dec 2020**

- Taught Network Security, Data Structure, Object-Oriented Programming, etc. undergraduate courses.

**Full Stack Software Engineer** **InfoSapex Limited** **Nov 2018 - Jul 2019**

- Successfully released a Procurement Management System in production with over 50% contribution.
- Served as a technical point of contact with clients and carried out requirement analysis.
- Significantly reduced server provisioning time by automating configurations with Puppet and recovery time by setting up monitoring service with Munin and Nagios.

## Selected Publications

---

- *RoVista: Measuring and Analyzing the Route Origin Validation in RPKI* in **Internet Measurement Conference 2023**.
  - *Authors:* Weitong Li, Zhexiao Lin, **Md. Ishtiaq Ashiq**, Emile Aben, Romain Fontugne, Amreesh Phokeer, Taejoong Chung.
  - Proposed a network measurement framework, RoVista, to determine the Route Origin Validation status at scale.
- *You've Got Report: Measurement and Security Implications of DMARC Reporting* in **USENIX Security 2023**.
  - *Authors:* **Md. Ishtiaq Ashiq**, Weitong Li, Tobias Fiebig, and Taejoong Chung.
  - Analyzed the DMARC Reporting landscape longitudinally and empirically. Proposed a couple of DoS vulnerabilities in 3 major email providers with amplification factor over 1400x leveraging DMARC and TLS-RPT reporting.
- *Measuring TTL Violation of DNS Resolvers in the Wild* in **Passive and Active Measurement 2023**.
  - *Authors:* Protick Bhowmick, **Md. Ishtiaq Ashiq**, Casey Deccio, and Taejoong Chung.
  - Designed the measurement infrastructure and APIs for the DNSSEC experiment using Docker and Django Rest.
- *Under the Hood of DANE Mismanagement in SMTP* in **USENIX Security 2022**.
  - *Authors:* Hyeonmin Lee, **Md. Ishtiaq Ashiq**, Moritz Muller, Roland van Rijswijk-Deij, Taekyoung Kwon, and Taejoong Chung.
  - Automated the DANE key rollover scheme in a popular open-source email provider.
- *Measurement and Analysis of Automated Certificate Reissuance* in **Passive and Active Measurement 2021**.
  - *Authors:* Olamide Omolola, Richard Roberts, **Md. Ishtiaq Ashiq**, Taejoong Chung, Dave Levin, and Alan Mislove.
  - Examined SSL certificates issued by leading CAs to identify certificate misissuances based on CAA records.
- *Domain Flux based DGA Botnet Detection Using Feedforward Neural Network* in **Military Communications Conference 2019**.
  - *Authors:* **Md. Ishtiaq Ashiq**, Protick Bhowmick, Md. Shohrab Hossain, and Husnu S. Norman.

## Selected Projects

---

- **Revisiting the NXNS Attack** (2022). Developed a scalable technique to measure patches for the attack in local resolvers leveraging a proxy network, [\[details\]](#).

- **Transferability of Adversarial Training in Text Domain** (2021). Conducted a study to check transferability of adversarial training across popular adversarial frameworks. Framework: PyTorch, [\[Link\]](#).
- **DNSSEC Debugger** (2021). Analyzed historical DNSViz data to understand the challenges for DNS administrators while deploying and managing DNSSEC. Presented in **36th DNS-OARC Workshop**, [\[Link\]](#).
- **Robustness Analysis of a Web Honeypot** (2021). Demonstrated common web vulnerabilities in a popular web honeypot framework (SNARE-TANNER), [\[details\]](#).

## Languages and Technologies

---

**Languages** Python, Java, C++, C, JavaScript, HTML, CSS, Assembly (x86), familiar with R and Go  
**Frameworks and Technologies** Django Rest, Tensorflow, Apache Spark, PyTorch, Node.js, Celery, Redis  
**DBMS** Oracle SQL, PostgreSQL, MongoDB  
**Tools** Docker, Vagrant, Hugo, Gulp, AWS Services (S3, EC2), Grafana etc.

## Additional Experience and Awards

---

- **Instructor, Virginia Tech:** Taught Intermediate Software Design course during Summer 2023.
- **Open Source Contributions:** Contributed to 3 open-source projects: [Mail-in-a-Box](#), [iRedAPD](#), and [TextAttack](#).
- Awarded *University Merit List Scholarship*, and *Dean's List Scholarship* during bachelor's.