Priyanka **Dodia**

Research Associate | Cybersecurity

Brief

Ms Dodia has been a Research Associate with the Cybersecurity group at the Qatar Computing Research Institute (QCRI), since 2018.
She is a curious research enthusiast by nature and has achieved a patent and published works in top tier security conferences.
Her research areas include network architectures such as Software Defined Networking (SDN) and The Tor anonymity network and attacks such as Distributed Reflected Denial of Service (DRDoS) and Traffic Fingerprinting over Tor.
She has conducted hands-on Threat Hunting and Enterprise Log Analysis on Terabytes of real network traffic and produced an Artificial Intelligence based malware detection solution for the Ministry of Interior, Qatar.

Contact

www.priyankadodia.com
www.linkedin.com/in/pdodia-cybersecurity
priyanka.g.dodia@gmail.com
+974 55804996
Doha - Qatar
Status: Single
Qatar Resident (since 2000, 23yrs)

Languages

Hindi - Native Language
English - Professional Proficiency
Arabic - Beginner

EDUCATION

2016-2018 — **Masters Degree** — Doha, Qatar
Hamad Bin Khalifa University
MS Cybersecurity
Thesis: Sorting the Garbage: Filtering Out DRDoS Amplification Traffic in ISP Networks
GPA: 3.9/4.0

2012-2016 — **Bachelors Degree** — Doha, Qatar
Carnegie Mellon University
BS Computer Science
Minor in Business Administration
GPA: 3.14/4.0

2002-2012 — **High School** — Doha, Qatar
M.E.S Indian School
Science Stream
Central Board of Secondary Education, New Delhi
Score: 91%, Regional Topper for Computer Science

R&D PROJECTS

2023 — **Android based Proxy Traffic Collection** — QCRI
R&D
Developed headless Android Emulator based data collection testbed to run proxy apks and collect traffic for research.

Mar 2021-Nov 2022 — **Using Traffic Analysis for Tor-based Malware Detection** — Los Angeles, USA
Published: ACM Computer and Communications Security, 2022
Trained AI models and engineered features to detect Tor-based malware activity from benign browsing over Tor.

Nov 2020-Feb 2021 — **Ministry Of Interior, Qatar Case Study** — NCSRL
Threat Hunting and Enterprise Logs Analysis
Threat hunted on 2TB of confidential network and host enterprise logs. The study **resulted in exposing Ransomware** in 2 ministry networks.

Apr-Oct 2020 — **Sijil: Log Analytics Platform** — QCRI
Web App Development
Assisted the SE team with **full stack web development tasks** in an Agile Scrum for a Cybersecurity Threat Intelligence platform built for local stakeholder.

2018-2019 — **Malicious Domains Detection** — QCRI
R&D Project
Developed ML features for squatting domains resulting in a high precision random forest classifier used in an in-house security platform.

2018 — **Filtering Out DRDoS Amplification Traffic in ISP Networks** — Paris, France
Published: IEEE Network Softwarization, 2019
Setup a virtual Software Defined Network (SDN) and developed a prototype SDN firewall app to filter out amplification traffic in DRDoS attacks using victim IP from installed honeypot.

PATENTS

US Patent
2021

Methods and systems for reducing unwanted data traffic in a computer network,
Authors: Yury Zhauniarovich, **Priyanka Dodia**,
Patent no. 11206286

Soft Skills and Strengths

Empathy | Honesty | Integrity | Team Player | Curious Learner | Problem Solver | Autonomous | Self Motivated | Articulate | Persistence | Patience | Understanding | Cooperative | Open Minded | Dynamic

Professional Skills

Threat Hunting | Enterprise Log Analysis | Cyber Threat Intelligence Research | Machine Learning | Data Analysis | Research Paper Writing | Malware Analysis | Web Development | Research Presentation

Tools and Technologies

- AutoML: Autogluon
- Android Studio
- Network Simulation: GNS3
- Database Management: MySQL, MongoDB, PostGres
- OS : Linux (8+ years experience), Windows (Intermediate)
- Big Data: Apache Spark
- VM Software: Docker, VirtualBox

PUBLICATIONS

Conference Paper
2022

Exposing the Rat in the Tunnel: Using Traffic Analysis for Tor-based Malware Detection,
Authors: **Priyanka Dodia**, Mashael AlSabah, Omar Alrawi, Tao Wang,
In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS), ***Access paper here***

Conference Paper
2019

Sorting the garbage: Filtering out DRDoS amplification traffic in ISP networks,
Authors: Yury Zhauniarovich, **Priyanka Dodia**,
In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), ***Access paper here***

</> PROGRAMMING LANGUAGES

- **Python**: Advanced
- **SQL**: Familiar
- **C/C++**: Familiar
- **Java**: Familiar

ONLINE COURSEWORK

Sept 2023

MITRE ATT&CK Defender Threat Hunting
www.cybrary.it

Leverage MITRE ATTA&CK framework to develop hypotheses and analytics for threat hunting. This included David Bianco's Pyramid of Pain and Tactics, Techniques and Procedure (TTP) based dection.

August 2023

Introduction to Cyber Threat Intelligence
www.cybrary.it

Covers the main definitions and concepts related to the CTI world, including CTI frameworks such as Diamond Model and Cyber Kill Chain