Mir Mehedi Ahsan Pritom

9400 Fredericksburg Rd, APT 1106
San Antonio, TX 78240
mirmehedi.pritom@my.utsa.edu
(706) 308-8671
www.linkedin.com/in/mpritom/

EDUCATION

Doctor of Philosophy (Ongoing) in Computer Science (January 2019 - Present)
Department of Computer Science, UT San Antonio, USA
CGPA: 4.00
Doctoral Advisor: Dr. Shouhuai Xu
Research Topic: Building A Framework for Quantifying Website Trustworthiness.

Masters of Science in Information Technology (December 2018)
Department of Software and Information Systems, UNC Charlotte, USA
CGPA: 3.70
Academic Advisor: Dr. Thomas Moyer
Concentration: Information Security and Privacy.

Bachelor of Science in CSE (June 2014)
Department of Computer Science and Engineering, University of Dhaka, Bangladesh
CGPA: 3.64
Thesis Supervisor: Dr. Md. Abdur Razzaque
Thesis Topic: QoS-Aware MAC Protocol for Cluster-based Cognitive Radio Sensor Networks.

RESEARCH INTERESTS

Data-Driven and AI-Driven Security

- *Designing proactive defense frameworks against website abuse and maliciousness*
- *Quantifying trustworthiness of AI-based defense systems*
- *Application of AI for proactive cyber defense against APTs, malware, insider threats, malicious logins, and rouge websites*
- *Detecting adversarial websites generated by Generative (e.g., GAN) models*
- *Drawing attack landscapes from security events/data*

Security Automation

- *Towards automated cybersecurity management (CSM)*
- *Towards automated cyber threat hunting*

Human-Factors in Security

- *Website trustworthiness quantification based on user observations and perceptions*

Core Cybersecurity

- *Mapping and unifying cybersecurity frameworks for modeling advanced threats and organizational defense*
- *Building a unified cybersecurity ontology and knowledge-graph for web security*

TECHNICAL SKILLS

Programming Languages: Python (advanced), Java (intermediate), R (intermediate), C (intermediate), C++ (proficient), JavaScript (proficient), PHP (proficient).
Web Technologies: Apache Tomcat, MySQL, HTML, CSS, Javascript, JQuery.
Cloud Technologies: Amazon AWS (EC2, EMR, S3), MapReduce, Apache Spark, Google Cloud Platform.

Theoretical and Practical Knowledge: Security Analytics, Trustworthy Machine Learning, Data Mining and Knowledge Discovery, Data Science, Statistical Techniques, Algorithms and Data Structures, NLP, Text Mining and Analytics, Threat Modeling, Vulnerability Management, Blockchain, IT Project Management.
Tools & IDEs: Jupyter, Visual Studio, Intellij IDEA, RStudio, PyCharm, Fortify SCA, IBM SPSS, NetLogo, Xampp, Burpsuite, Palo Alto Firewall, VBox, VMWare Workstation, WireShark, Protege, ELK stack, Git, MS Project, Trello.
OS: Mac, Linux, Windows
Problem Solving: UVa Online Judge: `http://uhunt.onlinejudge.org/id/618960`

EXPERIENCES

Graduate Research Assistant May 2019 - Present
Laboratory of Cybersecurity Dynamics
Department of Computer Science, UTSA, TX, USA

My research aims to design methodologies, frameworks, and systems for a trustworthy web environment by incorporating data-driven approach. Some highlighted projects are:

- `Trustworthy Content-based Quantification of Website Abuse:` Proposing a novel framework for website abuse quantification with trust based on page contents, page screenshots, and underlying hosting features. (*In progress*)
- `Data-Driven Detection of Event Themed Malicious Websites:` Case study on detecting COVID-19 themed malicious websites using Ensemble-based machine learning models. (*Published in ISI 2020*)
- `Analyzing the Landscape of Event-themed Cyberattacks:` By mapping past and future attack events into existing Kill Chain framework we tried to understand the landscape for various COVID-19 themed cyberattacks, which can pave the way to systematically understand the nature of future global event themed cyberattacks. (*Published in ISI 2020*)
- `Automated Cyber Security Management (CSM) with Blockchain`: Building a tamper-resistant CSM framework for retrospective analysis for suspicious events using Blockchain. (*Submitted in CODASPY 2021*)
- `Mapping of Existing Cybersecurity Frameworks:` Map of all defense-centric and attack-centric cybersecurity frameworks and standards such as ATT&CK, Lockheed Martin Cyber Kill Chain, FireEye Kill Chain, DoD, NTCTFv2, ODNI, NIST, CIS Controls, and Mitre Threat Defense. Once we map all of these frameworks, we work towards defining a new robust cybersecurity framework. (*In progress*)
- `Towards Building a Robust Cybersecurity Ontology and Knowledge Graph:` This project is a sub-part of building a novel and complete cybersecurity ontology and knowledge graph, which can be applied for extracting relevant literature, and summarizing security articles. (*In progress*)
- `Detecting and Correcting COVID-19 Health Misinformation:` Analyze Twitter dataset to detect COVID-19 health misinformation with NLP and ML; analyze human subjects to correct users' psychological aspects (e.g., cognitive bias, continued influence effects) through presenting facts, and compelling stories. (*In progress*)

Graduate Teaching Assistant January 2019 - May 2019
Department of Computer Science, UTSA, TX, USA

- Cyber Operations (CS 4723) [Spring 2019]
- Secure Software Development and Analysis (CS 4683) [Spring 2019]

- Responsibilities: Grading assignments, exams, term projects, along with mentoring students.

Graduate Research Assistant May 2016 - July 2017
Center for Cybersecurity Analytics and Automation (CCAA)
Department of Software and Information Systems, UNC Charlotte, NC, USA

- We have built proactive defense system for predicting zero-day malicious IP addresses. Our proposed strategy predicts 88% of the zero-day malware instances missed by top AV vendors and predicts 68% of the Phishing websites before reported in Phishtank repository.

Graduate Teaching Assistant August 2015 - December 2018
Department of Software and Information Systems, UNC Charlotte, NC, USA

- Advanced Network Security (ITIS 6167/8167) [Fall 2015]
- Introduction to Information Security and Privacy (ITIS 3200) [Spring 2016, Fall 2018]
- Network Based Application Development (ITIS 4166) [Fall 2016, Summer 2018]
- IT Infrastructure II: Design and Practise (ITIS 3110) [Fall 2017, Spring 2018]

- Responsibilities: Assist in hands-on labs, conducting labs, mentoring students, grading assignments, projects and exams.

Software Engineer September 2014 - July 2015
Samsung Research and Development Institute (SRBD), Dhaka, Bangladesh

- Developed efficient and robust web-based mobile applications (e.g., games, utility applications) for Tizen Mobile Platform (using JavaScript, JQuery, HTML, CSS, C++).
- Learned agile software development with SCRUM in full SDLC.

LEADERSHIP & COMMUNITY SERVICES

Program Committee Member May 2019
International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT) 2019, Dhaka, Bangladesh

Paper Reviewer 2019 - 2020

- CoronaDef Workshop: Call for Innovative Secure IT Technologies against COVID-19 (Co-Located with NDSS 2021)
- The 16th International Conference on Information Security and Cryptology 2020 (Inscrypt 2020)
- The 15th International Conference on Information Security and Cryptology 2019 (Inscrypt 2019)
- 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW 2019)
- 2019 IEEE International Conference on Intelligence and Security Informatics (ISI 2019)
- The 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2019)

Executive Member January 2020 - Present
Bangladesh Student Association (BSA) at UTSA

President March 2018 - December 2018
Ekush, Bangladesh Student Organization (BSO) at UNC Charlotte

General Secretary October 2017 - October 2018
College of Computing and Informatics Grad Students Organization, UNC Charlotte

AWARDS & HONORS

- ***UTSA Doctoral Fellowship*** August 2019 - Present
- 1^{st} ***Place, COVID-19 Transdisciplinary Team Grand Challenge (UTSA Grad School)*** *September 2020*
- ***UNC Charlotte GASP Tuition Award*** August 2015 - December 2018
- 2^{nd} ***Place, Engineering and CS Poster Presentation, 17th Graduate Research Symposium at UNC Charlotte*** *March 2017*

CERTIFICATES

Text Mining and Analytics August 2016
University of Illinois at Urbana-Champaign on Coursera.
`https://www.coursera.org/account/accomplishments/verify/EQASMJXL594A`

PUBLICATIONS

[1] ***M.M.A. Pritom****, K. Schweitzer, R. Bateman, M. Xu, S. Xu, "Data-Driven Characterization and Detection of COVID-19 Themed Malicious Websites", 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Virtual Event (accepted)*

[2] ***M.M.A. Pritom****, K. Schweitzer, R. Bateman, M. Xu, S. Xu, "Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses", 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Virtual Event (accepted)*

[3] S. He, E. Ficke, ***M.M.A. Pritom****, H. Chen, Q. Tang, Q. Chen, M. Pendleton, L. Njilla, S. Xu, "Blockchain-Based Automated Cyber Security Management", Proceedings of the 11th ACM Conference on Data and Application Security and Privacy (CODASPY 2021), Virtual. (submitted)*

[4] A. Niakanlahiji, ***M.M.A. Pritom****, B. Chu and E. Al-Shaer, "Predicting Zero-day Malicious IP Addresses", In Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '17). Association for Computing Machinery, New York, NY, USA, 16. DOI:https://doi.org/10.1145/3140368.3140369*

[5] ***M.M.A. Pritom****, C. Li, B. Chu, X. Niu, A Study on Log Analysis Approaches Using Sandia Dataset", 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-6, doi: 10.1109/ICCCN.2017.8038522.*

[6] M.N.S. Miazi, ***M.M.A. Pritom****, M. Shehab, B. Chu, J. Wei, "The Design of Cyber Threat Hunting Games: A Case Study", 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-6, doi: 10.1109/ICCCN.2017.8038527.*

[7] ***M.M.A. Pritom****, S. Sarker, M.A. Razzaque, M.M. Hassan, M.A. Hossain, A. Alelaiw, "A Multiconstrained QoS Aware MAC Protocol for Cluster-Based Cognitive Radio Sensor Networks", International Journal of Distributed Sensor Networks (IJDSN) 2014.*

[8] ***M.M.A. Pritom****, A. Niakanlahiji, B. Chu, "POSTER: Proactive Connection Blocking Based on Cyber Threat Intelligence (CTI), 17th Annual Graduate Research Symposium at UNC Charlotte, March 2017*