Mir Mehedi Ahsan Pritom, Ph.D.

Address: 500 Dry Valley Rd #G302, Cookeville, TN 38506
Email: mpritom@tntech.edu
Website: www.mirmehedipritom.com

Education

- **University of Texas at San Antonio (UTSA)**, San Antonio, Texas, USA
  Ph.D. in Computer Science, 2019 to 2022 [CGPA 4.00]
  Advisors: Dr. Ravi Sandhu and Dr. Shouhuai Xu
  Dissertation Topic: "Defending Against Malicious Websites: Themed Threats, Detection, and Law-enforcement."
- **University of North Carolina at Charlotte (UNCC)**, Charlotte, NC, USA
  M.S. in Information Technology (InfoSec concentration), 2018 [CGPA 3.70]
  Academic Advisor: Dr. Thomas Moyer
- **University of Dhaka (DU)**, Dhaka, Bangladesh
  B.S. in Computer Science and Engineering, 2014 [CGPA 3.64]
  Thesis Advisor: Dr. Abdur Razzaque
  Thesis Topic: "A multiconstrained QoS aware MAC protocol for cluster-based cognitive radio sensor networks"

Professional Work Experiences

- **Department of Computer Science, Tennessee Technological University**, Cookeville, TN, USA
  - **Assistant Professor (Tenure-track)** **[Aug 2023 - Present]**
    - **Secure Software and Systems** (CSC 4585/5585) [Fall 2023]
    - **Research and Student Advising**
- **Department of Computer Science, Appalachian State University**, Boone, NC, USA
  - **Assistant Professor (Tenure-track)** **[Aug 2022 - July 2023]**
    - **Discrete Mathematics** (CS 1100) [Fall 2022, Spring 2023]
    - **Intro to Information Security and Privacy** (CS 3545) [Fall 2022]
    - **Introduction to Security Analytics** (CS 3546) [Spring 2023]
    - **Machine Learning for Cybersecurity** (CS 3541) [offering Summer II 2023]
    - **Research and Student Advising**
- **Department of Computer Science, UTSA**, San Antonio, Texas, USA
  - **Course Instructor (Teaching Assistant II)** **[Aug 2021 - Jul 2022]**
    - **Discrete Mathematical Structures** (CS 2233) [Fall 2021, Spring 2022]
    - **Computer Architecture** (CS 3853) [Summer 2022]
  - **Teaching Assistant I** **[Jan 2019 - Aug 2021]**
    - **Cyber Operations** (CS 4673) [Spring 2019]
    - **Secure Software Development and Analysis** (CS 4683) [Spring 2019]
    - **Advanced Software Engineering** (CS 4783) [Spring 2021]

  - * **Data Structures** (CS 2124) [Spring 2021, Summer 2021]

- **Department of Software and Information Systems, UNC Charlotte**, North Carolina, USA
  - **Graduate Teaching Assistant** **[Aug 2015 - Dec 2018]**
    - * **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 Practice** (ITIS 3110) [Fall 2017, Spring 2018]
  - **Graduate Assistant** **[Jan 2017 - Aug 2017]**
    - * Developed course contents for **"Intro to Security Analytics (ITIS 4260)"** [First offered in Fall 2017]

- **Institute for Cyber Security (ICS), UTSA**, San Antonio, Texas, USA
  - **Graduate Research Assistant**, Laboratory of Cybersecurity Dynamics (LCD) **[May 2019 - Dec 2020]**
    - * **Hands-on research within the intersection of cybersecurity and data science domain**

- **Center for Cybersecurity Analytics and Automation (CCAA), UNC Charlotte**, North Carolina, USA
  - **Graduate Research Assistant** **[May 2016 - Aug 2017]**
    - * **Hands-on research experience on cyber threat intelligence, threat hunting, and data-driven security analytics**
    - *

- **Green Networking Research (GNR) Lab, University of Dhaka**, Bangladesh
  - **Student Researcher** **[Jan 2013 - Jun 2014]**
    - * **Hands-on research experience on sensor networks, MAC protocols, cognitive radio networks, dynamic spectrum allocation, network environment simulation, and e-health development strategies**

- **Samsung Research and Development Institute (SRBD)**, Dhaka, Bangladesh
  - **Software Engineer**, Mobile Lab **[Sep 2014 - Aug 2015]**
    - * **Developed efficient and robust Tizen OS-based mobile applications (i.e., games, utility apps)**
    - * **Worked with agile software development process (i.e., SCRUM) in full software development life cycle**

Research Interests

1. Decision-Support System (DSS) for Cyber Defense

- Supporting Law-enforcement with an intelligent decision-support system for dealing with URL blacklists and effective decision-making against truly malicious websites versus compromised websites
- Designing preventive and proactive cyber defense strategies against deceptive emerging event-themed (e.g., Russia-Ukraine war, COVID-19, national election, or natural disasters) malicious websites
- Using trustworthy and interpretable machine learning (ML) to explain why and what decisions to make in the face of malicious websites or malicious activities
- Leveraging data-driven Causal inference to explain uncertain decision-making in cybersecurity against cyberattacks, intrusions or malicious websites

2. Security Analytics

- Machine Learning (ML) and Deep Learning (DL) based detection/prediction of malicious domain (DNS), malware, and intrusions

- Leveraging Natural Language Processing (NLP) for extracting malicious indicators and TTPs (Techniques, Tactics, and Procedures) from security reports
- Web Analytics and Cyber Threat Intelligence based malicious website detection
- Leveraging threat intelligence data (e.g., VirusTotal) and vulnerabilities within the technology (i.e., PHP, WordPress, javascript) used for the websites to quantify the probability of compromise
- Detecting Vulnerabilities in coding projects with NLP/AI and connect with CVEs
- Detection and characterization of cyber social threats (e.g., themed misinformation, cyber bullying) in social media platforms

2. Human Factors in Security (Usable Security)

- What is the effectiveness of current user-centric defenses against web, email, and social engineering attacks?

3. Automation in Security

- Towards automated and robust cyber threat hunting processes- from hypothesis generation to finding threats
- Towards an automated, robust, and secure cyber threat intelligence sharing

4. Core Cybersecurity, Cyber Education, Knowledge Graphs (KGs)

- Towards a unified cybersecurity and risk frameworks (e.g., DoDCAR + ODNI + NIST + ATT&CK + Kill Chain) for modeling advanced threats and enterprise defenses
- Building a comprehensive web security and defense ontology and knowledge graphs (KGs) for defense recommendation against web-based attacks
- Developing effective experiential learning approaches for advanced security analytics and threat hunting cyber education

Teaching Interests

1. Computer Science

- Core and applied courses in the areas of Computing such as Discrete Mathematics, Logic & Algorithms, Data Structures, CS I, Computer Programming, Computer Networks, Operating Systems, and Database Design & Implementation.

2. Cybersecurity and Information Security

- Fundamental and Advanced courses in the directions of Information and Cyber Security such as Principles of Information Security and Privacy, Security Analytics, ML for Security, Threat Hunting, System Admin and Security, Network Security, Software PenTesting, Cyber Defense, and Incident Response with Threat Intelligence.

3. Data Science and Analytics

- Fundamental and Advanced courses in areas of Data Science such as Fundamentals of Data Science, Knowledge Discovery from Databases (KDD), Predictive Analytics, Data/Text Mining, Introduction to Machine Learning, Applied Machine Learning, Python Programming for Data Science, and Cloud Computing for Data Analysis.

Publications

Refereed Conference and Workshop Proceedings

1. **Mir Mehedi A. Pritom**, Jacob Villemagne, and S. Xu "Characterizing the Russia-Ukraine war themed websites in the wild," (manuscript in preparation).

2. **Mir Mehedi A. Pritom** and S. Xu, "Supporting Law-Enforcement to Cope with Blacklisted Websites: Framework and Case Study," 2022 IEEE Conference on Communications and Network Security (CNS), 2022, pp. 181-189, `doi:10.1109/CNS56114.2022.9947260`.

3. **Mir Mehedi A. Pritom**, K. M. Schweitzer, R. M. Bateman, M. Xu and S. Xu, "Data-Driven Characterization and Detection of COVID-19 Themed Malicious Websites," 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, 2020, pp. 1-6, `doi:10.1109/ISI49825.2020.9280522`.

4. **Mir Mehedi A. Pritom**, K. M. Schweitzer, R. M. Bateman, M. Xu and S. Xu, "Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses," 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, 2020, pp. 1-6, `doi:10.1109/ISI49825.2020.9280539`.

5. A. Niakanlahiji, **Mir Mehedi 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, 1–6. `doi:10.1145/3140368.3140369`.

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

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

Refereed Journal Articles

8. Songlin He, Eric Ficke, Mir Mehedi Ahsan Pritom, Huashan Chen, Qiang Tang, Qian Chen, Marcus Pendleton, Laurent Njilla, Shouhuai Xu, "Blockchain-based automated and robust cyber security management", Journal of Parallel and Distributed Computing, Vol 163, 2022, Pages 62-82,ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2022.01.002. (Impact factor: 3.734)

9. **Mir Mehedi A. Pritom**, Sujan Sarker, Md. Abdur Razzaque, M. Mehedi Hassan, M. Anwar Hossain and Abdulhameed Alelaiwi, "A Multiconstrained QoS Aware MAC Protocol for Cluster-based Cognitive Radio Sensor Networks", International Journal of Distributed Sensor Networks (IJDSN), Article ID 262871, Dec 2014. SCIE. (Impact factor: 1.787)

Patents

10. S. Xu, S. He, E. Ficke, M. M. A. Pritom, H. Chen, Q. Tang, Q. Chen, M. Pendleton, and L. Njilla, "Method and system for blockchain-based cyber security management," Patent US20230042816, February, 2023. [Online].
Available:https://www.freepatentsonline.com/y2023/0042816.html

Pre-print Articles

1. **Mir Mehedi A. Pritom**, Rosana Montanez Rodriguez, Asad Ali Khan, Sebastian A. Nugroho, Esra'a Alrashydah, Beatrice N. Ruiz, and Anthony Rios, "Case Study on Detecting COVID-19 Health-Related Misinformation in Social Media.", arXiv preprint 2021, `https://arxiv.org/abs/2106.06811`.

Posters

1. **Mir Mehedi A. Prit om**, A. Niakanlahiji, B. Chu, "POSTER: Proactive Connection Blocking Based on Cyber Threat Intelligence (CTI)", 17th Annual Graduate Research Symposium at UNC Charlotte, March 2017.

Google Scholar: Profile link (**94+** citations)

Research Project Highlights

- **Project: Defending Against Smishing.** Proposing methodology to characterize and defend against SMS-based Phishing attacks known as Smishing. We propose to study the current status of defense and understand what services attackers are abusing to propagate these attacks. We want to leverage NLP, explainable AI, and predictive analytics for building the defense mechanisms. We want to generate a robust and complete solution to mitigate the smishing problem in US mobile network ecosystem. (Ongoing, Contribution: lead)

- **Project: Characterization and Quantification of Russia-Ukraine War Themed Malicious Websites.** Proposing methodology to detect and quantify malicious websites those are themed with Russia-Ukraine war related topics and contents. Identify the effective features and methodology to detect these malicious websites effectively. We also want to explore how they are different from COVID-19 themed malicious websites and if a unified themed-website quantification framework can be achieved. (Ongoing, Contribution: lead)
- **Project: Supporting law enforcement in coping with URL blacklists.** Proposing frameworks, mechanisms, and case studies for quantifying compromised versus malicious websites based on their URL structures, domain structures, hosting infrastructures, and user perceptions. In parallel, we also propose confidence measures and interpretability measures to enhance the trustworthiness of law enforcement's domain-level interventions (e.g., domain takedowns). (Contribution: lead)
- **Project: From Vulnerable Codes to CVEs.** Proposing methods to connect CVE database to real-world vulnerable codes based on NLP and ML models. This project is currently in its early preparation phase, and any potential collaboration is more than welcome. (Contribution: lead with collaboration)
- **Project: Tackling the emerging threats of COVID-19 themed cyberattacks.** Proposing methodologies to systematically understand the threat landscapes of the emerging threats known as *COVID-19 themed cyberattacks*, which is influenced by the novel Coronavirus. We also propose and discuss defense spaces for these threats to enhance the situational awareness. Finally, we propose methodologies for detecting COVID-19 themed malicious websites and COVID-19 themed health-related misinformation leveraging ML models. (Contribution: lead)
- **Project: B2CSM: Blockchain-based automated cyber security management.** Proposing systems and methods for automated and robust Cyber Security Management (CSM) leveraging Ethereum blockchain. We presented several case studies with various CSM functions to show how blockchain can provide the tamper resistant feature in day to day cyber threat management along with minimal added latency. We also presented the design and implementation of a prototype CSM platform. (Contribution: part of design team)
- **Project: Mapping existing cybersecurity frameworks with a comprehensive cybersecurity ontology.** Our proposal aims to map all of the existing defense-centric and attack-centric cybersecurity frameworks and standards such as Mitre ATT&CK, Lockheed Martin's Cyber Kill Chain, FireEye's Kill Chain, DoD, NTCTFv2, ODNI, NIST, CIS Controls, and Mitre Threat Defense by building a comprehensive and unified cybersecurity ontology of these frameworks. We expect to find gaps within these frameworks and systematize the way of intelligence sharing among security communities. (Ongoing, Contribution: co-lead)
- **Project: Predicting zero-day malicious IP addresses.** Proposed a proactive defense system for predicting zero-day malicious IP addresses infecting enterprise networks. Our proposed system predicts 88% of the zero-day malware instances missed by top Anti Virus vendors and 68% of the Phishing websites before reported in Phishtank repository. (Contribution: co-lead)
- **Project: Cyber threat hunting as defense.** Developed and hosted an in-house cyber threat hunting competition at UNC Charlotte in 2017 with our self-created augmented anomalous enterprise logs. Later, we presented a study on what we learnt from the competition about the participants' approaches, and what we need to train high quality next-gen threat hunting experts. (Contribution: co-lead)
- **Project: Log analysis on large host and network logs.** Conducted meta analysis on various log analysis techniques using an existing publicly available host and network log dataset from Sandia National Lab. We discovered the limitations and faults of the existing studies, which is caused by wrong assumptions and usage of logs without proper validation. (Contribution: lead)
- **Project: Reputation analysis of open-source cyber threat feeds.** Analyzed a number of publicly available threat intelligence feeds from *Hailataxi.com* portal to account for update frequency, overlapping, coverage, geolocation distribution, and data variations. We provide a qualitative assessments of the feeds, which provides further grounds for a more comprehensive and quantitative reputation analysis of the threat feeds. (Contribution: lead)

Community Services and Leadership Roles

Academic Committees

- CS Undergraduate Program Committee (Cyber Curriculum Representative), Tennessee Tech University [August 2023 - Present]
- CS Student House "Lovelace" Faculty Affiliate, Tennessee Tech University [August 2023 - May 2024]
- Departmental Transfer advisor, Computer Science, Appalachian State University [August 2022 - July 2023]
- Departmental Scholarship committee, Computer Science, Appalachian State University [August 2022 - July 2023]
- Departmental AdHoc committee to improve Discrete Mathematics Course syllabus for more cohesive Computer Science learning experience, Appalachian State University [February 2023-May 2023]
-

Program Committee Member

- ACM Workshop on Secure and Trustworthy Cyber Physical Systems (SaT-CPS) 2023, Charlotte, NC, USA
- International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT 2019), Dhaka, Bangladesh

Ad Hoc and Volunteer Reviewer/Sub-reviewer

- IEEE Communications Magazine 2022/23
- ACM Asia CCS 2022, Melbourne, Australia
- IEEE International Conference on Communications and Network Security (CNS 2021), virtual conference
- Military Communications Conferecene (MICOM 2021), San Diego, USA
- CoronaDef Workshop: Call for Innovative Secure IT Technologies against COVID-19 (Co-Located with NDSS 2021)
- Secure and Trustworhty Cyber Physical Systems (SaT-CPS 2021), Virtual (Co-located with ACM CODASPY 2021)
- 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI 2020), Dhaka, Bangladesh
- 16th International Conference on Information Security and Cryptology (Inscrypt 2020), Guangzhou, China.
- 15th International Conference on Information Security and Cryptology (Inscrypt 2019), Nanjing, China
- IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW 2019), Berlin, Germany
- IEEE Conference on Intelligence and Security Informatics (ISI 2019), Shenzhen, China
- 15th International Conf. on Security and Privacy in Communication Networks (SecureComm 2019), Orlando, FL

Professional and Volunteer Memberships

- **Member**, Association for Computing Machinery (ACM) **[October 2022 - Present]**
- **Member**, Institute of Electrical and Electronics Engineers (IEEE) **[Jan 2021 - Present]**
- **Executive Committee Member**, Bangladesh Student Association (BSA) at UT San Antonio **[Jan 2020 - Jan 2022]**
- **Founding President**, Ekush, Bangladesh Student Organization (BSO) at UNCC **[Mar 2018 - Dec 2018]**
- **General Secretary**, College of Computing and Informatics Grad Students (CCI Grads), UNCC **[Oct 2017 - Oct 2018]**

Technical Skills Highlights

Core and Applied Computing knowledge from finished graduate-level courses: Principle of Information Security and Privacy, Cybersecurity Data Science, Secure Software DevOps and Pen Testing (Threat modeling, VAPT), Infrastructure Protection, Machine Learning, Data Mining for Knowledge Discovery, KDD, Advanced Statistical Techniques, Blockchain for Cybersecurity, Algorithms and Data Structures, Operating Systems, Computer Architecture, Compiler Design and Analysis, Human Computer Interaction, and IT Project Management.

Programming Languages	: Python, Java, R , C , C++, Javascript, and PHP
Web Technologies	: Xampp, Apache Tomcat, MySQL, HTML, CSS, and JQuery
Cloud/Distributed Tech	: Amazon AWS (EC2, S3), MapReduce, Apache Spark, Hadoop, and Google Cloud
IDEs	: PyCharm, Visual Studio, Intellij IDEA, and RStudio
Security Tools	: Wireshark, Metasploit, Burp Suite Pen Tester, Fortify Static Code Analyzer, Palo Alto Firewall, Kali Linux, and Powershell script, OWASP Top 10 threats
Data Analysis Tools	: Jupyter Notebook, IBM SPSS, ELK Stack
Management Tools	: Git, GitHub, GitLab, MS Project, Trello, MS Office Suite
Modeling Tools	: NetLogo, NS-3
Ontology Tool	: Protege
Libraries and Frameworks	: Numpy, Scipy, Scikit-learn, Mrjob, NLTK, Tweepy, matplotlib, Tensorflow, Keras, NLP BERT
ML Methods	: Classification (Naive Bayes, Random Forest, SVM, kNN, Logistic Regression), Clustering (K-means, DBSCAN), Deep Neural Nets (CNN, RNN, LSTM), and NLP/Text mining (n-gram, TF-IDF, word embedding, bag-of-words, topic modeling)
Operating Systems	: Mac, Windows, Linux
Problem Solving	: Participated and Solved **5** security challenge tasks in NSA Codebreaker 2021

Talks, Presentations, and Conferences Attended

- **Invited Lecture** on "COVID-19 themed cyber attacks and defenses" in the *Cyber Security Data Science* course taught by Dr. Shouhuai Xu in Fall 2020 at UTSA
- **Attended & Presented 2 conference papers** in IEEE ISI 2020 virtual conference.
- **Attended & Presented 2 Workshop papers** in IEEE ICCCN 2017 conference in Vancouver, Canada.
- **Attended** SIG KDD 2020 (Aug 23-27, 2020), virtual conference.
- **Attended** IEEE Euro S&P 2020 (September 7-11, 2020), virtual conference.
- **Attended** ACM AsiaCCS 2020 (Oct 5-9, 2020), virtual conference.
- **Attended** ACM CCS 2020 (Nov 9-13, 2020), virtual conference.
- **Attended** ACM CODASPY 2021 (Apr 26-28, 2021), virtual conference.
- **Attended** IEEE S&P ('Oakland' SP) 2021 (May 24-27, 2021), virtual conference.
- **Attended** ICWSM 2021 (June 7-10, 2021), virtual conference.
- **Attended** 3rd International Conference on Science of Cyber Security (SciSec) 2021 (Aug 13-15, 2021), virtual.
- **Attended** SIG KDD 2021 (Aug 15-19, 2021), virtual conference.
- **Attended & presented 1 conference paper** in IEEE CNS 2022 (Oct 3-5, 2022), Austin, TX.

Awards and Honors

- **AppState SWAG 2023 Stipend** **[November 2022]**
  This is a competitive $3500 stipend award for writing external grants provided by University Research Council (URC) at AppState where all faculties could submit their proposals.
- **Running to PhD Scholarship, Department of Computer Science, UTSA** **[August 2022]**
  This is a $3000 one time award/scholarship for finishing PhD earlier than estimated graduation semester.
- **UTSA Graduate Research Fellowship** **[Aug 2019 - Dec 2020]**
- **1^{st} place, COVID-19 Transdisciplinary Team Proposal Grand Challenge** (UTSA Grad School) **[Aug 2020]**
  Our team won $21K worth of prize money for a proposal on ways to tackle COVID-19 themed health-related misinformation propagation in social media. Media Coverage
- **2^{nd} place, Engineering and CS Poster Presentation** (17th Grad Research Symposium, UNCC) **[Mar 2017]**
  Won $200 as prize money for securing the second place.

Certificates

Text Mining and Analytics **[August 2016]**
University of Illinois at Urbana-Champaign on Coursera (Course certificate link)

References

Dr. Shouhuai Xu
Gallogly Chair Professor, Department of Computer Science
University of Colorado Colorado Springs, Colorado, USA
Contact: (210)-857-0160; Email: sxu@uccs.edu
Dr. Xu's Personal Website

Dr. Ravi Sandhu
Executive Director and Chief Scientist, Institute of Cyber Security (ICS)
Lutcher Brown Endowed Chair in Cyber Security and Professor of Computer Science
University of Texas at San Antonio, Texas, USA
Contact: (210)-458-6081; Email: ravi.sandhu@utsa.edu
Dr. Sandhu's Personal Website

Dr. Raymond Bateman
U.S. Army Combat Capabilities Development Command
Army Research Laboratory South - Cyber
University of Texas at San Antonio, Texas, USA
Contact: 240-532-0525; Email: raymond.m.bateman4.civ@army.mil