

Cover Letter

Makhdumabanu Farukali Saiyed

She/Her

Ph.D.

Electronic Systems Engineering

University of Regina, SK, Canada

Work Permit Holder (Eligible to Work in Canada)

Email : mfs208@uregina.ca

Contact : 639-554-3310

March 21, 2025

Dear Members of Hiring Committee

I am writing to apply for the position of Instructor in the BTech program in Cyber Security of the School for Advanced Digital Technology (SADT). I am pleased to see how well my experience aligns with the course requirements and the expectations of this role.

I have successfully completed my Ph.D. in Electronic Systems Engineering within the Faculty of Engineering and Applied Science at the University of Regina. My research focuses on artificial intelligence-based cybersecurity systems for detecting and mitigating cyberattacks in IoT networks, with a particular focus on high- and low-volume Distributed Denial of Service (DDoS) attacks. By combining statistical analysis, machine learning, and deep learning approaches, I have developed effective systems for detecting, classifying, and mitigating DDoS attacks in Internet of Things (IoT) networks. One of my major contributions to cybersecurity is the generation of realistic high- and low-volume DDoS attack datasets, specifically designed for IoT networks. Furthermore, I have developed an interactive user interface (UI) using Streamlit to improve the usability and transparency of the detection system for network administrators. This UI integrates SHAP values, which provide an explainable layer to the AI models, thereby supporting administrators in understanding ongoing cyberattacks effectively. In addition to detection, my research also explores optimal cybersecurity strategies for defense, including the use of game-theoretic models to dynamically select defense strategy, such as deploying honeypots or applying rate limiting. I further integrated a genetic algorithm to optimize these strategies, ensuring a balance between resource utilization and effective attack mitigation. During my Ph.D. research journey, I have made significant contributions in the field of cybersecurity by publishing articles in peer-reviewed IEEE and Elsevier journals. I have published four journal papers, and three additional papers are currently under review in journals. I presented a paper at a flagship conference, the International Conference on Communications (ICC), as well as at IEEE Globecom 2024. Additionally, another paper has been accepted for IEEE ICC 2025. Overall, my research advances the field of cybersecurity by providing practical and optimized solutions for IoT network protection, equipping me with both the theoretical and applied expertise that I look forward to bringing into my teaching and research.

My future research aims to advance adaptive, explainable, and intelligent cybersecurity solutions for IoT networks by integrating Hierarchical Reinforcement Learning (HRL), game theory, federated learning, and cyber forensics. I intend to build HRL-based defense systems that enhance security by dividing detection and mitigation tasks into structured decision-making layers. These systems will employ deep learning for anomaly detection and HRL for dynamic mitigation strategies such as rate limiting and traffic isolation, reducing computational overhead while ensuring efficient defense. To improve trust and transparency, I plan to integrate Explainable AI (XAI) techniques like SHAP and LIME, ensuring AI-driven cybersecurity decisions are interpretable for administrators and security professionals. This will help bridge the gap between machine learning models and human decision-making, making security systems more transparent and user-friendly. I also plan to explore game-theoretic and evolutionary defense strategies, where attack-defense interactions are mathematically modeled. By applying genetic algorithms, I will develop adaptive cyber defense mechanisms that optimize honeypot deployment, traffic control, and resource allocation, allowing security systems to respond dynamically to cyber threats. Furthermore, I will investigate federated learning for cybersecurity, enabling collaborative attack detection across distributed IoT systems without sharing raw data. This approach will support scalable, real-time security solutions while preserving user privacy, making it ideal for large-scale IoT deployments. In the long term, I aim to expand into cyber forensics, developing frameworks for post-attack analysis to strengthen network resilience and improve forensic investigations for IoT-based cyber incidents.

I have a diverse set of teaching skills, and I am particularly effective at engaging and motivating students. I believe these qualities make me a strong candidate for the Assistant Professor position. I have twelve years of teaching experience, primarily in the Department of Computer Science and Engineering, Faculty of Engineering and Technology, at Parul University, India, along with experience in Electronic Systems Engineering, Faculty of Engineering and Applied Science, at the University of Regina. I worked as a sessional lecturer in the Electronic Systems Engineering program, Faculty of Engineering and Applied Science, at the University of Regina. I taught ENEL 442 (Digital Communications) for eight months, conducted tutorials, and taught labs for ENEL 441 (Communication Theory) once and ENEL 443 (Design of Computer Networks) three times. Previously, I worked as an Assistant Professor from 2017 to 2021 and as a Lecturer from 2011 to 2014 in the Department of Computer Science and Engineering at Parul University, India. In addition, I worked as a lecturer in Information Technology at Sigma Polytechnic, India. During my time at Parul University and Sigma Polytechnic, I taught courses such as Cybersecurity, Information Security, Software Engineering, Machine Learning, Computer Networks, C Programming, Object Oriented Analysis and Design, Parallel and Distributed Computing, Operating Systems, Wireless Communications, Digital Communication, and Computer Graphic. Beyond my teaching responsibilities, I actively contributed to academic, technical, and social services through various roles. In the academic domain, I served as a Board of Studies Coordinator, Course Coordinator, Exam Coordinator, Women's Development Coordinator, and International Relations Coordinator. On the technical domain, I contributed as a technical committee member for conferences, a session chair at various conferences, and a reviewer for reputed journals. In the social domain, I actively participated in mental health awareness initiatives at Parul University, India, and took part in food distribution drives, working towards community well-being and social responsibility in Regina, Canada.

In my teaching philosophy, I believe that each student is unique, and my role as a teacher is to identify their strengths and create a learning environment that supports their growth. Open communication is essential, and I actively seek student feedback to adjust my teaching approach accordingly. When students struggle, I reach out personally to understand their challenges and provide guidance. My teaching style includes group discussions, storytelling, and hands-on activities to improve critical thinking, collaboration, and creativity in offline classes. In online classes, to enhance engagement, I integrate Google Classroom, Moodle, Zoom, and Google Meet for learning. I also use Mentimeter to encourage interactive participation. Additionally, I offer extra tutorials (online and offline) for complex topics, connecting theory with practical applications. I align learning objectives with Bloom's taxonomy and use clear assessment strategies to ensure students are well-prepared for real-world challenges.

At Bachelor of Technology – Cyber Security program of the School for Advanced Digital Technology (SADT) at the Southern Alberta Institute of Technology, I am prepared to teach courses, including but not limited to CMPN 3010, CMPN 3000, CMPP 3030, ITSC 4000, ITSC 4010, ITSC 4020, ITSC 4020, and CPSY 3000. In addition to these existing courses, I propose to introduce two new courses if required: IoT Security and Privacy and Machine Learning for Cybersecurity. In IoT Security and Privacy, I will cover key challenges in device authentication, data privacy, and network security, using Internet of Things Security: Principles and Practice by Fei Hu. In Machine Learning for Cybersecurity, students will learn how ML detects and mitigates threats like DoS, DDoS, malware, and phishing, drawing from Machine Learning and Security by Clarence Chio and David Freeman.

I am especially interested in this position at SADT because of its focus on applied learning and industry-based curriculum. The hands-on approach to teaching cybersecurity fits well with my teaching style, which focuses on practical applications, student involvement, and skill development. I am excited about the chance to help students prepare for real-world careers and contribute to a program that values both innovation and effective teaching. SADT's focus on digital technologies and advanced learning also matches my background in AI-based cybersecurity and my goal of turning research into practical knowledge for students.

I am enthusiastic about the opportunity to bring my teaching experience, research expertise, and passion for cybersecurity education to SADT. My Ph.D. is awarded on March 26, 2025, and I hold a valid post-graduation work permit (PGWP), making me eligible to work in Canada. I look forward to the opportunity to discuss how my expertise and qualifications can contribute effectively to this role and to SADT's mission. I also look forward to contributing to your academic community and supporting students in building the skills they need to succeed in the cybersecurity field.

Thank you for your time and consideration.

Sincerely,
Makhdumabanu Farukali Saiyed