March 16, 2020

Search Committee
Division of Tropical Environments and Societies
College of Science and Engineering
James Cook University
Cairns, Australia

Dear Search Committee,

I am writing to apply for the Lecturer position advertised by the James Cook University, Australia (17078: Lecturer, Information Technology). I am currently working as a Research Fellow with Toby Murray in the School of Computing and Information Systems, University of Melbourne, Melbourne. My research area is primarily focussed on formal verification of mission critical software programs. Currently, I am working on Security Concurrent Separation Logic, and the aim of the project is to formally reason about security and information flow for a concurrent program. Moreover, during my PhD at the Australian National University, Canberra, I worked on the formal verification of electronic voting scheme, mainly Schulze method. I am enthusiastic about contributing to your growing and innovative department, specifically in the area of formal verification and software security.

My graduate research with Dirk Pattinson was to bring electronic voting close to paper ballot election. Since the introduction of secret ballots in Victoria, Australia in 1855, paper (ballots) are widely used around the world to record the preferences of eligible voters. Paper ballots provide three important ingredients: correctness, privacy, and verifiability. However, the paper ballot election brings various other challenges, e.g. it is slow for large democracies like India, and error prone for complex voting method like single transferable vote, and poses operational challenges for large countries like Australia, specifically areas like Northern Territory. In order to solve these problems and various others, many countries are adopting electronic voting. However, electronic voting has a whole new set of problems. In most cases, the software programs used to conduct the election have numerous problems, including, but no limited to, counting bugs, ballot identification, etc. Moreover, these software programs are treated as commercial in confidence and are not allowed to be inspected by general member of general public. As a consequence, the result produced by these software programs can not be substantiated. I answered the three main concerns posed by electronic voting, i.e. correctness, privacy, and verifiability. I addressed the correctness concern by using theorem prover to implement the vote counting algorithm, privacy concern by using homomorphic encryption, and verifiability concern by generating a independently checkable scrutiny sheet (certificate). My research goal is to keep pushing the boundaries and continue the further development of secure electronic voting, specifically focussing on correctness, privacy, and verifiability. Moreover, I would carry on the collaboration with Dirk Pattinson, Rajeev Gore, and Thomas Haines and local faculty at the James Cook University, having the expertise in cryptography, specifically homomorphic encryption, zero-knowledge-proof, multi-party computation.

As a Research Fellow at the University of Melbourne, I am investigating the information flow security in weak memory model in presence of concurrency with Toby Murray. Verifying the correctness of functional programs without any side effect in a theorem prover is not very difficult. Moreover, in most of cases, the proofs are simple pen-and-paper proof. However, in case of side effects, the reasoning about the correctness of program is difficult, mainly in the context of heap manipulating programs, and this situation gets more complicated in the presence of concurrency in weak-memory. Our project is geared towards a formal reasoning about information flow security and the method we will develop will be applied to verify the security of seL4-based software for critical embedded devices. It is still in nascent phase; however, our ultimate goal is to add the information flow reasoning logic for C/C++11, formally prove it in Coq theorem prover, and develop a tool to automate it. In future, I would continue working with Toby Murray and seL4 team.

In addition to my research, I have facilitated the success of students through teaching and mentoring. I would be delighted to use these skills to enhance the success of your university in developing future generation leaders in security. In addition, I believe, my research would contribute to your department's goal in engagement with industry, community agencies and professional bodies. In long term, I want to expand my field of study to privacy preserving machine learning, using fully homomorphic encryption to perform computation and its use in healthcare data, designing domain specific languages to automate the security policies of an organization, and using multi-party computation to design electronic voting schemes.

Please contact me if you need any further information. Thank you for your consideration.

Sincerely,

mukesh Tiwari

Mukesh Tiwari
Research Fellow
School of Computing and Information Systems
University of Melbourne
Melbourne, Victoria
mukesh.tiwari@unimelb.edu.au
https://findanexpert.unimelb.edu.au/profile/860472-mukesh-tiwari