Mukesh Tiwari
Cambridge, United Kingdom
+447824648138
mt883@cam.ac.uk

To
Dr. Surya Nepal
Group Leader,
CSIRO's Data61 & Deputy Research Director Cybersecurity

May 15, 2022

Application for the post of Research Scientist in Cybesecurity (74837)

Dear Dr. Surya Nepal,

I am writing to apply the job **Research Scientist in Cybersecurity**. I have an extensive experience in security research, and I find that CSIRO would be a perfect place to continue my research and expand my horizons in other areas, including machine learning, AI, etc. I have a PhD from the Australian National University, Canberra and have been working as a Senior Research Fellow at the University of Cambridge since October 2021. Before moving to Cambridge, I was a research fellow at the University of Melbourne.

In my PhD, I have verified the Schulze vote counting method, a widest path problem. I have addressed ballot privacy by using homomorphic encryption, and verifiability by means of producing an independently verifiable scrutiny sheet, consisting of various zero-knowledge-proofs, the validity of which can be independently substantiated, that witnesses the correctness of the execution of an election. At CSIRO, as a Research Scientist, I would like to expand my research area in to cybersecurity using machine learning and AI, in addition to carrying out the cybersecurity using formal method.

As a senior research associate at the University of Cambridge, I am working on a mathematical correct-by-construction framework based on theory of routing algebra to alleviate network-engineers from proving the correctness of their protocol and focus entirely on protocol design. All they need to do is express their protocol in my (mathematical) framework, and it will tell what property the protocol follows and what it does not. In addition, my framework can also be used in operation research, given that its underlying principles are very similar to protocol design.

As a research associate at the University of Melbourne, I did acquire hands-on knowledge of separation logic and information flow security. I have spearheaded three projects: (i) A formally verified auction server, (ii) A formally verified location server, and (iii) A formally verified machine learning algorithm that is resistant to side-channel attacks and can run inside the Intel SGX (Software Guard Extensions) enclave for learning on senstive data. All three implementations have been proven memory safe (using separation logic) and free from information leaks (applying information flow security), using the SecCSL tool.

I look forward to hearing from you. Let me know if you have any questions.

Your Sincerly,

Mukesh Tiwari