Yasod Ginige

+61403352214 yasod.ginige@sydney.edu.au yasod-ginige YasodGinige

SUMMARY AND RESEARCH INTERESTS

A highly motivated, individual who is passionate and willing to learn new concepts to solve problems. Currently, pursue a PhD in computer science at the University of Sydney. My fields of interest are **Machine Learning**, **Computer Networks and Security**, and **Computer Vision**.

EDUCATION

Jan. 2024 - Present — **UNIVERSITY OF SYDNEY, Australia**

- Ph.D. Candidate in the School of Computer Science.
- Title : AI Enhanced Cybersecurity for Red Teaming and Blue Teaming Tasks.
- Build autonomous cybersecurity tools integrating AI technologies with security tools. The aim is to cater the skill shortage in security industry and increase the usability of security tools for the general public.
- Finalist in the **Google Student Fellowship**. Was one of the two nominees of the University of Sydney.

Nov. 2018 - Jul 2023 — **UNIVERSITY OF MORATUWA, Sri Lanka**

- BSc. Engineering (Honors), specialized in Electronic and Telecommunication Engineering.
- Cumulative GPA : 4.05/4.20 *(First Class Honors)*.
- Was nominated for the Most Outstanding Graduate of the Year.

Jul. 2015 - Aug. 2017 — **RICHMOND COLLEGE - GALLE, Sri Lanka**

- The most outstanding student of the year 2017.
- National Rank : 8^{th} in the G.C.E. Advanced Level Examination (from ∼20,000 candidates).

PROFESSIONAL EXPERIENCE

Aug. 2024 – Present | **CASUAL ACADEMIC**
University of Sydney, Australia

- Conduct tutorials for the COMP5618, CSEC3616, CSEC5616, and INFO3616 Cybersecurity Engineering courses.
- Conduct tutorials for the INFO6007 Project Management in IT course.

Apr. 2024 – Dec 2024 | **CASUAL ADMINISTRATIVE OFFICER - CYBER EVENT ORGANIZATION**
University of Sydney, Australia

- Conducted cybersecurity workshops for engineering students. Explained practical applications of theories.

Jul. 2023 – Dec. 2023 | **SOFTWARE ENGINEER**
Axiata Digital Labs (Pvt) Ltd, Sri Lanka

- Worked on a project to build a low latency, high throughput API manager using C++ and Java. Used concepts such as OOP, lambda functions, api, multi-threaded coding, and used relevant tools.

Dec. 2021 – Sep. 2022 | **STUDENT RESEARCH AFFILIATE**
University of Sydney, Australia

- Worked on two research projects on ML based network security. Studied and researched on traffic fingerprinting attacks, membership inference attacks, and model quantization effects.
- Completed and submitted two papers.

Jan. 2022 – Jul. 2022 | **VISITING RESEARCHER**
Monash University, Australia

- Worked on a project based on developing a DNA alphabet to store data using the Nanopore technology.
- Used first-order filters for signal processing, statistical models like Markov models for classification.
- Developed machine learning models to identify DNA patterns of the alphabet with 96% accuracy with higher throughput.

Oct. 2022 – Jul. 2023 | **VISITING INSTRUCTOR**
University of Moratuwa, Sri Lanka

- Conducted lab sessions for the “EN3143 : Electronic Control Systems” module. Explained theories and their applications.

PUBLICATIONS

- **Ginige Y.**, Akila N., Jain S., Seneviratne S. AutoPentester : An LLM Agent-based Framework for Automated Pentesting - Accepted for IEEE TrustCom 2025 (A).

- **Ginige Y.**, Silva B., Dahanayaka T., Seneviratne S. TrafficLLM : LLMs for Improved Open-Set Encrypted Traffic Analysis - Accepted for Computer Networks Journal (Q1).
- Dahanayaka T., **Ginige Y.**, Huang Y., Jourjon G., & Seneviratne S. (2023). Robust open-set classification for encrypted traffic fingerprinting. Computer Networks (Q1), 236, 109991. [pdf]
- Karunanayake, N., Silva, B., **Ginige Y.**, Seneviratne S., Chawla S. Quantifying and Exploiting Adversarial Vulnerability : Gradient-Based Input Pre-Filtering for Enhanced Performance in Black-Box Attacks - ACM Transactions on Privacy and Security Journal (Q1). [pdf]
- **Ginige Y.**, Dahanayaka T., Seneviratne S. TrafficGPT : An LLM Approach for Open-Set Encrypted Traffic Classification - Asian Internet Engineering Conference. [pdf]
- **Ginige Y.**, Gunasekara R., Hevawithara D., Ariyarathne M., Rodrigo R., Jayasekara P. Object Tracking, Reidentification and Activity Detection for Maritime Surveillance - Under review at the Machine Learning and Cybernetics Journal (Q2).[video]
- Tang L., Bogahawatta N., **Ginige Y.**, Xu J., Sun S., Ranathunga S., Seneviratne S. A Framework to Assess Multilingual Vulnerabilities of LLMs - International World Wide Web (WWW) Conference (A*).

ARTICLES

- E-Carrier magazine : Official magazine of the Department of Electronic and Telecommunication Engineering
  Published two articles, namely "Silicon to DNA" and "Website Traffic Fingerprinting".

RESEARCH EXPERIENCE

PHD RESEARCH — University of Sydney, Australia
LLM Agents Based Autonomous Penetration Testing — *2024 - Present*
Advisors : Dr. Suranga Seneviratne and Prof. Aruna Seneviratne

- Developed an automated pentesting tool based on LLMs and ML techniques to address the skill shortage in cybersecurity.
- Used a multi-agent-based system with a hierarchical RAG architecture to solve the dynamic attack environment mapping and strategy identification in the pentesting processes.
- Used LLMs and RAG architectures along with techniques such as chain-of-thought reasoning, reinforcement learning, and in-context learning. Used OOP principles in coding and frameworks like PyTorch, LangChain, OpenAI, and Transformers.

INTERNSHIP RESEARCH — University of Sydney, Australia
Robust Open Set Classification for Encrypted Traffic Fingerprinting [code] — *2021 - 2022*
Advisors : Dr. Suranga Seneviratne and Dr. Thilini Dahanayake

- Developed a novel network traffic classification method that can be deployed in resource constrained network devices using deep learning and statistical methods.
- The method could quantize classifier models to a 4-bit state with only 4% of performance degradation.

Quantifying and Exploiting Adversarial Vulnerabilities using Gradient-Based Input Pre-Filtering — *2022*
Advisors : Dr. Suranga Seneviratne and Dr. Sanjay Chawla

- Proposed a novel adversarial perturbation technique to optimize adversarial inputs for trained machine learning models using a novel technique called zero gradients.
- The method outperformed the state-of-the-art. We proved the transferability of our method between ML models using different datasets and shadow models.

HONORS RESEARCH — University of Moratuwa, Sri Lanka
Object Tracking, Reidentification and Activity Detection for Maritime Surveillance [code] — *2022-2023*
Advisors : Dr. Peshala Jayasekara and Dr. Ranga Rodrigo

- Developed a thermal-based maritime surveillance system with real-time object tracking, suspicious activity detection, and viewpoint-invariant vessel re-identification, integrated into an interactive GUI for continuous 24×7 monitoring and alerting.
- The novel re-identification algorithm can re-identify vessels from different viewpoints, paying attention to even minor features of the vessel's shape. The work is under review.
- The activity detection algorithm identifies suspicious activities like human trafficking by processing the video feed in real time.

EXTERNAL RESEARCH — Monash University, Australia
Encoding and Decoding Data into DNA Using an Alphabet of DNA Sequences — *2022*
Advisors : Prof. Emanuele Viterbo and Dr. Viduranga Wijekoon

- Involved in a next generation technological research where we store data in high density DNA patterns.
- Researched on deep learning approaches to classify nanopore signals (small electric signals) corresponding to a given alphabet. Used CNN and LSTM architectures and obtained 95% accuracy.
- Used first order filters and Markov chains to optimize results for real world data.

IEEE Signal Processing Society - ICAS Challenge — University of Moratuwa, Sri Lanka
Self-Awareness in Heterogeneous Multi Robot System [code] — *2021*
Advisors : Dr. Chameera Edussooriya

- The project aims to identify anomalies of a multi-robot system using IMU, camera, and Lidar sensor data.
- Implemented an auto-encoder model to identify anomalies in IMU data of an autonomous robot.
- Used a GAN model to reconstruct the next frame of a frame sequence, thereby identifying anomalies in the camera sensor data.

OTHER PROJECTS

SMART BREADBOARD : TO FACILITATE REMOTE LAB EXPERIMENTS. [*Skills : Electronics, Arduino, IoT, Python*]
Designed a smart breadboard using a MOSFET matrix to support virtual experiments during pandemic periods. Connections between columns and rows are made by switching on MOSFETs according to a user input. Users design circuits through the GUI, which are automatically implemented on the smart breadboard by switching MOSFET switches. The project won the IEEE CAS Student Design Competition 2020/21 in Sri Lanka and was selected for the IEEE Region 10 finals. [video]

ELDERBOT : ELDERLY CARE ELECTRONIC PRODUCT. [*Skills : Electronics, Arduino, HTML, Solidworks*]
Designed an electronic product to assist elderly people in a fall or an emergency situation by sending alarm messages. Used an MPU6050 sensor, NodeMCU, and MQTT, and HTTP protocols. Developed software and a UI for user login and profile management. [video]

AUTONOMOUS MOBILE AND ASSISTING ROBOT FOR SLRC 2018. [CODE] [*Skills : Electronics, Arduino, Solidworks*]
Designed and developed two robots. A mobile autonomous robot that follows lines and dashed lines, solves a line maze (using the DFS algorithm), collects, detects, sorts by color, and unloads coins. It communicates with an immobile assisting robot, which removes obstacles from its path.

IMAGE DOWNSAMPLING PROCESSOR DESIGN AND FPGA IMPLEMENTATION. [CODE] [*Skills : Verilog, FPGA*]
Designed and implemented a RISC processor to downsample an image on the Altera DE2-115 FPGA board.

FILE COMPRESSION AND DECOMPRESSION ALGORITHM [CODE] [*Skills : C++*]
Implement both code compression and decompression using C++ for a given input file. A customized rule set was used for the compression and decompression tasks.

HONORS AND AWARDS

Honnorable Mention Award : International Physics Olympiad — *2018*
- Organized by the International Physics Olympiad Board

World Champions :IEEE ICAS 2021 Challenge (Montreal, Canada) : — *2021*
- Organized by IEEE Signal Processing Society

World Champions :IEEE IES Student Branch Chapter Competition : — *2022*
- Organized by IEEE Industrial Electronics Society

World Runner-up :IEEE International Humanitarian Technology Video Competition : — *2022*
- Organized by IEEE Canada

Represented Sri Lanka in the Asian Physics Olympiad — *2018*
- Organized by the Physics Olympiad Committee of Vietnam

NSW Connectivity Innovation Network(CIN) PhD scholarship — *2023*
- Awarded by Connectivity Innovation Network, NSW, Australia

Champions : 2nd International Energy and Electricity Market Business Decision Competition — *2020*
- Organized by the Shanghai University, China

Nominee for the Most Outstanding Graduate of the Year 2023 — *2023*
- University of Moratuwa, Sri Lanka

Gold Medalist : Sri Lankan Physics Olympiad 2018 — *2018*
- Organized by the Institute of Physics, Sri Lanka

Dean's List in Semesters 1, 2, 4, 5, 6, 7, and 8 — *2018 - 2023*
- Faculty of Engineering, University of Moratuwa

Darrel Medal : The Most Outstanding Advanced Level Student Award — *2017*
- Awarded by Richmond College, Galle, Sri Lanka

Small Medal : Best Student in Mathematics — *2015*
- Awarded by Richmond College, Galle, Sri Lanka

School Colors for Cricket — *2013*

- Awarded by Richmond College, Galle, Sri Lanka

TECHNICAL SKILLS

PROGRAMMING LANGUAGES	Python, C/C++, Java, Verilog
LIBRARIES	Tensorflow, Pytorch, NumPy, Keras, Scikit-learn, Pandas, LangChain
SOFTWARE TOOLS	MATLAB, Altium, SOLIDWORKS, Spring Boot, Git, LaTeX, SonarQube, NodeRed
HARDWARE	Atmel AVR, Altera DE2, Raspberry Pi, NodeMCU

COURSES AND CERTIFICATION

Jun. 2020 **IMPERIAL COLLEGE, LONDON, COURSERA**
- Mathematics for Machine Learning-Linear Algebra

Aug. 2020 **DEEPLEARNING.AI**
- Deep Learning Specialization – 5 Courses

Aug. 2023 - Present **EC COUNCIL**
- Certified Ethical Hacker Certification

VOLUNTEERING AND LEADERSHIP SKILLS

IEEE Industrial Electronics Society - Student Branch Chapter of University of Moratuwa

- Chairman (2022-2023) and Vice Chairman (2021-2022)
- Provided leadership for a 150 member base to organize workshops, seminars, competitions, and social events.
- Emerged as “The best IES student branch chapter” in the worldwide competition in 2022.
- Won the “Emerging Student Branch Chapter” award in the IEEE Sri Lanka section awards – 2022.

Young Professionals Coordinator : Institute of Engineers Sri Lanka (IESL) NSW Chapter

- Main organizer HDR student gathering at Universities in Sydney.
- Organized a traditional event to celebrate the Sinhala and Hindu New Year.

HDR Student Representative : School of Computer Science, University of Sydney.

- Organized technical and non-technical HDR events to build the network and improve social skills in HDR students.

Mathematics Society, University of Moratuwa

- Chairman in 2020-2021
- Provided leadership for a 300 member base to organize seminars, workshops and competitions.

Co-chair of the Gold Chasers project - Rotaract Cub, University of Moratuwa

- Organized practical and tutorial sessions for the Sri Lankan Physics Olympiad team, 2019.
- The team obtained 2 bronze medals and one honorable mention in the International Physics Olympiad 2019.

Member of the Cricket Team, Richmond College Galle

- Won the all island championship in 2013 and semi-finalists in 2012.

REFERENCES

Dr. Suranga Seneviratne
Senior Lecturer in Security
School of Computer Science
University of Sydney
suranga.seneviratne@sydney.edu.au

Prof. Aruna Seneviratne
Mahanakorn Chair of Telecommunications
School of Electrical Eng. and Telecom.
University of New South Wales
a.seneviratne@unsw.edu.au

Dr. Peshala Jayasekara
Senior Lecturer
Dept. of Electronic and Telecom. Eng.
University of Moratuwa
peshala@uom.lk