Research Statement

Nguyễn Đình Đức Nhã (Nha/Tony)
VinUniversity, Gia Lam, Ha Noi, Viet Nam

As the Founder and Principal Investigator of VCyber Lab (https://vcyber.work) at VinUniversity, I am at the forefront of advancing Post-Quantum Cryptography (PQC), cybersecurity for robotics, and AI-driven cybersecurity. My research is driven by the urgent need to develop next-generation security solutions that can withstand quantum-era threats, safeguard autonomous systems, and harness AI for proactive cyber defence.

With a strong track record of high-impact research, my work has been published in top-tier venues, including IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Mobile Computing (TMC), and IEEE Transactions on Information Forensics and Security (TIFS). These contributions not only push the boundaries of cybersecurity theory but also translate into real-world applications, ensuring the resilience of critical systems in an increasingly complex digital landscape.

Through VCyber Lab, I aim to bridge the gap between academic innovation and practical cybersecurity solutions, fostering a research ecosystem that shapes the future of secure computing.

Current & Future Research Directions

Post-Quantum Cryptography (PQC)

Quantum computing is set to revolutionize the cybersecurity landscape, posing a major threat to all classical cryptographic schemes. My research is focused on pioneering Post-Quantum Cryptography (PQC) solutions to ensure long-term security in the face of this quantum revolution. Unlike classical cryptography, PQC does not require quantum computers for its development but is designed to withstand quantum-based attacks. This aligns with the principle that even if we do not fully understand how to create quantum computers, we must proactively secure our systems against their potential threats. My experience in PQC has culminated in establishing my own research lab, **VCyber Lab (https://vcyber.work)**, where I lead efforts to design and implement cryptographic solutions resistant to quantum adversaries. Our work focuses on hybrid cryptographic models, integrating PQC with existing protocols to ensure a seamless and secure transition from traditional cryptographic infrastructures to quantum-resistant ones.

AI Agents for Penetration Testing and Cybersecurity Enhancement

Traditional cybersecurity assessments, including penetration testing, vulnerability discovery, and system monitoring, are time-consuming and require significant human expertise. My research aims to develop AI-driven security agents capable of automating these processes, enabling continuous and intelligent threat detection. AI has the ability to store vast amounts of cybersecurity knowledge, learn from new attack vectors, and dynamically update itself to counter emerging threats. These AI agents will provide an always-on cybersecurity monitoring system, reducing human intervention while increasing efficiency and accuracy. At **VCyber**

Lab, I am leading efforts to integrate advanced AI techniques, including deep learning and reinforcement learning, to develop intelligent cybersecurity tools capable of self-learning, adapting, and responding to sophisticated cyber threats in real-time.

Cybersecurity for Robotics

Robotics is increasingly becoming an integral part of modern society, with applications ranging from healthcare and industrial automation to autonomous vehicles and smart homes. However, security vulnerabilities in robotic systems present significant risks, including unauthorized control, data breaches, and operational disruptions. I believe that cybersecurity for robotics will be a defining research area in the coming decades, and my goal is to establish a leading position in this domain. My research will focus on securing robotic networks, ensuring safe human-robot interactions, and preventing cyber-physical threats. By applying my expertise in cryptography, AI, and network security, I aim to develop novel frameworks that protect robotic infrastructures from cyberattacks while ensuring compliance with emerging security standards.

Past Research

Intrusion Detection in IoT and Next-Generation Networks

AI and Machine Learning in Cybersecurity

The integration of AI into cybersecurity has been a key theme in my research. AI-driven models enable more adaptive and efficient security systems that can respond to threats in real time. My work on federated learning-based intrusion detection schemes, published in IEEE TNSM, demonstrates the potential of distributed AI models to secure large-scale networks without compromising user privacy. These models learn from distributed datasets while keeping the data localized, reducing risks associated with centralized data storage.

Moreover, my research proposed effective framework for intrusion detection in 5G networks by leveraging data dimension reduction and anomaly detection architecture at the network edge. This design significantly decreases the training time of traditional machine learning models and enables faster anomaly detections. This framework represents a significant step towards providing an efficient and effective way to empower networks to detect attacks in 5G. The work has been published in IEEE Transactions on Information Forensics and Security, a widely recognized top-tier venue known for its high citation rates and influence within the academic and professional cybersecurity communities.

Furthermore, one of my research focuses is on the challenges of data sparsity in AI models. Data is the backbone of AI models. However, in many real applications, data collection may introduce missing or compromised data caused by device faults, environmental impacts, and attacks. Data sparsity affects the accuracy of AI models, which leads to inaccuracies in any applications based on these models. By exploring correlation values and Fuzzy Information Decomposition theory, we can predict compromised or missing data samples and recover the original values. This method addresses an important problem: recovering compromised or missing sensor values in IoT environments by proposing a sound theoretical approach. This work was funded by the Australian Department of Defence, and it has been submitted to IEEE Transactions on Mobile Computing, where it received a major revision.

Post-Quantum Cryptography and Hybrid Security Models

My past research centres around hybrid security models that integrate both traditional cryptography and PQC methods, ensuring robust protection against quantum and classical computational threats. As part of the SOCRATES project at Deakin University, I have developed and implemented an automatic hybrid PQC system. This system leverages post-quantum algorithms such as Dilithium and Falcon, alongside traditional algorithms like RSA and ECDSA, to build a secure VPN solution. By testing this system under varying network conditions, we evaluated its resilience and performance in mitigating potential threats posed by quantum computing advancements. This work is critical, as current cryptographic systems are vulnerable to future quantum attacks, and transitioning to quantum-resilient systems is paramount for the security of sensitive data.

Conclusion

My research is at the forefront of **PQC, AI-driven cybersecurity, and robotic security**, addressing the most pressing challenges in the cybersecurity landscape. As technology rapidly evolves, these research areas will define the future of secure computing. Through **VCyber Lab** and ongoing collaborations with academia, industry, and government partners, I am committed to making impactful contributions that strengthen global cybersecurity resilience against present and future threats.