Nguyen Dang Quynh Nhu

listimdn10 | NDQN | quynhnhu170218@gmail.com | 0909501046

Summary

I am currently a junior in Cybersecurity at University of Information Technology – VNU-HCM, with a strong focus on AI-driven security in LLMs and Smart Contracts. At the same time, I am committed to leveraging Blockchain and AI to build a sustainable future, pursuing the convergence of AI and Security as the foundation of my career path.

Awards & Honors

- Second Prize – VietFuture Awards 2025 (National Innovation Competition)
  Role: Team Leader
  Project: Reasoning-Aware Adaptive Prompt Protection (RAPP)
- Selected for NextStart Incubation Program (NextTech Group) – supporting promising startups to realize their ideas
- Awarded Local Grant to attend ACM AsiaCCS 2025 – Selective competitive grant for outstanding students in Vietnam.

Work Experience

Department: The UIT Information Security Laboratory Aug 2025 – present

Fuzzing Smart Contract with Agentic AI *Github*

Role: Team Leader

- Applied TextCNN and GATv2 on DappScan dataset to detect vulnerabilities in smart contracts.
- Integrated Multi-LLM Agents to locate vulnerable code lines and generate fuzzing seeds.
- Defeated nondeterminism in LLMs to ensure consistent outputs, providing fixed solutions despite repeated inputs.
- Replicated `FinanceFuzz()` framework and enhanced it with an agentic system to improve performance and coverage.

Security-related Projects

A Multi-Agent Architecture for Detecting Smart Contract Vulnerabilities via Multi-Modal Embeddings and Retrieval-Augmented Generation *Github*

Role: Team Leader

- Utilized EtherSolve, Mythril, and Slither for control flow graph (CFG) generation and smart contract analysis.
- Designed a four-agent architecture coordinated with CrewAI:
  - Fetch Agent – Scrapes vulnerable smart contracts from GitHub repositories.
  - RAG Agent – Retrieves enriched context using Neo4j Knowledge Graph and fine-tuned LLMs (Qwen-Coder-2.5-14B, Qwen-3-14B, Deepseek-r1-distill-llama-8B).
  - Parser Agent – Parses smart contract code into CFGs, functional semantics, and source code; embeddings with GATv2, all-MiniLM-L6-v2, and CodeBERT.

  - Fusion Agent – Combines multi-view embeddings and classifies vulnerabilities using a custom MLP classifier.

RAPP: Reasoning-Aware Adaptive Prompt Protection *Github*

Role: Team Leader

- Finetuned SLMs to identify and classify PII in text into predefined categories.
- Built a ML/DL models to classify PII tasks Vs non-PII tasks.
- Developed a PII mapping database to support reversible masking and unmasking workflows.
- Designed system extensibility for future integration of a Reinforcement Learning Agent to prevent direct and indirect leakage by LLMs
- Solve the nondeterminism in Large Language Models by convert normal kernels into batch-invariant kernels

AgriCarbonDEX – A Carbon Credit and Environmental Data Trading Platform Based on Digital Twin, Blockchain, and LLM Agents *GitHub*

- Built an on-chain carbon credit system using **ERC-721** (positive/negative NFTs) and **ERC-20 CCT tokens**, with DIDs for polluter traceability.
- Developed a Multi-Agent LLM system with:
  - Manager Agent: routes user queries and delegates tasks.
  - Retriever Agent: searches internal knowledge via FAISS and HuggingFace embeddings.
  - Search Agent: performs real-time web search with DuckDuckGo and HTML parsing.
- Powered agents with Qwen2.5-72B-Instruct as the central reasoning engine.
- Contributed to the design of future Specialized ESG Agents (e.g., Regulation, Risk, Digital Twin) and Trading Bot.

RAG-SmartVuln: Enhancing Smart Contract Vulnerability Detection via Retrieval-Augmented LLMs *GitHub*

Accepted at the 8th International Conference on Multimedia Analysis and Pattern Recognition (MAPR 2025)

Role: Team Leader

- Designed a multi-stage processing architecture, beginning with data enumeration and culminating in comparative analysis of vulnerability detection techniques.
- Constructed a Vulnerability Knowledge Base/Graph using LLMs, augmented by Slither and Mythril, and stored in a Pinecone vectorstore to enable Retrieval-Augmented Generation (RAG).
- Fine-tuned the open-source models (Qwen-3-14B, Qwen-Coder-2.5-14B, and Deepseek-R1-Distill-Llama-8B) using PEFT and BitsAndBytes for efficient adaptation to smart contract vulnerability detection tasks.

CRYSTALS-DILITHIUM: The Implementation of Digital Signature in Digital Government *GitHub*

Role: Team Leader

- Designed and implemented a secure digital signature framework using the post-quantum algorithm **CRYSTALS-Dilithium**, ensuring authentication, integrityand non-repudiation of government documents.
- Built a Certificate Authority (CA) system with OpenSSL integration for key generation, signing, and verification workflows.
- Developed secure publication of government news in signed PDF format, embedding QR codes with timestamp and publisher identity, and stored them in **MongoDB GridFS**.

- Implemented modules for searching, downloading, and verifying official PDF records, including robust signature and public key validation.
- Created both CLI and Flask-based GUI interfaces to streamline usability for administrators and end-users.

Education

2022 - present Bachelor's Degree at **University of Information Technology** (GPA: 3.3/4.0)

Publications

Nhu, Nguyen et al. (Aug. 2025). "RAG-SmartVuln: Enhancing Smart Contract Vulnerability Detection via Retrieval-Augmented LLMs". In: pp. 1–6. DOI: 10.1109/MAPR67746.2025.11134018.

Skills

Programming Languages	Python, C++, Solidity
Smart Contract Security	Mythril, Slither, Oyente; Smart contract fuzzing
Smart Contract Development	Metamask; Ethereum Virtual Machine (EVM); Hardhat
LLM Frameworks & Ecosystem	LangChain, LlamaIndex; CrewAI; Hugging Face Transformers; Ollama; OpenAI API
LLM Techniques	Retrieval-Augmented Generation (RAG); Fine-tuning & prompt engineering; Multi-agent orchestration
Machine Learning Foundations	Supervised; Unsupervised; Reinforcement Learning; Feature engineering; Deep Learning (RNN, LSTM, GRU)
Vector Databases	FAISS, Pinecone
Knowledge Graph	Neo4j
Data Storage	SQL Server, MongoDB, MongoDB GridFS, MySQL
Version Control	Git
Languages	Vietnamese (native), English (fluent)

Certificates

IELTS 6.5
Natural Language Processing on Google Cloud
Introduction to Generative AI Learning Path – Google Cloud
Transformer Models and BERT Model – Google Cloud
Google AI Essentials – Google Cloud