|  |  |
| --- | --- |
| ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH  **TRƯỜNG ĐẠI HỌC**  **CÔNG NGHỆ THÔNG TIN** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc Lập - Tự Do - Hạnh Phúc** |

# ĐỀ CƯƠNG CHI TIẾT

|  |  |
| --- | --- |
| **TÊN ĐỀ TÀI:**  -Tên tiếng Việt: Phát hiện lỗ hổng trong hợp đồng thông minh trên mạng liên chuỗi khối bằng phương pháp học máy  -Tên tiếng Anh: Smart contract vulnerabilities automatic detection on the cross-chain network using machine learning | |
| **Cán bộ hướng dẫn:** TS Phạm Văn Hậu và ThS Trần Tuấn Dũng | |
| **Thời gian thực hiện:** Từ ngày 11/9/2023 đến ngày 31/12/2023 | |
| **Sinh viên thực hiện:**  Võ Anh Kiệt – 20520605 – 0365642317 | |
| **Nội dung đề tài:***(Mô tả chi tiết mục tiêu, phạm vi, đối tượng, phương pháp thực hiện, kết quả mong đợi của đề tài)*  Mục tiêu  Mục tiêu của đề tài này là nghiên cứu và phát triển một phương pháp sử dụng học máy để phát hiện lỗ hổng trên các hợp đồng thông minh trong môi trường mạng liên chuỗi khối. Điều này nhằm tăng cường tính bảo mật và độ tin cậy của các hợp đồng thông minh, từ đó giúp ngăn chặn và giảm thiểu các rủi ro tiềm ẩn, bảo vệ quyền lợi của các bên tham gia.  Phạm vi  Phạm vi của đề tài bao gồm:   * Tìm hiểu về công nghệ mạng liên chuỗi khối và triển khai tấn công trên mạng liên chuỗi: Nắm vững kiến thức về cấu trúc, hoạt động và ứng dụng của mạng liên chuỗi khối, đặc biệt về hợp đồng thông minh trên nền tảng mạng liên chuỗi và thực hiện tấn công trên mạng liên chuỗi khối. * Xác định lỗ hỏng và sự cần thiết phát hiện lỗ hỏng: Định rõ các lỗ hổng phổ biến trên hợp đồng thông minh trên mạng liên chuỗi và lý do cần phải phát hiện chúng. * Thiết kế mô hình học máy cho việc phát hiện lỗ hỏng: Xây dựng một mô hình học máy phù hợp để phát hiện lỗ hổng trên hợp đồng thông minh trên mạng liên chuỗi, sử dụng các kỹ thuật học máy hiện đại và tối ưu hóa để đảm bảo hiệu suất và độ chính xác cao. * Đánh giá mô hình: Áp dụng mô hình phát hiện lỗ hỏng đã thiết kế vào một số hợp đồng thông minh thực tế trên mạng liên chuỗi khối và đánh giá hiệu suất của mô hình.   Đối tượng  Các đối tượng của nghiên cứu bao gồm:   * Công nghệ chuỗi khối * Công nghệ liên chuỗi * Bảo mật smart contract * Công nghệ học máy   Phương pháp thực hiện  Để đạt được mục tiêu và phạm vi đã đề ra, đề tài này sẽ triển khai các phương pháp sau:   * Nghiên cứu lý thuyết: Tìm hiểu sâu về lĩnh vực blockchain, mạng liên chuỗi khối và hợp đồng thông minh để xác định các lỗ hỏng thường gặp và cách xử lý chúng. * Phân tích dữ liệu và thiết kế mô hình học máy: Xây dựng tập dữ liệu, phân tích dữ liệu và xây dựng mô hình học máy phù hợp để phát hiện lỗ hỏng trên hợp đồng thông minh. * Triển khai mô hình và thử nghiệm: Áp dụng mô hình đã xây dựng vào các hợp đồng thông minh thực tế, thu thập dữ liệu và đánh giá hiệu suất của mô hình dựa trên các tiêu chí như độ chính xác, độ nhạy và độ cụ thể. * Tối ưu hóa và điều chỉnh mô hình: Dựa vào kết quả thử nghiệm, tiến hành tối ưu hóa và điều chỉnh mô hình học máy để đảm bảo hiệu suất tốt nhất.   Kết quả mong đợi  Kết quả dự kiến từ đề tài này gồm:   * Mô hình học máy hiệu quả: Xây dựng một mô hình học máy có khả năng phát hiện lỗ hỏng trên hợp đồng thông minh trên mạng liên chuỗi với độ chính xác và độ nhạy cao. * Hiểu biết sâu về lỗ hổng trên hợp đồng thông minh: Tìm hiểu và phân tích kỹ hơn về các lỗ hổng phổ biến trên hợp đồng thông minh và cách để ngăn chặn chúng. * Đóng góp cho cộng đồng blockchain: Cung cấp kiến thức và công cụ hữu ích cho nhà phát triển hợp đồng thông minh và cộng đồng blockchain, từ đó tăng cường tính bảo mật và độ tin cậy của hệ thống. | |
| **Kế hoạch thực hiện:**  1/9/2023 – 10/9/2023: Hoàn thành dàn ý cho ý tưởng, nghiên cứu các công trình liên quan, đưa ra mô hình tổng quan  11/9/2023 – 1/10/2023: Hoàn thành thực nghiệm triển khai cầu nối và tấn công trên cầu nối  2/10/2023 – 20/10/2023: Hoàn thành thu thập dữ liệu nhằm dựng file dataset  21/10/2023 – 14/11/2023: Hoàn thành prediction model, đưa ra số liệu đánh giá, tối ưu hoá mô hình  15/11/2023 – 31/12/2023: Hoàn thành báo cáo Khoá luận tốt nghiệp, hiệu chỉnh những thông tin cần thiết | |
| **Tài liệu tham khảo:**   1. Feng, Z., Li, Y., & Ma, X. (2023). Blockchain-oriented approach for detecting cyber-attack transactions. Financial Innovation, 9(1), 81. 2. Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), 7162. 3. Yingjie Xu, Gengran Hu, Lin You, and Chengtang Cao. 2021. A novel machine learning-based analysis model for smart contract vulnerability. Security and Communication Networks 2021 (2021), 1–12. 4. Weichu Deng, Huanchun Wei, Teng Huang, Cong Cao, Yun Peng, and Xuan Hu. 2023. Smart contract vulnerability detection based on deep learning and multimodal decision fusion. Sensors 23, 16 (2023), 7246. 5. Lejun Zhang, Weijie Chen, Weizheng Wang, Zilong Jin, Chunhui Zhao, Zhennao Cai, and Huiling Chen. 2022. Cbgru: A detection method of smart contract vulnerability based on a hybrid model. Sensors 22, 9 (2022), 3577. 6. Mirko Staderini, Caterina Palli, and Andrea Bondavalli. 2020. Classification of ethereum vulnerabilities and their propagations. In 2020Second International Conference on Blockchain Computing and Applications (BCCA). IEEE, 44–51. 7. Terje Haugum, Bjørnar Hoff, Mohammed Alsadi, and Jingyue Li. 2022. Security and Privacy Challenges in Blockchain Interoperability-A Multivocal Literature Review. In Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering. 347–356. 8. Daojing He, Zhi Deng, Yuxing Zhang, Sammy Chan, Yao Cheng, and Nadra Guizani. 2020. Smart contract vulnerability analysis and security audit. IEEE Network 34, 5 (2020), 276–282. | |
| **Xác nhận của CBHD 1 Xác nhận của CBHD 2**  (Ký tên và ghi rõ họ tên) (Ký tên và ghi rõ họ tên)  A black background with white text  Description automatically generated | **TP. HCM, ngày 25 tháng 09 năm 2023**  **Sinh viên**  **A close up of a signature  Description automatically generated**(Ký tên và ghi rõ họ tên) |