Thesis proposed by: COSIC	
(Title:) Hunting Vulnerabilities in Smart Contract Bytecode	
GUIDANCE	
• For more information, please contact:	*yunwen.liu@kuleuven.be*, *enrique.argonesrua@kuleuven.be*
• Promotor(s): (name)	Yunwen Liu
• Daily advisor(s)	Enrique Argones Rúa
• Number of students	1
CONTEXT	
Smart contracts manage digital assets through programs running on blockchains, where a single vulnerability can lead to major financial losses. Recent advances in AI agents have increased their ability to discover and exploit smart contract vulnerabilities, creating new challenges for defenders. Developers often keep source code private to protect trading strategies and business logic, leaving only the deployed bytecode publicly available. This makes security analysis particularly challenging.	
GOAL	
This thesis will investigate machine learning for detecting multiple vulnerability types directly from smart contract bytecode.	
METHODOLOGY	
You will train a detection model, evaluate its effectiveness and robustness, and explore its potential to uncover previously unknown vulnerabilities in decentralized finance (DeFi) contracts.	
Focus on GenAI: Optional	
If yes, students are encouraged to explore GenAI tools in depth (beyond standard use) within their thesis topic. This includes documenting how they use these tools effectively, focusing on process and strategy. Note: this excludes manuscript writing, which must follow KU Leuven's GenAI code of conduct. If no, standard use of GenAI following the KU Leuven's GenAI code of conduct remains allowed. However, the focus is not on the strategy or optimization of such tools.	
PROFILE/REQUIRED SKILLS e.g. rather theoretical / rather practical implementation, required knowledge (courses, methods, computer language(s), etc.)	
30% literature, 20% theoretical work, 50% software	

REFERENCES
Other relevant information