Title: Trustworthy, Explainable and Responsible AI-Driven Software Vulnerability Detection: A Computational Design Science Approach

Revathi Karri, Junior Researcher, LUT University

INTRODUCTION/BACKGROUND

A software vulnerability is a defect or weakness in software that could allow an attacker to gain control of a system.

Detecting Software Vulnerabilities: A Critical Need

- **Context:** The increasing reliance on third-party libraries and code reuse has heightened the risk of software vulnerabilities, which can lead to significant economic and social losses.
- **Key Fact:** Cybercrime costs are expected to exceed $13 trillion annually by 2028 (Figure 1), emphasizing the urgent need for effective software vulnerability detection.
- **Rising Threat:** The number of common IT security vulnerabilities and exposures (CVEs) has grown exponentially from 2009 to 2024 YTD (Figure 2), highlighting the escalating challenge of maintaining secure software systems.

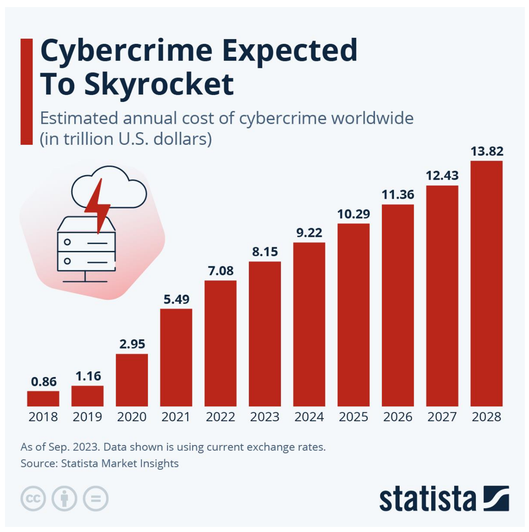


Figure 1. *Projected annual cost of cybercrime worldwide (in trillion U.S. dollars) Source: Statista [2] Market Insights, 2023*

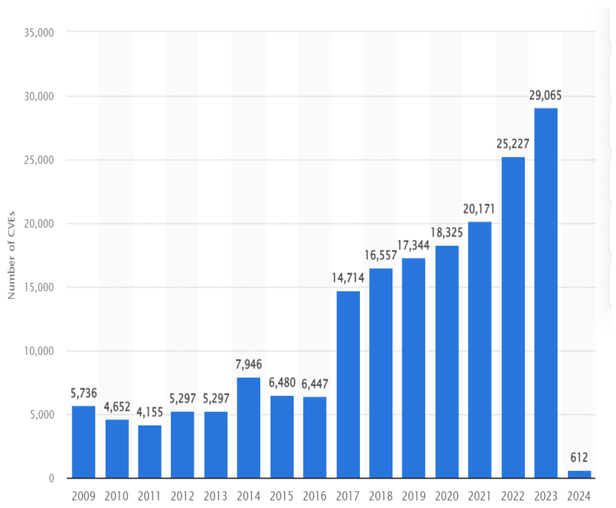


Figure 2. *Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD Source: Statista [2]*

KEY CHALLENGES

1. **Accuracy vs. Efficiency:** Existing methods struggle with balancing high precision and low false positives/negatives in AI-driven Software Vulnerability Detection (SVD) systems [1].
2. **Data Dependency:** Heavy reliance on large, labelled datasets limits scalability and adaptability in real-world scenarios.
3. **Hidden Vulnerabilities:** Many vulnerabilities are overlooked by developers but exploited by attackers, highlighting the need for more sophisticated detection mechanisms.
4. **Responsible AI:** Ensuring transparency, fairness, and bias reduction in AI models remains a complex challenge.
5. **Interpretability:** Making AI-driven SVDs explainable and traceable without compromising performance.

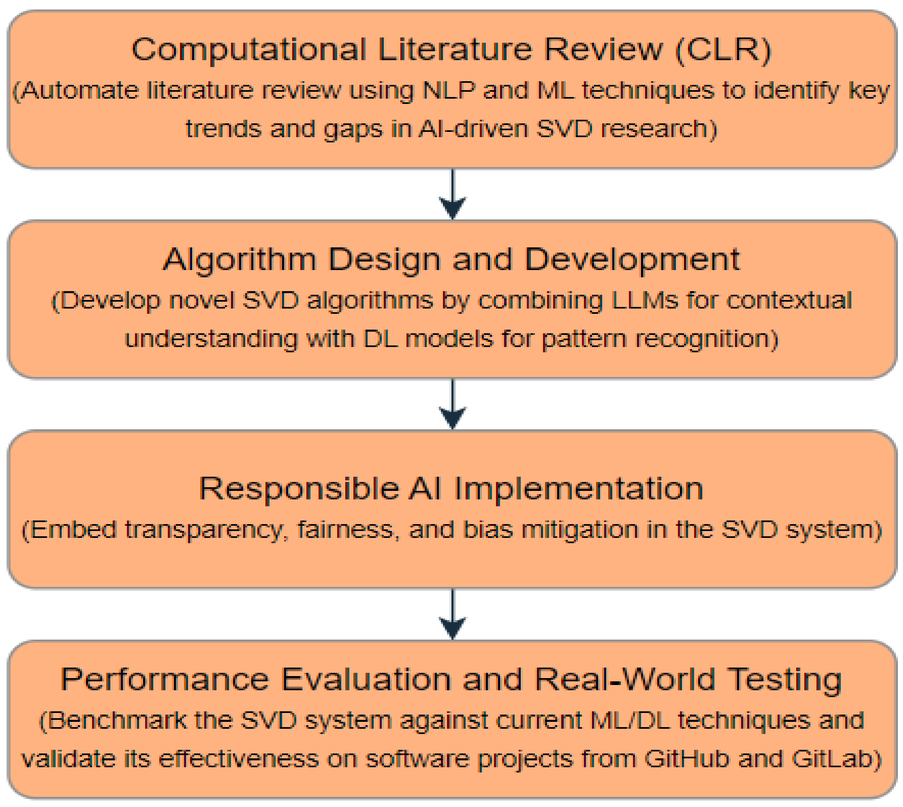
SUMMARY

This research aims to improve software vulnerability detection using AI and addresses critical research gaps in the field. By enhancing the integration of LLMs, ensuring responsible AI practices, and focusing on scalability and real-world applicability, this work sets new standards in software security and contributes to the ongoing fight against cybercrime.

OBJECTIVES

1. **Develop Advanced SVD Algorithms:** Integrate Large Language Models (LLMs) and Deep Learning (DL) to enhance SVD accuracy.
2. **Implement Responsible AI Practices:** Embed transparency, fairness, and bias reduction into SVD models.
3. **Evaluate System Performance:** Test the SVD system against existing ML and DL techniques using benchmarks and real-world datasets.
4. **Assess Real-World Effectiveness:** Validate the system on software projects from GitHub and GitLab for practical robustness.

METHODOLOGY



POTENTIAL IMPACT

1. **Enhanced Software Security:** Improved detection reduces vulnerabilities, boosting software reliability.
2. **Ethical AI Practices:** Setting new standards for fairness and accountability in software security.
3. **Broader Adoption:** Success could lead to widespread use of AI-based SVD tools in the industry
4. **Foundation for Innovation:** Establishing groundwork for future AI-driven cybersecurity advancements.

REFERENCES

[1] Tian, Z., Tian, B., Lv, J., Chen, Y., & Chen, L. (2024). Enhancing vulnerability detection via AST decomposition and neural sub-tree encoding. Expert Systems with Applications, 238, 121865.

[2] https://www.statista.com/

Contact information

Revathi Karri, Junior Researcher, LUT University
revathi.karri@lut.fi, +358504674262

Supervisors

1) Najmul Islam, Professor, LUT University, najmul.islam@lut.fi
2) Prabhat Kumar, Post-doctoral researcher, LUT University, prabhat.kumar@lut.fi