

CYBER SECURITY IN HEALTHCARE:

Utilizing Artificial Intelligence and Database Technology to Enhance Understanding of Cyberattacks

Authors

EMMANUEL Song Shombot
Gilles DUSSERRE
Robert BESTAK
Nasir Baba AHMED

Partners



Université de Nimes



PTDF Nigeria



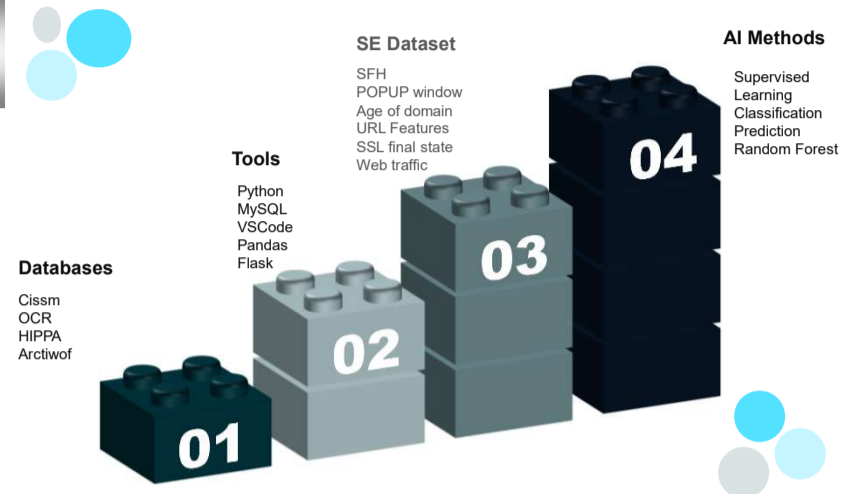
Campus France



Czech Technical University in Prague

BACKGROUND

- ▶ Over 500 healthcare companies reported a variety of cyber breaches that compelled a shutdown in operations.
- ▶ Hospital's sensitive services create obscurity in their cyber infrastructure, hindering security experts from assessing their actual cybersecurity needs.
- ▶ This work propose a comprehensive database that will provide a representation into existing threat landscape.



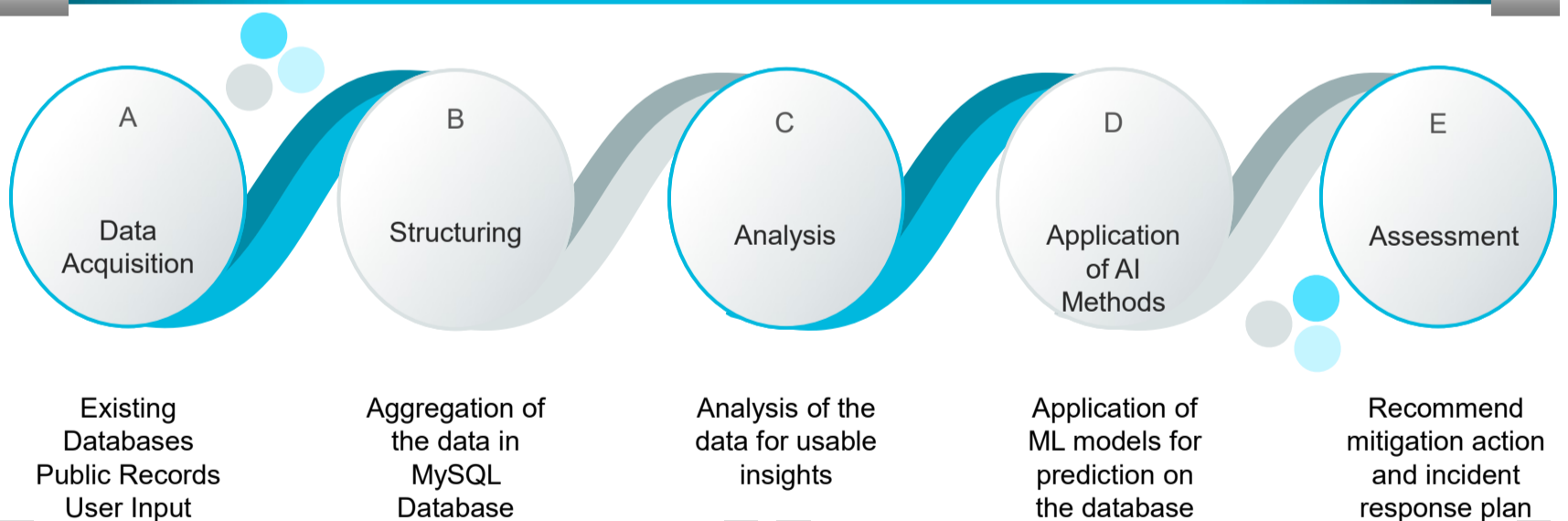
RESEARCH OBJECTIVES

- ✓ Review existing data sources of cyberattack in healthcare.
- ✓ Design a database of existing cyberattacks in healthcare.
- ✓ Use AI tools to analyze and build predictive models of cyberattack patterns.
- ✓ Evaluate the model to infer outcomes.

EXPECTED OUTCOMES

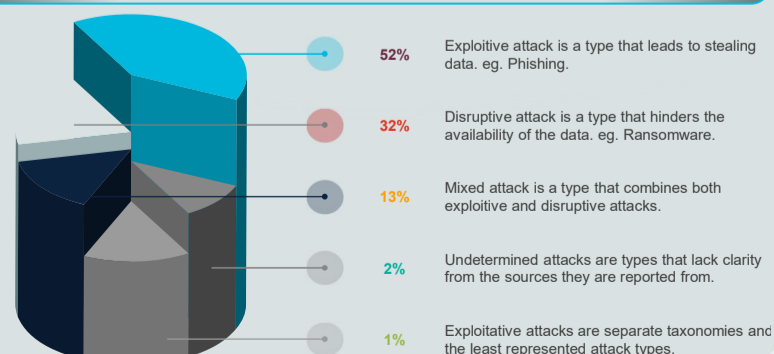
- 01 Comprehensive database that fairly represents the threat landscape of cyberattack in healthcare.
- 02 An interface that permits the continuous growth of the database based on new cyber attacks.
- 03 Real time visualization of the threat distribution based on predictive machine learning models.
- 04 A risk assessment plan for dealing with cyberattack of high prevalence.

METHODOLOGY



ANALYSIS OF EXISTING DATABASE (CISSM) -TYPE

The center for international and security studies at Maryland (CISSM) provides a database and, analysis into the database provides the statistics on cyberattack Types.



ANALYSIS OF EXISTING DATABASE (CISSM) - MOTIVE

Analysis of the motive of the threat actor based on the underlying published source material.

