

Cyber Security in Healthcare: Utilizing Artificial Intelligence and Database Technology to Enhance Understanding of Cyberattacks

Song Shombot Emmanuel, Gilles Dusserre, Robert Bestak, Nasir-Baba Ahmed

▶ To cite this version:

Song Shombot Emmanuel, Gilles Dusserre, Robert Bestak, Nasir-Baba Ahmed. Cyber Security in Healthcare: Utilizing Artificial Intelligence and Database Technology to Enhance Understanding of Cyberattacks. Colloque IMT 2023: "Sécurité et Résilience", Apr 2023, Palaiseau, France. 2023, 10.5281/zenodo.7937270. hal-04097931

HAL Id: hal-04097931 https://imt-mines-ales.hal.science/hal-04097931

Submitted on 15 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



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.

SE Dataset SFH POPUP window Age of domain URL Features SSL final state Web traffic Python MySQL VSCode Pandas Flask Cissm OCR HIPPA Arctiwof Al Methods Supervised Learning Classification Random Forest

RESEARCH OBJECTIVES

\bigcirc

Review existing data sources of cyberattack in healthcare.



Design a database of existing cyberattacks in



Use Al tools to analyze and build predictive models of cyberattack patterns.

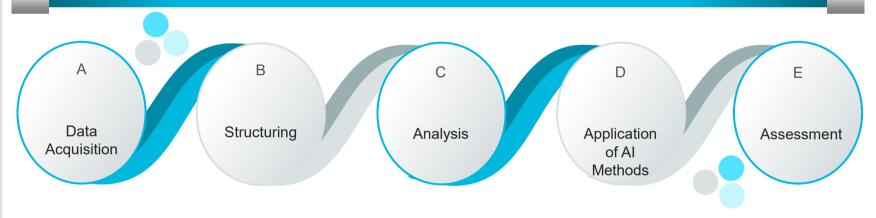


Evaluate the model to infer outcomes.

EXPECTED OUTCOMES

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

METHODOLOGY



Existing
Databases
Public Records
User Input

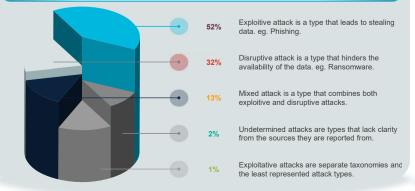
Aggregation of the data in MySQL Database Analysis of the data for usable insights

Application of ML models for prediction on the database

Recommend mitigation action and incident response plan

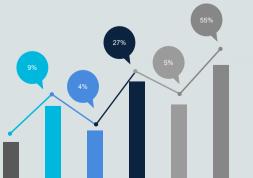
ANALYSIS OF EXISTING DATABASE (CISSM) -TYPE

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.

Financial
Monetary gains appears to be the likely motivation for cyberattacks.

Protest

statement or show disapproval.

Undetermined

When motivation is unclear from the

7% When motivation is unclear from the public records.

Others

Personal drive, sabotage and a breach of more than one motivation.

Espionage
Intent to uncover sensitive information.

Contact: emmanuel.song@mines-ales.fr