Scientific Research & Methodologies CSE 418

Research Proposal

Submitted To:

Md. Moradul Siddique
Lecturer
University of Information Technology & Sciences

Submitted By:

Group Name: **Innovators**

Name: Sadia Akter _ **Id:** 2125051059_7B1

Name: Israt Jahan Eva **_ Id:** 2125051057_7B1

Name: Irin Sultana Poly **_ Id:** 2125051091_7B2

Name: Asadur Rahman Asif _ **Id:** 2125051079_7B2

Title: Enhancement of Healthcare Security through Machine Learning Innovations.

Research proposal.

1. Introduction

Context & Motivation

Healthcare institutions deal with highly sensitive information and documents about patients and even their families: their medical history and insurance, and sometimes their financial records. Such systems, however, have become useful tools for criminals whose sole endeavor is to harvest and abuse such data. More and more attacks are being reported against healthcare institutions year after year and such information protection is no longer enough.

Machine learning (ML) is an application or form of artificial intelligence that empowers computers to carry out certain tasks or solve problems by looking at data rather than using specific instructions. To counter cyber-attacks in healthcare systems, it will be appropriate and informative to apply machine learning techniques to improve the health care security systems preventing any future cyber-attacks.

Proposal Summary

The aim of this research proposal is to enhance the security of the healthcare system through machine learning techniques. The objective is to develop a model that will be able to prevent threats from becoming a risk. Importantly, it allows for greater security of patient information and the healthcare system by use of machine learning in healthcare security.

Why?

The healthcare sector remains a rich target for cyber-attacks due to the highly sensitive nature of its data. A health care data breached can result in Identity theft, financial fraud and it could also lead to Medical Malpractice. They can also cause disruption to a healthcare services, which will have an impact on patient care.

Hacker's constantly changing tactics make them impossible to catch for traditional security systems. Machine learning aids by constantly updating its model for new threats, memorizing previous hacks and forecasting upcoming risks.

What?

This research will concentrate on securing the healthcare environment by employing machine learning. In particular, it will investigate:

- What machine learning methods are most effective in identifying and mitigating security threats?
- These measures in real healthcare systems
- In contrast, the only way to create a data lake of unlabeled student data would be through another program or hack — a very risky practice (for students as it means this is also how individual genetic privacy could be taken without healthcare and its complex data files too!).

Research Question(s)

1. The challenge becomes how can we apply machine learning to improve our present healthcare security systems (beyond the realm of academic exercises)?
2. What are the best machine learning models that can identify security threats in healthcare?
3. What are the challenges to add machine learning, and how do we solve it for health security?

Aims & Objectives

- **Analysis:** Review the current security deficiencies in healthcare systems and where areas need to be improved.

- **Identify (ID):** Discover which machine learning algorithms offer the best detection and prevention capabilities to counteract the same threats.
- **Design & Test:** Develop, design and paint a machine learning-based security model that can easily be implemented to secure patient data stored in healthcare systems.

2. Literature Review

Identify a Research Gap

While Machine Learning is already being used all over different sectors of the industry for security, there has yet to be as much research dedicated to how ML can be adapted to security in healthcare. However, there are very few research items that regularly address the problems of cyber security and healthcare while not exploring how machine learning may assist in this context.

Summarized Literature

Why?

Recent research concentrates either on machine learning without specific applications or employs traditional approaches in health-care security. Clearly, there is a gap in research combining both areas and the use of machine learning to directly address their specific security needs.

Who?

Key researchers and organizations in this space range from cyber security professionals, to healthcare data analysts, down to machine learning practitioners that are looking for innovative means of enhancing security throughout all sectors.

What?

Most of the literature highlights these key themes:

- That led to the vulnerabilities with healthcare systems towards cyber-attacks.
- Benefits of using other industry threat detection machine learning techniques (decision tree, neural networks, anomaly detection…)
- Security remains one of the biggest ethical fears; this is particularly sensitive in the realm of machine learning security solutions due to medical professionals needing data controlled even under the watchful human eye.

Literature on Topic

Hackers are increasingly targeting healthcare systems because they contain important and sensitive data. Many studies suggest that current security systems are insufficiently rapid to detect modern threats, making them reactive rather than proactive.

Literature on Method

Various machine learning models, such as neural networks and anomaly detection systems, have been used successfully to detect fraudulent activity in industries such as finance and retail. These methods may be applicable to healthcare, but the unique nature of healthcare data, including privacy concerns and complexity, necessitates careful attention.

Literature Synthesis

While machine learning has proven useful in other industries, little study has been conducted on how these models may be tailored to address the unique goals and challenges of healthcare. This study seeks to bridge that gap by investigating how machine learning might be used to improve the security of healthcare systems.

---

3. Methodology

Methods Selection

This study will combine qualitative and quantitative methodologies to investigate how machine learning may improve hospital security. It will entail studying real-world examples of healthcare security breaches and conducting interviews with cyber security professionals.

Research Design

How?

We will create a machine learning model that detects and prevents weaknesses in security in healthcare systems. This model will be tested on simulated healthcare data to ensure its ability to handle real-world conditions.

Data Collection

We will collect data using case studies of recent healthcare breaches, expert interviews, and actual healthcare datasets (simulated to secure genuine patient data). This will help us understand the specific security challenges that healthcare systems confront.

Data Analysis

The machine learning model will be determined depending on how well it detects threats and responds to them. The data will be analyzed using statistical methods to ensure that the model is reliable.

Ethics

The study will carefully follow to ethical rules to ensure patient privacy and confidentiality. To avoid any ethical issues about patient confidentiality, all data utilized will be made public or completely cleaned.

4. Plan & Timeline

Research Plan

- **Months 1-2**: Complete an in-depth review of existing literature to identify the major challenges in healthcare security. Document key findings and gaps in current knowledge.
- **Months 3-4**: Select and refine the most suitable machine learning algorithms for the project. Develop a clear plan for implementing these algorithms in the prototype.
- **Months 5**: Develop and test a prototype machine learning model using simulated healthcare data. Gather initial performance metrics and feedback.
- **Month 6**: Analyze the results of the prototype, refine the model based on performance and feedback, and finalize the research report.

Write-up Plan

- **Month 6**: Document the research findings, including detailed results and practical applications for healthcare security. Prepare a comprehensive report.

Milestones

- Completion of literature review.
- Development of a working prototype machine learning model.
- Final analysis and report writing.

Deliverables

- A comprehensive report detailing the challenges and potential solutions for improving healthcare security using machine learning.
- A prototype of the proposed machine learning model tested on simulated healthcare data.

5. Conclusion

Importance

The healthcare industry handles highly sensitive data, thus its security systems must be capable to stand up to increasingly complex attacks from hackers. Improving healthcare security is critical to ensuring that patients' personal and medical information remains secure.

What?

The goal of this study is to create a machine learning-based security system capable of identifying and avoiding cyber-attacks in healthcare systems, ensuring patient data protection and healthcare service reliability.

Why?

Machine learning can help us design better, faster, and more adaptive hospital security systems. This will not only protect sensitive data, but will also ensure that healthcare services continue to operate normally without the threat of cyber-attacks.

Contributions

This research will add to the developing subject of healthcare cyber security by offering a detailed review of how machine learning may be effectively employed to improve security. It will also provide a practical solution in the shape of a fully tested prototype model.

THE END