

ALUMNI SERIES

Security Hardening of Pharmacy Information System Against Machine Learning Attack

A pharmacy information system (PIS) is a specialised software application designed to support and manage the operations of a pharmacy or a pharmacy department within a healthcare organisation. It is a comprehensive solution that automates various tasks and processes involved in pharmacy management, including medication dispensing, inventory management, patient data management, billing and invoicing, and other administrative functions. The PIS streamlines pharmacy workflows, reduces medication errors, improves efficiency, and enhances patient safety. They play a vital role in supporting the day-to-day operations of pharmacies, ensuring accurate dispensing of medications, and maintaining proper medication management practises.

When it comes to securing a PIS against machine learning attacks, there are several steps that the users can take to enhance its security. Machine learning attacks typically involve exploiting vulnerabilities in the system to manipulate or compromise the machine learning models. Here are some security hardening measures for the users to consider:

1. Data Protection:

- Ensure that sensitive patient and prescription data is stored securely using strong encryption techniques.
- Implement access controls to restrict data access based on user roles and privileges.
- Regularly backup the data and store it securely to prevent data loss or corruption.

2. Secure Model Development:

- Follow secure coding practises when developing machine learning models to prevent common vulnerabilities such as injection attacks or buffer overflows.
- Regularly update and patch the machine learning frameworks and libraries to address any security vulnerabilities discovered.

3. Robust Model Training:

- Use quality, diverse, and representative data for training the machine learning models. This helps prevent biased models that could lead to discriminatory or unfair outcomes.
- Regularly retrain the models to incorporate new data and address concept drift, ensuring the models are up-to-date and accurate.

4. Adversarial Robustness:

- Consider implementing techniques to detect and defend against adversarial attacks, where an attacker intentionally manipulates inputs to deceive the machine learning models.
- Techniques like adversarial training, input sanitization, or anomaly detection can help improve the resilience of the models against such attacks.

5. Model Validation and Testing:

- Perform rigorous testing and validation of the models to ensure their effectiveness and security.
- Conduct penetration testing and vulnerability assessments to identify and address any weaknesses in the system.

6. Monitoring and Anomaly Detection:

- Implement monitoring and logging mechanisms to detect unusual or suspicious activities within the PIS.
- Utilise anomaly detection techniques to identify potential attacks or abnormalities in the system's behaviour.

7. User Authentication and Access Control:

- Enforce strong user authentication mechanisms, such as multi-factor authentication, to prevent unauthorised access.
- Implement role-based access controls to ensure that users only have access to the information and functionality they require.

8. Security Awareness and Training:

- Educate system users, administrators, and developers about machine learning security best practices, potential threats, and common attack vectors.
- Foster a culture of security awareness to ensure that everyone involved in the system understands their role in maintaining its security.

Remember that security is an ongoing process, and it is important to stay updated with the latest security practises, vulnerabilities, and defence techniques. Regularly review and update your security measures to address emerging threats and protect your PIS effectively.

Mr. Mohd Ghazali Ismail
RX2 Alumni



Issue 8/2023

August 2023

PRESCRIPTION



NEWSLETTER EDITORIAL TEAM

Editorial Advisor:

Prof. Dato' Dr. Abu Bakar Abdul Majeed

Authors:

Dr. Nurhuda Manshoor, Dr. Norkasih Ibrahim, Mdm Nor Zaleha Ishak, Mr Hizwan Nizam Abdul Rahman, Dr Fazleen Haslinda Mohd Hatta, Mr Muhammad 'Izzuddin Zamery, Dr Mohd Shahezwan Abd Wahab, Dr Nurul Izzati Osman, Mdm Syahida Fathiah Ahmad Kamal, Dr Hannis Fadzillah Mohsin, Dr. Aisyah Hasyila Jahidin, Dr Shubashini Gnanasan, Ms. Zakiah Mohd Noordin, Associate Prof. Dr. Mahmathi Karuppannan, Dr. Siti Azma Jusoh@Yusof, Dr. Gurmeet Kaur Surindar Singh, Mdm Nor Elyzatul Akma Hamdan, Mdm. Farhana Fakhira Ismail, Mr. Mohd Ghazali Ismail, Ms. Nik Aisyah Najwa Nik Mustaffa Shapri

Illustrator:

Mdm. Nurul Izzati Ismail

PRESCRIPTION

Faculty of Pharmacy,
Universiti Teknologi MARA,
Kampus Puncak Alam,
42300 Bandar Puncak Alam, Selangor.

 @pharmacyuitm



 @pharmacy_uitm




 Faculty of Pharmacy UiTM



 <https://pharmacy.uitm.edu.my/>



 +603-3258 4645

 korporatff@uitm.edu.my