CASE STUDY

AUTOMATING IDENTITY AND ACCESS MANAGEMENT (IAM)

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

PROJECT SNAPSHOT

The CSCRC is developing an automated intelligent support system for dynamic organisations whose employees' roles change frequently, allowing staff to effectively carry out their work, without compromising security. Identity and access management (IAM) is the task of accurately assigning and administering the required IT system access privileges and resource entitlements to employees within a business or organisation.

WHO'S INVOLVED

This project is funded by the CSCRC in collaboration with CSIRO's Data61 and National Australia Bank (NAB).

WHAT'S THE ISSUE?

In large modern enterprises, employees' business roles frequently change to meet the needs of emerging projects and opportunities and the restructuring of teams due to mergers and demergers. This makes it difficult for IT system administrators to keep up with user requirements to access relevant applications to perform their work, while also quickly revoking access when necessary to mitigate security threats. This project develops systems and techniques capable of detecting, predicting, recommending, and enforcing changes to employees' access privileges and entitlements. By broadening, limiting or adjusting access based on employees' changing business roles and job execution patterns, system security and productivity of employees is enhanced.

WHAT WERE THE OBJECTIVES?

This project employs advanced machine learning and data mining techniques to develop an automated support for IAM systems.

Automating the IAM process is beneficial to a modern organisation because it can:

- Reduce the time and effort needed by employees to apply for access privileges and resource entitlements and assess the applications
- Reduce the risk of security breaches in IT systems and inappropriate use of resources
- Improve user experience of IT systems and resources
- Improve overall productivity of employees

TECHNOLOGY DESCRIPTION

This project leverages deep learning, clustering and natural language processing techniques to identify and categorise different/similar business roles and their associated IT system access privileges and resource entitlements within an organisation.

By deploying process mining, time-series and sequential pattern mining techniques, it discovers the various business processes within an organisation and their associated access and resource requirement patterns.

It uses unsupervised/semi-supervised learning and generative predictive analytics to detect and predict user access and user behavioural changes within an IT system for dynamic access change recommendations. It also exploits adversarial machine learning and anomaly detection to identify suspicious, risky and anomalous user behaviours in an IT system.