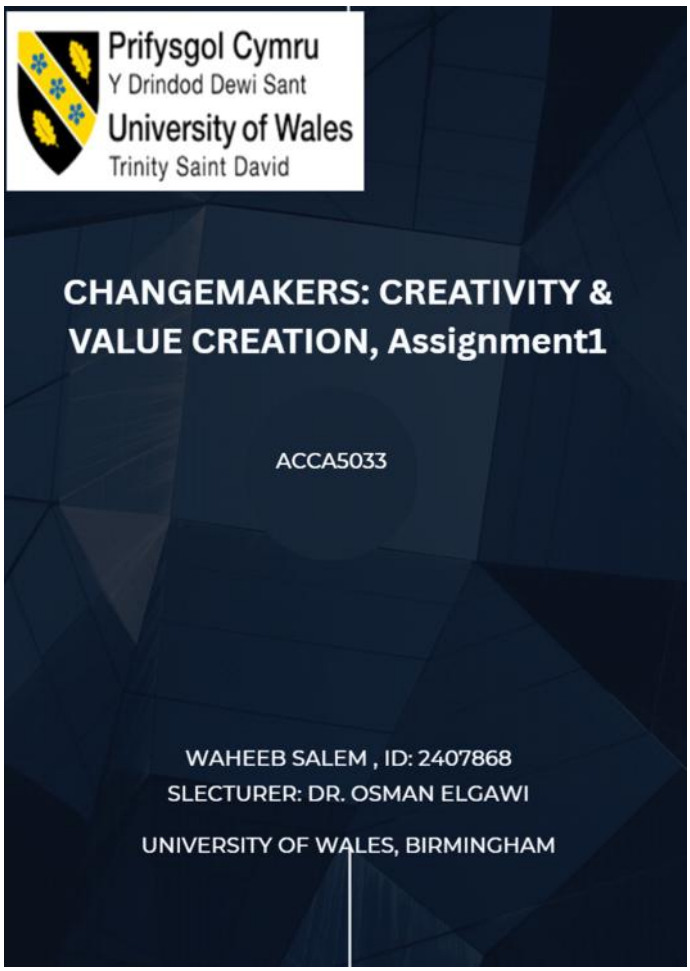
Changemakers: Creativity & Value Creation

Tuesday, February 10, 2026 2:42 PM



Submission Date : 01/03/2026

Contents

Tuesday, February 10, 2026 2:43 PM

Contents....2

Introduction....3

Task 1....4

The Art of the Possible: Ideation & Mind Map for PABW....4

The Mind map structure for PABW....5

Ideation: Selected Project Idea....6

Task 2: Aim & Objectives and Research area....7

Research Philosophy for PABW....9

Research Tools for PABW project....10

Task 3: Research Strategies....12

Appendices....14

References....15

Introduction

Sunday, February 22, 2026 10:01 PM

This work documents the development of a smart security system for bank computer networks. Banks today face constant danger from hackers trying to steal money and information. Thus, many small banks and corporations cannot afford expensive security systems, leaving them vulnerable to attacks. This project creates a simple, smart guard program that protects these banks using artificial intelligence (AI) and Python programming [1] [2].

The program, Python AI Bank Watchdog (PABW), acts like a digital security guard inside the bank's computer network. It simply learns what normal work looks like by watching employee logins, file access and network traffic for two weeks. Once it understands normal patterns, it can spot suspicious activity, such as strange login times or unauthorized file access and take immediate action.

This solution makes strong cybersecurity accessible to banks with limited budgets. By automatically detecting and stopping threats, it helps prevent financial losses and protects sensitive customer information from cyber criminals.

Task1: The Art of the Possible: Ideation & Mind Map for PABW

Tuesday, February 10, 2026 2:31 PM

This project explores **the art of the possible** by asking how existing technologies can be combined in new ways to solve real problems. The Python AI Bank Watchdog (PABW) concept emerges from this creative thinking, using accessible tools like Python and machine learning to address complex security challenges of insider threat detection in banks and other sensitive organisations.

Mind Map

Tuesday, February 10, 2026 2:33 PM

The Mind map structure for PABW

The Python AI Bank Watchdog mind map is organized into several key branches, each exploring a different aspect of the project. One important branch focuses specifically on the benefits that system would bring to financial institutions. This section highlights how the PABW can improve security, reduce costs and build trust customers.

Mind map is produced by www.mindmiester.com

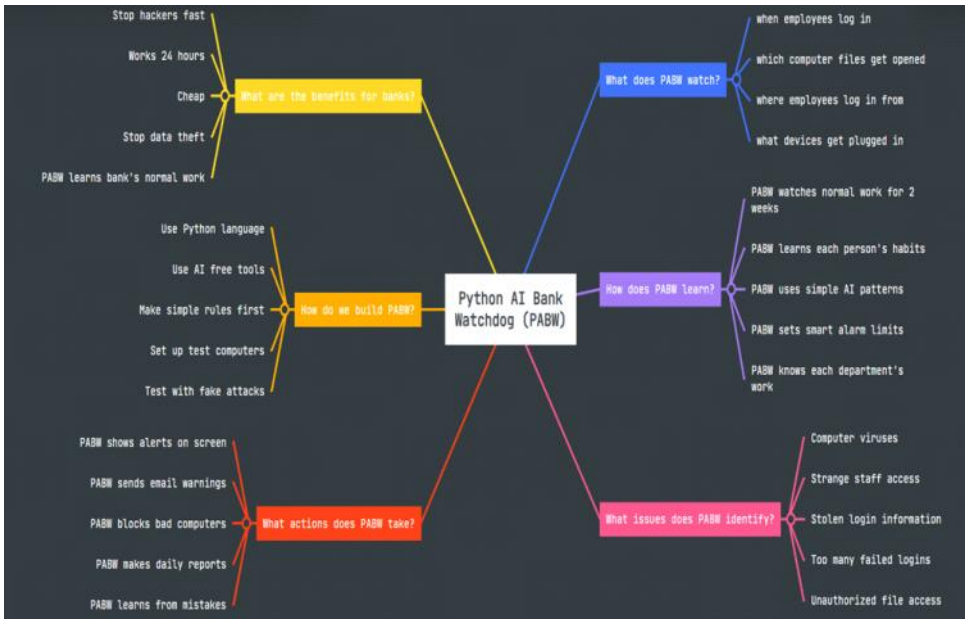


Figure 1: Python AI Bank Watchdog (PABW) Mind map

Ideation: Selected Project Idea

Tuesday, February 10, 2026 2:44 PM

Figure 2: Project idea

The idea has been chosen to develop the AI Employee Behaviour Watchdog for Banks (shown in Mind Map figure 1). This project will create a smart computer program that protects banks or businesses for corporations from insider threats and stolen logins. The system uses artificial intelligence to learn how each employee normally works, then spots unusual behaviour that could mean a security problem.

This idea was selected because it solves a real problem for smaller business such as small banks and dental surgeries. Many community banks and credit unions cannot afford expensive security systems. They need simple, effective protection against employees who might do harmful things or hackers using stolen passwords. Online security resources show that insider threats cause significant financial losses for financial institutions every year [3].

The project focuses on watching employee computer activities like login times, files accessed, and network connections. The AI learns what is normal for each person during a training period. After learning, it can detect strange actions such as an accountant accessing secret customer files at midnight, or someone downloading hundreds of files quickly. The system will alert security staff and can automatically block suspicious activities.

This idea explores how Python-based detection can improve bank security [4]. It also offers a valuable solution for financial institutions with limited resources.

Task 2 : Aim , Objectives and Research Area

Tuesday, February 10, 2026 2:46 PM

PABW Aim

This research aims to design and develop an AI-based employee behaviour monitoring system that can automatically detect and respond to insider threats within bank computer networks. The project is motivated by the escalating financial impact of such threats, as the global average annual cost of insider incidents reaches $ 17.4 million in 2025 [5].

PABW Objectives

Sunday, February 22, 2026 10:15 PM

Figure 2: Five SMART Objectives for Success

The five original objectives for the Python AI Bank Watchdog (PABW) project are reframed as SMART goals, a method for making objectives clear and trackable [6].

First Objective

To analyse cybersecurity challenges by identifying three specific weaknesses in current protection methods for small banks through a literature review, to be completed by the end of the project's first month.

Second Objective

To develop a Python AI tool that learns user login and file access patterns, achieving a test accuracy rate of 90% in identifying simulated security threats, with a functional prototype ready by the end of the third month.

Third Objective

To create an alert system with a dashboard that displays real-time security warnings, ensuring the system shows an alert within five seconds of a threat being detected, to be implemented by the end of the fourth month.

Fourth Objective

To test the system in a virtual bank environment, successfully detecting 95% of pre-programmed insider threat scenarios during a two-week evaluation period in the project's fifth month.

Fifth Objective

To evaluate the AI solution by producing a final report that compares its potential cost to two commercial alternatives, demonstrating how it could reduce security expenses for smaller banks, for submission by the end of the sixth month. This process of setting measurable goals supports successful project and career planning [7].

Research Philosophy

Sunday, February 22, 2026 10:23 PM

Research Philosophy for PABW

There are many research philosophies applicable for the Python AI Bank Watchdog (PABW) project, but the suitable and appropriate one is pragmatism. This practical philosophy prioritizes actionable results and solving real-world problems over abstract theory. It strongly supports the use of mixed methods, which is essential for this research [8]. The project will use a mixed-methods approach. This includes training machine learning models on user behaviour data and evaluation system usability for security staff. The main measure for success in pragmatism is whether the solution works effectively. This makes it the ideal foundation for developing and testing a functional AI tool designed to detect insider threats in a simulated banking environment [8].

Research Tools

Sunday, February 22, 2026 10:24 PM

Research Tools for PABW project

This report identifies two free research tools for the Python AI Bank Watchdog (PABW) project: UWTSD Library Search and Google Scholar.

The UWTSD Library Search provides access to university databases and student projects, which is useful for targeted, academic sources [9]. Effective searches for PABW are built using Boolean operators (AND, OR). Suitable search terms include "insider threat detection", "anomaly detection", banking, and security. An example search query is: ("insider threat" OR "anomaly detection") AND banking AND security. This string is entered into the library's search bar.

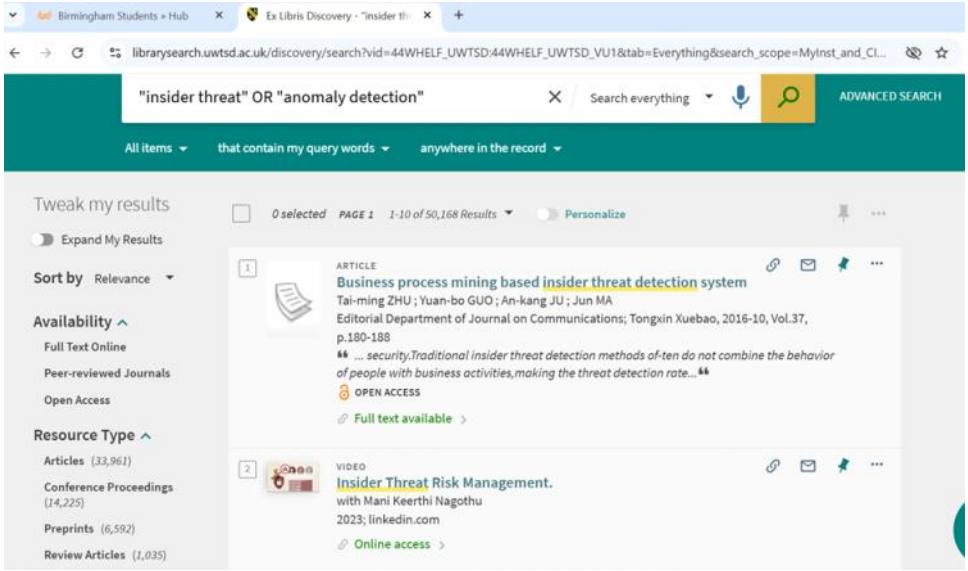


Figure 3:UWTSD Library Search

The Google Scholar tool searches a wide range of scholarly literature [10]. For PABW research, key search phrases are used, such as "machine learning for banking security" and "AI insider threat detection". An example of a professional search string is: "insider threat detection" AND ("machine learning" OR AI) AND bank. Quotation marks are used to find exact phrases like "user behaviour analytics".

Figure 4: Google Scholar Search

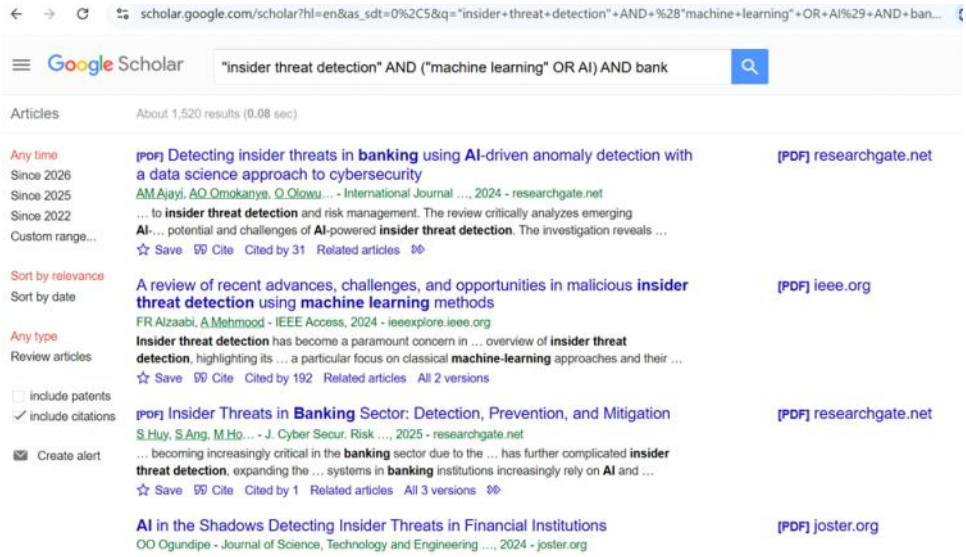


Figure 5: Google Scholar Academic Search

Research Strategies

Thursday, February 12, 2026 3:58 PM

For Python AI Bank Watchdog (PABW) project, robust research strategies are necessary to establish the system's validity, reliability, generalisability and ethical considerations.
To establish **validity**, the AI model should be evaluated using explainable AI methods. These techniques, such as creating clear decision explanations, help clarify why a specific user behaviour was flagged as a threat [11]. This makes it possible to confirm that the system detects actual risks, not accidental findings.

Reliability is achieved through consistent performance testing. The model is tested under difficult conditions by using data that has been alerted in small ways [11]. This process checks whether the system still performs well when data changes in normal ways or when someone tries to trick it.

For **generalisability**, the AI should be trained on diverse datasets. This means using data from various sources or departments to prevent the model from becoming too specialized. Training on varied information helps ensure the system can perform effectively in new, unseen environments, such as different bank branches [12].

Ethical considerations are critical when monitoring employee behaviour. Key principles include implementing strong data anonymization to protect individual privacy, actively auditing the AI for potential biases that could lead to unfair targeting, and ensuring the system operates with clear human oversight [13].
For the PABW system, a systematic review of existing literature serves as the primary data collection method. This involves searching databases like Google Scholar [10] and the UWTSD online library [9] to find academic papers and case studies on AI for bank security and insider threat detection.

Pilot Data Collection Method
A pilot study involves testing this search and review process on a small scale [14]. A sample of ten relevant publications is identified using targeted search terms. Key information such as the AI techniques used, reported accuracy, and types of threats detected is systematically extracted into a table.

Feedback for Project Focus
The pilot results are analysed. For example, if the pilot reveals extensive research on certain AI models but very little on others, the final project's focus can be refined accordingly. This feedback ensures the project direction is well-supported by available academic evidence.

Various analysis methods are applicable to evaluate the Python AI Bank Watchdog (PABW) system.
Quantitative Analysis
Quantitative Analysis examines numerical data to find patterns and test hypotheses, providing objective evidence of system performance. Descriptive statistics are used to summarize and describe data features, such as calculating the average number of security alerts the PABW system generates per day [15]. Inferential statistics allow for drawing conclusions about larger populations from sample data; a technique like a t-test could

determine if the PABW system detects threats significantly faster than a traditional method [15].

Qualitative Analysis

Qualitative Analysis interprets non-numerical data like text or interview responses, which is essential for understanding user experience and practical challenges. Thematic analysis is a foundational method for identifying, analysing, and reporting patterns (themes) within this data [16]. This method could be applied to categorize feedback from bank security officers on the PABW system's usability. The core activity is coding data to discover recurring themes [16].

Appendices

Thursday, February 12, 2026 3:22 PM

Poster

Figure 6: PABW Academic Poster

Poster link:

https://uowtsd-my.sharepoint.com/:i:/g/personal/2407868_student_uwtsd_ac_uk/IQB1KamXXiDZRagdr57GXcgoAfaV5qhgROvWJo2wMalH_kc?e=oZvbx7

E-portfolio link:
https://sites.google.com/view/waheeb-salem-eportfolio-l5/home

References

Thursday, February 12, 2026 3:58 PM

[1] CISA, “Cybersecurity and Infrastructure Security Agency,” , Cyber Essentials Toolkit, U.S. Department of Homeland Security, 2023. [Online]. Available: https://www.cisa.gov/cyber-essentials . [Accessed 25 Jan 2026].

[2]GeeksforGeeks, '' Intrusion Detection System (IDS),” GeeksforGeeks, 2025. [Online]. Available: https://www.geeksforgeeks.org/intrusion-detection-system-ids/ . [Accessed 26 Jan 2026].

[3] IBM Technology,“What is Cybersecurity?,” YouTube, 7 July 2022. [Online]. Available: What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn . [Accessed 27 Jan 2026].

[4]Programming with Mosh "Python Machine Learning Tutorial (Data Science),” YouTube, 17 Oct 2022. [Online]. Available: Python Machine Learning Tutorial (Data Science) . [Accessed 31 Jan 2026].

[5] Ponemon Institute , 2025 Cost of Insider Threats Global Report, Traverse City, MI, USA: Ponemon Institute , 2025. [Online]. Available: https://ponemon.dtexsystems.com/ [Accessed 1 Feb 2026].

[6]B. Isom “Setting and Pursuing SMART Goals: Your 5-and 10-Year Plan” New York , NY , USA : Springer , 2024 ,pp.647-651.

[7]C. N. Fuhrmann, J. A. Hobin, P. S. Clifford, and B. Lindstaedt, “Goal-setting strategies for scientific and career success,” Science, 2013. [Online]. Available: http://sciencecareers.sciencemag.org/career_magazine/previous_issues/articles/2013_12_03/caredit.a1300263, [Accessed 2 Feb 2026].

[8] A. Allemang, K. Sitter, and G. Dimitropoulos, "Pragmatism as a paradigm for patient-oriented research," Health Expectations, Wiley Online Library 2022 ,vol. 25, no. 1, pp. 38–47.

[9]University of Wales Trinity Saint David, "Library and Learning Resources," 2024. [Online]. Available: https://www.uwtsd.ac.uk/library/, [Accessed 2 Feb 2026].

[10]Google Scholar, "About Google Scholar," 2025. [Online]. Available: https://scholar.google.com/intl/en/scholar/about.html, [Accessed 2 Feb 2026].

[11]IBM , "What is Explainable AI (XAI)?,"2024 [Online]. Available : https://www.ibm.com/topics/explainable-ai . [Accessed 3 Feb 2026].

[12]X.Zang, H. Wang , Y. A, Hseih, Z. Yang, A.Yezzi , and Y. C Tsai, "Deep Learning for Crack Detection: A Review of Learning Paradigms, Generalizability, and Datasets,"University of Wales Trinity Saint David: Library and Learning Resources,2025 [Online]. Available: https://librarysearch.uwtsd.ac.uk/discovery/fulldisplay?docid=cdi_arxiv_primary_2508_10256&context=PC&vid=44WHELF_UWTSD:44WHELF_UWTSD_VU1&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=Everything&query=any,contains,Datasets%20on%20Generalizability%20of%20Deep%20Learning%20Models%20for%20Early%20Detection%20of%20Adverse%20Events&offset=0 . [Accessed 3 Feb 2026].

[13] Finansforbundet, "Financial sector employees are being monitored: three examples from the sector," May 2025. [Online]. Available: https://finansforbundet.dk/en/news/2025/financial-sector-employees-are-being-monitored-three-examples-from-the-sector/ . [Accessed 3 Feb 2026].

[14] MIM Technovate, “Pilot Study in Research”, YouTube, May 8, 2024 [Online]. Available: Pilot Study in Research . [Accessed 6 Feb 2026].

[15] A. Field, Discovering Statistics Using IBM SPSS Statistics, 5th ed. London, U.K.: Sage,

2017.
[16] V. Braun and V. Clarke, "Using thematic analysis in psychology," Qual. Res. Psychol., vol. 3, no. 2, pp. 77–101, 2006.