Deep Science Publishing
https://doi.org/10.70593/978-93-49307-51-3_1

Chapter 1

Background study of Identity and Access Management (IAM)

Esther Chinwe Eze

University of North Texas, United States

1.0 Introduction

This chapter recounts an overview of the project, with the aim and objectives. It presents a summary of the project investigation report as well as an overall structure of the entire report.

1.1 Overview

In today's ever-evolving business environment, businesses have become global, highly interconnected, and completely dependent on the internet, and with this, the probability of organizations becoming victims of data breaches or various cyber-attacks and threats is increasingly high. As the use of the Internet increases, the number of users who use the Internet and access the information using the Internet within or outside the organization also increases, hence the implementation of Identity and Access Management (IAM). This has made IAM an important area of technology. The concept of IAM is simply the process of managing who has access to a piece of information and what information. The key activities involved in IAM include creating identities for users and systems. Identity and Access Management (IAM) holds a crucial foundation for business benefits in terms of saving cost, management control, productivity in the operation of a business, and most especially, improving business growth for e-commerce purposes (Mayuri & Sridevi, 2017).

However, given the growing demands for data and information, IAM technology is confronted by increasingly diversified threats and attacks. With this situation, security has become particularly essential because of the issues of attacks on IAM. Deciding who should get access to whatever information is a matter of difficulty for many organizations

and businesses which leaves vulnerabilities in their system. As of now, businesses and corporate companies of various sizes are beginning to utilize and understand the need for implementing an IAM framework. Over the years, business leaders and more especially the IT department in several organizations have been placed under increased regulatory and organizational pressure to make sure that corporate resources are protected by way of controlling access to corporate resources and tracking user privileges (Phil & Gittlen, 2020). As a result of this, corporate businesses can no longer rely on manual and error-prone processes to assign and track user access to resources hence the adoption of IAM. IAM helps automate access control and auditing of corporate resources (Phil & Gittlen, 2020). While the implementation of IAM systems has provided organizations with the appropriate level of security through the use of policies, authentication, validation, and privileges within and outside organizations, the emergence of innovative and sophisticated threats and attacks in recent times has sparked up concerns that question the efficiency of IAM in terms of security. Thus, the risk of attacks posed on IAM is significantly higher than before.

This implies that the implementation of IAM alone is not enough, therefore, proper IAM implementation is necessary to tackle security challenges. Proper IAM implementation, however, requires more than just human work and that is why many organizations are turning to Artificial Intelligence (AI) and Machine Learning (ML) to help implement a proper and well-secured IAM. Utilizing AI and ML capabilities enhances the efficiency of IAM. This project focuses on implementing a Machine Learning algorithm with IAM to help detect IAM attacks.

1.2 Motivation

The growing volume and range of new IAM attacks pose a major challenge to protect. This research is focused on implementing a Machine Learning algorithm that helps in detecting Identity and Access Management (IAM) attacks.

1.3 Problem Overview

In our rapidly evolving world, organizations encounter significant obstacles in protecting information and infrastructure while maintaining smooth user access through Identity and Access Management (IAM). The management of numerous identity sources and inadequate authentication systems creates security vulnerabilities while complicating regulatory compliance efforts. Nowadays, hackers have launched more sophisticated techniques and methods for attacks on IAM systems which has resulted in several reoccurrences of breaches. Research shows that over 80 percent

of breaches happen as a result of weak or stolen credentials. Although many businesses try to incorporate new IAM security methods sadly, many of these approaches still fall short due to many reasons (reliance on outdated technologies being the most). The fact remains that no business is immune to attacks therefore, the solution would be the continuous effort of updating and improving these security technologies. In recent years, Machine Learning (ML) has made a tremendous impact in fraud detection, image recognition, and many others, many researchers have also been able to incorporate ML technology for security purposes in the field of attack detection. Machine Learning (ML) technologies are effective in distinguishing normal behavior patterns from malicious anomalies, this provides a more intelligent solution for access control. This comes down to the fact that there is an urgency for IAM systems to expand and align with organizational development while taking advantage of and incorporating new technologies like Artificial Intelligence (AI). Similarly, we see that strict access controls can contribute to hindering user experience and productivity. Ultimately, organizations must seek to implement a strong IAM framework that effectively balances security measures with compliance requirements and user accessibility (Aboukadri et al., 2024). Even though its application is still in the early stages, AI-driven authentication and adaptive access controls are considered to boost security without sacrificing efficiency.

1.4 Aim and Objectives

Aim

This project aims to utilize ML capabilities in the Identity and access management process to make it more efficient, and resilient to IAM attacks.

Objectives

- Review various types of attacks targeted against IAM.
- Review existing Machine Learning (ML) approaches, techniques, and tools in IAM attack detection.
- Collect data by Setting up a testbed that mimics normal and malicious activities.
- Use data to train machine learning algorithms that distinguish normal activities from malicious activities.
- Select the best Machine Learning (ML) algorithm that predicts normal from malicious activities.

1.5 Project Specification

This section of the project outlines the requirements of the project including the functional and non-functional requirements.

1.5.1 Functional Requirements

The functional requirements describe what exactly the proposed system should do. The list below shows the expected functionalities and features of the proposed IAM attack detection model. The functional requirement is prioritized using the MOSCOW method.

S/N	REQUIREMENT DECLARATION	PRIORITIZATION
1	The model must be able to detect IAM attacks.	Must
2	The model should be able to detect attacks based on the input dataset.	Should
3	Achieve an accuracy above 75% in the testing phase	Should

Table 1: Functional requirement

1.5.2 Non-Functional Requirements

The non-functional requirement of the proposed model describes how it should work and behave. This is also prioritized using the MOSCOW method.

S/NO	REQUIREMENT	DESCRIPTION	PRIORITISATION
1	Reproducible	The result and code should be reproducible and accessible for reproducing the result. Therefore, the code will be written in Python to ensure that it can be reusable.	Should
2	Adaptability	The proposed detection model should be able to adjust to modifications in terms of features.	Should
3	Security Necessities	The model should be able to detect unauthorized access	Must

4	Compatibility	It should be compatible with either desktop or laptop Windows operating system.	Should
5	Performance	The system should work as expected.	Must
6	Efficiency	The output is required to be more accurate and should have a low false-positive (FP) rate.	Should

Table 2: Non-functional requirements

1.6 Report Structure

The rest of the report is structured as follows:

Chapter 2 – Systematic Review

This section presents a critical analysis of existing research, summarizing findings, identifying gaps, and providing context for new studies.

Chapter 3 - System Design

This section presents a detailed description of all the design considerations of this project, with the justification of the choices of the design and development tools. The IAM dataset, the cleaning, and processing techniques were also presented.

Chapter 4 – Evaluation and Performance Analysis

This section deals with the description of how the functionalities of the system were implemented following the design and architecture of the approach. The testing and evaluation processes performed on the ML algorithms to determine the efficiency, accuracy, and usability of the selected algorithm are also included in this section.

Chapter 5 – Conclusion and Future Direction

This section provides a conclusion for the project. It summarises the overall findings of the project as well as the achievements, lessons learned, and recommendations for possible future research work in this area.