Provisioning and De-provisioning for Identity Management in Cloud Computing from Service Provider's Perspective Using Blockchain and Machine Learning.

Amey Bhilegaonkar
Arizona State University
abhilega@asu.edu (1225368924)
Tempe USA

November 14, 2022

Abstract

Identity management, usually referred to as identity and access management, is a set of regulations and tools to guarantee that only authorized people have access to technological resources. In this project, from the service provider perspective, we will focus on security issues related to Identity management in provisioning and de-provisioning for Identity Management from the service providers view This report contains my contributions to the project which includes Leveraging Machine Learning Research , Research on Identity Management with Machine Learning, Research on Identifying Fraud Detection Using ML, Research on Machine Learning Methods for Provisioning And Deprovisioning In IAM. Additionally, I have discussed AWS Fraud detection method to analyze and mitigate the issues such as, Online Identity Fraud, Identity theft.

1 Overview

Identity management, often known as identity and access management, is a system of rules and instruments to ensure that only those with the proper authorization can access technological resources. A system to create and manage public key infrastructure (PKI) certificates, a provisioning framework, a directory integration platform, a system to store and manage user information, a run-time model for user authentication, and a delegated administration model are some of the components of an identity management system.

Manual and automated provisioning and deprovisioning are the two main types of provisioning and deprovisioning. There is ad hoc manual provisioning. HR submits a request to IT, typically via email or through the helpdesk. An IT specialist then manually grants the required permissions. An entitlement is any internally managed IT resource, such as group memberships, file sharing, network folders, directory accounts, email addresses, and software licensing.

Manual provisioning's drawbacks include laborious and expensive compliance requirements, employee productivity being hindered, phantom accounts exceeding license costs. By ensuring that employees only have access to the apps they require, automated user provisioning keeps your company secure. The development of a successful IAM strategy requires the use of machine learning technology, which can also help to avoid many troublesome situations. Going Beyond Compliance, Precise Access Control, Breach Detection and Prevention, Automation and Flexibility, Increased Visibility, and Advanced Analytics are all supported by it.

Amazon Fraud Detector is a fully managed

service enabling customers to identify potentially fraudulent activities and catch more online fraud faster. Applications ranges from Identity Fraud, Payment frauds. Amazon Fraud Detector automatically trains, tests, and deploys custom fraud detection machine learning models based on your historical fraud data, with no ML experience required. For those who want to want to add own models, that utility is also provided using Sagemaker. With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. Amazon Fraud Detector supports specific actions, resources, and condition keys with which we can specifically defined who can have what access and to what resource.

2 CONTRIBUTIONS

Throughout the project, I worked on many sub-topics under IAM to improve security. My findings are detailed below.

AWS Fraud detection

Identity is the key concept to keep in mind when discussing identity theft. Identity theft is when a thief uses a victim's personal information, like their social security number or banking information, to masquerade as them in order to conduct fraud. Instances when a loan is formed in the person's name, a false tax return is submitted to the IRS, or a credit card is opened without the person's knowledge all fall under this category. Even though fraud is the outcome of identity theft, there is a significant distinction in this case regarding the effects on the victim. The harm to the victim of identity theft is more serious. It may take months or years to repair the harm the fraudster caused, which will have a significant negative impact on credit ratings.

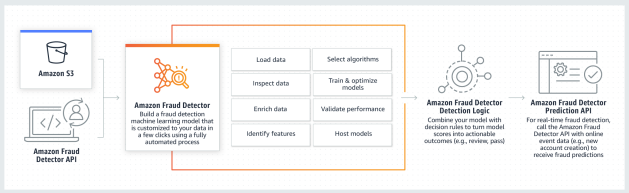
What's the solution?

Amazon Fraud Detector is a fully managed service that makes it easy to identify potentially fraudulent online activities such as online payment fraud and fake account creation. Amazon Fraud Detector uses machine learning (ML) and 20 years of fraud detection expertise from Amazon Web Services (AWS) and Amazon.com to automatically identify potential fraudulent activity in milliseconds. Some of more examples where Amazon Fraud Detection can be used:

1. New account fraud, within an account sign-up process
2. Online identity fraud
3. Payment fraud for online orders
4. Guest checkout fraud
5. Loyalty account protection

Amazon Fraud Detector automatically trains, tests, and deploys custom fraud detection machine learning models based on your historical fraud data, with no ML experience required. For developers with more machine learning experience, you can add your own models to Amazon Fraud Detector using Amazon SageMaker.

How does AWS Fraud Detector Works?



1. First, you define the event you want to assess for fraud.
2. Next, you upload your historical event dataset to Amazon Simple Storage Service (Amazon S3) and select a fraud detection model type, which specifies a combination of features and algorithms optimized to detect a specific form of fraud.
3. The service then automatically trains, tests, and deploys a customized fraud detection model based on your unique information.

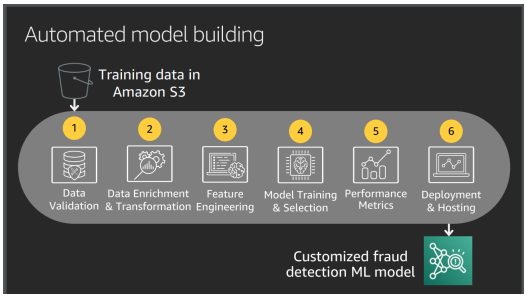
4. During this process, you can boost your model performance with a series of models pre-trained on fraud patterns based on AWS and Amazon's own fraud expertise.

5. The model's output is a score ranging from 0 to 1,000 that predicts the likelihood of fraud risk. At the final stage of the process, you set up decision logic (e.g. rules) to interpret your model's score and assign outcomes such as passing or sending transactions to a human investigator for review.

6. After this framework is created, you can integrate the Amazon Fraud Detector API into you website's transactional functions, such as account sign-up or order checkout.

7. Amazon Fraud Detector will process these activities in real time and provide fraud predictions in milliseconds to help you adjust your end-user experience.

Steps for Automated Model building



1. Data Validation

2. Data Enrichment and Transformation

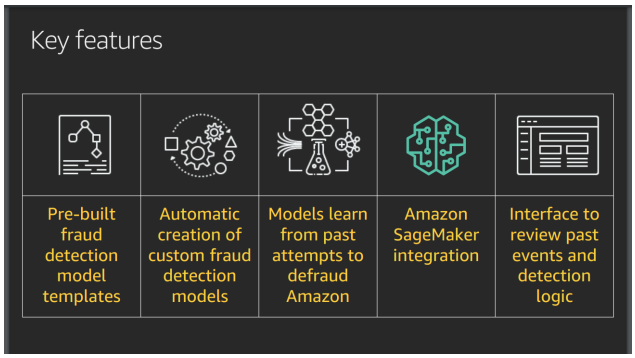
3. Feature Engineering

4. Model training and Selection

5. Performance Metrics

6. Deployment and Hosting

Key Features of AWS Fraud Detector



1. Pre-built Fraud detection model templates

2. Automatic Creation of Custom Fraud detection

3. Models learn from past attempts to defraud Amazon

4. Amazon SageMaker Integration

5. Interface to review past events and detection logic.

3 Lessons Learned

When I read the literature on the aforementioned subjects for the project, I picked up a lot of valuable lessons. I gained knowledge about the practical applications of machine learning in the field of cyber security. I learned how block-chain and Machine learning can be utilized to improve and mitigate issues related too security and Identity Management. I learned about the numerous ways machine learning can be utilized to improve security and detect threats. It provided me with a couple ideas to apply and consider for future development.

I learned how businesses are utilizing the power of AWS Fraud detection to save billions of dollars. Tens of billions of dollars are wasted on internet fraud globally each year. In the past, businesses relied on rule-based fraud detection programs, which aren't precise enough and can't keep up with fraudsters' evolving habits. Companies may proactively and more precisely identify and stop online fraud with the help of

AWS Fraud Detection machine learning technologies. While adjusting to shifting threat patterns, these solutions will aid in lowering revenue losses, preventing brand damage, and delivering a friction-less online consumer experience.

With Amazon's Fraud Detection Machine Learning solutions, customers can instantly apply containment or remediation measures intended to block or deny fraudsters and expedite low-risk activity to improve customer experiences for legitimate customers. These solutions score the risk of an event in real-time. Amazon's Fraud Detection ML Solutions enable individuals who aren't machine learning experts but are familiar with fraud issues to participate in constructing and updating highly accurate models by automatically managing the complicated activities necessary to train, optimize, and deploy a fraud detection model.

After going through, the working of cloud based methods to improve security and mitigate attacks related to user provisioning and deprovisioing. I also learned the importance of user provisioning and de-provisioning. How the concept of Granular Access is so important from the perspective of companies. Overall, I expanded and sharpened my edges for knowledge base in cyber-security and Identity Access Management areas.

4 References

The following lists the references and technical materials.

1 S. Chaisiri, B. S. Lee and D. Niyato, "Optimization of resource provisioning cost in cloud computing", IEEE TSC, vol. 5, no. 2, 2012.

2 Becker, M., Drew, M. "Overcoming the challenges in deploying user provisioning/identity access management backbone". BT Technol J 23, 71–79 (2005). https://doi.org/10.1007/s10550-006-0009-x

3 S. Ostermann, R. Prodan and T. Fahringer, "Dynamic cloud provisioning for scientific grid workflows", GRID 2010, 2010.

Websites

(a) How Amazon Fraud Detector works with IAM

(b) Build a fraud detection system with Amazon SageMaker

(c) Amazon Fraud detection Block Diagram

(d) How Amazon Fraud Detector Works

(e) What is Amazon Fraud Detector

(f) What is user provisioning and Deprovisioning?

(g) Provisioning and Deprovisioning of cloud resources block diagram