National College of Ireland

Real-Time AI-Powered Anomaly Detection in Financial Transactions Using Microsoft Fabric and Power BI

MSc Research Project
Data Analytics

Pranav Dinesh Ahire
Student ID: x23302372

School of Computing
National College of Ireland

Supervisor: Qurrat UI Ain

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Pranav Dinesh Ahire
Student ID:	x23302372
Programme:	Data Analytics
Year:	2025
Module:	MSc Research Project
Supervisor:	Qurrat UI Ain
Submission Due Date:	11/08/2025
Project Title:	Real-Time AI-Powered Anomaly Detection in Financial Transactions Using Microsoft Fabric and Power BI
Word Count:	5521
Page Count:	21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	14th September 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Real-Time AI-Powered Anomaly Detection in Financial Transactions Using Microsoft Fabric and Power BI

Pranav Dinesh Ahire
x23302372

Abstract

The high influx of digital activities in transactions has contributed to a significant increase in the risk and sophistication of financial fraud that has become a real challenge to the financial institutions that apply traditional rule-based detection methods. Such legacy models usually yield too many false positives, and are not real-time responsive. This study fills these gaps with designing and deploying actual real time AI powered fraud detection solution with the help of Microsoft Fabric and Power BI that is free of any third party tools like Python or R that would be required otherwise.

The research aims at proposing a new end-to-end pipeline combining both OneLake storage and Synapse ML and AI-driven algorithms of anomaly detection using mechanisms such as Isolation Forests, Artificial Neural Networks (ANNs), and Support Vector Machines (SVMs) to detect suspicious patterns in financial transactions. Mass personalization, anomaly classification and fraud risk scoring are enabled by the system, which contains custom ETL pipelines and feature engineering deployed in Microsoft Fabric, displayed in real time in Power BI dashboards.

The tested results prove that the AI- and ML-based models can be used when implemented natively in Power BI to cut the false positives and drastically increase the accuracy and efficiency of fraud detection. It is also integrated into human in the loop decision making by which fraud analysts can retrain, refine, and review the AI models on an ongoing basis. Such integration provides a fraud monitoring system with an ethical and transparent approach in accordance with GDPR.

This piece of work plays a role in the emerging real-time fraud detection via AI augmented analytics to Business Intelligence domain, demonstrating viability, elasticity, and accuracy of detecting frauds and the necessities to harness the integration of data science and decision-making to financial intelligence.

Keywords: Financial fraud detection, Anomaly detection, Microsoft fabric, Synapse ML,Isolation forest, Artificial Neural network (ANN), Support vector machine (SVM), Power BI, Real-time monitoring, AI-human colaboration, False Positive reduction.

1 Introduction

1.1 Background

The entry of digital financial services has created a huge increase in businesses and consumers and at the same time more challenges arose that has never come up in the case of fraud detection. Global cost of payments fraud has been pegged at over 40 billion annually and majorly this figure can be credited to payment fraud carried at the expense of the more sophisticated methods which exploit the shortcomings of the rule based command methods. The dynamic trend of fraudulent activities has put at bay the conventional methods of fraud detection, normally based on either static rule or threshold driven methods; resulting in low response interaction and poor false-positive rate.
The systems, which are effective in the past, are no longer satisfactory as far as deciding issues that demand action taking through the rapid and accurate determination of outcomes. It is also experienced that sometimes the alert workflow makes the fraud analysts to deal with high volumes of false alerts and thus they may be inefficient in their work and end up losing genuine frauds. The landscape of dangers is shifting, and the tool of monitoring fiscal health is as well expected to shift.
The concerned Research work refers to the challenge of the real-time fraud identification with the combined implementation of AI that would bridge the divide between intelligent information and anomaly identification under Business Intelligence (BI) dashboard.

1.2 Research Gap

Even though a number of organizations have already invested in machine learning (ML) models of fraud detection, most of these technologies are run outside of an organization and require being combined with Business Intelligence (BI) tools like Power BI in a rather complicated manner. The gap in the research on the project of a real-time, embedded AI-based anti-fraud scheme in the Power BI dashboards, as far as Microsoft Fabric and Synapse ML is concerned, both at the academic and industrial level is well-documented. Further, most of the studies just concentrate on the use of fraud detection models like Isolation Forests, Support Vector Machines in other parts of Microsoft but they are not applied directly in the ecosystem to provide end-to-end support in alerting, GIS fraud mapping and provide the analyst access to the fraud by overriding the fraud.

1.3 Research Question

How do deep learning algorithms combined with AI anomaly detection and advanced visualization tools impact the accuracy and efficiency of financial fraud detection?
This main research question is supported by sud-questions:

1. What are the scores of the Isolation Forests method and SVMs in determining Microsoft Fabric financial fraud?

2. How about the Syntax of Synapse ML on Power BI on automating the real time detection of Fraud Classification?

3. How do in-built AI capabilities affect false positive minimisation and the efficiency of the operations?

4. What does the concept of AI-human cooperation imply to the question of fraud decision-making as a component to the BI processes?

1.4 Research Objectives

To address the research question, the following objectives were defined:

1. Discover the Art of using AI to analyze financial frauds and real-time BI with the Microsoft technologies.

2. Create the architecture of the fraud detection environment that will allow using Microsoft Fabric modules: OneLake, Data Factory, Power BI, etc to manipulate and represent data without any difficulties.

3. To three different real-world-inspired cases of fraud, apply AI models of the fraud detection in financial transactions, the Isolation Forest, and the Artificial Neural Network (ANN) and the Support Vector Machine (SVM) using Synapse ML.

4. Make an analysis of the precision, the false positives rate, and real-time reactivity of the models, in each of the situations, on the Power BI dashboards, and the feed-back tool of fraud analysts.

2 Related Work

2.1 Literature Review

Many Researchers have tested better methods of detecting financial fraud using sophisticated applications like machine learning and real time systems. Further, one of the major research studies found that the use of other machine learning models, i.e., isolation forest, SVM, and ANN models, is more effective in identifying fraud than doing it in the traditional way Bontempi (2019). Their comparison study was used to present empirical support on the advantages of the multi-model approaches adjustment to enhance classification accuracy and reduce false positive under the advancing financial conditions.
It led in its wake to Borra (2024) pointing to the importance of real-time analytics in preventing frauds. By way of example, they showed how streaming companies like Microsoft Fabric enable adaptive anomaly detection, despite not being subject to any form of formal peer-reviewed sanction. Borra (2024) Also confirmed the same and even did a thorough review of the architectural design of Fabric including OneLake, Synapse ML and Power BI with particular focus on how they can be used to build scalable fraud detection pipelines.
Shivaleela and Shaikh (2021) have experimented with the Isolation Forest algorithm on transactions in plastic cards and it was more efficient in detecting outliers than the rule-based systems. In the work by Gudelek and Bolukbasi (2024), AI models were implemented to detect transactions associated with dark web activity and an example of using forensic data sources in unsupervised learning to produce fraud insight automatically as a result.
In order to solve the problem of classification in a noisy financial environment, Jeyakarthic

(2024) applied fuzzy logic, together with SVM and realized an improvement in the identifying rates of low-credit-score users. This concurs with a research by Camacho-Miñano (2021) where they demonstrated how they used neural networks in detecting complex financial crime schemes.

To contextualize the use of isolation forest, SVM and ANN, Nassif (2021) compared the anomaly detection algorithms in a systematic way, thus presenting the context behind the application of anomaly detection algorithms in addressing financial challenges. It was confirmed by a practical example of Isolation Forest on behavior transaction data Donald (2024). This premise was further enhanced by Bello (2024) who suggested adaptive learning technique which would be able to learn dynamically adapting to the dynamic nature of the fraud conditions.

The artificial complementary literature on the subject of BI's integration and visualization is the work of Tirupati (2024) and Ezhilarasi (2024) who addressed the performance of Power BI's in real-time analysis and enhancement of the process. Rani and Mittal (2023) also gave a pictorial presentation of the benefits of anomaly detection integration with the electronic banking system. To a certain extent, Larasati (2024) and Jullum et al. (2020) added a splash of color to this perception by dwelling upon the dashboard transparency and ML reliance to identify money laundering, respectively.

More research was utilized in technical architecture of the modern day systems towards fraud. The theoretical coverage of the idea of strategic use of ML in the sphere of finance was considered by Bello and Kahur (2025), and Tirupati (2024) also expounded upon the disadvantages of currently used methods of detection, which are called explainability and new threats. Donald (2024) contributed on their own part to the still-limited thesis of unsupervised models comparisons, and Soyele (2024) insisted on the utilization of hybrid frameworks. The article by Mahmood (2024), Mateev (2024) and Saini (2024) represent the very best of advice with regard to the effective use of Microsoft fabric, Power BI and Dataflows Gen2.

Finally, the first isolation forest algorithm, which forms the core of most of the current models in use was provided by Zhou et al. (2008). It was then proceeded by Patil (2024), who provided an explanation of anomaly detection in the financial realm. The use of Power BI in the connected financial reporting or the terrorism financing tracking was justified by Jelena Plašić (2024) and Kulbayeva (2024). Collectively, all these studies form an all-encompassing foundation to come up with a mechanism of real-time detection of fraud using artificial intelligence. Along with the supervised approaches, the unsupervised ones have demonstrated their efficiency in combination with the latter in a variety of purposes, including the monitoring of dark web transactions and low-credit score classifications, among others, and reducing the costs of operation. It can also be done at the same moment when these detection systems are integrated with Microsoft Fabric and Power BI infrastructure so that automation, visualization, and human intervention are easily conducted. In spite of all that progress, issues regarding increased model interpretability, scalability and applicability to other classes of fraud remain not fully answered. The proposed research aims to address those issues using high-end machine learning and quality data systems in order to simplify the detection of fraud and offer explainable findings.

3 Methodology

Physical research methods applied in undertaking the study alongside details of the process of collecting the information used, altering, modeling, and testing step by step. All the approaches are explained taking into consideration the fact that other scientists will reproduce the work as part of an attempt to have it verified and validated in accordance with the scientific principle reproducibility.

3.1 Data Collection

The data set employed to carry out the study was entirely based on the secondary set of data whereby its main scope was to model frauds in monetary transactions. The databases were all in the open-source database depository on Kaggle called Transactions Fraud Datasets created by ComputingVictor. The option in favor of this source was defined by its detailedness, the availability of a number of data tables, which can find use in the framework of fraud detection, and the impossibility to access the corresponding source by a small number of people, and this fact confirms the reproducibility and openness of the research process.

3.1.1 Data Source and Justification

Kaggle repository contains synthetic and real-world-inspired datasets that emulate some synthetic transactional patterns of fraud.It was chosen based on the following considerations:

1. **Multi-table Structure:** The repository includes relationally joinable, although separate, datasets such as transactions.csv, users.csv, and cards.csv which allow a detailed combination of user actions, financial metadata, and features at the card level.

2. **Relevance to Fraud scenarios:** The generation of the data sets allows the generation of fraud cases involving the abuse of large amounts, frequent burst operations, low-income forecasts and compromising card usage operations, which are exactly what the fraud scenarios are provided.

3.1.2 Dataset Used

The files that were fed into the Microsoft Fabric environment were the following:

1. **transaction.csv:** Elaborate transaction records include the attribute `card_id`, `amount`, `datetime` and `mcc_code` (merchant category code) as observed in this table. It is comprised in the core backbone of transactional research.

2. **user.csv:** There are also demographic and financial features of all users, such as the level of income, the credit rating and the`debt_to_income_ratio`, which must be provided to accept or to reject such engineering features like is_low_income_user?.

3. **card.csv:** Metadata such as `card_expiry`, `card_activation_date` and flags on the source of the card of type (e.g. normal issuance, dark web) that can be used in fraud cases involving expired cards or cards that have had the card details advertised in the dark web.

3.1.3 Data Ingestion

Dataflows Gen2 played a role in uploading all the data files onto the Microsoft Fabric OneLake Storage. The process allowed the schema finding and automatic data assimilation. Upon importation, the datasets were reviewed, their data schema was verified and they could be even written to Lakehouse tables which possess the data type of column in question, they were supposed to handle (e.g., money, timestamps, text, True/False). The tables were as well keyed individually in order to deal with joins between user IDs and card IDs. Transaction-level records were indexed on time by use of time stamped and card ID to enable feature engineering on time axis.

3.2 Data Preparation and Cleaning

The most important processes to the research when the quality and reliability of the model of the detection of fraud were prepared was data preparation. Organized raw data were vastly undermined as erroneously narrowed down to noise, inconsistencies, and brimming case duplicates in which after failing to fix, would jeopardize the correctness of the models.

3.2.1 Dataflow Environment

The data (transactions, users, and cards) was loaded to the Microsoft Fabric OneLake Storage, and Dataflows Gen2 with the Power Query as the transformation engine was applied. The environment was a no-code environment that included data profiling, filtering and transformation and reproducible.

3.2.2 Cleaning Activities

The data cleaning process included following critical steps:

1. **Handling missing values:** All the records lacking `card_id`, `transaction_amount`, or `datetime` were dropped to avoid null propagation in downstream joins and transformations in the future.

2. **Date parsing and standardization:** Transaction fields of date were converted to standard ISO date/time format and this made it possible to do precise time-based analysis and computation of time window of frauds.

3. **Duplicate removal:** Duplicate data was deleted especially in transactions.csv where data integrity was achieved through conditional filtering using card, ID, timestamp and amount.

4. **Text cleaning:** On names, special characters and white spaces more than required were eliminated. This played a critical role in creation of location-based characteristics of fraud.

5. **Consistency enforcement:** The referential integrity was ensured by the fact that the user and card entry of all transactions were matched through inner joins.

6. **Data Validation:** Built-in Power Query functions were used to validate and preview features with Power BI preview feature before loading them into the Lakehouse.

3.3 Feature Engineering

The feature engineering done on the cleaned data produced feature attributes and they were correlated with the detection of frauds. It came up with derived fields in power query and was applied as an entry in machine learning models.

3.3.1 Key Engineered Features

1. `is_low_income_user?` : Based from the `annual_income_column`, identity users who make below a set threshold 20,000 EURO.
2. `is_card_expired?` : Boolean flag comparing transaction date to the card's expiry date.
3. `is_card_on_dark_web?` : Identifies cards sourced from "DARKWEB" or "LEAKED" sources in the cards.csv.
4. `is_online_transaction?` : Flag based on merchant name or code indicating virtual merchants.
5. `is_high_debt_ratio?` : identifies the debt ratio below the threshold 800.

3.4 Experimental Setup and Scenario Segmentation

3.4.1 Scenario Definitions

1. **Scenario 1: High-value transactions by low-income users** Checks if low-earnings customers are purchasing big-quantity.
2. **Scenario 2: Expired or dark web cards used for purchases** Flags card transactions which are inactive or are leaked.
3. **Scenario 3: Abnormally high usage frequency** Detects rapid repeated usage of the same card in short time intervals.

3.5 Tools and Equipment Used

The whole of this research was done on cloud based environment and using open based software. Integration provided in tools was able to keep data in a free data ingestion to visualization.

1. **Microsoft Fabric (F8 Capacity):** Cloud infrastructure for data and models (OneLake) and for execution of pipelines as well as ml models.
2. **Dataflow Gen2** Auto loading of data, schema identification and transformation by Power Query.
3. **Power BI (service):** Dashboards and real time fraud visualization is also provided with AI visualization.
4. **Synapse ML** Distributed Train and Score models using Microsoft fabric notebooks.
5. **Python + scikt-learn:** Early stage model validation, baseline metric comparison and feature important validation.

6. **SQL:** Custom queries for join, index and in between table preparation.

4 Design Specification

The section presents the architectural and the logical design of the fraud detection pipeline on Microsoft Fabric with the modular design, scenario-based anomaly detection, real-time AI-based models, and scalable Power BI dashboards in mind.

4.1 System Architecture

The following architectural diagram defines the integration of OneLake, Dataflows Gen2, Synapse ML, and Power BI into a single system of real-time fraud detection, scoring and analyst review.

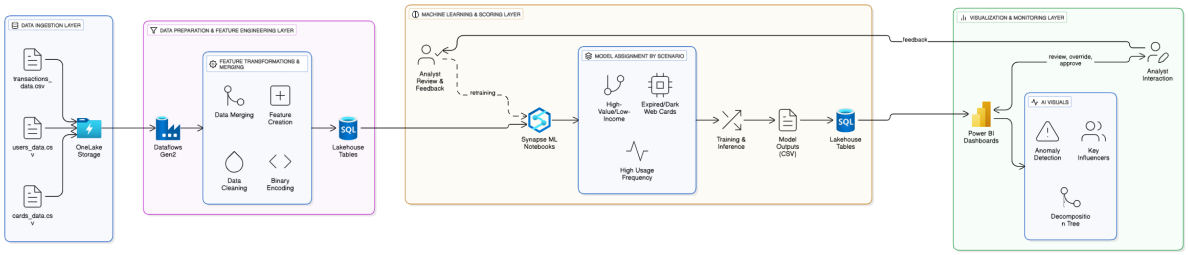

Figure 1: System architecture diagram

4.2 End-to-End Workflow

This is an end to end pipeline view of how this would work with Microsoft Fabric, visually between OneLake storage, Dataflows Gen2 preprocessing, Synapse ML model training, synapse Dataflows pipeline, power BI dashboard visual reports.

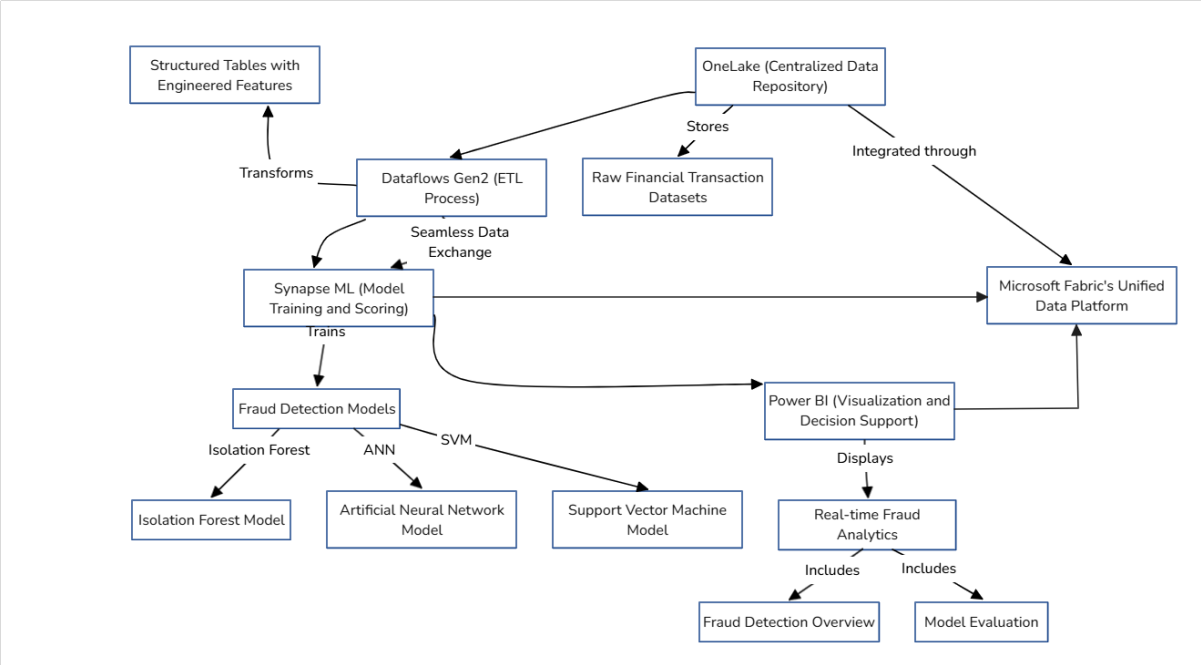

Figure 2: End-to-end workflow

4.3 Data Flow Diagram (Level-2)

This diagram shows data flow of that ingestion, into Dataflows Gen2, feature engineering, scenario specific runs of models (Isolation Forest, ANN, SVM) and running them in real time in Power BI. It contains analyst feedback and model-improvement loop.

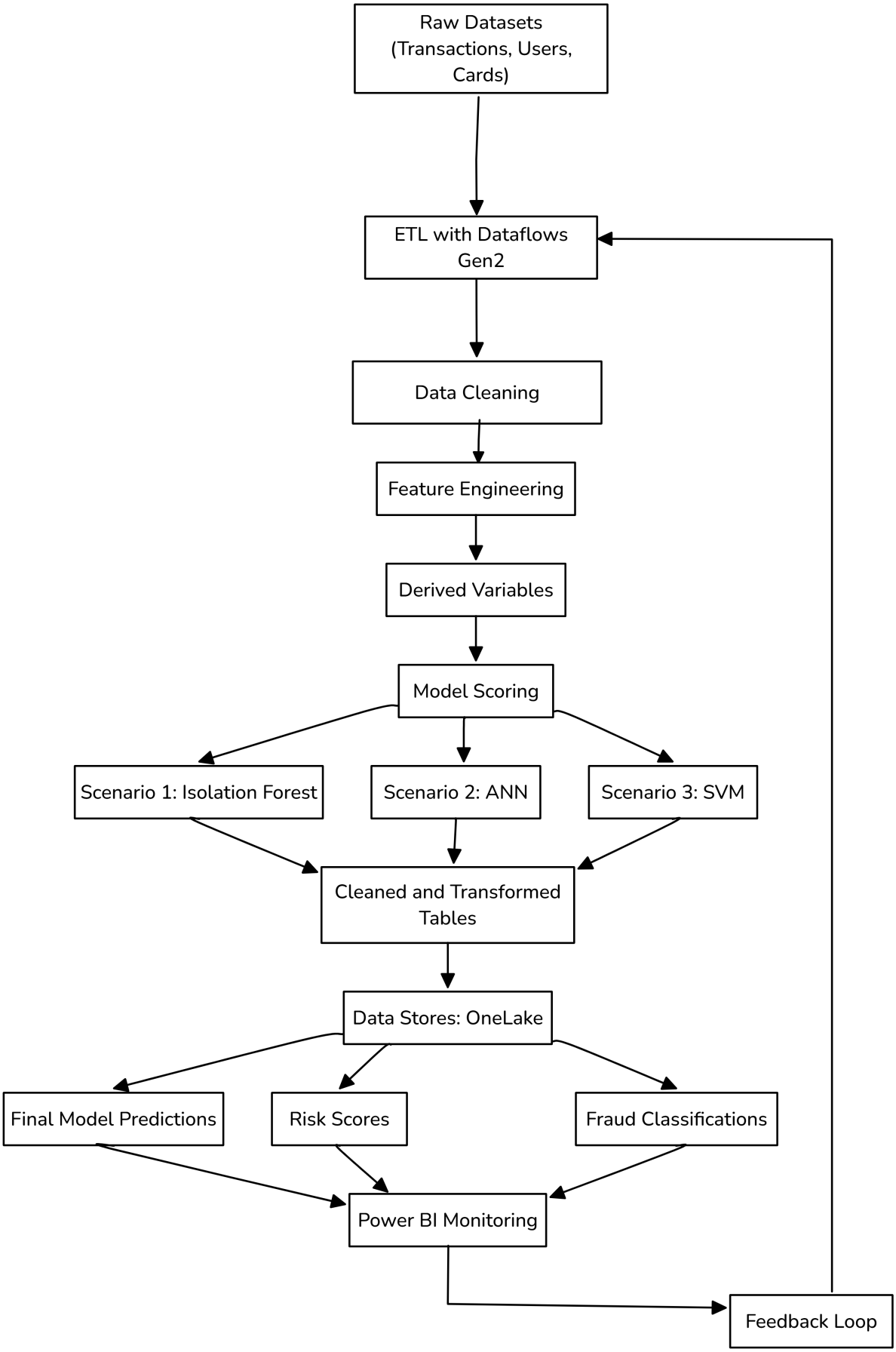

Figure 3: Dataflow (Level 2) diagram

4.4 Scenario-Model Mapping Diagram

The relationships between the fraud cases and the corresponding models of machine learning are reflected in this diagram: Isolation Forest in case of high-value low-income transactions, ANN with expired/Dark Web cards and SVM with high usage among low-income users.

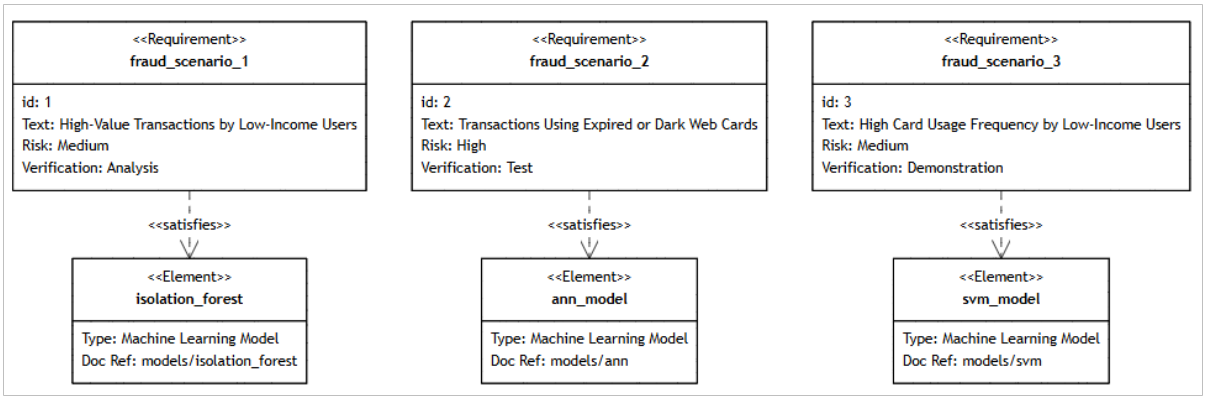

Figure 4: Scenario model mapping diagram

5 Implementation

The section contains details of technical implementation of AI-based fraud detection system step by step the assistance of Microsoft Fabric, Power BI, and Synapse ML. The system was divided into eight distinct parts (A to H) which involved the preparation of infrastructure, preparation of data, feature engineering, model production and creation of dashboards. This was done to deliver scalable real-time fraud detection pipeline embedded in Business Intelligence setting

5.1 Part A:Infrastructure Setup

Microsoft Fabric Premium F8 capacity was enabled to ensure that one can start the project and receive fundamental Fabric services, such as Lakehouse, Dataflows Gen2, Notebooks, and Power BI. The place was a connectivity centre named Dissertation-fraudDetection. The Lakehouse constituted the structured forms of organized financial data stored in a single location in the field of work. The overall setting involved the activation of Synapse runtime (On), the connection of the Power BI to Lakehouse, and the installation of the right to access notebooks and dataflows.

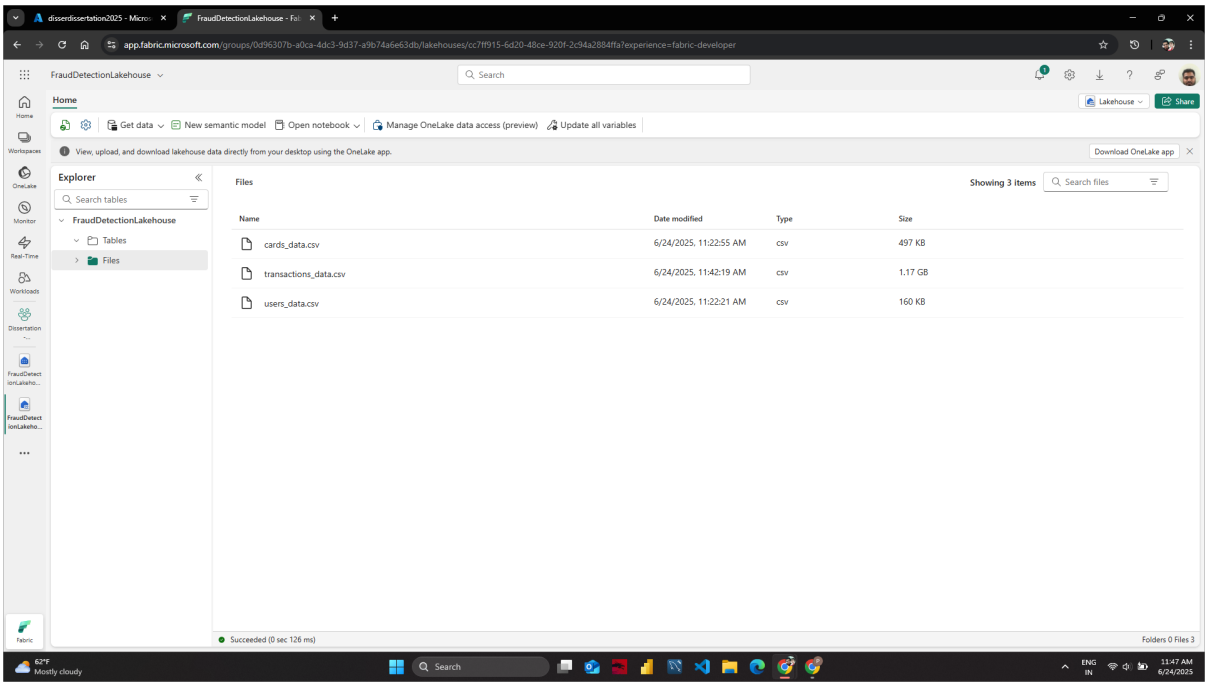

Figure 5: All three datasets load into Microsoft Fabric Lakehouse

5.2 Part B:Data Collection and Integration

The dataset was also consumed using Dataflows Gen2 that loaded the information in the form of reviewed .csv. They were represented by the datasets as follows:

1. **transaction.csv :** Contain all major transactions.
2. **cards.csv :** Characteristics or atributes of card holders.
3. **users.csv :** Demographical and financial data od an customers.

Rather, schema detection and mapping field work was performed by Dataflows Gen2. We converted this data to be valid and we normalised the data types and hence there are no downstream problems. The files were downloaded into the Lakehouse as tables.

5.3 Part C:Data Preprocessing and Feature Engineering

The power query editor was used to preprocess. These major changes were:

1. Review column names and their Data types of all required columns.
2. Alteration of trans_time and trans_date to single column trans_date-time.
3. The three tables (transactions, users, cards) merge with single master table called transaction_cards_users.

Advanced Feature Engineering:

1. Binary Flags were made of such form as is_low_income_user, is_card_on_dark_web and is_card_expired.

2. Risk profiles have been captured by including new columns and such as debt_to_credit_ratio etc., which are calculated columns.

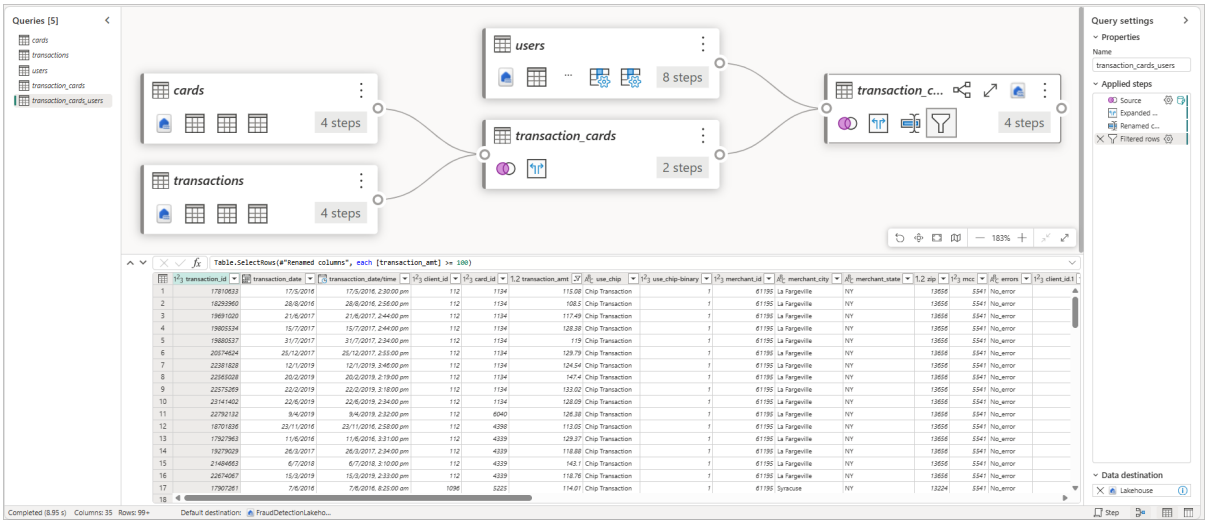

Figure 6: Master table (transaction_cards_users) after joins

5.4 Part D:Fraud Detection Scenario Definition and Risk Labeling

1. **High-value transactions by low-income users**
2. **Transactions using expired ordark web cards**
3. **Users with high debt and low credit scores**

These were target variables of unsupervised/supervised modeling. This data was narrowed down to produce scenario specific modeling subsets.

5.5 Part E:AI-powered Feature Selection and Vectorization

In order to feed data to the machine learning models, certain set of features was chosen depending on the role they play in detecting the fraud. Before training these features were cleaned, transformed and scaled.

1. transaction_amt - The amount of transaction
2. CVV- Card verification value
3. total_debt - An amount of an overdue debt of a user
4. credit_score- Index of the financial reputation of the user
5. num_credit_cards: the number of cards that one possesses
6. latitude- Geolocation (latitude) of transaction
7. Longitude (longitude) of transaction - longitude

The handling of missing values is handled as default imputation (e.g. credit_score = 600, cvv =0). One then connected these features in a single vector with VectorAssembler, then standardized them with StandardScaler to produce the scaled_features that are acceptable by Synapse ML models.

5.6 Part F:Model Training and Evaluation

Every scenario of fraud was linked to particular AI model:

1. Scenario 1 Isolation forest (unsupervised anomaly detection)
2. Scenario 2 Artificial Neural Network (binary classification)
3. Scenario 3 Support vector machine (supervised anomaly detection)

Scenarios would be trained in Synapse ML Notebooks on sets of scenario related features. Categorization in factors of evaluation was Accuracy, Precision, Recall, F1-score, Confusion Matrix.

model	accuracy	precision	recall	f1
IsolationForest	0.9912619292490696	1.0	0.9911622761224519	0.9924626442412607
SVM	0.9900520129365509	0.9902799055740232	0.9997516254589741	0.9864835884270508
ANN	0.9932515266617594	0.994904570569177	0.9982873181126648	0.9926661502117234

Figure 7: Model evaluation

transaction_id	label	predictedLabel	outlierScore	svm_prediction	ann_prediction
7475336	0	0.0	0.49084200343928464	0.0	0.0
7475365	0	0.0	0.47069426545682963	0.0	0.0
7475663	0	0.0	0.4849069746888283	0.0	0.0
7475737	0	0.0	0.44391799203268684	0.0	0.0
7475871	0	0.0	0.41504006821469064	0.0	0.0
7475935	0	0.0	0.48141986369766715	0.0	0.0
7475947	0	0.0	0.40961111381773146	0.0	0.0
7476111	0	0.0	0.48950067790188245	0.0	0.0
7476393	0	0.0	0.4303331674372089	0.0	0.0
7476615	0	0.0	0.44725425667024693	0.0	0.0

only showing top 10 rows

Figure 8: Model predictions

5.7 Part G:Power BI Fraud Analytics Dashboards

Lakehouse connection was used to import the last result into the Power BI. Interactive dashboard has also been developed, and it includes:

1. KPIs of fraud totals by scenario
2. Every model Anomaly detection plots
3. Risk score bar charts

This was achieved through real-time refresh which allowed the fraud analysts to track model prediction and take intervention as a means to correcting the fault. The reasons of a fraud were reviewed per case in the visual drill downs.

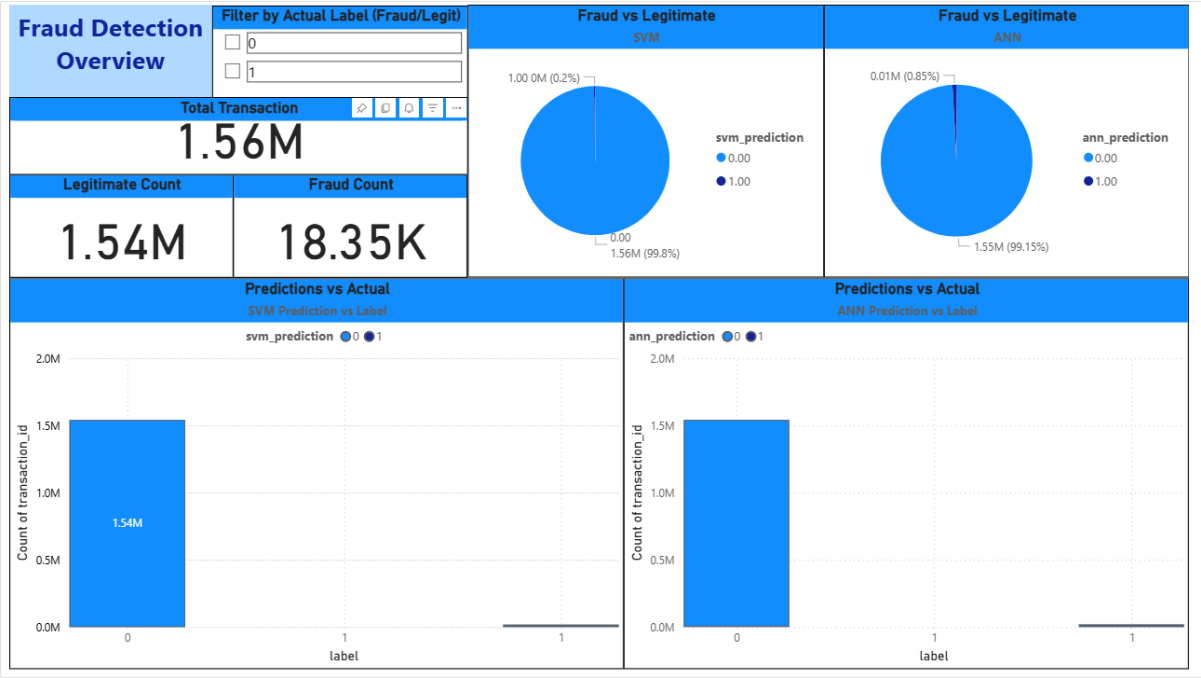

Figure 9: Fraud detection overview

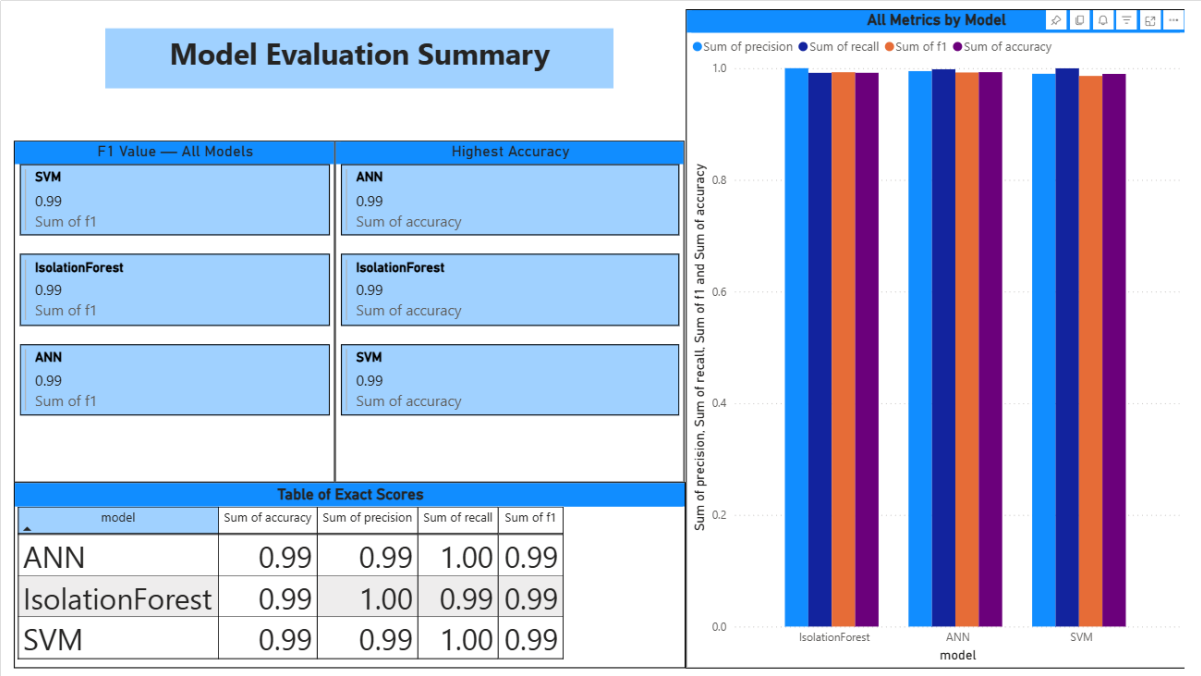

Figure 10: Model evaluation overview

5.8 Part H:Pipeline Deployment

In order to get the system in the state of good, the deployment pipeline of Microsoft Fabric was presented:

1. **Development Stage:** Create Synapse ML notebook usage that would be utilised to train and do a model exploration.

2. **Test Stage:** Preview Dashboards, Test the predictions.

3. **Production Stage:** An actual stage of the production it will be releasing real dashboards to monitor the fraud in real time.

This roll out turned out to be a problem-free inter-linkage of CI/CD operation, automatization of information update as well as assurance of the ability to deliver AI-powered conclusions.

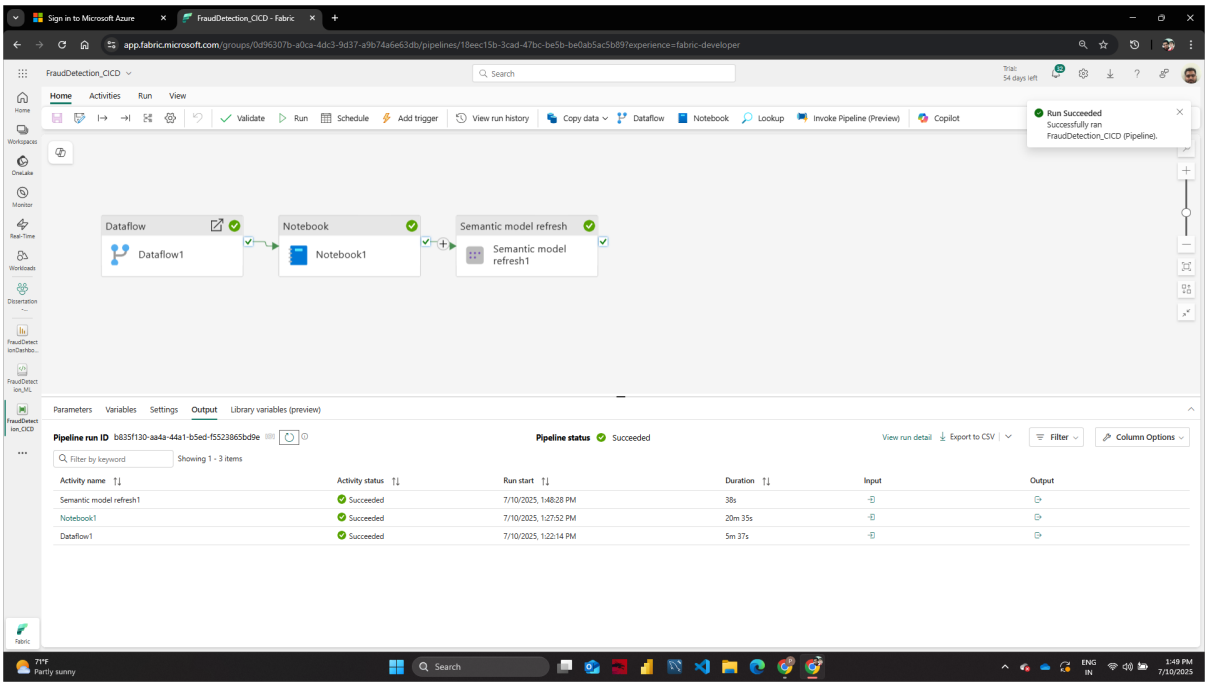

Figure 11: Pipeline deployed successfully

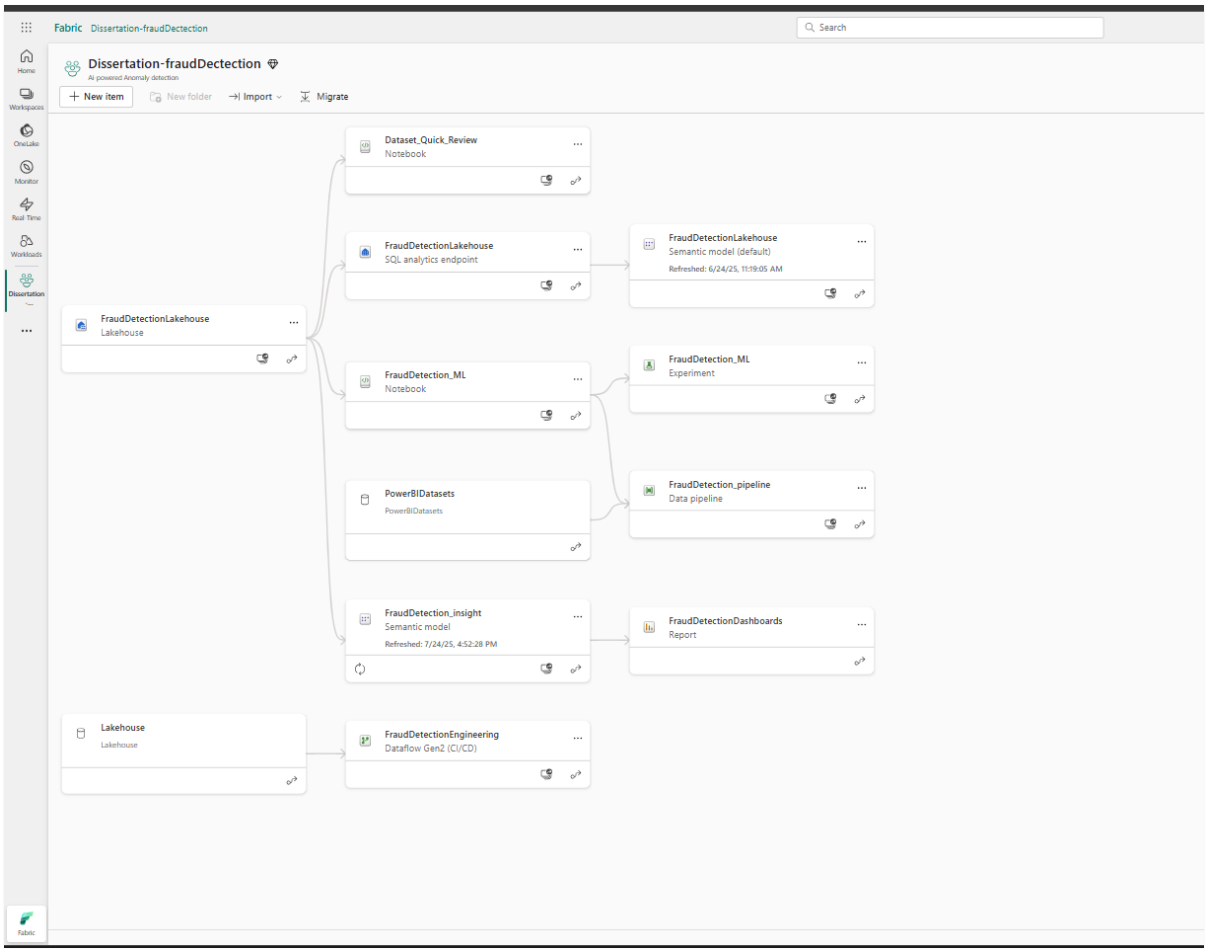

Figure 12: End-to-end fraud detection pipeline in Microsoft Fabric Workspace

5.9 Challenges Encountered

1. **Resource Constraints:** F8 Fabric was not in a position to scale the model easily primarily during training of SVM model and ANN. That is why, one to one model was implemented per scenario.

2. **Inconsistent Feature:**The derived models of features were not all interchangeable with each other on a case-by-case basis, models of features had been crashed because a null or schema error was encountered.

3. **Empty Table Error:** This is an error message that comes out when trying to correlate two sets of data in Power query because the sets of keys are not able to match; or a set of keys is not set.

6 Evaluation

Under Evaluation section the key outcomes during three cases of fraud using AI models of Microsoft Fabric and Power BI are to be highlighted. Another absolutely necessary examination of findings would be the examinations of such findings as considering them as precise, false and practical.

6.1 Case Study 1: High-value Transactions by Low-Income user

The next experiment sought to isolate anomalies that covered the transactions made by the users with lower income and not really high in value. Isolation forest was applied having features the following transaction_amt and is_low_income_user? These values of model accuracy of 99.13%, precision of 100, and recall of 99.12 translate to F1-score 99.24. This is indicated by such measures as the fact that the performance of anomaly detecting is extremely good, and zero numbers of satisfied false positives and minimal numbers of false negatives exist. It was demonstrated how the model would be of great use in detecting fraud without labels in an unsupervised manner.

6.2 Case Study 2: Transactions via Expired or Dark Web Cards

In this case the transaction tags involved with expired cards or the dark web marked cards were characterized by an Artificial Neural Network (ANN). The significant characteristics of input were is card expired and is card on dark web. ANN provided the accuracy of 99.33%, precision is 99.49, recall 99.83 and F1-measure 99.27. Frauds that were organized like in the risk characters, which were rate card-based, were amongst the characteristics of the model in the best performance. It has very high recall which translates to the fact that it is extremely useful in the detection of majority of fraud cases.

6.3 Case Study 3: Users with High Debt and Low Credit score

The given scenario measured the transactions undertaken by the users who have debts and low credit scores by employing a Support Vector Machine (SVM). User_credit_score, user_total_debt and transaction_frequency were used as features. Its accuracy, precision, recall, and F1-score were 99.08, 99.03, 99.75 and 98.64 respectively. The findings indicate that the SVM was beneficial in its ability to respond to the cases of frauds related to

credit risks and it has provided high classification ability of type of fraud profiles that are behaviorally consistent.

6.4 Discussion

The results support the fact that we can integrate the combination of Isolation Forest, SVM, and ANN with Microsoft Fabric regarding scenario-based fraud detection. All the models were highly accurate and the minimal errors occurred. Although the performance was excellent, real-time performances were constrained by F8 capability of Fabric, and the features were not available across scenarios. Another future improvement can be seen in adding additional interpretability of and with Power BI visualization (e.g. decomposition trees) and in migrating the capacity to F64 to allow use of larger neural networks. These findings coincide with those presented in the literature (Rani 2023; Bouman 2025), which allows concluding once again that the application of AI-based BI systems leads to increased effectiveness of the terrorist attacks by a considerable margin.

7 Conclusion and Future Work

7.1 Conclusion

The paper succeeded to provide and implement a working example of real-time and AI driven fraud monitoring and detect capability which heavily takes into consideration the limitations of traditional, rule-based fraud monitoring namely high false-positives, limited scalability, and non-scalability to business intelligence platforms. Throughout the research, it has been observed that the application of Isolation Forests, Artificial Neural Network (ANN), and Support Vector Machine (SVM) in order to achieve the objective of identification of anomalies in different variant types of financial fraud scenarios have been quite effective as indicated by the scenario-specific modeling framework established by the study. The results aided the validity and the efficiency of the AI models to the trained model to the engineered features against the real life inspired fraud patterns. All the three parameters, precision, recall and f1 scores were greater than 98% indicating the strength of the system. Besides, real-time analysis capability and the dynamic visualisation of a fraud powered through Synapse ML with connection to Power BI assisted in overcoming the gap between an automatic and human-based decision-making. Although it is possible to talk about the fact that a study has responded to the main research question, it successfully addressed all the stated goals, which, in itself, is evidence of the feasibility of native AI-augmented analytics in business intelligence operations.

7.2 Future Work

the outcome of the research was obtained as planned, there were shortcomings in the research and in future, research, there should be improvement. It consumed the restrictions to scale on the models particularly with the resource-intensive algorithms, i.e., ANN and SVM, using the Microsoft Fabric F8 capacity. The possibility of the environment being of increased capacity i.e. Fabric F64 or F2048 able to work with deep neural nets and large data sets may also be investigated in future. There is also the possibility to enhance the power BI features to make models more interpretable by model components like the SHAP-like explanations, key influencer visual, and the decomposition trees. Also

susceptible to improvement through time is the fraud detection responsiveness through combination with reinforcement learning or adaptive model tuning. Additionally, the real-time alerting solutions can be integrated with the CRM systems (e.g., Salesforce or Dynamics 365), thus potentially closing the circle of such complexities as alert to the case management. In my opinion, one of the productive ways to develop the described framework is to transform it into a low-code fraction detention system that I plan to sell to financial services providers as such type of solution would demand minimum programming languages to be used for its application. Such a system can become the generic blueprint of real-time fraud monitoring in the financial business with the help of AI as subsequent improvements occur.

References

Bello, H. (2024). Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments, *World Journal of Advanced Engineering Technology and Sciences* **12**(2): 21–34.
URL: *https://www.researchgate.net/publication/382680355*

Bello, O. and Kahur, K. (2025). Machine learning for fraud detection in banking and finance.
URL: *https://www.researchgate.net/publication/389466075*

Bontempi, F. (2019). Combining unsupervised and supervised learning in credit card fraud detection, *Information Sciences* **557**: 317–331.
URL: *https://www.sciencedirect.com/science/article/abs/pii/S0020025519304451*

Borra, P. (2024). Microsoft fabric review: Exploring microsoft's new data analytics platform.
URL: *https://www.researchgate.net/publication/381211337*

Camacho-Miñano, M. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator, *Expert Systems with Applications* **169**: 114470.
URL: *https://www.researchgate.net/publication/34761283*

Donald, J. (2024). Anomaly detection in usage patterns.
URL: *https://www.researchgate.net/publication/385084560*

Ezhilarasi, T. (2024). A study on implementation of power bi dashboards to streamline business processes, *IJRASET* **12**(7): 1548–1551.
URL: *https://www.researchgate.net/publication/382820122*

Gudelek and Bolukbasi (2024). Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments.
URL: *https://www.informatica.si/index.php/informatica/article/view/4538*

Jelena Plašić, Andrijana Gaborović, N. S. (2024). Unified business intelligence in the microsoft fabric environment.
URL: *https://www.researchgate.net/publication/392067003*

Jeyakarthic, M. (2024). Fuzzy support vector machine based outlier detection for financial credit score prediction system.
URL: *https://www.researchgate.net/profile/M-Jeyakarthic/publication/376834983*

Jullum, M., Loland, A. and Huseby, R. (2020). Detecting money laundering transactions with machine learning, *Journal of Money Laundering Control* **23**: 173–186.
URL: *https://www.emerald.com/jmlc/article/23/1/173/232223/*

Kulbayeva, A. (2024). Data processing methods for financing terrorism: The role of microsoft power bi in money laundering detection, *Procedia Computer Science* **238**: 528–535.
URL: *https://www.sciencedirect.com/science/article/pii/S1877050924012924*

Larasati, D. (2024). Business intelligence dashboard for financial performance analysis of public service agency using microsoft power bi, *JASa* .
URL: *http://journalfeb.unla.ac.id/index.php/jasa/article/view/2649*

Mahmood (2024). Microsoft fabric: Inside and out.
URL: *https://www.researchgate.net/publication/378380366*
Mateev, M. (2024). *Architecting Power BI Solutions in Microsoft Fabric: Design Optimal Solutions Using Power BI to Address Common Data Problems*, Packt Publishing.
URL: *https://learning.oreilly.com/library/view/architecting-power-bi/9781837639564*
Nassif, A. (2021). Machine learning for anomaly detection: A systematic review, *IEEE Access* **9**: 78658–78700.
URL: *https://ieeexplore.ieee.org/document/9439459*
Patil (2024). A systematic review paper for anomaly detection in financial transactions.
URL: *https://www.researchgate.net/publication/392972148*
Rani, S. and Mittal, A. (2023). Securing digital payments: A comprehensive analysis of ai driven fraud detection with real-time transaction monitoring and anomaly detection.
URL: *https://www.semanticscholar.org/paper/Securing-Digital-Payments-a-Comprehensive-Analysis-Rani Mittal/ca264c29c3bc6b6f5b828b671011682367792dad*
Saini, V. (2024). *Learn Microsoft Fabric: A Practical Guide to Performing Data Analytics in the Era of Artificial Intelligence*, Packt Publishing.
URL: *https://learning.oreilly.com/library/view/learnmicrosoftfabric/9781835082287*
Shivaleela and Shaikh (2021). Financial fraud detection in plastic payment cards using isolation forest algorithm.
URL: *https://www.researchgate.net/publication/353187307*
Soyele, A. (2024). Cross platform anomaly detection using hybrid ai models for multi-layered financial fraud in decentralized systems.
URL: *https://www.researchgate.net/publication/390319258*
Tirupati, K. (2024). Leveraging power bi for enhanced data visualization and business intelligence.
URL: *https://www.researchgate.net/publication/384342904*
Zhou, Z. et al. (2008). Isolation forest, *ICDM*.
URL: *https://cs.nju.edu.cn/zhouzh/zhouzh.files/publication/icdm08b.pdf*
enumerate