Evolutionary algorithm model for fraud detection in banking transactions

Selma Kocabıyık 2759524 , Isabella van Die 2786184

May 31, 2024

1 Domain and task

Even though nowadays there are a lot of advanced security measures, it is crucial to improve the current methods, especially with the upcoming online payment methods that are being used more frequently [1]. Current fraud detection systems often work with machine learning techniques, and do work well. However, fraudsters are also aware of these techniques and incorporate them in their work to look legitimate [2]. This calls for new ways to detect fraud.

This project aims to improve the current fraud detection systems of banks to ensure that fraudulent activities do not go unnoticed. It specifically focuses on banking transactions that are done through an online payment method. The main purpose of this project is to create an intelligence system that can detect fraudsters in banking transactions by applying advances machine learning techniques and analyzing transaction data by typical user behaviors. In the process of creating this system, there are legalities and ethics considered for the use of Artificial Intelligence (AI).

Our research question hereby is: How can current fraud detection systems be improved in order to accuracy of the detectors can be better than traditional systems?

To build a fraud detection model, the system needs to analyze banking transaction records, transaction time, geographical location, frequency, type of transaction (e.g., transfer, withdrawal, deposit), and type of user with their history of transactions. This ensures the system to have comprehensive data for fraud cases. For each transaction, the system will calculate a fitness score based on the given data. If the fitness score is higher than the threshold we set at 85%, the system classifies the user as a high risk of fraudulent activities. Transactions marked as high risk will trigger fraud alerts and a detailed analysis for fraud suspicion will be provided.

2 Literature overview

2.1 Literature summaries

"Review on fraud detection methods in credit card transactions" written by K. Modi and R. Dayma [3] references different machine learning techniques that could be used in fraud detector systems. The authors later emphasised certain methods that could also improve detectors, along with further advancements that could significantly impact secure banking transactions.

"Application of artificial intelligence for fraudulent banking operations recognition" by Mytnyk B. et al. [4] focuses on a study on the pre-processing of the data and various machine learning techniques. The results demonstrated that the logic regression model performed a notable higher value for the AUC compared to other techniques, which highly recommends the usage of logistic regression models for detection. However, AI systems can be complex to implement and there are certain limitations such as data privacy. The importance of AI applications within the digital activities of financial transactions increased significantly, especially due to global crises like COVID-19.

"A review of fraud detection techniques: Credit card" written by Chaudhary et al. [5] mentioned a definition of credit card fraud: "When an individual uses another individuals' credit card for personal use while the owner of the card as well as the card issuer are not aware of the fact that the card is being used.". The authors state that credit card fraud can be divided into two types: online and offline.

Online, being committed by using a stolen physical card, offline, being committed via internet, phone, web, etc. The article mentions other types of fraud that are not necessarily important for this report.

"Online payment fraud detection model using machine learning techniques" written by Almazroi, Abdulwahab Ali, and Nasir Ayub [6] discusses the use of counterfeit credit cards and the total reported fraud cases. The authors state that modern fraud detection systems are typically trained on large datasets of labeled transactions, allowing them to differentiate between regular and fraudulent activity. The ultimate result is the development of binary classification models capable of distinguishing between valid and fraudulent transactions, which is a difficult task that requires constant innovation and flexibility.

2.2 Research gaps and possible solutions

In the modern world, just as machine learning systems in artificial intelligence evolve, so does fraud in online banking. There are multiple variants and methods for designing algorithms, but none of the designs provide a hundred percent security against fraud. Researchers then discuss the best possible algorithms to address this problem. One of them is Evolutionary Algorithms (EAs) which was presented by Alan Turing in 1948[7]. EAs are generally used in numerous models and algorithms. Considering the importance and a huge impact of EAs on algorithm designs, they should be mentioned more.

However, Modi and Dayma [3], in their research failed to mention how adaptive algorithms like EAs could make a huge impact and even emerge undiscovered fraud tactics. Additionally, in the research of Mytnyk et al. where they discussed how EAs dynamically evolve with the transaction data should be highlighted. This feature of EAs could provide a more resilient detection system [4].

Moreover, Almazroi and Ayub [6] highlighted detailed machine learning techniques but never mentioned how the continuous learning system of EAs improves scalability and flexibility in adapting to new fraud patterns over time. Considering these research gaps, a possible solution would be designing a complete, perfect EA model for fraud detection to point out how EA might outperform other machine learning methods.

3 Computational solution

The computational solution in our system is provided by Evolutionary Algorithm (EA). Banks have a wide variety of customers, each with unique transaction scenarios and user information. Evolutionary Algorithms (EAs) are able to learn and adapt in real-time, even after the initial training phase. EA can generalize from complex data, such as transaction scenarios based on existing user information. Additionally, compared to other Neural Network models [6], in EA there is no Gradient optimization or back propagation [6] which might cause computation problems for super complex tasks.

In our system, the best hyper parameters and methods are selected for the training and learning phases of EA. Therefore, the algorithm not only learns from past data but also continuously adapts to new patterns and behaviors. With these capabilities, the system can detect fraudulent behavior by comparing the generated scenarios against historical data and real-time transaction information.

3.1 Model development

The evaluation of the model performed with the prepared training 60%, validation 20% and test 20% of the datasets. After the model's training and validation, required changes on the hyper parameters and methods of the functions made according to the results of validation. Completed training followed by testing and evaluation. In the evaluation, the performance of the algorithm was determined by statistical analyses.

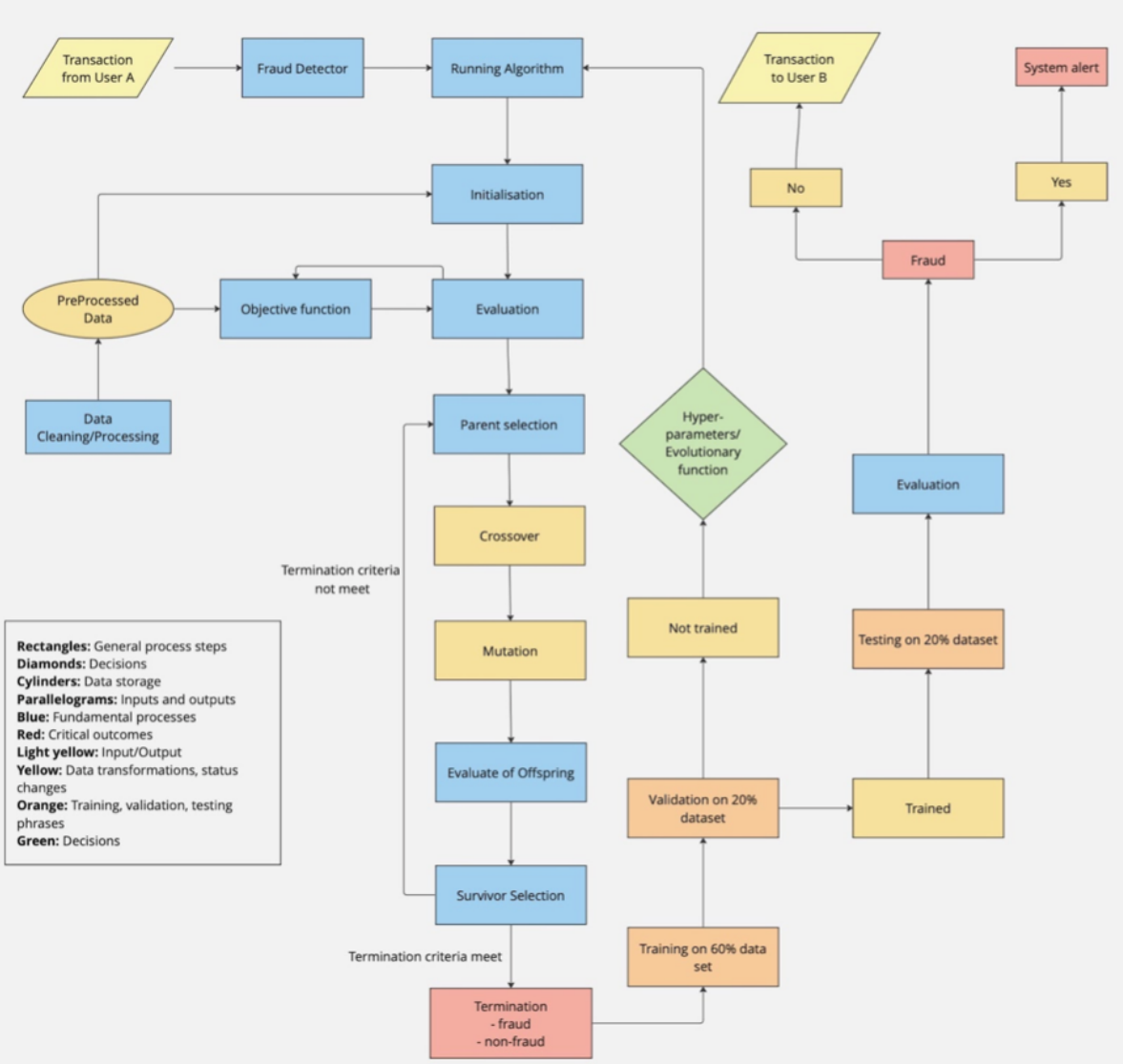

Figure 1: Flowchart of model in Machine Learning phase

The completed training and evaluation processes are placed in the system (Figure 1). Hereby, whenever a user intends to make a transaction, the algorithm runs automatically to detect any potential fraudulent behavior before the transfer. In this phrase the model receives data of UserA as long as UserB along with the historical data. So the system would be capable of detecting UserA or/and UserB as a fraud. If one of the users was detected as fraud, the transaction would be stopped by the system (Figure 2).

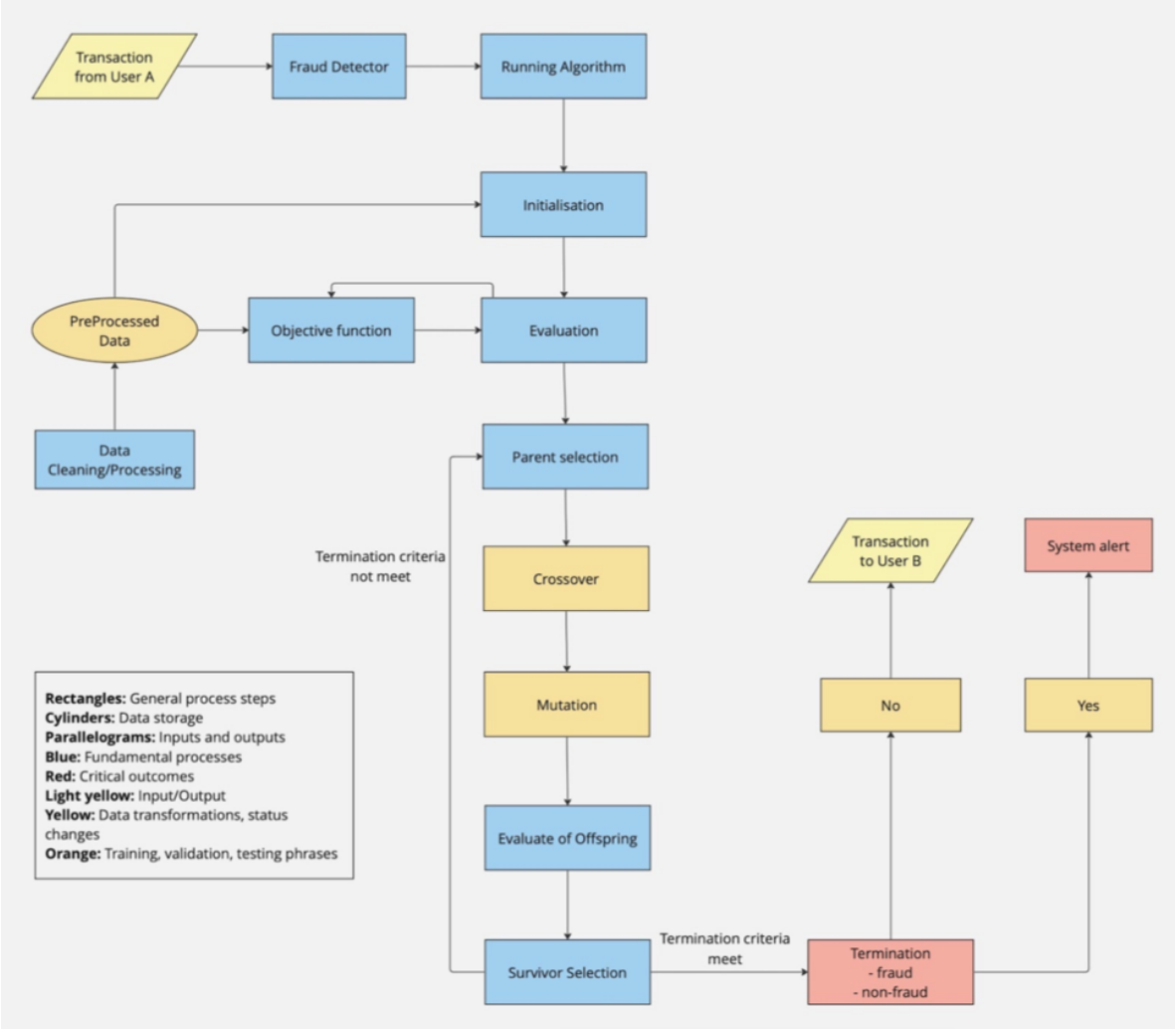

Figure 2: Flowchart of completed model

3.2 EA functional details

The model works with the scoring system which algorithm sets each user a score, called fitness score. If the output fitness score is above 85% individuals are marked as fraud. Since EA can continuously improve itself with the existing and new incoming data, the algorithm can adapt the fraud threshold, which enhances detection accuracy.

3.2.1 Initialization function

This function initializes individuals in the population from the processed data with their respective transaction details. Initialized individuals(transactions) stored as an array format, which is used in the algorithm later to determine the fraud users.

3.2.2 Objective function

The pre-processed data, which contains past fraud records, is used in the objective function to calculate the fitness score of the individuals. Each of the individuals is getting a fitness score based on their transaction information, which is initialized in the initialization function. The calculated fitness scores were later used in the other functions of the algorithm to determine the individual as fraud or non-fraud

3.2.3 Evaluation function

This function applies the objective function to set fitness scores for each individual. These scores determine the probability rate of each transaction to be fraud.

3.2.4 Parent selection function

Hereby, parents are selected from individual arrays based on their fitness scores; the highest scoring individuals chosen as parents. Hereby, the tournament method is used to choose the best parents by comparing individuals with each other. The chosen parents maintain fraud detection capabilities in the next generations.

3.2.5 Crossover function

This function generates offspring, which introduces various new combinations of traits that potentially could indicate new fraud or non-fraud behaviors. Hereby, the uniform crossover method is used which generates more offspring from paired parents.

3.2.6 Mutation function

Mutation aims to generate random variations to offspring traits that reveal potential changes in user behavior or possible fraud tactics. Therefore, EA learns or adapts to fraud strategies that were previously not observed. From the mutation function individuals evaluated again to be selected in survivor selection.

3.2.7 Survivor Selection Function

This function selects the best-performing individuals from the current generation with the highest fitness score. Due to the continuously learning nature of EA; If these individuals meet the fraud detection threshold, they influence the next generation. Additionally, if the selected individuals meet the termination criteria, the system would return an output.

3.2.8 Termination

If the concluded fitness-score is above 85% the system will be terminated with an output as 'fraud'. If the system decides after several generations that there is no fitness score above 85%, then output will be returned as non-fraud. If criteria are not met for the termination, the algorithm would then return to the parent selection from survivor selection to generate new populations

4 Interactive mock-up

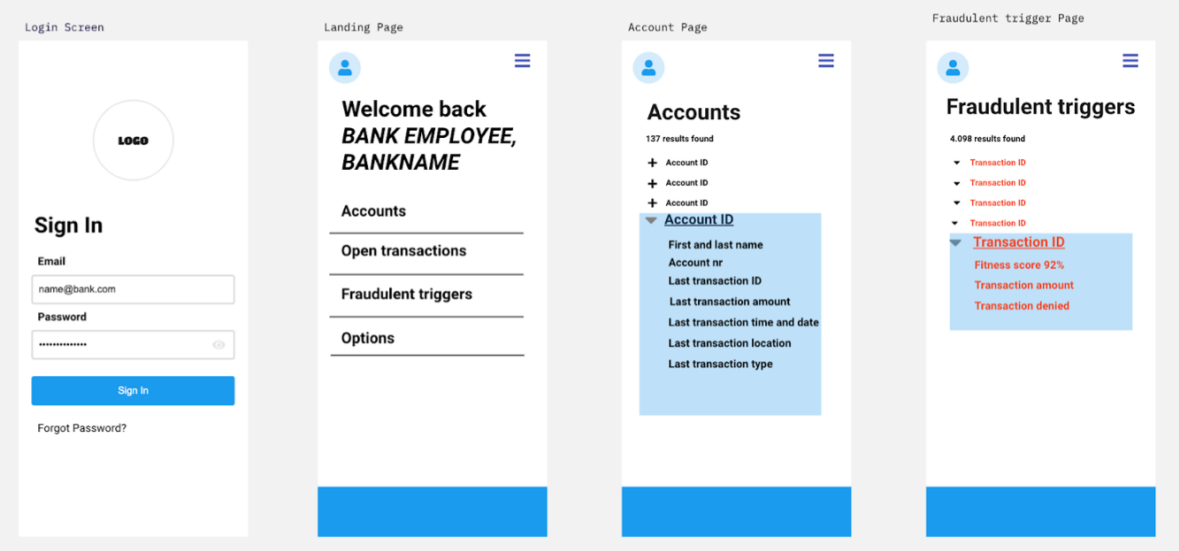

Figure 3: Mock-up of the application used by bank employees

The fraud detection system integrated within the banking application represents a critical tool in our efforts to maintain the security and integrity of the customers' financial transactions. As a bank employee tasked with overseeing transaction processes, understanding the intricacies of this system is crucial.

Upon initiation of a transaction by a user, the system automatically triggers the fraud detection algorithm to scrutinize transaction details alongside historical data. Each transaction is assigned a fitness score based on various parameters, including user behavior and transaction patterns. Transactions surpassing a predefined threshold are flagged as potentially fraudulent, prompting further investigation.

From the bank employee's perspective, the application provides a user-friendly interface through which transactions can be monitored and managed. Real-time feedback regarding the status of transactions, including any flagged as potentially fraudulent, enables prompt action to be taken to safeguard customer accounts and assets.

5 Evaluation

The evaluation concerned in this case is that the Evolutionary Algorithm (EA) will increase the performance of the fraud detectors compared to traditional based methods. Hereby, for traditional methods, Neural Networks, Logistic Regression or Derivative Free Methods of Machine Learning techniques can be taken as examples. These are highly used in current banking transaction systems to check frauds [6] . Therefore, as mentioned above, the research question is: How can current fraud detection systems be improved in order to detect frauds more accurate than traditional systems?

H0 (Null Hypothesis): Evolutionary Algorithm (EA) does not increase the performance of the fraud detection system.

H1 (Alternative Hypothesis): Developing a fraud detection system with an Evolutionary Algorithm (EA) will increase the performance and accuracy of the model for detecting fraud.

Independent variable (predictor):

- Previously used system

- New developed EA model

Dependent variable (outcome):

- Fraud detection accuracy for both previously used (e.g., traditional-based) system and new developed EA model
- **Measurement:** percentage of detected fraud cases / total number of cases.

5.1 Data

For the system's evaluation, many cases and historical data are used. Hereby, AI generated fraud users prepared to test performance of the models.

Control condition: Bank employees using their previous fraud detection techniques

Experimental condition: Bank employees using the new improved EA system to detect fraud.

5.2 Experiment Set-Up

The experiment could be designed to find out which model performed better for detecting the frauds. Hereby, two experimental groups, A and B, out of 10,000 users for each of them are created.

- Users from group A interact with their previously used fraud detection system.
- Users from group B interact with the newly generated EA model.

Experimenters prepare AI-generated fraud users to test model performance efficiently. Out of 10,000 users, 2,000 are AI generated fraud users that are assigned for each experiment group. To find out which scenario the model performed better, results obtained from the experiments are compared. Results are measured in percentages and later used in statistical tests. A higher percentage indicates better performance of the model to detect the frauds during the experiment.

5.3 Possible results

With the percentage levels of fraud accuracy, a paired t-test can be conducted. The obtained results of this statistical test would be a p-value. If the obtained p-value is less than the significance level, the null hypothesis can be rejected. Generally, 0.05 can be set for the significance level [8]. If p-value less than 0.05, reject the null hypothesis, and this would mean that EA would perform better than the previously used models.

Internal validity: The accuracy of the system.

External validity: How well the system generalizes to other cases.

5.4 Possible confounding factors

There are several possible confounding factors such as feature selection. The features that are selected for training the model highly influence the accuracy of the model. If important features that could be related to fraud would be left out, the performance of the model would be compromised. The same goes for the other way around. Other factors that are related to preparing the data could impact the performance of the model like imbalance data or the quality of the data. But with these points in mind, this can be prevented by carefully preparing the data.

External factors such as changes in the business environment/economy might also influence the detection of fraud. Changes in economic conditions or consumer behavior can change the perspective or pattern of the previously trained model which causes shifts in the fraud detection. However, these changes can not only affect the new EA system, but also the traditional rule-based systems.

Lastly, the interactions between variables could influence the performance of both EA systems and the traditional rule-based systems. For example, the frequency of a made transaction and the amount of the transaction may influence the accuracy of the fraud detection. A high-frequency transaction with a low-value transaction might flag the system, while it would be regular activity for certain customers. The same goes for low-frequency transactions with high-value transactions, this would likely be pinned as fraudulent behavior, while this could be perfectly normal activity for certain customers.

6 Privacy and ethical considerations

This EA model does collect data such as transactional data, time, geographic location, frequency, type of transaction and historical transaction behavior of the account holder.

6.1 Legality

According to GDPR (General Data Protection Regulation) article 3 [9, p. 115], data should be collected lawfully and should be transparent to users. Therefore, there will be a privacy policy in our system which states our purpose of data collecting, and how data will be securely stored. The collected data in the system will be accurate and collected within the storage limitations. Considering the risk levels within the AI Act [10]; the model is on a high risk level so a registration, conformity assessment should be taken. Therefore, if users accept the terms of the privacy conditions in their apps, then the model is allowed to use their data.

6.2 Ethical problems

There are several potential ethical problems with our solution. Since the system works with sensitive transactional data, it is of utmost importance that the data is being handled confidentially and securely. There also has to be written consent of the users whose data will be collected, just that they understand correctly why and how their data is being stored and used; transparency.

References

[1] D. G. Beju and C. M. Făt, *Frauds in Banking System: Frauds with Cards and Their Associated Services*. Springer International Publishing, 2023, pp. 31–52.

[2] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," *IEEE Access*, vol. 11, pp. 3034–3043, 2022.

[3] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," in *2017 International Conference on Intelligent Computing and Control (I2C2)*, 2017, pp. 1–5.

[4] B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko, and Y. Syerov. (2023) Application of artificial intelligence for fraudulent banking operations recognition. [Online]. Available: https://www.mdpi.com/2504-2289/7/2/93#metrics

[5] K. Chaudhary, J. Yadav, and B. Mallick, "A review of fraud detection techniques: Credit card," *International Journal of Computer Applications*, vol. 45, no. 1, pp. 39–44, 2012.

[6] A. A. Almazroi and N. Ayub, "Online payment fraud detection model using machine learning techniques," *IEEE Access*, vol. 11, pp. 137 188–137 203, 2023.

[7] M. Burgin and E. Eberbach, "Evolutionary turing in the context of evolutionary machines," *University of California and Rensselaer Polytechnic Institute*.

[8] O. Guy-Evans, "Understanding p-values and their significance in statistical hypothesis testing," *Simply Psychology*, 2024, available online: https://www.simplypsychology.org/p-value.html.

[9] European Data Protection Supervisor, *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018, available at: edps.europa.eu.

[10] European Commission. (2024) Regulatory framework on ai — shaping europe's digital future. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai