

# Project Numa

Split Federated Intelligence  
for Combating Cross-  
Border Financial Crime  
(FedShield)



[Stained glass is used in the homes of upper-class Romans during the rule of the Roman Empire. The split glass pieces are joint together, producing a lasting, beautiful artwork, yet providing privacy to the space behind the stained glass.]

---

Core Team (authors): Abhiraaj a/I Sithambaram, Chang Kai Boon, Vincent Lee Wai Seng

Other contributing members: Ho Chiung Ching, Ahmad Shazwan, Mohd Akmal Amri, Pam Chun Onn, Nur Aisyah, Nurhaziqah, Rifqah, Adam Fadhli, Lee Tong Ming, Shuhaira


Organisation: Bank Negara Malaysia (Central Bank of Malaysia)

Note: The views expressed are those of the authors and do not necessarily reflect the views of the Bank Negara Malaysia.



# Content

1. Background	3
2. Proposed Solution	4
3. Model Framework	6
3.1 Data standardisation module	6
3.2 Differential privacy module	7
3.3 Split federated learning module	7
4. Dataset	9
5. Experiment Setup and Results	11
6. Limitations and Future Considerations	16
7. Conclusion	17
8. References	18



# 1. Background

The global payments industry has grown 7% annually from 2018 to 2023, contributing 3.4 trillion transactions with USD1.8 quadrillion in value in 2023, according to McKinsey<sup>1</sup>. Similarly, global e-commerce has expanded by 10% in 2023, surpassed USD6.1 trillion or 14.4% of all commerce globally<sup>2</sup>. The increasing adoption of digital wallets<sup>3</sup> and fast payments<sup>4</sup> represents the biggest area of growth in the global and cross-border payments landscape. However, this shift towards electronic payments has also given rise to the financial crime i.e. money laundering.

An estimated USD3.1 trillion in illicit funds flowed through the global financial system in 2023 alone, contributed mainly by top crimes including drug trafficking (USD782.9 billion), fraud (USD485.6 billion), human trafficking (USD346.7 billion) and terrorism financing (USD11.5 billion)<sup>5</sup>. Another study<sup>6</sup> also highlights that the money lost to ecommerce fraud will rise from USD44 billion in 2024 to USD107 billion in 2029. This issue poses significant challenges to financial integrity. Combating financial crime can no longer be approached at the country level. There needs to be collaboration not just at the financial institutions (FIs) level but also with the public sector e.g. the regulators. However, existing cross-country efforts among regulators and FIs to collaborate efficiently and effectively on combating financial crime face challenges, including unharmonized and inconsistent transaction data formats and structures, as well as privacy and confidentiality concerns regarding data sharing.

<sup>1</sup> See P. Bruno, U. Jennah (2024).

<sup>2</sup> See WorldPay (2024).

<sup>3</sup> See PYMNTS.com (2021).

<sup>4</sup> See Frost et al (2024).

<sup>5</sup> See Nasdaq and Verafin (2024).

<sup>6</sup> See Finextra (2024).

## 2. Proposed Solution

Project Numa focuses on the development a cross-border collaborative financial crime detection proof-of-concept, called FedShield, based on privacy-enhancing technologies (PETs), machine learning and deep learning.

FedShield presents a novel approach, which implements a combination two PETs: (1) linear dimensionality reduction (LDR) [e.g. truncated singular value decomposition<sup>7</sup> (Truncated SVD)] with differential privacy (DP) and (2) split federated learning<sup>8</sup> (SFL) to allow more secure cross-border predictive model for global financial crime detection. Similar to BIS Project Aurora<sup>9</sup>, the use of PETs and machine learning are important tools to enhance public-private partnerships in detecting financial crime effectively and securely.

The simplified pipeline of FedShield is as follows:

- 1) Financial institutions (FIs) from different jurisdictions collate their payment transactions dataset (including known and unknown financial crime labels).
- 2) FIs performs Truncated SVD on the dataset on their own server (FI server), reducing the data to top k components that explains most of the variance.
- 3) A DP layer injects a level of noise into the reduced dimension dataset, to avoid any parties from reconstructing the original features. This is commonly called as output perturbation DP<sup>10</sup>.
- 4) The reduced dimension plus noise layer dataset is processed at the SFL architecture for predictive model training. In SFL, the model training would be split between the FI server (feature extraction part) and the global server (classifier part). At the same time, updates to FI local model are sent to the global server for aggregation.
- 5) After model training is completed, the predictions are generated and returned to the individual FI server.

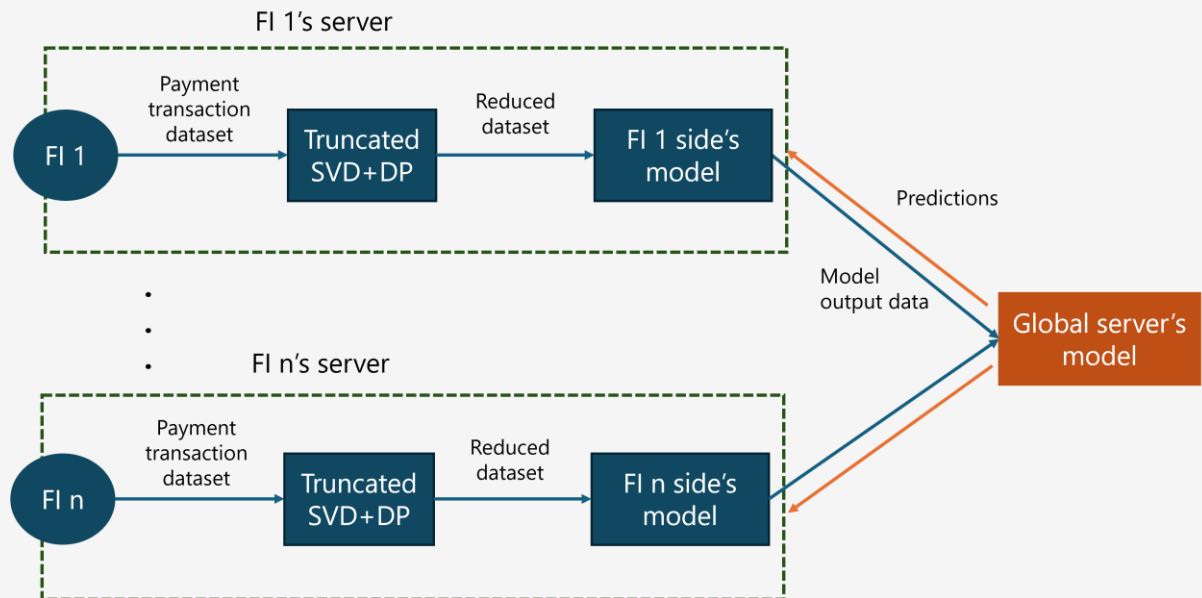
<sup>7</sup> See Halko et al (2011).

<sup>8</sup> See Thapa et al (2022).

<sup>9</sup> See BIS (2023).

<sup>10</sup> See Lowly et al (2021).

Flow chart on the simplified pipeline:



## 3. Model Framework

As briefly mentioned in the proposed solution, FedShield's model framework leverages on a combination of PETs namely LDR with DP and SFL. While LDR can address the issue of unstandardised data across jurisdictions, it can also facilitate privacy preserving<sup>11</sup> in terms of the transaction dataset by adding DP post-TruncateSVD. In addition, SFL can further enhance the privacy preservation of the sensitive information in the dataset as well as the predictive model.

### 3.1 Data Standardisation Module via LDR

LDR via Truncated SVD is done on the FI's end of the model to decompose a matrix into its singular values and vectors and then select only the top k singular values and vectors. This enables the matrix to reduce dimensions and retain most of the original information.

Standardising the data format (e.g. time zone, currency type, transaction category) can be a challenge and resource intensive for some jurisdictions, especially when the data standardisation requires changes to the payment system design. Hence, LDR techniques are good alternatives to allow differences in the FIs' transaction data to collaborate in the predictive model.

The number of top components from Truncated SVD can vary across FIs and jurisdictions based on the format and granularity of payments transaction data collected. For example, not all jurisdictions capture the same levels of payment type, methods and the type of institutions.

While there are many LDR techniques, Truncated SVD is selected as it is suitable for data that is sparse and with categorical variables, which is the case for payments data. Truncated SVD can also reduce the impact of noise and redundancy in the data, which helps with the accuracy of the predictive models<sup>12</sup>. It is also more computationally efficient as compared to other LDR techniques such as traditional SVD and principal component analysis (PCA)<sup>13</sup>.

<sup>11</sup> See Banu and Nagaveni (2009).

<sup>12</sup> See Dataaspirant (2023).

<sup>13</sup> See Mishra et al. (2017).

### 3.2 Differential Privacy (DP) Module

Since the reduced dimension dataset can still be reconstructed back to original features, applying it with DP provides a layer of privacy preservation on the FIs' original data<sup>14</sup>. Upon applying LDR or Truncated SVD, the DP is added to the top components of the reduced dimension dataset. This is called DP via output perturbation, which is a common standard<sup>15</sup> to privacy preserve the results of a model (Truncated SVD in this case), to ensure any information derived from the original data is protected before it goes into the next stage i.e. predictive model training.

The DP experimented in FedShield is the random Gaussian noise. A fairly recent study highlighted that Gaussian DP could strike a better balance between the privacy guarantees and model accuracies, especially for deep learning, as compared to other DP techniques<sup>16</sup>.

### 3.3 Split Federated Learning (SFL) Module

SFL is a hybrid approach that combines the strengths of Federated Learning (FL) and Split Learning (SL) (see comparison diagram). In FL, multiple devices (clients) collaboratively train a machine learning model. Each client (FI in our context) trains the model at its local server and only shares the model updates with the centralised server, which aggregates these updates to improve the global model. Although FL does not require sharing of original dataset, local clients need high computation resources to train the full machine learning model. Model privacy is also a concern as both clients and global server have full access into the machine learning model.

As for SL, it involves splitting the model into parts that are trained separately by different clients and the global server. Commonly, the client server works on the feature extraction part of the model and the global server works on the classifier part of the mode. This approach enhances privacy on the model because only

<sup>14</sup> See Fan (2019).

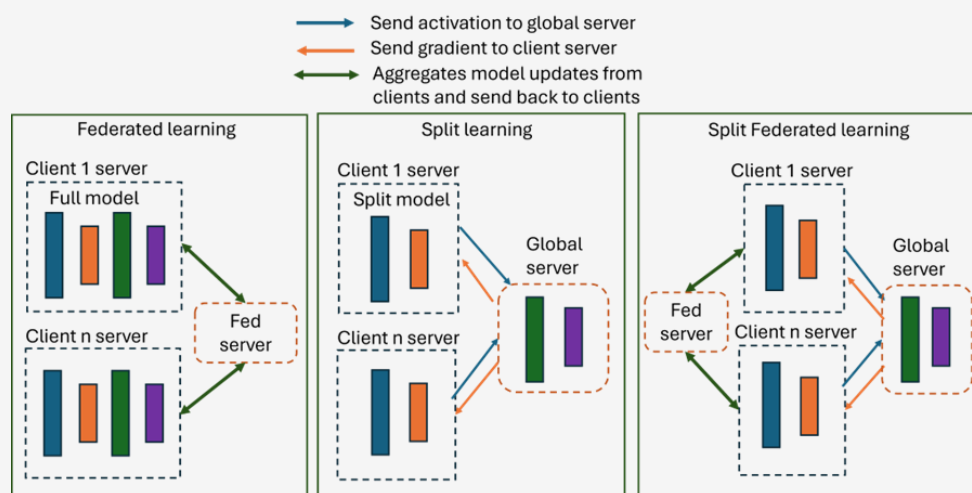
<sup>15</sup> See Tianxi and Pan (2024).

<sup>16</sup> See Bu et al (2020).

intermediate activations are shared between the clients and the global server. However, the communication overhead in SL is an issue as only one client can engage the global server at one time.

Hence, SFL can address both model privacy issue in FL as well as communication overhead issues in SL, without needing to share the client's original data. SFL also reduces the computation time per global epoch compared to pure SL or FL, making it more efficient and robust for training models across multiple clients.

Comparison diagram of FL, SL, and SFL:



For the SFL framework to work on predictive models, deep learning models are more suitable, especially for the split learning part. This means neural networks are easier to be split between client and global server as compared to machine learning models.

The models we experimented for FedShield are the classical feedforward neural network i.e. Multilayer Perceptron (MLP) as base model and comparing it with the residual neural network i.e. ResNet. While MLP is commonly used for classification tasks on tabular datasets and more computational efficient, MLP may not able to converge well when it comes to large datasets. Although ResNet is more commonly used on image data, there are also use-cases for tabular data prediction and classification<sup>17</sup>. The experiment was conducted via local environment but for deployment, the global server would be hosted in the shared private cloud and a connection would need to be established from the client server to the global server.

<sup>17</sup> SeeKulkarni (2024).



## 4. Dataset

For the proof-of-concept, we leverage on two different variants of datasets: (1) open-sourced credit card fraud detection dataset<sup>18</sup>, which contains transactions made by credit cards in September 2013 by European cardholders; and (2) synthetic payment dataset provided by the BIS Analytics Challenge 2025. Two datasets are selected for comparison in terms of model performance under the SFL module and also to highlight that the SFL module works with different datasets.

### 1) Open-sourced credit card fraud detection dataset:

This dataset is chosen because linear dimensionality reduction via principal component analysis (PCA) has been carried out on the dataset to ensure privacy of the original data; hence, mainly principal components (PCs) are made available to be used for learning. There are three (3) variables, on which PCA was not applied, namely "Amount", "Time" and "Class". Description are as follows:

Variables	Description
Amount	The transaction amount
Time	Seconds elapsed between each transaction and the first transaction in the dataset
Class	Response variable which takes value of 1 if fraud and 0 otherwise.

The other twenty-eight (28) columns in this dataset are the top 28 principal components (PCs) obtained with PCA, namely V1 until V28. The descriptions of the 28 PCs were not provided due to data confidentiality but it is mentioned that the PCs can be of use to predict the class variable.

<sup>18</sup> See Machine Learning Group (2018).

## 2) Analytics Challenge's synthetic payment transaction dataset

There are three main datasets provided namely the payment transaction dataset, account holders dataset (of various FIs) and target dataset (tags the illicit transactions based on various financial crime typologies). After we joined the dataset, several preprocessing steps were performed to achieve the desired dataset for our proof-of-concept experiment.

- a) Due to the limitation on computational resources, only a subset (2 million) of records were randomly extracted from the 308 million transactions records. After that, some variables were dropped including:
  - those that are of purely identifier data i.e. transaction id, account id, counterparty id, assigned bank) (since our use-case is more on detecting illicit transactions rather than on the accounts or individuals)
  - granular time variables i.e. 'min', 'sec' (to differentiate from the credit card fraud dataset)
  - granular transaction "category\_1" and "category\_2" (to focus on the high-level category only)
- b) The target variable is the laundering scheme types and ids. Since the illicit target label are of the minority class, we group the laundering scheme types as one illicit target class, making the target variable binary. This aligns with the credit card fraud dataset. For experimental purposes, we only limit the target variable to the top 2 laundering schemes.
- c) Additional preprocessing for different variable types:
  - Numerical variables, e.g. 'amount', 'initial\_balance' and 'age', are standardized.
  - Cyclical variables, e.g. 'month', 'day' and 'hour', were converted to a cyclical format using sine and cosine functions to better capture the temporal nature of the data.
  - Categorical variables, e.g. 'transaction\_direction', 'channel', 'payment\_system', 'category\_0', 'assigned\_bank\_type', are one-hot encoded to enable seamless TruncatedSVD on the data.

For comparison with the credit card fraud dataset, we applied a different LDR technique i.e. Truncated SVD, which is appropriate for this dataset since it is sparse and involves categorical variables. In terms of the decomposition, we also reduced the dataset to the top 10 singular matrices, for experimental purposes as well as due to limited computational resources.

## 5. Experiment Setup and Results

Here is the experiment setup approach on the datasets for the LDR and SFL modules, in order to better capture the potential issues with the payments data in the real world:

### 1) Experiment setup for data standardisation via LDR

Each FI (client in the experiment context) has its own set data, on which the FI can perform either Truncated SVD or PCA locally (depending on the data structure) and generate the top PCs or singular matrices (that covers most of the variance). FI then proceeds to inject DP noise into the reduced dataset before passing it to the split model training process at client server. In the real world setting, we would expect clients differs in the size of institution setup as well as the data; hence, each client's data should reflect a different variance threshold.

### 2) Experiment setup for SFL

We split the two datasets mentioned in the above Part 4 across 5 clients. As for the credit card fraud dataset, we fix the first 10 PCs and then randomised 5 more PCs for each client, making it a total of 15 PCs per client. The range of variance cover by each client is between 70 to 80%.

As for the synthetic payment dataset, each client receives top three (3) singular matrices, and two (2) singular matrices randomly assigned from the remaining 7 singular matrices. The mix of fixed and randomised assignment of PCs/singular matrices for both datasets is to reflect the real world scenario, where different FIs from various jurisdictions have a combination common and unique variable of the transaction data. With this setup, we can mirror the unstandardised data patterns in the real world setting.

### 3) Predictive modelling setup via Python:

- a) The data was randomly split into 80% for training and 20% for testing.
- b) To align with the credit card dataset, which is a binary target variable, as mentioned earlier, we grouped the top 2 money laundering scheme types into a single illicit target class for synthetic payment data.
- c) Since illicit/fraudulent label is of minority, under-sampling and over-sampling techniques are applied on the training set while leaving the testing set imbalanced.
- d) For under-sampling, random under-sampling technique was used to reduce the majority class to the size of the minority class.
- e) For over-sampling, Synthetic Minority Oversampling Technique (SMOTE) and Conditional Tabular Generative Adversarial Network (CTGAN) were employed to expand the minority class via synthetic data generation to match the majority class<sup>19</sup>.
- f) To assess the impact of model complexity on performance, we compared the Multi-Layer Perceptron (MLP) model against the ResNet model.
- g) Additionally, we compared single client's model performance vs SplitFed framework involving 5 clients. Instead of partitioning the data equally among five clients in the SplitFed setup, all the data was used to train the single MLP and ResNet models.
- h) All models were trained with consistent hyperparameters: a learning rate of 0.001, a hidden dimension of 32, and a weight decay of 0.0001, using the Adam optimizer throughout the training.
- i) Evaluation metrics:
  - F1-score (harmonic mean of precision and recall, which is more suitable due to the imbalanced dataset)
  - Precision (share of true illicit predictions over all illicit predictions)
  - Recall (share of true illicit predictions over all actual illicit labels)

<sup>19</sup> See Khosravi et al (2024).

#### 4) Experiment results for the credit card fraud dataset:

##### a) MLP model: Test result

Server	Sampling Technique	F1-score	Precision	Recall
Single client	Under-sampling	0.07	0.04	0.93
	SMOTE	0.07	0.03	0.92
	CTGAN	0.16	0.09	0.70
SplitFed (5 clients)	Under-sampling	0.02	0.01	0.88
	SMOTE	0.06	0.03	0.96
	CTGAN	<b>0.41</b>	0.32	0.65

##### b) ResNet model: Test result

Server	Sampling Technique	F1-score	Precision	Recall
Single client	Under-sampling	0.06	0.03	0.96
	SMOTE	0.12	0.06	0.92
	CTGAN	0.53	0.41	0.74
SplitFed (5 clients)	Under-sampling	0.07	0.04	0.90
	SMOTE	0.28	0.17	0.99
	CTGAN	<b>0.75</b>	0.79	0.71

#### 5) Experiment results for the synthetic payment dataset:

##### a) MLP model: Test result

Server	Sampling Technique	F1-score	Precision	Recall
Single client	Under-sampling	0.43	0.28	0.86
	SMOTE	0.43	0.28	0.86
	CTGAN	0.43	0.30	0.81
SplitFed (5 clients)	Under-sampling	0.46	0.32	0.83
	SMOTE	0.45	0.31	0.85
	CTGAN	<b>0.48</b>	0.35	0.79

##### b) ResNet model: Test result

Server	Sampling Technique	F1-score	Precision	Recall
Single client	Under-sampling	0.45	0.31	0.86
	SMOTE	0.44	0.29	0.87
	CTGAN	0.44	0.30	0.82
SplitFed (5 clients)	Under-sampling	0.45	0.31	0.87
	SMOTE	0.48	0.32	0.86
	CTGAN	<b>0.55</b>	0.44	0.76

## **6) Discussions on the results:**

### **a) Comparison of sampling techniques**

- While under-sampling balances the training data by removing a substantial number of majority-class samples, it can result in the loss of critical information and generally produces lower F1-scores.
- In contrast, both over-sampling techniques tend to yield higher F1-scores by retaining majority-class information while augmenting minority-class examples. Notably, CTGAN consistently produced higher F1-scores compared to SMOTE across all setups.
- Specifically, the SplitFed ResNet combined with CTGAN achieved the highest F1-scores, recording values of 0.75 and 0.55 for the Credit Card dataset and the BIS subset, respectively, in comparison to the SMOTE-based approach.
- These results indicate that CTGAN is more effective at capturing the complex distributions of the minority class, thereby enhancing recall and overall performance relative to the more straightforward SMOTE method.

### **b) Comparison of deep learning models**

- ResNet models consistently outperformed their MLP counterparts across all sampling techniques and datasets, highlighting ResNet's superior ability to capture intricate patterns within the training data. This advantage is likely due to its deeper architecture and the benefits of residual learning mechanisms.
- Although ResNet typically offers a greater capacity for learning nuanced patterns, it is essential that the training data retain sufficient dimensionality. For example, in the Credit Card dataset, retaining 70% of the principal components ensured that more discriminative features were preserved.
- Conversely, if dimensionality is reduced too aggressively, such as retaining only 40% of the principal components in the BIS subset, key features may be lost. This reduction makes the classification task more challenging and diminishes the performance advantage of a deeper architecture, thereby narrowing the performance gap between ResNet and MLP.

### c) Single Model vs. SplitFed

- The experimental results clearly demonstrate that while standalone models perform adequately, the proposed SplitFed setup frequently outperforms them in terms of F1-score. This performance gap reaffirms the value of SplitFed learning in fraud or illicit activity detection.
- By distributing the model across multiple clients, the system aggregates knowledge from different segments of the data, leading to more robust decision boundaries, especially in imbalanced scenarios.
- Additionally, the SplitFed approach captures a wider variety of minority class patterns without directly transmitting sensitive data to the server. In this framework, data remains on the client devices; only the parameters and gradients from local client models are sent to the server for federated aggregation.

### d) Fine-tuning the best model

- To improve model accuracy, we explored fine-tuning the best-performing model, namely the SplitFed ResNet combined with CTGAN. Fine-tuning was performed by adjusting key parameters, including the hidden dimension, learning rate, and the number of residual blocks in the ResNet architecture.
- The results indicate that, after fine-tuning with a hidden dimension of 128, a learning rate of 0.005, and five residual blocks, the proposed model achieved an F1-score of 0.64.
- Fine-tuned ResNet model's test results:

Server	Hidden Dimension	Learning Rate	Residual Blocks	F1-score
SplitFed with ResNet and CTGAN	32	0.001	3	0.55
	64	0.001	5	0.61
	128	0.001	5	0.60
	<b>128</b>	<b>0.005</b>	<b>5</b>	<b>0.64</b>

## 6. Limitations and Future Considerations

### 1) Limitations:

#### a) **Accuracy of prediction can still be affected by PETs**

Since the prediction model can only take in PCs or singular matrices as inputs rather than the original variables, the model accuracy can still be affected by some loss of information in the reduced dataset as well as the noise from the differential privacy techniques.

#### b) **Communication overhead between the global and client's server increases as the number of clients increase**

More clients mean more communication between the client server and global server in FSL to pass information on the model updates and outputs e.g. activation functions, gradients, even though lesser than FL alone. A study suggests a global one-to-many broadcast route (instead of one-to-one broadcast) from the global server back to the client servers<sup>20</sup>.

#### c) **Model information can be compromised by malicious clients**

Although client's dataset is not transmitted and no server has the full model in SFL framework, the partial model information, e.g. gradients at the global server side, can still be compromised by malicious clients<sup>21</sup>. Hence, there is a need for proper governance and cybersecurity protocols to be put in place in the connectivity with the global server to regulate the client onboarding and ensure secured connectivity with the global servers.

<sup>20</sup> See Liang et al (2025).

<sup>21</sup> See Wu et al (2025).



## 2) Future considerations:

### a) **Explore other advanced PETS e.g. zero-knowledge proof**

We want to explore advanced PETS, e.g. zero-knowledge proof, that can allow FIs to share more sensitive information of the transaction (e.g. sender and receive profile) to improve model performance, while securing the information. Having more secured PETS can also facilitate compliance with various data protection regulations from different jurisdictions. However, the challenge is scalability as huge computing power is required for such PETS.

### b) **Explore multi-class and multimodal for prediction**

We can expand the binary prediction to a multi-class prediction to detect more specific illicit crimes. Also, we can explore multimodal prediction so that we do not have to limit to tabular data but can consider other forms of data e.g. text, images, biometric information.

## 7. Conclusion

Project Numa demonstrates that FedShield, a proof-of-concept for cross-border financial crime detection using PETS, machine learning and deep learning, offers a robust and secure framework for FIs to share payments data for better identification of financial crime in the payments system. A unique framework is presented in FedShield by combining the use of linear dimensionality reduction, differential privacy and split federated learning.

The experimental results show the potential of this framework in improving predictive accuracy while preserving data privacy. However, communication overhead and model information security remain a challenge to be addressed. Future work explores the inclusion of more advanced PETS and exploration of more prediction classes and data types to enhance the prediction use-cases in FedShield.

## 8. References

- Bank of International Settlements (BIS) (2023): "Project Aurora: the power of Data, Technology and Collaboration to Combat Money Laundering Across Institutions and Borders", May, "<https://www.bis.org/publ/othp66.pdf>".
- Banu, R Vidya, N. Nagaveni (2009): "Preservation of Data Privacy Using PCA Based Transformation", *Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, IEEE Computer Society*, October, "<https://doi.org/10.1109/ARTCom.2009.159>".
- Bu, Z., Dong, J., Long, Q., and Su, W. (2020): "Deep Learning With Gaussian Differential Privacy", *Harvard Data Science Review*, 2(3), "<https://doi.org/10.1162/99608f92.cfc5dd25>".
- Dataaspirant.com (2023): "Ultimate guide for using Truncated SVD for dimensionality reduction", "<https://dataaspirant.com/truncated-svd>".
- Finextra (2024): "Ecommerce fraud to exceed \$100bn by 2029", October, "<https://www.finextra.com/newsarticle/44835/ecommerce-fraud-to-exceed-100bn-by-2029>".
- Fan, L (2019): "Practical Image Obfuscation with Provable Privacy", *IEEE International Conference on Multimedia and Expo (ICME), Shanghai, China*, pp. 784-789.
- Frost, Jon, P Koo Wilkens, A Kosse, V Shreeti and C Velasquez (2024): "Fast payments: design and adoption", *BIS Quarterly Review*, March, "[https://www.bis.org/publ/qtrpdf/r\\_qt2403c.pdf](https://www.bis.org/publ/qtrpdf/r_qt2403c.pdf)".
- Halko, N, P G Martinsson, J A Tropp (2011): "Finding Structure with Randomness: Probabilistic Algorithms for Constructing Approximate Matrix Decompositions", *SIAM review* 53(2), 217-288, "<https://arxiv.org/pdf/0909.4061>".
- Khosravi, H, et al (2024): "Strategic data augmentation with CTGAN for smart manufacturing: Enhancing ML predictions of paper breaks in pulp-and-paper production", October, "<https://doi.org/10.1016/j.mfglet.2024.09.158>".
- Kulkarni, A. D. (2024): "Fuzzy Convolution Neural Networks for Tabular Data Classification", October, "<https://arxiv.org/abs/2406.03506>".
- Liang, Y., Chen, Q., Zhu, G., Awan, M.K., and Jiang, H. (2025): "Communication-and-Computation Efficient Split Federated Learning: Gradient Aggregation and Resource Management", January, "<https://arxiv.org/pdf/2501.01078>".

Lowy, A, and M. Razaviyayn (2021): "Output Perturbation for Differentially Private Convex Optimization: Faster and More General", February, "<https://arxiv.org/html/2102.04704v2>".

Machine Learning Group (2018). "Credit Card Fraud Detection", *Kaggle*, "<https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>".

Mishra, S, Sarkar, U, Taraphder, S, Datta, S, Swain, D, Saikhom, R. et al. (2017): "10.5455/ijlr.20170415115235.Multivariate Statistical Data Analysis- Principal Component Analysis (PCA)", *International Journal of Livestock Research*, 7(5), 60-78, "[https://www.researchgate.net/publication/316652806\\_Principal\\_Component\\_Analysis](https://www.researchgate.net/publication/316652806_Principal_Component_Analysis)".

Nasdaq and Verafin (2024): "2024 Global Financial Crime Report", January, "<https://elements.visualcapitalist.com/wp-content/uploads/2024/04/1711973384569.pdf>".

P. Bruno, U. Jennah (2024): "Global payments in 2024: Simpler interfaces, complex reality", October, "<https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-in-2024-simpler-interfaces-complex-reality>".

PYMNTS.com (2021): "Mastering Multichannel Commerce Playbook", March, "<https://www.pymnts.com/wp-content/uploads/2021/03/PYMNTS-Mastering-Multichannel-Commerce-Playbook%E2%80%93March-2021-2.pdf>".

Thapa, C., Arachchige, P. C. M., Camtepe, S., & Sun, L. (2022): "Splitfed: When federated learning meets split learning", *In Proceedings of the AAAI Conference on Artificial Intelligence, Jun*, (Vol. 36, No. 8, pp. 8485-8493).

Tianxi, J, P. Li (2024): "Less is more: revisiting the Gaussian mechanism for differential privacy", *In Proceedings of the 33rd USENIX Conference on Security Symposium (SEC '24). USENIX Association, USA*, Article 53, 937-954. "<https://arxiv.org/abs/2306.02256>".

WorldPay (2024): "9<sup>th</sup> Edition of the Global Payments Report 2024", "<https://worldpay.globalpaymentsreport.com/en>".

Wu, X, H Yuan, X Li, J Ni, R Lu (2025): ""Evaluating Security and Robustness for Split Federated Learning Against Poisoning Attacks," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 175-190, "<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10741585>".