Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures

Predictive Analytics for Cyber-Physical Threat Intelligence in Financial Sector Infrastructures – 14/01 -2021

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Predictive Analytics for Cyber - Physical Threat Intelligence in Financial Sector Infrastructures

Habtamu Abie
Norwegian Computing Center, FINSEC Project

Agenda

- What is predictive analytics
- Use case in Financial Services
- Findings
- Key takeaways

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

What is predictive analytics

Predictive analytics is the use of historical data and machine learning to develop mathematical models that can then be applied to predict what will happen next

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Predictive Analytics cyber-physical security

- Proactively identifying assets at risk
- Anticipating threats
- Prediction of attack indicators
- Filtering and prioritizing security risks
- Automated identification of security insights
- Providing earlywarning of abnormalities and irregularities

Use Case in Financial Services: Predictive Analytics Service for Security of Blockchain and Peer-to-Peer Payment Solutions

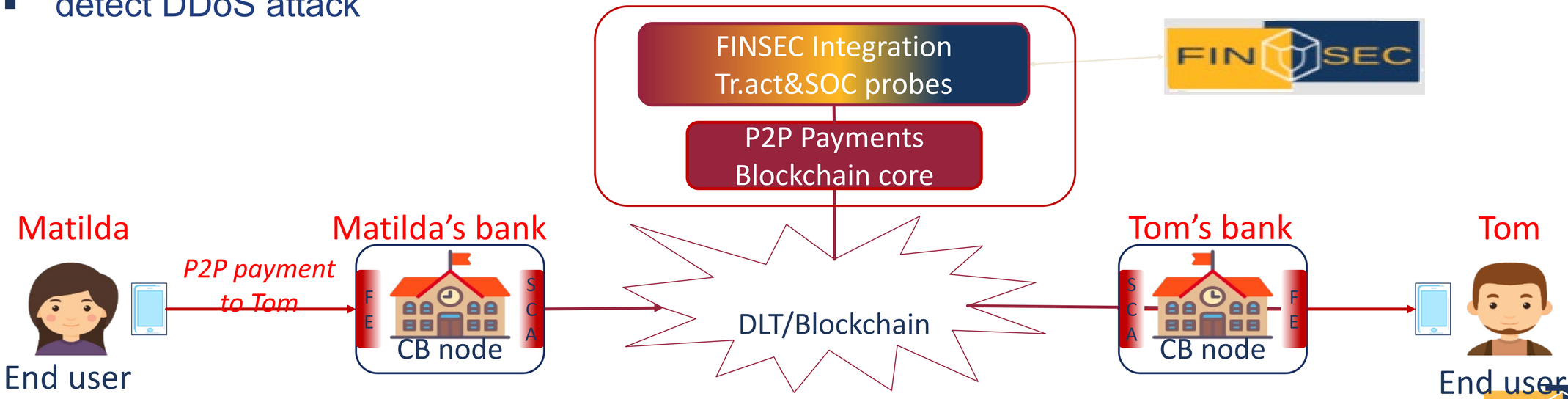
Background

- The financial sector is highly digitised and interconnected
  - BigData, Internet of Things (IoT), Artificial Intelligence (AI), blockchains, mobile Apps, Cloud services and web infrastructures
- Blockchain and P2P solutions become widely adopted by financial institutions to secure the payment system
  - the attackers follow the development by detecting and exploiting vulnerabilities in blockchain solutions
- An advanced cyber-defence infrastructure is required

Securing Blockchain Peer-to-Peer payments: monitor, detect and mitigate

- Demonstrate the capability of the FINSEC platform to predict and detect suspicious behaviors or attacks to a Blockchain based P2P Payments application
  - identify common trends
  - detection of abnormal behavior
  - critical node fault(s), node hijacking
  - overloading
  - detect DDoS attack

- Aim to secure the solution both at application and infrastructure level
- Two classes of use cases: security for alerting and transaction filtering

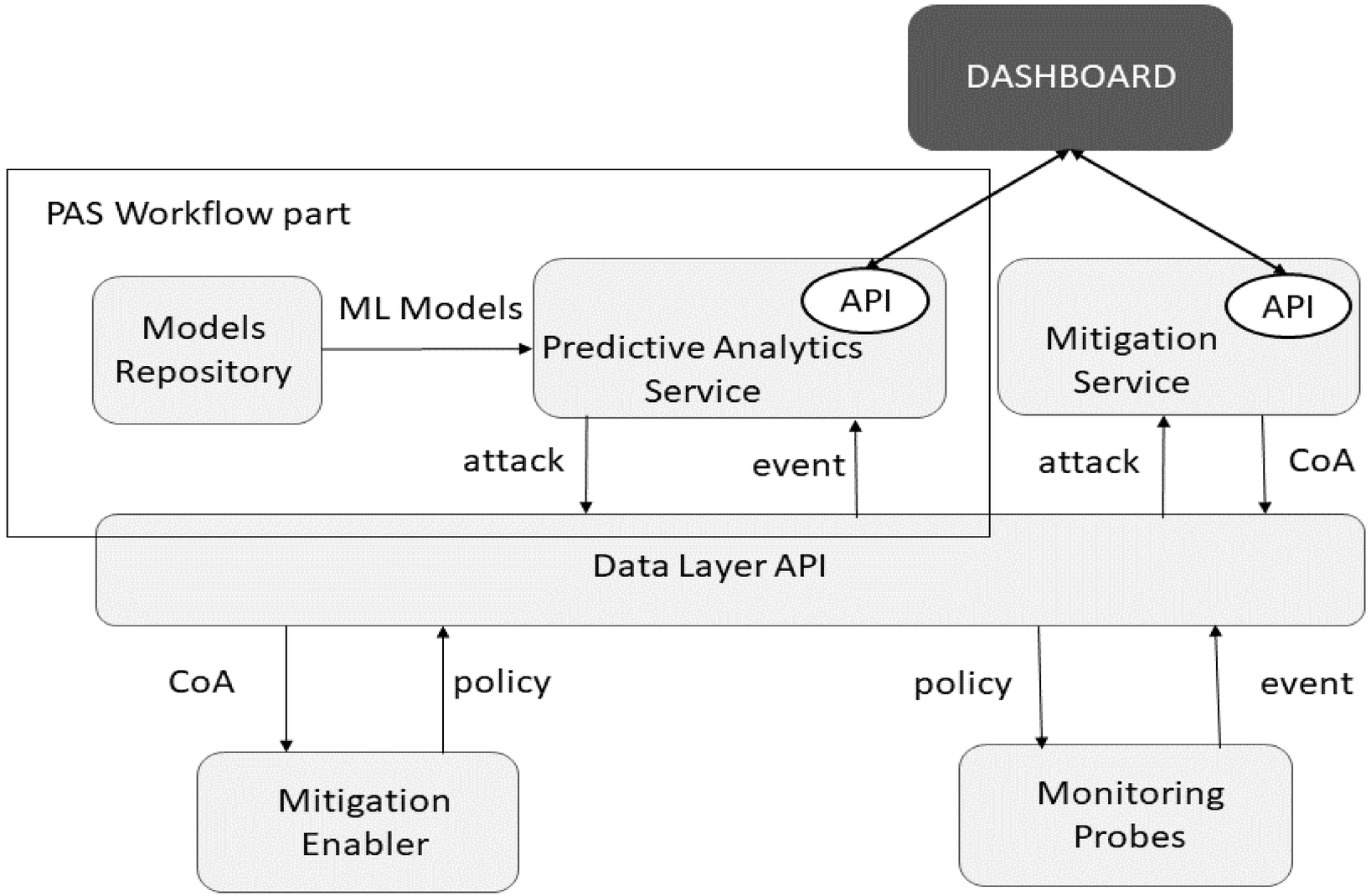


Environment

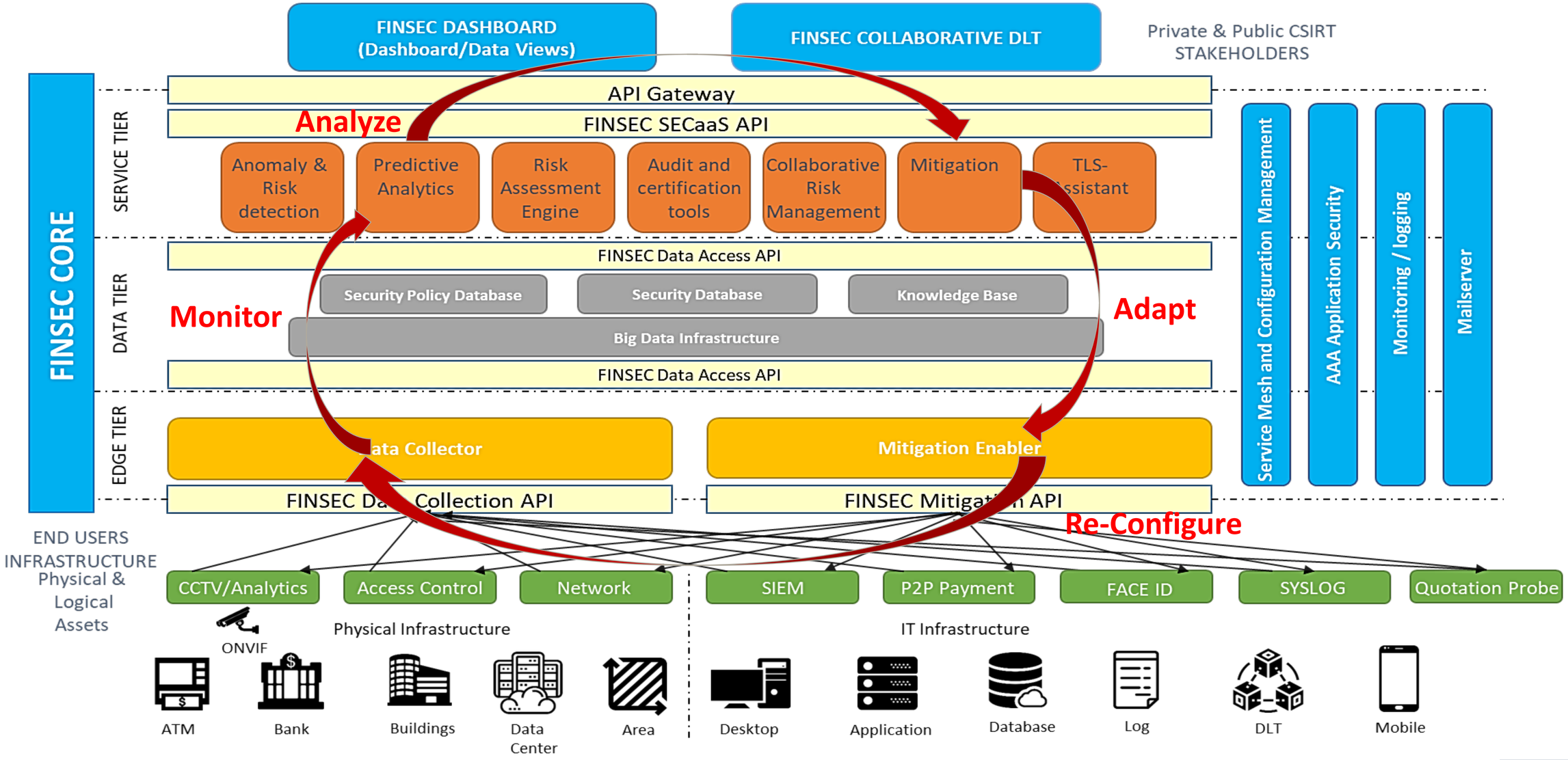
- A private and permissioned blockchain
- To identify abnormal behaviours
- To assess the blockchain network behaviour
- Datasets were produced separately
- Data were pre-processed in the temporal domain

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Predictive Analytics Service Workflow



Mapping to FINSEC Reference Architecture



Evaluated Algorithms

- Several ensemble methods (100, 200, 300 estimators)
  - Random Forest Classifier
  - AdaBoost Classifier
  - Gradient Boosting Classifier
  - Extreme Gradient Boosting
- Support Vector Machines
- Decision Tree Classifier
- K-Nearest Neighbors algorithm
- Stochastic Gradient Descent algorithm
- Multilayer Perceptron classifier

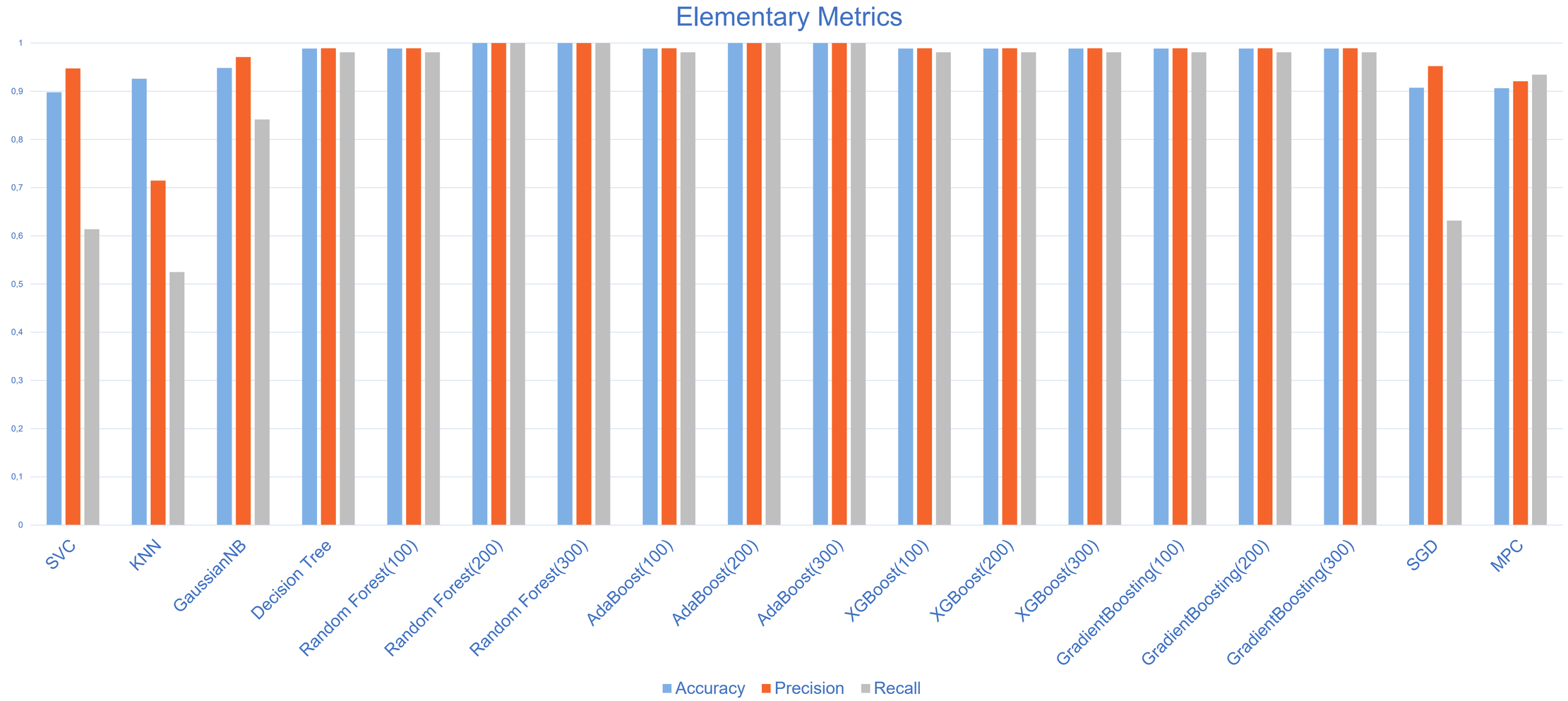
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Evaluation metrics

- Accuracy (*a*)
  - defines the ratio of correctly predicted values to the total number of values
- Precision (*p*)
  - the ratio of correctly predicted positive values to the total number of values predicted as positive
- Recall (*r*)
  - the ratio of correctly predicted positive values to all positive values
- Weighted average metric (*m*)
  - ä $= w_a a + w_p p + w_r r$

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

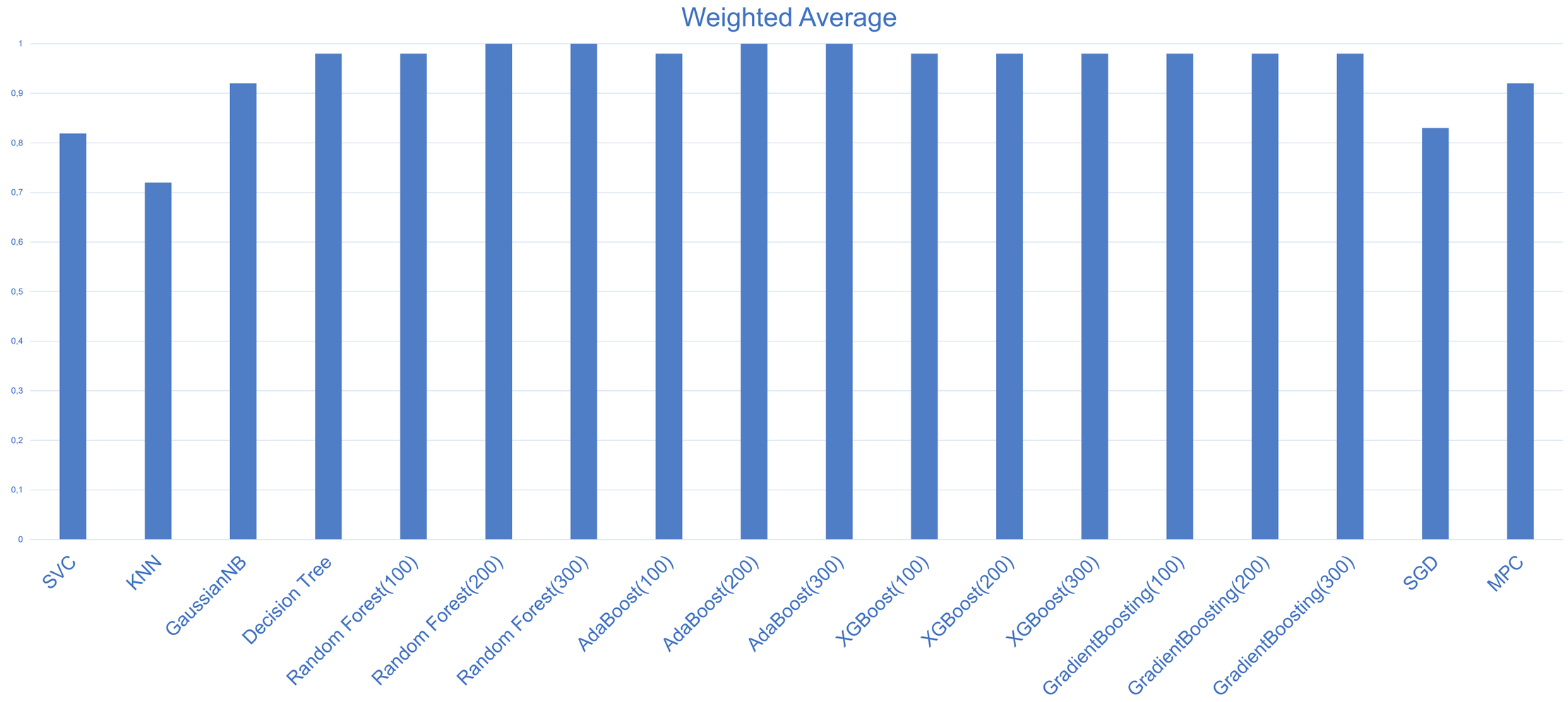
Results



We used predictive analytics service to predict cyber-physical attacks on Peer-to-Peer Payment Solution close to 99% accuracy, precision and recall

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Results



We used weighted average to evaluate the predictive analytics algorithms how good they predict cyber physical attacks on Peer-to-Peer Payment Solution with close to 99%.

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Key Takeaways: Predictive Analytics for Security

- Predictive analytics provides increased automation and flexibility
- Predictive analytics improves detection capability by correlating wide-ranging data sources
- Predicts cyber-physical security attacks, threats and anomalies and alerts security officers
- Triggering of preventive and mitigation measures in advance of the occurrence of the attacks
- Predictive analytics helps to thwart whatever attacks adversaries are attempting to launch
- Predictive analytics is enabling the computer to predict threats and observe any anomalies with a lot more accuracy than any human can.
- Predictive analytics helps to understand patterns of behavior which can then be used to identify activities that could compromise infrastructures and applications

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Thank You

habtamu.abie@nr.no

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727