Dealing with and Preventing Fraud via Privacy-Enhancing Technologies

PI: Prof. Steven Murdoch

RA: Aydin Abadi

Institution: UCL

Abstract

Many people and banks in the UK and all around the world have been suffering from various online payment frauds. In the PAYMENT project, we developed (1) technical solutions to help victims of fraud receive compensation for their financial losses and (2) Privacy-Enhancing Technologies (PETs) to help financial institutions and banks prevent fraud.

Helping Fraud Victims Receive Reimbursement

An "Authorised Push Payment" (APP) fraud is a type of cybercrime where a fraudster tricks a victim into making an authorised online payment into an account controlled by the fraudster. APP fraud has various variants, such as romance, investment, CEO, or invoice fraud.

The total amount of money lost to APP fraud is substantial. Only in the first half of 2021, a total of £355 million was lost to APP fraud, which has increased by 71% compared to losses reported in the same period in 2020. APP fraud is a global phenomenon. According to the FBI's report, APP fraud victims reported at least a total of $419 million in losses, in 2020. Recently, Interpol warned its member countries about a variant of APP fraud called investment fraud via dating software.

As part of the PAYMENT project, we have developed a technical solution (i.e., cryptographic protocol) to facilitate the compensation of APP fraud victims for their financial losses. The solution lets honest victims (of an APP fraud) independently prove their innocence to a third-party dispute resolver, in order to be reimbursed.

Our solution offers transparency by:

(i) formalising reimbursements conditions
(ii) offering traceability
(iii) providing an evidence-based final decision

It also offers accountability, as it is equipped with auditing mechanisms that help identify the party liable for an APP fraud loss. The auditing mechanisms themselves are accompanied by our privacy-preserving threshold voting protocols, which let auditors vote privately without having to worry about being retaliated against, for their votes.

We evaluated its asymptotic cost and runtime via a prototype implementation. Our evaluation showed that the protocol is efficient. It takes a dispute resolver 0.09 milliseconds to settle a dispute between the two parties.

Developing PETs to Prevent Fraud

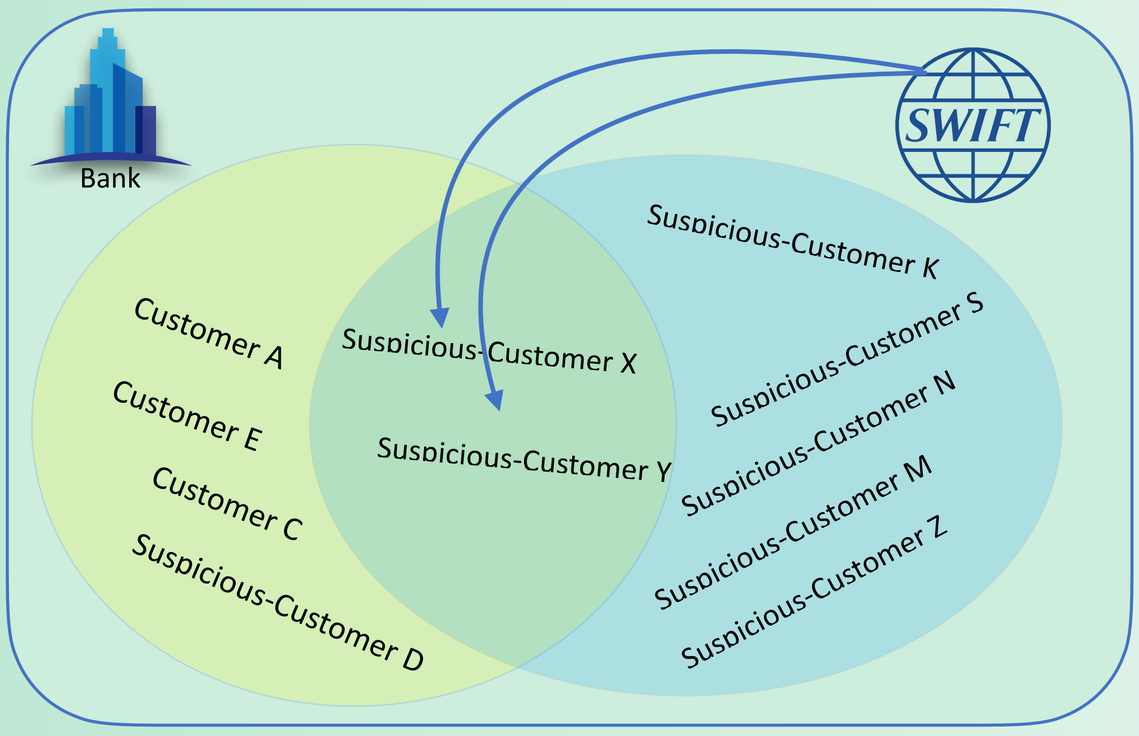

Fig 1. Private Set Intersection to find suspicious customers without violating other customers' privacy

Privacy-enhancing Technologies (PETs) such as Private Set Intersection (PSI) have been considered by the "Financial Action Task Force" as one of the vital tools for enabling collaborative analytics between financial institutions to strengthen "Anti-Money Laundering" (AML) and "Countering the Financing of Terrorism" (CFT) compliance. It can play also play a role in preventing APP fraud.

At UCL we have:

- invented new attacks that can be mounted at one of the state-of-the-art PSIs.
- developed a new PSI that incentives data owners to share their data and participate in a PSI.
- devised a new efficient PSI that allows parties to delegate the storage of their private data and the computation of PSI to a cloud server that itself can be untrusted. Our PSI allows parties to update their outsourced data securely.

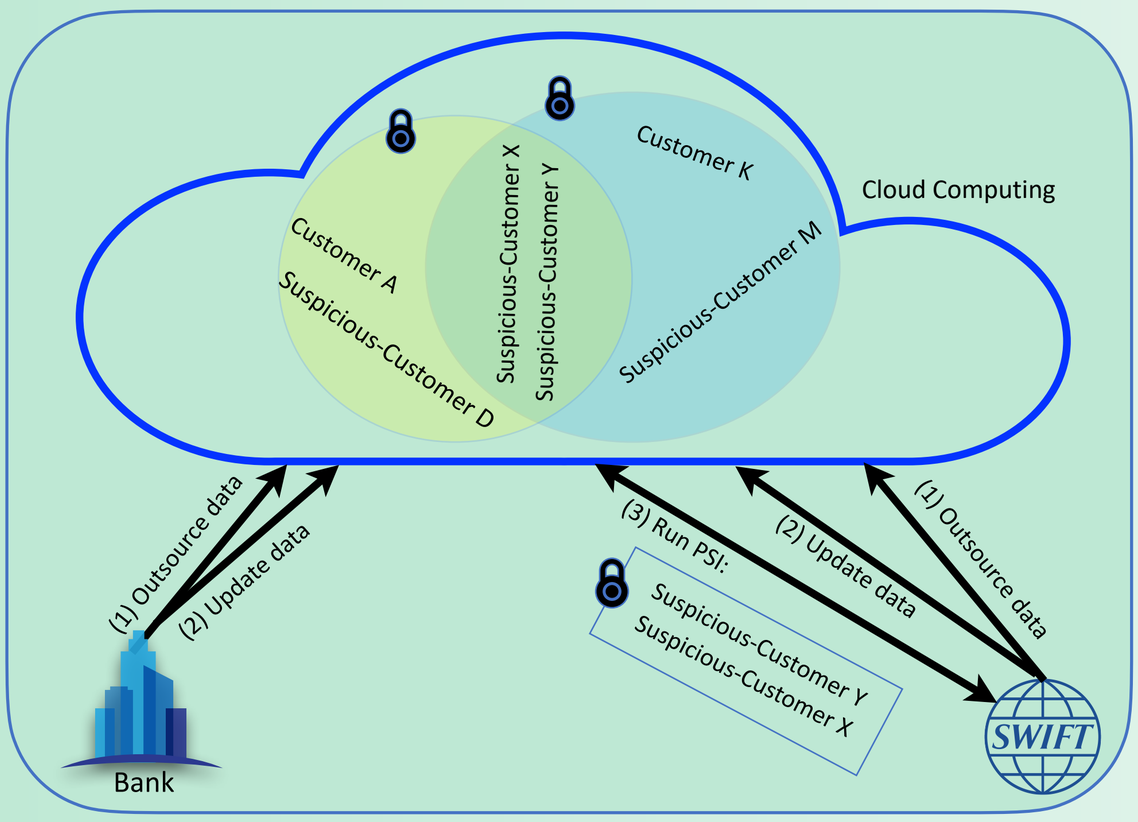

Fig 2. Delegated Private Set Intersection where storage and computation are outsourced to a powerful but untrusted cloud

For related publications and more details see: https://murdoch.is/:/payment

UK Research and Innovation · University of Bristol · UCL · University of Bath · The University of Edinburgh · King's College London