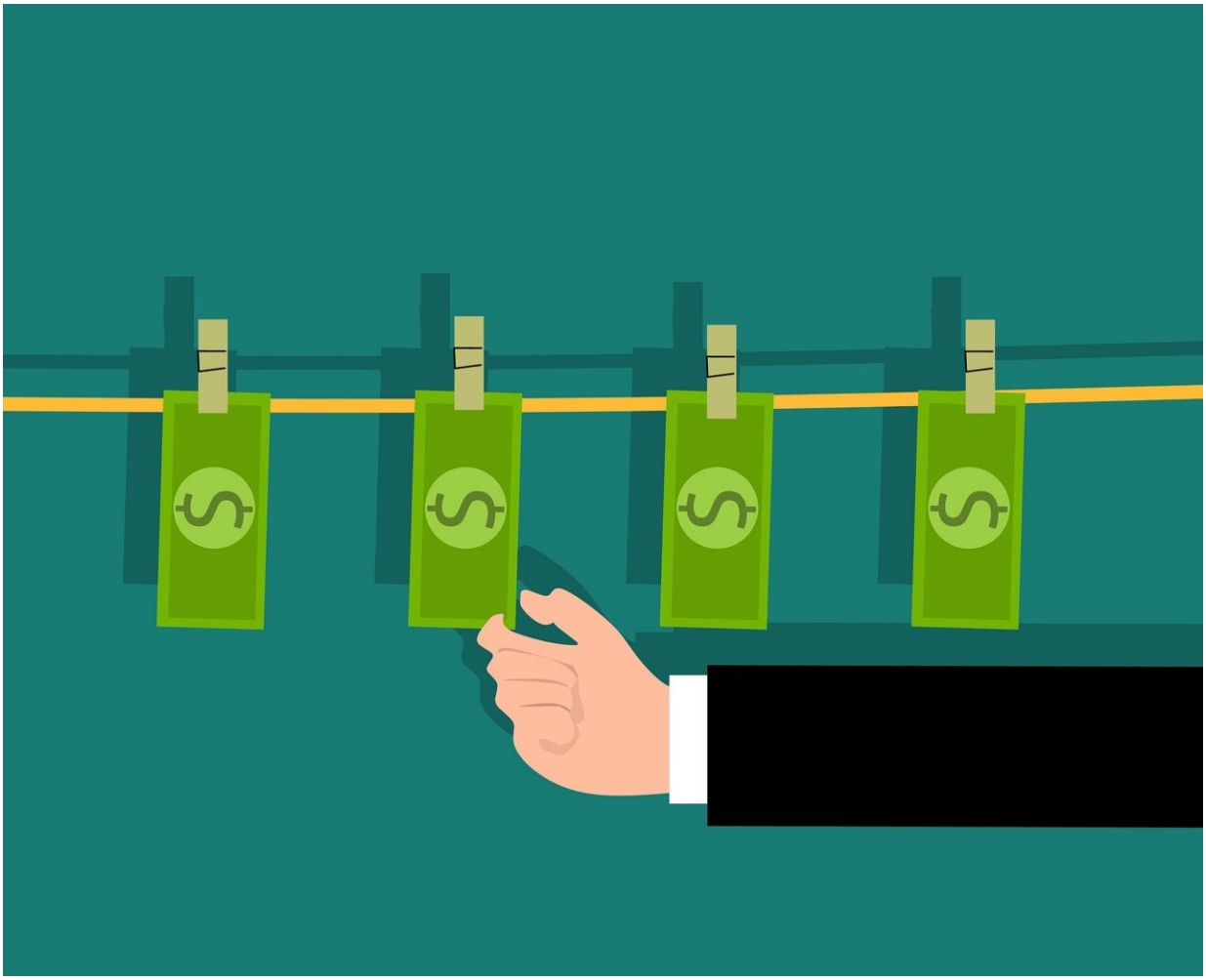
New software detects money laundering faster than ever before

September 22 2023



Credit: Pixabay/CC0 Public Domain

Computer scientists have developed a new tool that enables quicker and more accurate detection of money laundering, with the ability to scan 50 million transactions in less than a second.

Researchers from the Department of Informatics have designed an entirely novel approach to detecting money laundering, based on algorithms which rapidly identify when criminals are dividing a large sum of money into multiple smaller transactions between many bank accounts—a technique known as "smurfing."

The algorithms run on data taken from several bank accounts which are represented as nodes on a large, complex graph, and the software is programmed to focus on the part of the graph where it detects the most suspicious activity.

For example, if there is a deposit of one million pounds, the software can monitor where this exact sum of money is being transferred—it has the ability to identify all combinations of related transactions that take place, even if the money is split between different accounts and outgoings.

As detailed in a paper published in the *Proceedings of the 2023 SIAM International Conference on Data Mining*, lead researchers Dr. Huiping Chen and Dr. Grigorios Loukides, together with Dr. Robert Gwadera and Dr. Solon Pissis, say the new software is over three times more effective than current detection methods and can also analyze larger amounts of data.

Current money laundering detection methods are rule-based or machine-learning (ML) based, which involve automated money laundering detection alarms set off by "suspicious" transaction scenarios like excessive cash deposits or process large sets of transaction histories to spot possible money-laundering activity along pre-set lines. These

methods can be ineffective or slow to uncover instances of the crime, especially with the practice of smurfing.

Both existing methods also require domain knowledge—for example, a bank must have successfully caught attacks in the past and used them to detect other attacks. If an organization does not have that data, which can be the case when dealing with novel or evolving money laundering methods, then that means reduced accuracy.

Dr. Chen, a Ph.D. student at the Department of Informatics, said, "Money laundering presents a major global challenge. Developing a quicker and more effective approach to detecting this criminal activity signals a major step in the right direction to address the issue and provide reassurance for financial institutions."

The United Nations Office on Drugs and Crime (UNODC) estimates that between 2% and 5% of global GDP is laundered each year, roughly between £632 billion and over £1.5 trillion.

Dr. Loukides states, "We have developed an optimal method that can find the best possible solution for detecting common classifications of smurfing attacks across millions of amounts of data, on average 3.2 times more effectively than the state-of-the-art methods currently used.

"Our tool is also more automated and enables a far more rapid analysis of the data than what's currently available. By allowing money laundering experts to survey vast amounts of data faster than ever before, we can empower them to pick up on actors with bad intent efficiently.

"We are now working to improve the tool further, with the aim of delivering a quicker speed than conventional approaches but with even higher accuracy."

The software for the new tool is open source and freely available to access. Because it can be used with much larger amounts of data than conventional detection methods, researchers say it can analyze large amounts of data over long periods of time, filtering out and sounding an alarm to indicate to the bank when it detects suspicious activity.

The approach has been tested using real data from an anonymous Czech bank, and on fictional cases based on predictions of common patterns and activity present in cases of real money laundering. In both instances, the algorithms were able to detect all suspicious patterns in the transactions.

Researchers say the new tool also has potential use beyond the detection of suspicious financial activity, as it could optimize marketing campaigns by enabling retailers to find and detect the most profitable bundles of products; improving the accuracy of retail data at speed.

More information: Huiping Chen et al, Heavy Nodes in a Small Neighborhood: Algorithms and Applications, *Proceedings of the 2023 SIAM International Conference on Data Mining (SDM)* (2023). DOI: 10.1137/1.9781611977653.ch35

Provided by King's College London