Current processes to extract and load this off-line data into the fraud processing engine take an excessive amount of time to plan and implement. The need to create code, modify jobs and the use of a "waterfall" methodology does not provide for an easy solution to this problem. Additionally, resources needed to perform these tasks are often already working on other tasks. Placing the tasks in queue for the resources to become available further delays the time it takes to implement changes that permit this off-line data to be made accessible to the fraud processing engine system.

BRIEF DESCRIPTION

In one aspect, there is provided a computer-implemented method of modifying an execution of a processing system during runtime, the processing system including at least one computing device including a fraud risk management (FRM) module and communicatively coupled to a payment card network, said method comprising: receiving, from the payment card network, by the at least one computing device including the FRM module, at least some of a plurality of payment card transactions being processed by the payment card network; processing, by the at least one computing device including the FRM module, the at least some of the plurality of payment card transactions to detect fraudulent transactions using a plurality of rules; receiving, by the at least one computing device including the FRM module, an indication of a fraud attack on the payment card network; generating, by the at least one computing device including the FRM module, in response to the received indication of the fraud attack, new rules related to remediating the fraud attack; defining, by the at least one computing device including the FRM module, a user defined table (UDT) that includes metadata specifying the new rules; storing the metadata for the UDT in a run-time server (RTS) database; and periodically executing, by the at least one computing device including the FRM module, a job, wherein periodically executing the job includes: reading the metadata stored in the RTS database; and modifying a workflow of the processing system during runtime to cause the processing system to detect fraudulent transactions using the new rules specified in the metadata.

In another aspect, there is provided a processing system including a fraud risk management (FRM) module, the processing system capable of modifying an execution of the processing system during runtime, the processing system

communicatively coupled to a payment card network, the processing system comprising: one or more memory devices; and one or more processors communicatively coupled to said one or more memory devices, said one or more memory devices including computer-executable instructions that when executed by the one or more processors cause the one or more processors to perform the programmed steps of: receiving, from the payment card network, at least some of a plurality of payment card transactions being processed by the payment card network; processing the at least some of the plurality of payment card transactions to detect fraudulent transactions using a plurality of rules; receiving an indication of a fraud attack on the payment card network; generating, in response to the received indication of the fraud attack, new rules related to remediating the fraud attack; defining, by the at least one computing device including the FRM module, a user defined table (UDT) that includes metadata specifying the new rules; storing the metadata for the UDT in a run-time server (RTS) database; and periodically executing a job, wherein periodically executing the job includes: reading the metadata stored in the RTS database; and modifying a workflow of the processing system during runtime to cause the processing system to detect fraudulent transactions using the new rules specified in the metadata.

In yet another aspect, there is provided one or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor of a processing system including a fraud risk management (FRM) module, the computer-executable instructions cause the at least one processor to: receive, from a payment card network, at least some of a plurality of payment card transactions being processed by the payment card network; process the at least some of the plurality of payment card transactions to detect fraudulent transactions using a plurality of rules; receive an indication of a fraud attack on the payment card network; generate, in response to the received indication of the fraud attack, new rules related to remediating the fraud attack; define a user defined table (UDT) that includes metadata specifying the new rules; store the metadata for the UDT in a run-time server (RTS) database; and periodically execute a job, wherein periodically executing the job includes: reading the metadata stored in the RTS database; and modifying a workflow of the processing system during runtime to cause the processing system to detect fraudulent transactions using the new rules specified in the metadata.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1-13 show example embodiments of the methods and systems described herein.

FIG. 1 is a schematic diagram illustrating an example multi-party payment card industry system with a fraud risk management (FRM) module.

FIG. 2 is a simplified block diagram of an example payment processing system including a plurality of computer devices including the FRM module in accordance with one example embodiment of the present disclosure.

FIG. 3A is an expanded block diagram of an example embodiment of a server architecture of the payment processing system including the FRM module.

FIG. 3B shows a configuration of a database within the database server of the server system shown in FIG. 1 with other related server components.

FIG. 4 illustrates an example configuration of a user system operated by a user, such as the cardholder shown in FIG. 1.

FIG. 5 illustrates an example configuration of a server system such as the server system shown in FIGS. 2 and 3.

FIG. 6 is a data flow diagram for modifying an execution of a processing system such as the FRM module shown in FIG. 1 during runtime.

FIG. 7 is a tool architecture for producing jobs that when run update a user-defined table (UDT) to inject updated data and/or instructions into the process executing on the fraud risk management module shown in FIG. 1.

FIG. 8 is a batch process workflow of the FRM module shown in FIG. 1.

FIG. 9 is a data flow diagram of the FRM module illustrating sources of data used in building the UDT shown in FIG. 6.

FIG. 10 is a listing of the UDT shown in FIG. 6 in accordance with an example embodiment of the present disclosure.

WHAT IS CLAIMED IS:

1. A computer-implemented method of modifying an execution of a processing system during runtime, the processing system including at least one computing device including a fraud risk management (FRM) module and communicatively coupled to a payment card network, said method comprising:

receiving, from the payment card network, by the at least one computing device including the FRM module, at least some of a plurality of payment card transactions being processed by the payment card network;

processing, by the at least one computing device including the FRM module, the at least some of the plurality of payment card transactions to detect fraudulent transactions using a plurality of rules;

receiving, by the at least one computing device including the FRM module, an indication of a fraud attack on the payment card network;

generating, by the at least one computing device including the FRM module, in response to the received indication of the fraud attack, new rules related to remediating the fraud attack;

defining, by the at least one computing device including the FRM module, a user defined table (UDT) that includes metadata specifying the new rules;

storing the metadata for the UDT in a run-time server (RTS) database; and

periodically executing, by the at least one computing device including the FRM module, a job, wherein periodically executing the job includes:

reading the metadata stored in the RTS database; and

modifying a workflow of the processing system during runtime to cause the processing system to detect fraudulent transactions using the new rules specified in the metadata.

2. The computer-implemented method of Claim 1, wherein the metadata further specifies a change data capture (CDC) type, and wherein the method further comprises performing, by the at least one computing device including the FRM module, a change data capture process using a previously defined table when a DELTA CDC type is specified.

3. The computer-implemented method of Claim 1, wherein the metadata further specifies a data source.

4. A processing system including a fraud risk management (FRM) module, the processing system capable of modifying an execution of the processing system during runtime, the processing system communicatively coupled to a payment card network, the processing system comprising:

one or more memory devices; and

one or more processors communicatively coupled to said one or more memory devices, said one or more memory devices including computer-executable instructions that when executed by the one or more processors cause the one or more processors to perform the programmed steps of:

receiving, from the payment card network, at least some of a plurality of payment card transactions being processed by the payment card network;

processing the at least some of the plurality of payment card transactions to detect fraudulent transactions using a plurality of rules;

receiving an indication of a fraud attack on the payment card network;

generating, in response to the received indication of the fraud attack, new rules related to remediating the fraud attack;

defining, by the at least one computing device including the FRM module, a user defined table (UDT) that includes metadata specifying the new rules;

storing the metadata for the UDT in a run-time server (RTS) database; and

periodically executing a job, wherein periodically executing the job includes:

reading the metadata stored in the RTS database; and

modifying a workflow of the processing system during runtime to cause the processing system to detect fraudulent transactions using the new rules specified in the metadata.

5. One or more non-transitory computer-readable storage media having computer-executable instructions embodied thereon, wherein when executed by at least one processor of a processing system including a fraud risk management (FRM) module, the computer-executable instructions cause the at least one processor to:

receive, from a payment card network, at least some of a plurality of payment card transactions being processed by the payment card network;

process the at least some of the plurality of payment card transactions to detect fraudulent transactions using a plurality of rules;

receive an indication of a fraud attack on the payment card network;

generate, in response to the received indication of the fraud attack, new rules related to remediating the fraud attack;

define a user defined table (UDT) that includes metadata specifying the new rules;

store the metadata for the UDT in a run-time server (RTS) database; and

periodically execute a job, wherein periodically executing the job includes:

reading the metadata stored in the RTS database; and

modifying a workflow of the processing system during runtime to cause the processing system to detect fraudulent transactions using the new rules specified in the metadata.

6. The non-transitory computer-readable storage media of Claim 5, wherein the metadata further specifies a data source.