Technical background for IBM Safer Payments

Architecture – Technology – Scaling

Contents

Introduction

IBM® Counter Fraud Management for Safer Payments is a standard software product for the prevention of abuse and fraud in any payment channel. This white paper explains its architecture, technology, and scaling considerations.

Objectives and specifications

IBM Safer Payments was developed with the following key objectives:

- Ultra-high real-time performance to process thousands of transactions per second with latencies of a few milliseconds. The current largest customer installation of IBM Safer Payments is sized for 4,000 transactions per second with guaranteed latency of 3.5 milliseconds.
- Maximum availability by designing IBM Safer Payments as a clustered system in which full operation is maintained as long as there is still one clustered instance operational. All customer installations of IBM Safer Payments are operated for availability of 99.999%.
- Simple installation, integration, and operation by complete integration of database, application server, and replication layer within the application. A recent implementation project for a customer processing seven billion financial transactions per year was completed in only five weeks.

Requirements and software technology

Fraud prevention requires high performance:

- Fraud patterns are getting more complex all the time, and thus increase computational demands for behavior profiling and pattern recognition.
- The artificial intelligence algorithms used to automatically create fraud prevention models require big data performance.
- Users of IBM Safer Payments need to be able to assess the impact of model changes or new fraud countermeasures for many millions of transactions within few seconds.

To deliver performance of this magnitude, IBM Safer Payments utilizes massive parallel computing—critical computations scale linearly with the number of CPU cores available. IBM Safer Payments is written in C/C++, the programming language of choice for any application requiring massive performance.

IBM Safer Payments is designed for full 24/7 operations and uses service-oriented architecture in which all tasks and jobs are spun off in their own separate thread, so that they can all be run in parallel to real-time operations.

User access is facilitated by standard web browsers, which can be operated on PC, tablet, and smartphone. The IBM Safer Payments user interface combines the advantage of a light web browser interface with the efficiency and comfort of a locally installed software product. This is achieved using an AJAX and JavaScript-based component in MVC architecture that requires no plug-in within the web browser.

Cluster architecture

An installation of IBM Safer Payments consists of a cluster of identical IBM Safer Payments instances. Interfaces connect the instances with each other and with external systems as shown in figure 1.

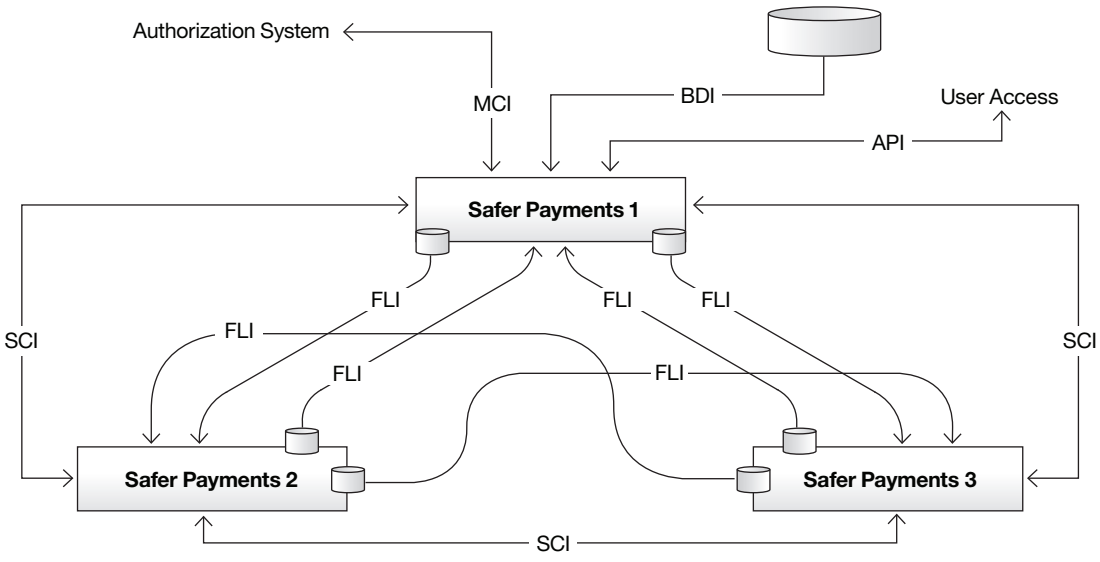

Figure 1: IBM Safer Payments is deployed as a cluster of identical instances.

Most clusters of IBM Safer Payments use three IBM Safer Payments instances for a number of reasons:

- If one IBM Safer Payments instance is shut down for hardware or software maintenance, such as patching, the operation is still supported by two redundant instances.
- Operational availability of the cluster of 99.999% can be achieved.
- IBM Safer Payments instances frequently are operated in physically separated data centers to protect operations against environmental risk.

The IBM Safer Payments instances within the cluster are connected by two internal, IP-based interfaces:

- FLI–FastLink Interface. Replicates transaction and configuration data. FLI is buffered so that temporary outages of network connections or instances are tolerated.
- SCI–Status Control Interface. Negotiation channel between instances, controls cluster functions and exchanges status data.

Additional interfaces connect the IBM Safer Payments cluster with external systems:

- MCI–Message Command Interface. Accepts and responds to XML formatted computation request transactions IP, https, IBM MQSeries®, and other transportation layers.
- BDI–Batch Data Interface. Complete ETL job engine that allows loading all data streams of the MCI as files in standard formats (CSV, fixed column, XML, and others).
- API–Application Programming Interface. The API is both IBM Safer Payments interface for custom extensions of its functionality, as well as the only interface for its browser based user access.

Since each IBM Safer Payments instance can access all other IBM Safer Payments instances via the SCI and perform all maintenance and control functions, there is no need for a central administration instance. Rather all cluster functions can be controlled from each of the IBM Safer Payments instances.

In an IBM Safer Payments cluster, MCI interfaces of all IBM Safer Payments instances are active and can process real-time transactions at any time. External systems connecting to the MCI can switch to any other IBM Safer Payments instance whenever there is a failure or network timeout with the one currently used.

If any of the IBM Safer Payments instances has downtime (scheduled maintenance or failure) when this instance restarts, it initiates communication with the other instances via SCI. It then negotiates with the other instances which transaction and configuration data it missed during its downtime and obtains this data from the other instances while they still serve full operations. Once this replication is complete, the restarted instance reports itself for duty by opening its MCI interface to the incoming transaction requests. All this is automatic and does not require any administrator intervention.

This functionality also supports:

- Updating software, operating system, and hardware components of individual instances in full operation of the cluster.
- Simple addition of new IBM Safer Payments instances into the IBM Safer Payments cluster in full flight.

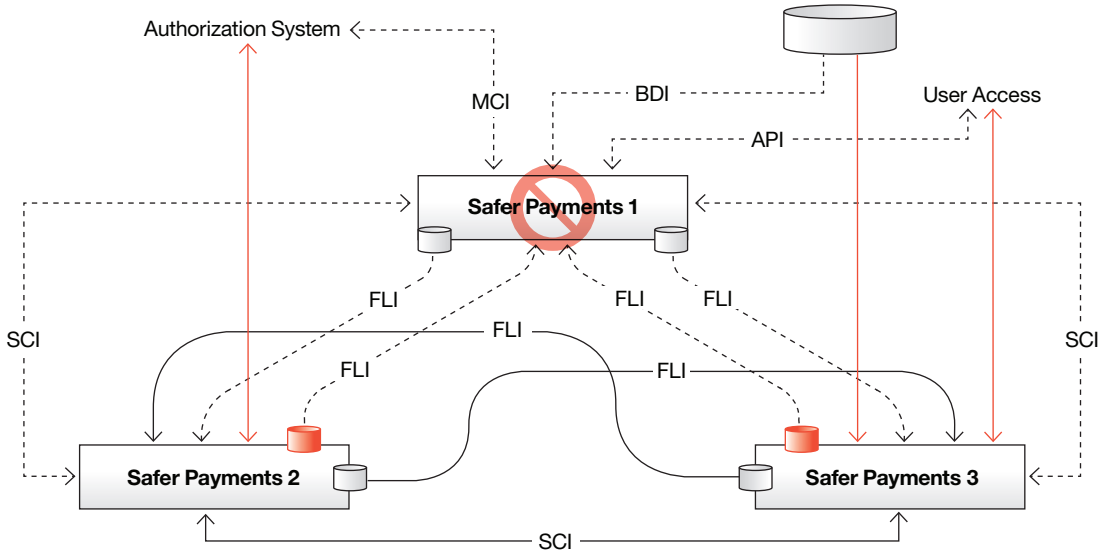

Figure 2: Once an IBM Safer Payments instance becomes unavailable, the other instances take over the full workload.

Purpose-built database

To securely detect even complex fraud patterns in real time, many hundred data points must be accessed for each transaction request. However, processing multiple hundreds or thousands of transactions requests per second that each require many hundreds of data points to be accessed overwhelms conventional, general-purpose database technology.

This is why IBM Safer Payments uses a purpose-built database that is based on not-only SQL and in-memory technologies. On top of this, IBM Safer Payments reaches significant further performance gains by running its real-time profiling and pattern recognition algorithms directly on the lowest data access level.

There are a number of additional advantages of using a purpose-built database:

- In addition to faster transaction processing, general database queries are significantly faster compared to general-purpose databases. Users often run database queries in IBM Safer Payments that traditionally were run in other systems since IBM Safer Payments responded 100 to 1,000 times faster during internal testing at IBM.

- Because the IBM Safer Payments database is completely embedded into IBM Safer Payments, installation and operation is greatly simplified. All information for the configuration and parameterization of the database is already contained in IBM Safer Payments so maintenance of the database reduces to zero.
- Any re-configuration of IBM Safer Payments can be done by fraud prevention experts themselves since consequential changes in the database are all automatically made by IBM Safer Payments.
- Even complex changes to the IBM Safer Payments data model can be committed in full flight, so that no real-time transaction is delayed.
- The embedded replication layer enables high availability without any additional component or any need of configuration or manual control.

The IBM Safer Payments database purpose-built compression that exploits the specific structure of payment data to significantly reduce main memory and disk space requirements. This allows IBM Safer Payments applications to store many years of full transaction history with modest hardware sizing.

Simulation, analysis and modeling

IBM Safer Payments comprises all analytics and simulation tools needed to continuously monitor the business performance of IBM Safer Payments, and to adapt the decision model to emerging and modified fraud patterns.

IBM Safer Payments continuously monitors the efficacy of all defined fraud countermeasures and decision rules, highlighting the ones that demonstrate declining performance over time to the fraud experts for review.

At the same time, IBM Safer Payments' artificial intelligence algorithms devise new fraud countermeasures and rules automatically from its internal database and presents them to the users for review.

The priority controller for IBM Safer Payments ensures that all computational resources are efficiently allocated. Since the computational performance of IBM Safer Payments servers are typically sized for maximum peak transaction load, in normal operational conditions most of the computational resources remain unused. IBM Safer Payments puts these resources to action by pre-computing complex statistical scenarios and using artificial intelligence algorithms to devise fraud countermeasure proposals.

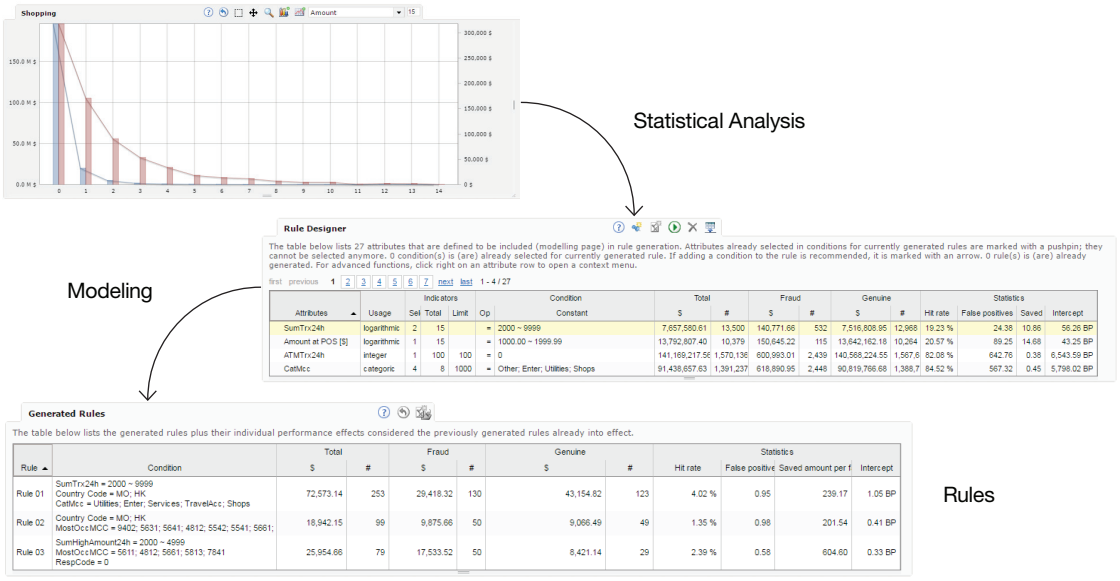

Figure 3: All simulation, analysis, and modeling functions are available through a web interface.

To safeguard that in peak load situations, processing of transactions in real time is never slowed down; the IBM Safer Payments priority controller reallocates computational resources within microseconds.

Platform

IBM Safer Payments can run on various hardware and software platforms. Many users of IBM Safer Payments opt for a combination of Intel Xeon-based server hardware and Linux (such as Red Had Enterprise Linux, Oracle Linux, CentOS)–this platform provides a favorable price/performance ratio, while IBM Safer Payments reaches high availability because of its inherent cluster architecture.

Since IBM Safer Payments embeds all components necessary for operation (database, high availability replication, application server, monitoring, and middleware), no other software component than the bare operating system is needed.

IBM Safer Payments is installed in minutes and immediately ready for operations. The IBM Safer Payments binary is distributed as a RPM package and also as manually installable archive.

Most users of IBM Safer Payments employ server virtualization and storage area network products. IBM Safer Payments is tested to run well with all standard products of this type.

IBM Safer Payments contains a fully configurable dashboard with key performance indicator monitoring, interactive drill down, and alarm management. In addition, centralized incident reporting (SNMP) and logging systems (syslog) can be connected to IBM Safer Payments to facilitate data center integration.

User accounts can be maintained locally in IBM Safer Payments, or served centrally by LDAP / Active Directory. IBM Safer Payments also supports optional two-factor authentication for user access.

IBM Safer Payments supports all standard backup systems.

All functions of IBM Safer Payments, including administrative and non-administrative processes, can also be controlled externally from scripts. This enables full automation of any administrative processes in a data center.

Additional detail

Other technical properties of IBM Safer Payments are:

- IBM Safer Payments uses both horizontal and vertical scaling to adapt to the needs of the application. Vertical scaling enables it to protect even the largest portfolios in the world in real time from fraud. Horizontal scaling enables IBM Safer Payments to achieve high levels of availability, since full operation is maintained with just one instance of IBM Safer Payments still running.
- The software and database technology of IBM Safer Payments are highly efficient. A commodity server with a single small Intel Xeon E3-1231V3 CPU in a standard card issuing application will process up to 1,000 transactions per second with maximum latency of 10 milliseconds.
- IBM Safer Payments is PCI PA-DSS certified. This implies that the highest standard of data security and data consistence of the payment industry are maintained. It also helps ensure that all development and quality assurance processes are in line with the highest standards of the industry. If you operate under PCI DSS scope, you do not need to include IBM Safer Payments in any certification; you may simply present our certificate to your PCI QSA.

For more information

To learn more about IBM Counter Fraud Management for Safer Payments, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/saferpayments

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Intel Xeon is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Please Recycle

WGW03260-USEN-01