

Online Transaction Processing

By
Team 8

Jing Sun
class ID: 28
University of Rochester
111 Elmerston Road
Rochester, NY, US
+1(585)2851779
jsun35@cs.rochester.edu

Xingdi Tan
Class ID: 79
University of Rochester
60 Crittenden Blvd
Rochester, NY, US
+1(716)262-5591
xtan9@cs.rochester.edu

ABSTRACT

In this paper, we describe the definition of online transaction processing (OLTP) and how to solve security problems.

Nowadays, an increasing number of online transactions are requesting for information retrieved from database, which means many clients based on different computer platforms may access to the database simultaneously. Databases must often allow the real-time processing of SQL transactions to support e-commerce and other time-critical applications. [3] So, the concurrency, efficiency, simplicity, correction for users to use the database information came to our priority topic. Meanwhile the safety for online transaction which ensures every item of transfer between different accounts, cards, and people can go to the correct place also invokes our huge consideration.

1. INTRODUCTION

1.1 Definition of OLPC

Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. [1]

The term “transaction” has different meanings in different scenarios. It typically refers to data entry and retrieval transactions in several industries, including banking, airlines, mail-order, supermarkets, and manufacturers. In the context of business or commercial transactions, OLTP refers to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application. In computer science, transaction processing is information processing that is divided into individual, indivisible operations, called transactions. Each transaction must succeed or fail as a complete unit; it cannot remain in an intermediate state. [1]

Online transaction processing increasingly requires support for transactions that span a network and may include more than one company. For this reason, new OLTP software uses client/server processing and brokering software that allows transactions to run on different computer platforms in a network. In large applications, efficient OLTP may depend on sophisticated transaction management software (such as CICS) and/or database optimization tactics to facilitate the processing of large numbers of concurrent updates to an OLTP-oriented database. For even

more demanding Decentralized database systems, OLTP brokering programs can distribute transaction processing among multiple computers on a network. OLTP is often integrated into service-oriented architecture (SOA) and Web services.

1.2 Advantages and Disadvantages

1.2.1 Advantages

simplicity and efficiency are two key benefits of Online Transaction Processing. Reduced paper trails and the faster, more accurate forecasts for revenues and expenses are both examples of how OLTP makes things simpler for businesses.

Online Transaction Processing (OLTP) has the following advantages:

- It provides faster and more accurate forecast for revenues and expenses.
- It provides a concrete foundation for a stable organization because of timely modification of all transactions.
- It makes the transactions much easier on behalf of the customers by allowing them to make the payments according to their choice.
- It broadens the customer base for an organization by simplifying and speeding up individual processes.

1.1.2 Disadvantages

As with any information processing system, security and reliability are considerations. Online transaction systems are generally more susceptible to direct attack and abuse than their offline counterparts. When organizations choose to rely on OLTP, operations can be severely impacted if the transaction system or database is unavailable due to data corruption, systems failure, or network availability issues. Additionally, like many modern online information technology solutions, some systems require offline maintenance which further affects the cost-benefit analysis.

Online Transaction Processing (OLTP) has the following disadvantages:

- It makes the database much more susceptible to intruders and hackers because it makes the database available worldwide.
- For B2B (business-to-business) transactions, businesses

must go offline to complete certain steps of an individual process, causing buyers and suppliers to miss out on some of the efficiency benefits that the system provides. As simple as OLTP is, the simplest disruption in the system has the potential to cause a great deal of problems, causing a waste of both time and money.

□ It can lead to server failure, which may cause delays or even wipe out large amounts of data from the database.

1.3 Transactions In SQL

In a program, multiple statements can be grouped together as an transaction. Grouping other actions (read & write) into transactions help with two goals. The first one is recovery and durability. It means keeping Database Management System data consistent and durable in the face of crashes, aborts, system shutdowns, etc. Recovery and durability is essential for reliable Database Management Systems usage. The Database Management Systems may experience crashes, such as power outages. Additionally, individual transactions may be aborted by users.

For example:

Client1:

```
INSERT INTO SmallProduct(name, price)
```

```
SELECT pname, price
```

```
FROM Product
```

```
WHERE price <= 0.99
```

```
DELETE FROM Product
```

```
WHERE price <=0.99
```

The idea to achieve this goal is to make sure that transactions are either durably stored in full, or not at all; keep log to be able to “roll-back” transactions. Code below shows one possible protection against crashes and aborts.

Client 1:

```
START TRANSACTION
```

```
INSERT INTO SmallProduct(name, price)
```

```
SELECT pname, price
```

```
FROM Product
```

```
WHERE price <= 0.99
```

```
DELETE FROM Product
```

```
WHERE price <=0.99
```

```
COMMIT OR ROLLBACK
```

The second goal is concurrency, which means achieving better performance by parallelizing transactions without creating anomalies. We will discuss concurrency in the next section. Concurrent execution of user programs is essential for good Database Management Systems performance. There are two problems that are needed to be solved. The first one is that disk accesses may be frequent and slow. We need to optimize the number of transactions and the time costs for each transaction. The second problem is that users should still be able to execute transactions as if in isolation and such that consistency is maintained. The idea of the solution is having the database management system running several user transactions

concurrently, in order to keep CPUs humming.

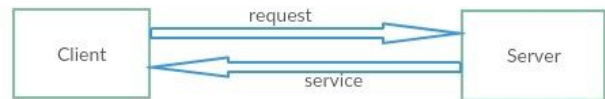
2. Concurrency

Today more and more people are having online transactions at the same time. So it is becoming more and more important to ensure that all those events can happen simultaneously, and all the transactions can be placed right without considering the memory size on different platforms. With a long time improvement, new OLTP software uses client/server processing and brokering software to allow computers worldwide based on different platforms to access database. And with the use of all these methods, the most widely used case is the CICS system.

2.1 Client/server processing

□ Client-Server Architecture

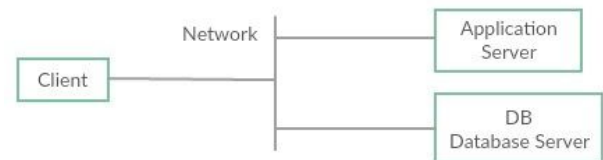
This is the first version in the progress developed in 1992. The data process is divided into two separate parts: the Client(requester) and the Server(provider). The Client sends requests to the Server, and the Server sends back the result after analyzing the database. The Client can be connect to several Servers, and the Client and the Server can change their role due to different tasks.



However, this kind of architecture has many fallbacks. One of the main disadvantage is that the Client and the Server are so tightly coupled that making that work process less efficient, and when there are so much work to be done on the net, other work has to wait until the bonding between the current couple is released.

□ The 3-tier Structures

The 3-tier Structures distributes different section modules of the application on mainly three sites: Client, Application, and Database.



Distribution:

1-tier: Presentation logic, lite client

2-tier: Business logic, application server

3-tier: Database logic, database server

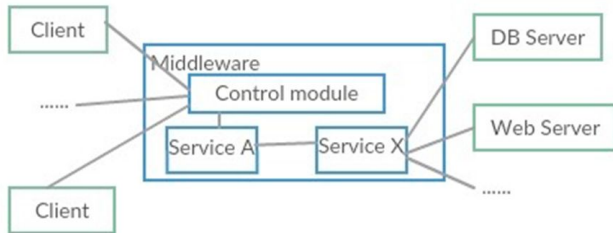
This kind of architecture is more flexible with the bonding between Client and Server. Distribution of the tasks within the same event, hugely influenced the efficiency of the online data requesting and retrieval. Separated task for different servers may shorten the time for each of them to perform their part, and also

get more events executed parallelly.

And this architecture extends its application to other fields, for example, the web browser.

□ The n-tier Architectures

After progressing from the Client-Server Architecture to today, the n-tier architecture. The efficiency of online transaction is much more enhanced than ever before. This architecture guarantees the execution of different task to perform at the same time. And also its mechanism can protect the data from being destroyed or dismissed or even invaded by malicious procedure.



Distribution:

- 1-tier: the Client
- 2-tier: the Middleware section
- 3-tier: the Database Server
- 4-tier: the Web Server
- ... servers on other tiers etc.

The Middleware is an integrating resource between clients and different servers. it contains many functions: translate different protocols for different kinds of use, optimize load-balancing, security control, and manage connections. The Services in the Middleware section deals with different parts of Information retrieval. For example, the Data Management Service deals with the write and read to the server from the client. It receives requests from users, and then translate them into correct database language. Finally, the transformed query will be sent to the next server for execution. And as for Distribution Service, it provides the real server directory for requested data.

Although it is also ok to obtain only one server for data retrieval, management control, etc. It is much better to obtain different servers to focus on different aspects of the query. By this method, the instruction will be executed faster, more efficient, and with better performance.

And here comes a problem: data retrieval or updating among thousands, or even millions of people at the same time may cause data exploding with another effect of lacking memory on the Middleware section. This comes to the optimization from the Customer Information Control System(CICS).same systems under z/OS and z/VSE. CICS is middleware designed to support rapid, high-volume online transaction processing. A CICS transaction is a unit of processing initiated by a single request that may affect one or more objects. This processing is usual

2.2 Customer Information Control System

Customer Information Control System (CICS) is a family of mixed language application servers that provide online transaction management and connectivity for applications on IBM Mainly

interactive (screen-oriented), but background transactions are possible. [Wikipedia]

CICS is the most widely used OLTP system today, which is designed by IBM firstly to ensure the safety and efficiency for online transaction processing. The traditional method to solve this problem is restricting the size of every program to run on the Middleware section, so that CICS can rearrange the memory to other programs which may happen concurrently.

With the process of optimization of Macro-level programming, Command-level programming, Run-time conversion, and New programming styles, CICS forms a regulation of a “two-stage” method: get result from the preprocessor first, and execute later, which greatly comes to a much higher level of efficiency towards query execution.

3. Safety and Correctness of OLTP

As the online transaction process improve so rapidly, safety and correctness for each piece of transaction definitely comes to people’s priority consideration. We need to guarantee that each piece of transaction from one person or one card goes directly to another card or account, and each time the result retrieved from the database is the correct number previously stored in the card. All these problems can be solved in different levels.

In the first level, customers can try to protect their data in the account by themselves. They can encrypt their data files when transfer the file on the Internet, which means no password, no authority to access the data file. And they can also use a PIN number which is set by their own, and authorized by the bank. This technology protect the data in accounts from both customers and the account establisher.

In the second level, the Internet as the medium can protect the data by using MFT software. With the use of the software, different online transactions can only happen between Client and Server within the same protocol or under the management of several agreeable protocols. This method hugely prevent a great amount of malicious invasion of other attempts and also prevent other malwares.

Before introducing some details of all the methods listed above, we need to illustrate the security features first, and the goals of safety concern to help us get a better view of this section content.

Security features have several categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logo to your Internet banking account.
- Authorization: Allows only you to manipulate you resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.
- Integrity: prevention against unauthorized data modification
- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact

□ Availability: prevention against data delays or removal.[2]

The safety concern on online transaction basically has two goals: to ensure the data through the process is exactly the same data retrieved from the database system, to ensure no interception of other procedures maliciously, unintentionally to interrupt the data execution process. And the most effective ways to solve the problem are to use a Personal Identification(PIN) from the user side, and to introduce the Managed File Transfer(MFT) into our way from the processing aspect.

- A PIN(Personal Identification Number) is a four to twelve digit number known by a cardholder and used to authenticate the cardholder to the card-issuing bank(or to the cardholder's ICC).[3] A PIN with the detailed card information will be sent to the bank merchant for verification. If all the information is correct, the card user will be given an authorization from the bank merchant to manage the money in the account.

- MFT refers to a software or a service that manages the secure transfer of data from one computer to another through a network. Features include reporting, auditability, and so on.[wikipedia of Managed file transfer] TechTarget defines MFT as "a type of software used to provide secure internal, external, and ad hoc data transfers through a network." [4]

- Especially, auditability is the ability to provide a cyber audit trail associated with a data transfer. It would capture important information, such as who sent the data, when they were sent, when they were received, what data structure (e.g., xls, csv, txt, xml) was used, how the data were sent (i.e., via what medium) and who received the data.[5]

Today, the most widely used system for banks worldwide to ensure account safety is the Asset Management.

Asset Management is a method used by banks separately to deal with their customers for controlling all the online transactions. These core functions include safeguarding assets, servicing securities, processing cash and securities transaction, maintaining internal controls, record keeping and reporting, and record retention.[6]

Core Asset Management accounting systems support these core functions by maintaining

- account and asset master files,
- account level asset and cash positions,
- department-level asset and cash positions, and
- securities movement and control (SMAC) capabilities.

These systems process such transactions as interest and dividend payments, cash receipts, disbursements, and fees. They can track key events and produce client statements and regulatory and management reports.[6]

To sum it up, people can just ensure their account safety by adding encryption and PIN to their account, and the Internet can use MFT to protect the online transaction. Based on all these methods, in the bank area, the most widely used system is the Asset Management system.

Larson, Pravin Mittal, Ryan Stonecipher, Nitin Verma, Mike Zwilling. Hekaton: SQL Server's Memory-Optimized OLTP Engine. Microsoft.

[2] Niranjana Murthy M, DR. Dharmendra Chahar. The study of E-Commerce Security Issues and Solutions. HOD. Dept. of CS & IT, Seth G. B. Podar College, Nawalgarh (Jhunjhunu) -333042, INDIA.

[3] visa-issuer-pin-security-guideline

[4] Jonathan Lampe, Peter Sedgwick. FILE GOVERNANCE for File Transfer. www.primeur.com

[5] Tommie W. Singleton. Testing Controls Associated With Data Transfers

[6] Comptroller of the Currency Administrator of National Banks. Comptroller's Handbook. January 2011.

4. REFERENCES

[1] Cristian Diaconu, Craig Freedman, Erik Ismert, Per-Ake