PHIẾU GIAO NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP

1. Thông tin về sinh viên
Họ và tên sinh viên: Nguyễn Thị Kim Dung
Điện thoại liên lạc 0979.354.338 Email: dungnkim@gmail.com
Lớp: CNPM A Hệ đào tạo: Đại học chính quy
Đồ án tốt nghiệp được thực hiện tại: Bộ môn Công nghệ phần mềm, khoa Công nghệ thông tin, Đại học Bách Khoa Hà Nội
Thời gian làm ĐATN: Từ ngày / /2009 đến 30 / 05 /2009

2. Mục đích nội dung của ĐATN

Tìm hiểu giao thức vi thanh toán Millicent. Thiết kệ công cụ API hỗ trợ cho cài đặt ứng dụng.

3. Các nhiệm vụ cụ thể của ĐATN

- Tìm hiểu chung về thanh toán điện tử
- Tìm hiểu một số giao thức vi thanh toán
- Tìm hiểu chi tiết giao thức Millicent
- Thiết kế các hàm thư viện, trợ giúp việc cài đặt giao thức Millicent trên ngôn ngữ java, sử dụng công nghệ lập trình phân tán RMI
- Viết chương trình demo, sử dụng một số lớp, hàm trong thư viện đã thiết kế.

4. Lời cam đoan của sinh viên:
Tôi – Nguyễn Thị Kim Dung- cam kết ĐATN là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của tiến sĩ Nguyễn Khanh Văn.
Các kết quả nêu trong ĐATN là trung thực, không phải là sao chép toàn văn của bất kỳ công trình nào khác.

Hà Nội, ngày 30 tháng5 năm 2009
Tác giả ĐATN

Nguyễn Thị Kim Dung

5. Xác nhận của giáo viên hướng dẫn về mức độ hoàn thành của ĐATN và cho phép bảo vệ:

Hà Nội, ngày 30 tháng 5 năm 2009
Giáo viên hướng dẫn

Tiến sĩ Nguyễn Khanh Văn

TÓM TẮT NỘI DUNG ĐỒ ÁN TỐT NGHIỆP

Các điểm cung cấp dịch vụ trên internet xuất hiện ngày càng nhiều với những hình thức phong phú, đa dạng, từ cung cấp thông tin , tra cứu, tìm kiếm, sử dụng phần mềm, đến giải trí… Các dịch vụ này đều có đặc điểm chung là được sử dụng với một tần suất lớn nhưng giá trị lại rất nhỏ và không yêu cầu người sử dụng phải thiết lập mối quan hệ lâu dài với người cung cấp. Với số lượng người sử dụng khổng lồ, khả năng thu phí các dịch vụ này một cách hiệu quả sẽ đem lại lợi nhuận to lớn về kinh tế .Tuy nhiên, có một số lí do khiến cho việc thực hiện chúng khó khăn.

Hầu hết các hệ thống thanh toán hiện nay đều sử dụng thẻ tín dụng hoặc tài khoản tiền mặt trong ngân hàng, không phù hợp với các giao dịch có giá trị thanh toán nhỏ (trong phạm vi 5$). Vì nếu áp dụng, chi phí cho các giao dịch dùng thẻ hoặc tài khoản ngân hàng quá lớn (từ vài đến vài chục cent), thậm chí còn lớn hơn cả lợi nhuận mà nó mang lại.

Những vấn đề trên yêu cầu, thúc đẩy việc nghiên cứu, xây dựng các mô hình thanh toán giá trị nhỏ. Điểm quan trọng nhất mà các mô hình loại này phải đạt được đó là tính đơn giản để đảm bảo hiệu quả về kinh tế. Các thuật toán tuy đơn giản nhưng không kém phần hấp dẫn do luôn có những cách tiếp cận độc đáo, bất ngờ. Trong đó, Millicent là một giao thức gọn nhẹ, an toàn được thiết kế để hỗ trợ các giao dịch có giá trị nhỏ tới dưới 1 cent. Nó dựa trên khả năng kiểm tra đồng tiền số một cách độc lập và các phương pháp mã hóa có chi phí thấp.

Việc xây dựng một hệ thống thanh toán trên phạm vi lớn ứng dụng giao thức Millicent sẽ đem lại hiệu quả to lớn về mặt kinh tế. Tuy nhiên, phát triển hệ thống lớn như vậy không phù hợp với đồ án này do những hạn chế về thời gian và kinh phí. Trong phạm vi đồ án của mình người viết đã thiết kế một thư viện các lớp, hàm trên ngôn ngữ Java để hỗ trợ cho việc phát triển các ứng dụng cài đặt giao thức Millicent cũng như tích hợp nó vào một hệ thống thanh toán có sẵn. Thư viện này được thiết kế dựa trên công nghệ RMI (Remote Method Invocation) của Java, mà thực chất là các hàm thư viện hỗ trợ cho lập trình phân tán.

Trong phần cuối của luận văn, người viết giới thiệu chương trình demo, sử dụng một số lớp, hàm trong thư viện này để thực hiện việc thanh toán bằng scrip giữa khách hàng và nhà cung cấp dịch vụ.

LỜI CẢM ƠN

Tôi gửi lời cám ơn chân thành đến các thầy cô trong khoa Công nghệ thông tin và trường đại học Bách khoa Hà Nội, những người đã hướng dẫn, giúp đỡ tôi trong quá trình học tập tại trường năm năm qua. Đặc biệt gửi lời cám ơn tới ***Tiến sĩ Nguyễn Khanh Văn****, vì sự tận tình hướng dẫn, góp ý của thầy đối với tôi trong quá trình hoàn thành đồ án này!*

Hà nội, tháng 5 năm 2009

Nguyễn Thị Kim Dung

MỤC LỤC

Danh sách các hình vẽ

Các từ viết tắt	
NVLV	Người viết luận văn

CHƯƠNG 1 Giới thiệu

Internet ra đời đã đem lại sự thay đổi to lớn trong cách thức giao dịch thương mại. Nhờ sự trợ giúp của mạng máy tính toàn cầu này, người bán và người mua không còn gặp phải sự trở ngại về không gian, thời gian nữa. Điều đó làm cho việc mua bán trên mạng trở nên cực kì hấp dẫn bởi thị trường nhiều tiềm năng với số người sử dụng khổng lồ của nó. Thực tế đã chứng minh điều này. Trong quý I năm 2009 các hãng nổi tiếng trong lĩnh vực này như Amazon.com đạt doanh thu 4.89 tỉ USD và 60 lượt khách sử dụng, eBay cũng đạt doanh thu 2 tỉ và khoảng 70 triệu lượt khách sử dụng, Skype có doanh thu 150 triệu USD và số lượt sử dụng 37.9 triệu (theo số liệu do các hãng này công bố).

Các hệ thống thanh toán nổi tiếng đó được xây dựng dựa trên các giao thức an toàn bảo mật mà nền tảng của chúng là các thành tựu trong lý thuyết mật mã với phương thức thanh toán bằng thẻ tín dụng, hoặc các tài khoản ngân hàng, tiền mặt điện tử. Tuy nhiên chúng chỉ phù hợp với các giao dịch thương mại có giá trị trung bình và lớn, cỡ vài USD trở lên, bởi chi phí phí cho việc thực hiện mỗi giao dịch như vậy thường là vài đến vài chục cent cộng với một lượng phần trăm nhất định của giá sản phẩm. Khi những chi phí này áp dụng lên những giao dịch có giá trị nhỏ, từ vài USD cho đến dưới một cent, thì chi phí giao dịch thật sự là một gánh nặng vì giá của nó thậm chí còn cao hơn lợi nhuận mà giao dịch mang lại. Do vậy để sử dụng các hệ thống như thế này một cách hiệu quả, thường là có một ngưỡng giá tối thiểu đối với hàng hóa và dịch vụ (cỡ vài USD).

Trên thực tế ngày càng xuất hiện nhiều điểm giao dịch trên mạng cung cấp các dịch vụ phong phú đa dạng từ cung cấp thông tin (giá cổ phiếu, báo, tạp chí…), dịch vụ tìm kiếm (việc làm…), sử dụng phần mềm (diệt virus,..) đến giải trí (xem phim, nghe nhạc…). Đặc điểm chung của tất cả các dịch vụ này là chúng được sử dụng với tần suất lớn nhưng giá trị lại rất nhỏ và không yêu cầu người sử dụng phải thiết lập mối quan hệ lâu dài với nhà cung cấp. Các nhà cung cấp này đều có nhu cầu bán các dịch vụ của mình, tuy nhiên nếu sử dụng các hệ thống thanh toán như trên thì rõ ràng là không hiệu quả. Cũng có một số website cố gắng thu tiền cho các dịch vụ của mình bằng cách thu phí thành viên, sau đó trừ dần trong quá trình sử dụng. Tuy nhiên, điều này lại hạn chế số thành viên, vì thường người ta không muốn bỏ vài USD để tạo quan hệ với một website mà người ta chỉ có nhu cầu sử dụng một vài lần.

Do đó, khả năng thực hiện các giao dịch thanh toán với giá trị nhỏ như vậy một cách an toàn, hiệu quả thực sự sẽ thu hút một lượng người sử dụng rất lớn và tổng lợi nhuận trên tất cả các giao dịch thu được sẽ là khổng lồ. Bên cạnh đó, các giao dịch như vậy còn hỗ trợ cho xuất bản trực tuyến, một lĩnh vực khá thú vị nhưng không thuộc phạm vi của đồ án này. Một người sử dụng chẳng mấy khi muốn mở một tài khoản vài dollar với một nhà xuất bản anh ta không biết rõ lắm, lại sẵn sàng chi vài cent để mua một vài thông tin từ họ.

Trên đây chính là cơ sở để nghiên cứu và phát triển các mô hình thanh toán điện tử với giá trị nhỏ và siêu nhỏ - MicroPayment.

Có một số mô hình thanh toán giá trị nhỏ này được xây dựng dựa trên nền tảng của các giao thức thanh toán giá trị trung bình và lớn (dùng thẻ tín dụng), như CyberCash, DigiCash… Các mô hình này thực hiện thu phí bằng cách tập hợp nhiều giao dịch nhỏ của một người sử dụng lại và chỉ chuyển khoản khi nó đạt giá trị đủ lớn để tiết kiệm chi phí cho giao dịch dùng thẻ tín dụng.

Bên cạnh đó một số mô hình đã được đưa ra để thực sự hỗ trợ cho các giao dịch có giá trị nhỏ và siêu nhỏ. Các mô hình này có một đặc trưng quan trọng đó là tính đơn giản để đảm bảo hiệu quả về kinh tế. Một số mô hình đã được giới thiệu và khá nổi tiếng như Millicent, PayWord, PayPal, MicroMint. Trong đó Millicent là một giao thức khá trong sáng, dễ cài đặt và gọn nhẹ. Khái niệm cơ bản nhất trong Millicent là Scrip, nó được dùng như tiền để thực hiện các giao dịch thanh toán. Các bên tham gia giao thức gồm có khách hàng (customer), người bán hàng – cung cấp dịch vụ (vendor) và nhà môi giới (broker). Điểm đặc biệt là mỗi scrip chỉ có giá trị thanh toán tại nơi tạo ra nó. Vendor và broker đều có thể tự tạo ra các scrip (đồng tiền) cho mình. Để bắt đầu hoạt động broker mua các scrip của vendor với số lượng lớn, customer mua scrip của broker (các giao dịch này thanh toán bằng tiền mặt hoặc thẻ tín dụng). Sau đó, customer mua các scrip của vendor từ broker (thanh toán bằng scrip của broker) và dùng các scrip này để thanh toán tại vendor. Giao thức sử dụng một số hàm băm (MD5, SHA) và các thuật toán mã hóa đối xứng (RC4, DES…) nên thời gian tính toán khá nhanh chóng, sử dụng hết ít tài nguyên của hệ thống, do đó hệ thống có thể đáp ứng đồng thời một số lượng lớn giao dịch thanh toán.

Hệ thống thanh toán hỗ trợ giao thức Millicent được triển khai theo mô hình phân tán, với chương trình ứng dụng ở các bên tham gia hệ thống là khác nhau. Ở server của Broker, chương trình có nhiệm vụ quản lý các tài khoản của các vendor và customer; cũng như làm nhiệm vụ kết nối với các bên, đảm bảo customer luôn có đủ scrip của

vendor mà anh ta yêu cầu. Chương trình tại server của vendor có nhiệm vụ sinh ra các scrip, bán cho broker; quản lý các thông tin scrip và xử lý các giao dịch thanh toán đến từ broker (mua scrip bằng tiền mặt hoặc tẻ tín dụng) và customer (mua dịch vụ, thanh toán bằng scrip). Tại phía khách hàng, ứng dụng sẽ là một ví điện tử, làm nhiệm vụ quản lý các scrip và thực hiện việc thanh toán cho các yêu cầu của khách hàng. Ví điện tử này có thể đặt ngay tại máy tính của khách hàng (có thể đặt trong USB chẳng hạn), hoặc đặt tại một server tập trung tất cả các ví điện tử của người sử dụng (có thể do broker quản lý), và khách hàng có thể sử dụng tại bất cứ đâu qua một trình duyệt web.

Hệ thống này nếu triển khai trong thực tế trên một phạm vi lớn sẽ đem lại nhiều lợi ích. Nó tạo nên một kênh cung cấp thông tin, dịch vụ trực tuyến nơi mọi người đều có thể thanh toán những khoản phí rất nhỏ một cách dễ dàng và hiệu quả, điều này sẽ thu hút một số lượng người sử dụng rất lớn. Các dịch vụ được cung cấp ở đây, tuy giá trị thanh toán nhỏ, nhưng những người cung cấp vẫn có thể thu phí từ dịch vụ của họ, dẫn đến sự cạnh tranh nâng cao chất lượng dịch vụ giữa các nhà cung cấp, và khách hàng được hưởng lợi từ sự cạnh tranh đó. Điều này hoàn toàn phù hợp với các quy luật cạnh tranh và "khách hàng là thượng đế"của kinh tế thị trường. Mặt khác, người trung gian đứng giữa cũng thu được lợi nhuận lớn từ việc môi giới, mua scrip từ các vendor với số lượng lớn, và bán lẻ lại cho các customer.

Tuy nhiên, phát triển một hệ thống lớn như vậy không phù hợp với đồ án này do những hạn chế về thời gian, kinh phí. Trong phạm vi đồ án tốt nghiệp của mình, người viết luận văn (NVLV) thiết kế một công cụ API, hỗ trợ cho việc cài đặt các ứng dụng thanh toán dựa trên giao thức Millicent hoặc có thể sử dụng đế tích hợp Millicent vào các hệ thống thanh toán sẵn có. Công cụ API này chính là thư viện gồm các lớp, hàm cơ bản cài đặt những khái niêm, hoạt động, tương tác trong Millicent, được gọi đến trong các ứng dụng ở cả ba bên, server broker, server vendor và ví điện tử của customer.

Có một số lựa chọn về ngôn ngữ khi thiết kế và cài đặt thư viện này như: C++, C#, Java, tất cả chúng đều là các ngôn ngữ lập trình hướng đối tượng. Tuy nhiên người viết lựa chọn Java trước hết do những ưu điểm nổi trội của nó như: là một ngôn ngữ hướng đối tượng thuần túy; các chương trình viết trên java chạy trên máy ảo java nên độc lập với mọi phần cứng và hệ điều hành khác nhau; ngôn ngữ java có một thư viện khổng lồ, hỗ trợ cho việc lập trình, thư viện của nó cũng chứa hầu hết các hàm mật mã được sử dụng trong Millicent như các hàm băm MD5, SHA hay mã hóa RC4, DES… Ngoài ra công cụ RMI (Remote Method Invocation) của java hỗ trợ đắc lực cho lập trình phân tán. Nó là một phần của bộ J2SDK (Java 2 Software Development Kit) và là các hàm thư viện hỗ trợ các lời gọi phương thức từ xa và trả về kết quả cho các ứng dụng tính

toán phân tán. Với những lợi điểm như trên, thư viện mà NVLV giới thiệu trong chương 4 được thiết kế trên ngôn ngữ Java, sử dụng công cụ RMI. Để thấy rõ hoạt động của các lớp và hàm trong thư viện này, NVLV xây dựng một chương trình demo, sử dụng một số lớp và hàm trong thư viện nói trên để mô phỏng quá trình thanh toán bằng scrip giữa customer và vendor.

Các vấn đề trình bày ở trên được trình bày chi tiết trong các phần còn lại của luận văn:

- **Chương 2:** Trình bày các kiến thức chung về thanh toán điện tử và một số mô hình vi thanh toán.
- **Chương 3:** Trình bày chi tiết về giao thức thanh toán giá trị nhỏ Millicent.
- **Chương 4:** Thiết kế thư viện các hàm API cho giao thức Millicent bằng ngôn ngữ java dựa trên công nghệ RMI
- **Chương 5:** Giới thiệu chương trình demo có sử dụng một số hàm trong thư viện trên và đánh giá kết quả đạt được cũng như các công việc trong tương lai.

Cũng giống như vendor, customer, broker được giữ nguyên văn tiếng Anh, một số thuật ngữ đặc biệt khác người viết cũng không dịch ra tiếng Việt, nhưng vẫn đưa ra giải thích cho nó để tránh việc gây hiểu lầm. Các thuật ngữ này nằm rải rác trong một số phần của luận văn.