BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

PHAN PHỤNG HÒA

NGHIÊN CỨU ĐÁNH GIÁ MỘT SỐ GIẢI PHÁP BẢO MẬT CLOUD COMPUTING

Chuyên ngành : **KHOA HỌC MÁY TÍNH**
Mã số : **60.48.01**

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

Đà Nẵng - Năm 2012

Công trình được hoàn thành tại
ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: PGS.**TS. LÊ VĂN SƠN**

Phản biện 1: **PGS.TS. PHAN HUY KHÁNH**

Phản biện 2: **TS. HOÀNG THỊ LAN GIAO**

Luận văn được bảo vệ tại Hội đồng chấm Luận văn tốt nghiệp thạc sĩ kỹ thuật họp tại Đại học Đà Nẵng vào ngày 03 tháng 03 năm 2012

Có thể tìm hiểu luận văn tại:

- Trung tâm Thông tin - Học liệu, Đại học Đà Nẵng
- Trung tâm Học liệu, Đại học Đà Nẵng

MỞ ĐẦU

1. Lý do chọn đề tài

Trong những năm gần đây, Cloud Computing (viết tắt là CC) đã có những bước tiến vượt bậc. Như chúng ta biết, CC không phải là một công nghệ gì mới, mà là sự sự kết hợp nhiều công nghệ trước đây. Những công nghệ này đã hoàn thiện ở các mức độ khác nhau trong những ngữ cảnh khác nhau, chúng không được thiết kế như một thể thống nhất. Tuy nhiên, chúng đã tạo ra một hệ thống kỹ thuật cho CC. Những tiến bộ mới trong bộ vi xử lý, công nghệ ảo hóa, đĩa lưu trữ, kết nối internet băng thông rộng, các máy chủ rẻ, mạnh và nhanh đã kết hợp với nhau tạo ra CC.

Các lợi ích CC đem lại cho người dùng rất lớn, trên thực tế CC đã thật sự được quan tâm và sử dụng hiệu quả ở nhiều nước phát triển trên thế giới. Khả năng giải quyết và đáp ứng tốt các nhu cầu bức thiết trong nhiều lĩnh vực. Vì vậy, CC ngày càng được các tổ chức, doanh nghiệp và cá nhân sử dụng và CC sẽ là xu hướng phát triển trong tương lai.

Tuy nhiên, điều mà các tổ chức, các doanh nghiệp, hoặc cá nhân e dè khi muốn chuyển đổi các ứng dụng quan trọng trong kinh doanh sang môi trường đám mây là do những thách thức có thể gặp phải như độ tin cậy, tính bảo mật, khả năng sẵn sàng của dịch vụ và hiệu suất hoạt động. Trong đó, vấn đề bảo mật của CC là điều mà nhiều người quan tâm nhất. Dữ liệu của khách hàng được nhà cung cấp CC bảo mật như thế nào? Người sử dụng tự bảo mật dữ liệu ra làm sao?

Vì thế tôi chọn đề tài luận văn là "***Nghiên cứu đánh giá một số giải pháp bảo mật trong Cloud Computing***" để trình bày và giải quyết những vấn đề trên.

2. Mục đích nghiên cứu

Giúp người sử dụng CC hiểu về cấu trúc hoạt động của CC, tìm hiểu các giải pháp bảo mật trong CC, đồng thời xây dựng thử nghiệm giải pháp bảo mật xác thực người dùng trong CC.

3. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu bao gồm: cloud computing, các tài liệu viết về bảo mật trong CC, các chuẩn bảo mật, xác thực, môi trường phát triển và triển khai hệ thống xác thực người dùng.

Phạm vi nghiên cứu gồm: Tổng quan về CC, các giải pháp bảo mật trong CC và xây dựng thử nghiệm giải pháp bảo mật xác thực người dùng CC.

4. Phương pháp nghiên cứu

Phương pháp chính là nghiên cứu qua nguồn tư liệu đã xuất bản, các bài báo, các báo cáo khoa học về CC và bảo mật trong CC. Xây dựng giải pháp bảo mật xác thực người dùng CC, kiểm thử và đánh giá kết quả hệ thống xác thực trong môi trường CC.

5. Ý nghĩa khoa học và thực tiễn của luận văn

Việc nghiên cứu và triển khai thành công luận văn sẽ đáp ứng nhu cầu tìm hiểu giải pháp bảo mật trong CC cho các cá nhân, doanh nghiệp trước khi quyết định đăng kí sử dụng các dịch vụ của CC. Giải pháp bảo mật xác thực người dùng giúp

các khách hàng CC tự bảo vệ các ứng dụng của mình khi triển khai trên CC.

6. Bố cục của luận văn

Bố cục của luận văn được tổ chức thành ba chương với nội dung cụ thể như sau:

Chương 1- **Tổng quan về Cloud Computing**, trình bày các vấn đề chung về CC như định nghĩa, lịch sử hình thành, tính chất, kiến trúc của CC, ảo hóa, …

Chương 2 – **Những vấn đề về bảo mật dữ liệu**, phân tích và đánh giá về hạ tầng bảo mật ở ba cấp độ: cấp độ mạng, cấp độ máy chủ và cấp độ ứng dụng. Đánh giá về hệ thống xác thực một yếu tố và xác thực đa yếu tố.

Chương 3 – **Xây dựng giải pháp bảo mật xác thực người dùng trong Cloud Computing**, trình bày giải pháp xác thực CC dựa trên mã nguồn mở Mobile-One Time Password (mOTP) phía client, xây dựng chương trình, triển khai thử nghiệm và đánh giá hệ thống xác thực trên CC.

Chương 1: TỔNG QUAN VỀ CLOUD COMPUTING

1.1 ĐỊNH NGHĨA CLOUD CONGPUTING

Có rất nhiều định nghĩa về Điện toán đám mây (Cloud Computing- viết tắt là CC). Một số người đề xuất rằng CC chỉ đơn giản là một tên khác cho các phần mềm như là một mô hình Dịch vụ (SaaS) trong xu hướng Web 2.0. Những người khác thì nói rằng CC là sự quảng bá tiếp thị một diện mạo mới trên công nghệ cũ, chẳng hạn như điện toán tiện ích, sự ảo hóa hoặc điện toán lưới. Suy nghĩ này làm giảm thực tế là CC có một phạm vi rộng hơn bất kỳ trong các công nghệ đặc biệt này. Để chắc chắn, các giải pháp đám mây thường bao gồm các công nghệ này (và những công nghệ khác), nhưng đó là chiến lược toàn diện đặt CC tách khỏi các công nghệ trước đây.

Theo tự điển bách khoa toàn thư số Wikipedia: *"Điện toán đám mây (cloud computing) là một mô hình điện toán có khả năng co giãn (scalable) linh động và các tài nguyên thường được ảo hóa được cung cấp như một dịch vụ trên mạng Internet".*

Theo Ian Foster: *"Điện toán đám mây là một mô hình điện toán phân tán có tính co giãn lớn mà hướng theo co giãn về mặt kinh tế, là nơi chứa các sức mạnh tính toán, kho lưu trữ, các nền tảng (platform) và các dịch vụ được trực quan, ảo hóa và co giãn linh động, sẽ được phân phối theo nhu cầu cho các khách hàng bên ngoài thông qua Internet".*

Nói chung, điện toán đám mây là một giải pháp bao gồm tất cả các tài nguyên điện đoán (phần cứng, phần mềm, mạng, lưu

trữ,…) được cung cấp cho người dùng theo yêu cầu. Các nguồn tài nguyên hoặc các dịch vụ được phân phát đảm bảo khả năng sẵn sàng cao, an ninh và chất lượng. Người dùng sở hữu khả năng điều chỉnh tăng hoặc giảm để có được những tài nguyên mà họ cần, không nhiều hơn và cũng không ít hơn.

Ông Steve Chang - Chủ tịch Hội đồng quản trị tập đoàn Trend Micro nói về CC theo cách đơn giản và dễ hiểu hơn: "Quan niệm về CC có thể hiểu đơn giản như dùng điện, dùng bao nhiêu trả tiền bấy nhiêu và đơn giản không phải đầu tư gì cả, chỉ việc mua phích điện". Nghĩa là, với môi trường CC, người sử dụng có thể truy cập đến bất kỳ tài nguyên nào tồn tại trong "đám mây" tại bất kỳ thời điểm nào và từ bất cứ đâu, thông qua Internet. Ngoài ra, người dùng chỉ phải trả chi phí cho những gì mình sử dụng khi mình cần. Như vậy, có thể thấy CC đem lại cho mọi người sự thuận tiện hơn trong việc tiếp cận thông tin, đặc biệt là hệ thống thông tin qua mạng Internet. [16]

1.2 NHỮNG LỢI ÍCH VÀ NHƯỢC ĐIỂM CỦA CC

1.2.1 Những lợi ích của CC

1.2.2 Những nhược điểm của CC

1.3 LỊCH SỬ HÌNH THÀNH CC

Lịch sử hình thành CC theo 6 giai đoạn:

Giai đoạn 1: Nhiều người dùng chia sẻ mainframes công suất cao thông qua các terminal giả (dummy terminals).

Giai đoạn 2: Chỉ một PC cũng đã đủ sức mạnh để đáp ứng nhu cầu tính toán của người dùng.

Giai đoạn 3: Các PC, laptop, và các server được kết nối vào mạng cục bộ để chia sẻ tài nguyên và nâng cao hiệu năng.

Giai đoạn 4: Mạng cục bộ này được kết nối với mạng cục bộ khác tạo thành một mạng toàn cầu như Internet để sử dụng các ứng dụng và tài nguyên từ xa.

Giai đoạn 5: Tính toán lưới (Grid Computing) cung cấp năng lực tính toán và năng lực lưu trữ dùng chung thông qua một hệ thống tính toán phân tán.

Giai đoạn 6: CC cung cấp các tài nguyên dùng chung trên Internet theo một cách đơn giản và cân bằng.

1.4 TÍNH CHẤT CƠ BẢN CỦA CC

Cloud Computing có năm tính chất nổi bật so với mô hình truyền thống:

1.4.1 Tự phục vụ theo nhu cầu (On-demand self-service)

1.4.2 Truy xuất diện rộng (Broad network access)

1.4.3 Dùng chung tài nguyên (Resource pooling)

1.4.4 Khả năng co giãn (Rapid elasticity)

1.4.5 Điều tiết dịch vụ (Measured service)

1.5 KIẾN TRÚC CỦA CC

Phần này trình bày mô hình kiến trúc của CC. CC hướng đến các cấp độ khác nhau của dịch vụ nhằm đáp ứng tối đa nhu cầu của người sử dụng như SaaS, IaaS và PaaS.

Dịch vụ hạ tầng (IaaS):

Dịch vụ nền tảng (PaaS):

Dịch vụ phần mềm (SaaS):

1.6 CÁC MÔ HÌNH TRIỂN KHAI CC

1.6.1 Đám mây chung (Public Cloud):

1.6.2 Đám mây riêng (Private Cloud)

1.6.3 Đám mây lai (Hybrid Cloud)

1.7 ẢO HÓA (Virtualization)

1.7.1 Kiến trúc Host-based

1.7.2 Hypervisor-based

1.8 CLOUD, GRID VÀ DISTRIBUTED SYSTEM

1.9 MỘT SỐ NHÀ CUNG CẤP CC

1.9.1 EC2 của Amazon

1.9.2 Blue Cloud của IBM

1.9.3 Azure của Microsoft

1.9.4 App Engine của Google

1.9.5 Salesforce

1.10 XU HƯỚNG PHÁT TRIỂN CỦA CC

1.11 KẾT LUẬN CHƯƠNG

Chương này tìm hiểu một cách tổng quát về CC, một khái niệm còn rất mới ở Việt Nam. Các định nghĩa, kiến trúc, những đặc điểm của CC, cũng như ảo hóa máy chủ, những lợi ích và bất lợi khi sử dụng CC, giúp tìm hiểu được một cách tổng quan về "diện mạo" của CC. Trong chương 2 sẽ tập trung phân tích và đánh giá chuyên sâu về hạ tầng bảo mật của CC, tìm hiểu các chuẩn quản lý bảo mật và cuối cùng là xác thực đa yếu tố trên CC.

Chương 2: NHỮNG VẤN ĐỀ VỀ BẢO MẬT DỮ LIỆU

2.1 HẠ TẦNG BẢO MẬT

Trong phần này sẽ tập trung vào phân tích và đánh giá về hạ tầng bảo mật của CC ở cấp độ mạng, máy chủ và ứng dụng theo ba mô hình cung cấp dịch vụ SaaS, PaaS, và IaaS. Phần này cũng sẽ nói đến đâu là trách nhiệm bảo mật của nhà cung cấp dịch vụ CSP (Cloud Service Provider) và đâu là trách nhiệm bảo mật của khách hàng CC (là một tổ chức, doanh nghiệp hay cá nhân sử dụng dịch vụ CC do CSP cung cấp).

2.1.1 Cấp độ mạng (Netwok Level)

2.1.1.1 Tính bảo mật và toàn vẹn dữ liệu

2.1.1.2 Bảo đảm kiểm soát truy cập

2.1.1.3 Bảo đảm tính sẵn có của các nguồn tài nguyên

2.1.1.4 Thay thế các tầng và các vùng mạng đã thiết lập bằng các tên miền

2.1.2 Cấp độ máy chủ (Host Level)

2.1.2.1 Bảo mật máy chủ SaaS và PaaS

2.1.2.2 Bảo mật máy chủ IaaS

2.1.2.3 Bảo mật phần mềm ảo hóa

2.1.2.4 Bảo mật Server ảo

2.1.2.5 An toàn các Server ảo

2.1.3 Cấp độ ứng dụng (Application Level)

2.1.3.1 DoS and EDoS

2.1.3.2 Bảo mật người dùng cuối

2.1.3.3 Bảo mật ứng dụng SaaS

2.1.3.4 Bảo mật ứng dụng PaaS

2.1.3.5 Bảo mật các ứng dụng triển khai của khách hàng

2.1.3.6 Bảo mật ứng dụng IaaS

2.2 CÁC CHUẨN QUẢN LÝ BẢO MẬT

Các chuẩn thực hiện quản lý bảo mật trên CC thường được sử dụng là ITIL (Information Technology Infrastructure Library) và ISO/IEC 27001/27002.

2.2.1 ITIL

2.2.2 ISO 27001/27002

2.3 XÁC THỰC TRONG CLOUD COMPUTING

Với sự phân tích và đánh giá trong phần hạ tầng bảo mật ở trên, chúng ta thấy rằng khách hàng cũng có trách nhiệm bảo mật CC ở tất cả các cấp độ mạng, cấp độ máy chủ và nhiều nhất là ở cấp độ ứng dụng. Việc xác thực với một mật khẩu mạnh là điều rất cần thiết đối với khách hàng CC, cũng như dựa vào các chuẩn quản lý bảo mật để khách hàng CC có sự hiểu biết và thực hiện đúng trách nhiệm bảo mật của mình.

2.3.1 Xác thực một yếu tố (mật khẩu tĩnh)

Thông thường các dịch vụ đám mây cũng như nhiều dịch vụ khác trên Internet thường sử dụng mật khẩu tĩnh (static password) để xác thực người dùng khi họ muốn đăng nhập vào. Mật khẩu tĩnh thường là một từ hoặc một cụm từ bí mật được chọn bởi người sử dụng và nó được dùng kết hợp với tên (username) của người sử dụng.

Điểm yếu chính của các mật khẩu tĩnh là khi người sử dụng lựa chọn các cụm từ bí mật. Nếu mật khẩu này là đơn giản, nó sẽ rất dễ dàng bị các hacker đoán đúng. Ngược lại, nếu mật khẩu là một cụm từ dài với các kí tự đặc biệt thì mật khẩu

sẽ rất khó nhớ, dẫn đến phải viết mật khẩu vào một mảnh giấy và đây chính là một nguy cơ bị đánh cắp mật khẩu.

Hơn nữa, mật khẩu khi gửi đến server để xác thực được gửi qua Internet dưới dạng plain text không được mã hóa rất dễ bị tóm trên đường truyền. Các hacker có thể lấy cắp mật khẩu người dùng bằng nhiều cách như dùng Phishing (hacker gửi một bức thư giả mạo nhà cung cấp để lừa người dùng truy cập vào một Web site và từ đó người dùng sẽ bị lộ mật khẩu). Hoặc sử dụng các dạng tấn công khác như Brute force, Keylogger (Hacker ghi lại tất cả những gì người dùng gõ lên bàn phím) để từ đó lần ra mật khẩu của họ.

2.3.2 Xác thực đa yếu tố

Các yếu tố xác thực (authentication factors) nói chung được phân loại theo ba trường hợp sau:

- Những cái mà người dùng sở hữu bẩm sinh (Something the user is): chẳng hạn, dấu vân tay hoặc mẫu hình võng mạc mắt, chuỗi DNA, mẫu hình về giọng nói, sự xác minh chữ ký, tín hiệu sinh điện đặc hữu do cơ thể sống tạo sinh (unique bio-electric signals), hoặc những biệt danh sinh trắc (biometric identifier)…
- Những cái gì người dùng có (something the user has): chẳng hạn, chứng minh thư (ID card), chứng chỉ an ninh (security token), chứng chỉ phần mềm (software token) hoặc điện thoại di động (mobile phone).
- Những gì người dùng biết (something the user knows): chẳng hạn, mật khẩu, mật khẩu ngữ (pass phrase)

hoặc số định danh cá nhân (personal identification number - PIN).

Một giải pháp được đưa ra là kết hợp nhiều yếu tố xác thực lại để tạo ra một hệ thống an toàn hơn, bảo mật hơn. Một hệ thống như vậy gọi là xác thực mạnh đa yếu tố.

2.4 KẾT LUẬN CHƯƠNG

Như vậy việc bảo mật cũng như trách nhiệm bảo mật đã được phân tích qua hạ tầng bảo mật với ba cấp độ mạng, máy chủ và ứng dụng. Rõ ràng ở cấp độ ứng dụng khách hàng có trách nhiệm chính trong việc bảo mật trong CC, tự bảo mật các ứng dụng của chính mình. Xác thực người dùng là một giải pháp bảo mật dễ nhất, và ít tốn kém về chi phí, nên được khách hàng quan tâm sử dụng nhiều. Xác thực đa yếu tố là giải pháp xác thực an toàn cho khách hàng CC. Trong chương 3 sẽ trình bày chi tiết giải pháp xác thực người dùng hai yếu tố. Triển khai cài đặt thử nghiệm và đánh giá hệ thống xác thực trên CC.

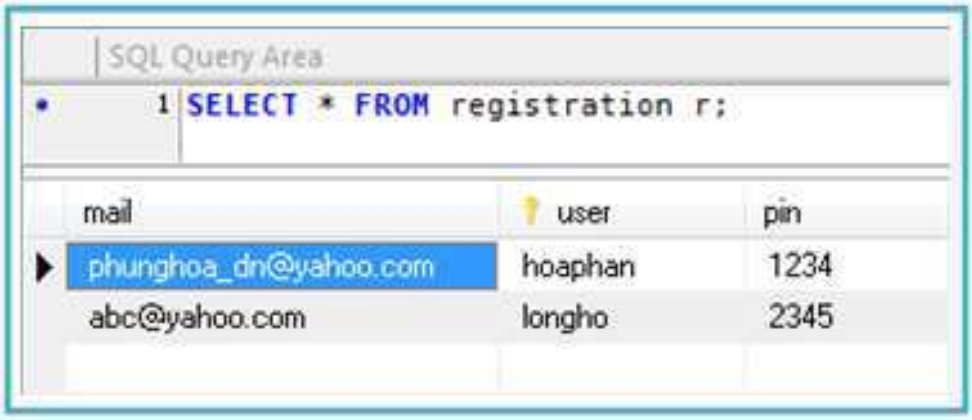
Chương 3: XÂY DỰNG GIẢI PHÁP BẢO MẬT XÁC THỰC NGƯỜI DÙNG TRONG CLOUD COMPUTING

3.1 CẤU TRÚC CỦA HỆ THỐNG

3.1.1 Thiết kế dữ liệu

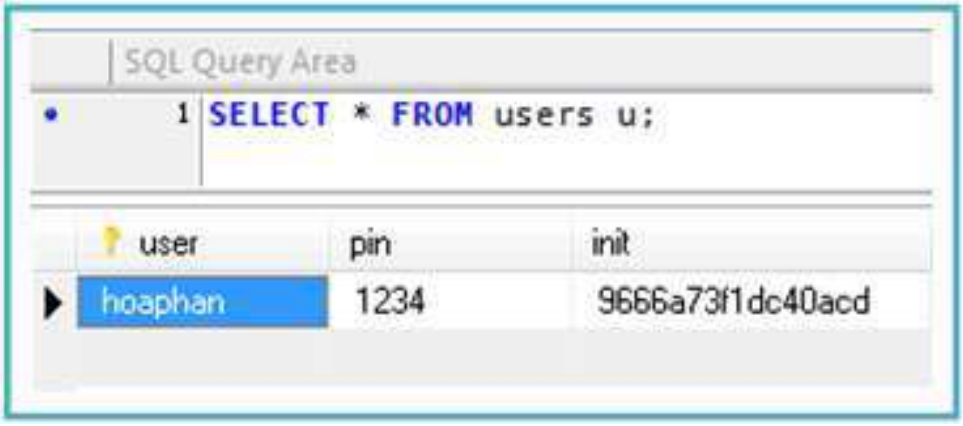
Chương trình được thiết kế với hệ quản trị cơ sở dữ liệu MySQL, phía server có ba bảng:

Bảng registration chứa các thông tin đăng ký của người dùng gồm: Địa chỉ email, tên người dùng user và số pin.



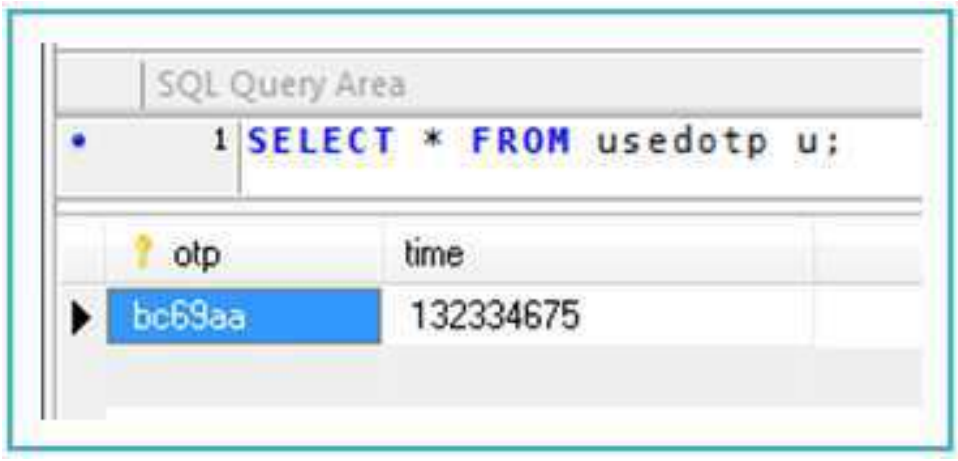
Hình 3.1: Bảng registration

Bảng users chứa thông tin người dùng gồm tên người dùng user, số pin và mã số bí mật init.



Hình 3.2: Bảng users

Bảng usedotp chứa các OTP người dùng đã login thành công vào hệ thống.



Hình 3.3 Bảng usedotp

3.1.2 Cài đặt công cụ và thư viện hỗ trợ lập trình

3.1.2.1 Cài đặt PHP 5.0

Sử dụng ngôn ngữ lập trình PHP, là ngôn ngữ lập trình mạnh mẽ phổ biến nhất hiện nay được sử dụng để tạo các các ứng dụng web. Đây là công cụ được cấp phép sử dụng hoàn toàn miễn phí, dễ sử dụng.

3.1.2.2 Cài đặt web server Apache 2.2

Sử dụng web server Apache, đây là một web server hoàn toàn miễn phí, hỗ trợ PHP và MySQL.

3.1.2.3 Cài đặt MySQL 5.1

Sử sụng hệ quản trị cơ sở dữ liệu MySQL, đây là một hệ quản trị cơ sở dữ liệu rất phổ biến và hoàn toàn miễn phí.

3.1.3 Giải pháp xác thực người dùng CC MOTP:

Luận văn này đề xuất giải pháp xác thực người dùng CC Mobile One Time Password (mOTP). Giải pháp này sử dụng mã nguồn mở mOTP [14] được cài đặt trên điện thoại di động

có hỗ trợ Java như một thiết bị xác thực, một thiết bị mà mọi người đều có thể có được và luôn mang theo bên mình. Sau mỗi lần người dùng nhập vào mã PIN gồm 4 chữ số, phần mềm mOTP sẽ tạo một mật khẩu một lần sử dụng (One Time Password - OTP) cho người dùng. Mật khẩu này chỉ có giá trị trong một thời gian nhất định (3 phút). Người dùng sử dụng mật khẩu này kết hợp với tên người dùng đã được đăng ký để đăng nhập. Mật khẩu này chỉ được sử dụng đăng nhập một lần duy nhất.

Mật khẩu một lần (One Time Password - OTP)

Mật khẩu dùng một lần hay còn được gọi là mật khẩu động với đặc điểm không lặp lại và chỉ có giá trị cho một lần đăng nhập. Phương pháp này an toàn hơn khi sử dụng mật khẩu tĩnh để xác thực người dùng. Mục đích làm cho mật khẩu lúc nào cũng thay đổi, cho dù các Hacker hoặc ai đó đánh cắp được mật khẩu thì nó cũng không có giá trị sử dụng. Mỗi người dùng cần phải có thiết bị "Token" để sinh ra mật khẩu có giá trị một lần. Giải pháp này sử dụng điện thoại di động thay cho thiết bị Token.

Hai yếu tố xác thực với mOTP

Giải pháp đưa ra sử dụng kỹ thuật xác thực dựa trên hai yếu tố:

- Thiết bị mobile phone cài ứng dụng mOTP lưu giữ mã bí mật Init-Secret (cái người dùng có).
- Mã PIN (cái người dùng biết).

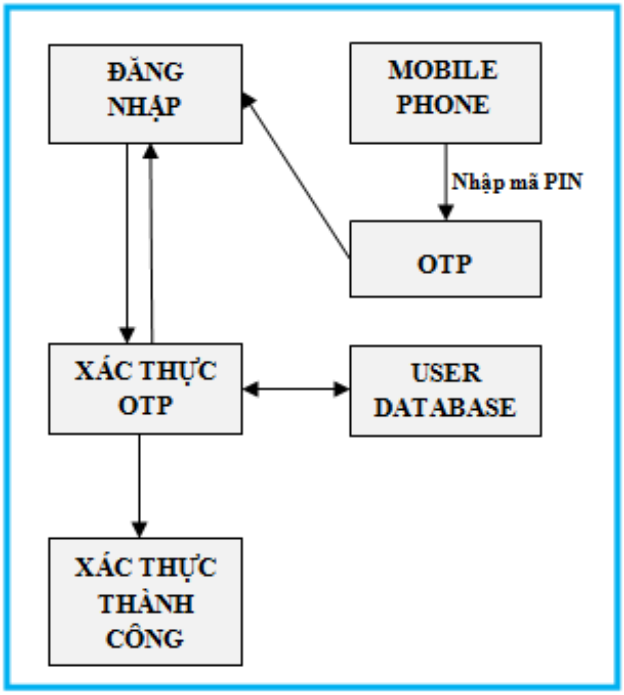
Sau khi người dùng nhập mã PIN (4 số) vào ứng dụng mOTP trên mobile phone, một mật khẩu một lần sử dụng OTP sẽ được tạo.

OTP được tạo trên mobile phone dựa trên ba thành phần:

- Bốn số PIN người dùng nhập vào.
- Mã số bí mật Init-Secret (16 hex-digit) được tạo khi khởi tạo phần mềm trên thiết bị điện thoại di động, mã bí mật này được lưu giữ trong thiết bị điện thoại di động.
- Thời gian hiện hành (phải thiết lập múi giờ (time zone) trên điện thoại di động cùng múi giờ với server)

Ba thành phần này được kết hợp với nhau và được băm (hash) bằng giải thuật mã hóa MD5. Sau khi băm, ứng dụng hiển thị OTP bằng 6 chữ số đầu tiên của dãy đã được băm. OTP chỉ có giá trị sử dụng trong ba phút.

3.1.4 Sơ đồ biểu diễn quy trình hoạt động của hệ thống



Hình 3.4: Quy trình hoạt động của hệ thống xác thực mOTP

3.1.5 Các trang web của hệ thống

Hệ thống xác thực mOTP được thiết kế bao gồm sáu trang web mã php cài đặt trên server.

(1) Trang *login.php*

(2) Trang *logout.php*

(3) Trang *connect.php*

(4) Trang *check.php*

(5) Trang *app.php*

(6) Trang *register.php*

3.1.6 Quá trình đăng kí:

3.1.7 Quy trình hoạt động của hệ thống xác thực

Quá trình xác thực của hệ thống được thực hiện theo các bước sau:

(1) Trước tiên, người dùng chạy ứng dụng mOTP trong điện thoại di động của người dùng. Nhập vào mã PIN đã đăng kí. Ứng dụng sẽ kết hợp thời gian hiện hành (múi giờ trên điện thoại di động phải đồng bộ với múi giờ trên server chạy hệ thống xác thực) cùng với mã bí mật Init-Secret (được lưu giữ trên điện thoại trong quá trình khởi tạo ứng dụng mOTP) và mã PIN tạo thành một tập các kí tự. Ứng dụng mOTP sẽ băm tập các kí tự này bằng giải thuật MD5. OTP được tạo ra chính là 6 kí tự đầu tiên của dãy các kí tự đã được băm. Để giữ đồng bộ về thời gian giữa server và client, biên độ thời gian sẽ được cộng trừ 3 phút ở phía server.

(2) Người dùng đăng nhập vào hệ thống xác thực với username và OTP ở trang ***login.php***.

(3) Hệ thống dựa vào username người dùng nhập vào để tìm mã PIN và mã bí mật Init-Scret của người dùng đó trong bảng *users* trong cơ sở dữ liệu trên server.

(4) Hệ thống thực hiện đồng bộ thời gian trên server và điện thoại di động bằng cách sử dụng một vòng lặp với biến thời gian $i chạy trong biên độ thời gian hiện hành trên server ±3 phút. Kết hợp biến thời gian $i cùng với mã bí mật Init-Scret và mã PIN tạo nên một chuỗi các kí tự. Sau đó băm chuỗi các kí tự này bằng thuật toán MD5 và lấy 6 kí tự đầu tiên làm thành một OTP.

(5) So sánh OTP trên server và OTP do người dùng nhập vào trang đăng nhập. Nếu chúng trùng khớp với nhau thì quá trình xác thực thành công. Người dùng sẽ được chuyển vào trang ứng dụng app.php.

(6) Ngược lại, tiếp tục thực hiện vòng lặp cho đến khi kết thúc.

3.1.8 Thuật toán thực hiện

Hàm kiểm tra username và password được cung cấp bởi người dùng:

CheckOTP ($username, $password)

Input: $username và $password.

Output: **True** (login thành công), ngược lại là **False.**

Bắt đầu:

1. Người dùng nhập vào $username và $password.
2. Mở kết nối cơ sở dữ liệu.
3. Kiểm tra có tồn tại $username trong bảng *users*, Nếu có:

- Gán init vào biến $secret.
- Gán pin vào biến $pin.

4. Đóng kết nối cơ sở dữ liệu.
5. Convert thời gian hiện tại sang dạng chuỗi và gán vào biến $time.
6. For ($i = $time -3; $i <= $time + 3; $i++)

   - Kết hợp 3 biến $i.$secret.$pin, hash bằng md5, lấy sáu kí tự đầu và gán vào biến $serverotp.
   - If ($serverotp==$password)

     Return True

   End for
7. Return False

Kết thúc.

3.2 TRIỂN KHAI CÀI ĐẶT THỬ NGHIỆM TRÊN CC VÀ ĐÁNH GIÁ

3.2.1 Cài đặt

Chọn nhà cung cấp dịch vụ nền tảng (PaaS) là PHPFog, với mô hình triển khai là Public Cloud (đám mây chung). PHPFog tích hợp đầy đủ các công nghệ phổ biến hiện nay để phát triển một ứng dụng web trên CC, bao gồm web server Apache 2.0, hỗ trợ PHP v5.3.2 và MySQL 5.1.41. Người dùng khi đăng kí một tài khoản free được cung cấp: shared RAM, shared CPU, 100MB Storage, Scalable MySQL Database, 15 GB Bandwidth, chạy 1 ứng dụng, sử dụng trong vòng 6 tháng.

Thực hiện đăng kí một account trên ***phpfog.com***. Tạo ứng dụng tên là: motp.phpfogapp.com, đây cũng chính là

domain (một subdomain) phpfog cung cấp cho khách hàng. Tiến hành triển khai hệ thống xác thực trên domain này.

3.2.2 Run ứng dụng:

Mở trình duyệt web, gõ địa chỉ: motp.phpfogapp.com/login.php

Hình 3.16: Trang Login của hệ thống xác thực

Click vào Register để đăng ký một account.

Hình 3.17: Trang đăng kí của hệ thống xác thực

Khi đăng kí thành công, hệ thống gửi một email đến địa chỉ email của người dùng đăng kí thành công. Trong email này cung cấp một link để người dùng tải ứng dụng phía client mOTP về cài đặt trên điện thoại di động. Sau khi cài xong, chạy ứng dụng và tiến hành khởi tạo cho ứng dụng bằng cách nhấn 0000, nhập vào 25 kí tự ngẫu nhiên. Quá trình khởi tạo hoàn thành, một mã bí mật Init được tạo ra (gồm 16 kí tự), lưu giữ mã bí mật Init này để nhập trực tiếp vào cơ sở dữ liệu (bảng **users**) trên server.

Bước tiếp theo, người quản trị hệ thống (Administrator) sẽ insert dữ liệu gồm username, PIN và mã bí mật Init bằng tay trực tiếp vào bảng **users** trong database (Hình 3.20):

Hình 3.20: Nhập giá trị các trường cho một account

Mở ứng dụng mOTP trên điện thoại di động, nhập vào mã PIN đã đăng kí (ví dụ 1234), ứng dụng sẽ tạo nên một OTP.

Trên trang đăng nhập của hệ thống xác thực, nhập Username và OTP vào, nhấp nút Login. Hệ thống xác thực sẽ so sánh với OTP được tạo phía server. Nếu bằng nhau, người dùng đăng nhập thành công.

Hình 3.22: Login thành công

3.2.3 Kết quả thử nghiệm hệ thống xác thực mOTP

Sau khi cài đặt hệ thống xác thực mOTP thành công trên đám mây được cung cấp theo kiểu Dịch vụ nền tảng PaaS tại địa chỉ *motp.phpfogapp.com* tôi đã tiến hành kiểm thử hệ thống xác thực với các trình duyệt web phổ biến như IE, Google Chrome, Firefox và vào nhiều thời điểm khác nhau trong nhiều ngày. Hệ thống chạy nhanh, email được gửi đến tất cả người dùng đăng kí thành công, xác thực người dùng chính xác trên tất cả các trình duyệt này vào mọi thời điểm, mọi nơi trong nhiều ngày thử nghiệm.

3.3 KẾT LUẬN CHƯƠNG

Trong chương ba này, luận văn đã giới thiệu giải pháp xác thực dựa trên phần mềm mã nguồn mở phía client mOTP được cài đặt trên điện thoại di động. Giải pháp được lập trình bằng ngôn ngữ php phía server với sáu trang web, cùng với các bước để đăng kí và triển khai thử nghiệm hệ thống trên CC, đây là bước ứng dụng thực tế cho luận văn.

KẾT LUẬN

Sau thời gian nỗ lực nghiên cứu, phân tích và xây dựng đề tài "***Nghiên cứu đánh giá một số giải pháp bảo mật trong Cloud Computing***" tôi đã hoàn thành các yêu cầu đặt ra của đề tài.

1. KẾT QUẢ ĐẠT ĐƯỢC CỦA LUẬN VĂN

- ✓ Đáp ứng nhu cầu tìm hiểu một cách tổng quan về CC, tìm hiểu về hạ tầng bảo mật của CC trong ba cấp độ mạng, máy chủ và ứng dụng.
- ✓ Dùng hai yếu tố để xác thực: yếu tố thứ nhất là thiết bị mobile phone cài ứng dụng mOTP lưu giữ mã bí mật Init-Secret (cái người dùng có), và yếu tố thứ hai là mã PIN (cái người dùng biết), đây là một hệ thống xác thực tương đối mạnh được áp dụng trong thực tế.
- ✓ Xây dựng hoàn chỉnh thuật toán xác thực sử dụng hai yếu tố kết hợp với thời gian hiện tại, được mã hóa bằng thuật toán mã hóa một chiều MD5.
- ✓ Triển khai cài đặt thử nghiệm hệ thống thành công trên CC.
- ✓ Sử dụng điện thoại di dộng để xác thực đem lại sự dễ dàng cho người dùng nhưng hệ thống vẫn được bảo mật với độ an toàn cao.
- ✓ Hệ thống xác thực người dùng được xây dựng dựa trên mã nguồn mở, sử dụng các công cụ web server Apache, ngôn ngữ lập trình php, cơ sở dữ liệu MySQL tất cả là free nên chi phí đầu tư cho dự án này rất thấp.

2. HẠN CHẾ CỦA LUẬN VĂN

- ✓ Giao diện hệ thống còn đơn giản.
- ✓ Việc lưu mã bí mật Init- Secret vào cơ sở dữ liệu được thực hiện trực tiếp bằng tay.
- ✓ Thông tin cá nhân được lưu trên cơ sở dữ liệu chưa được mã hóa.

3. HƯỚNG PHÁT TRIỂN

- ✓ Tiếp tục xây dựng giao diện hệ thống.
- ✓ Nghiên cứu tìm cách để lưu mã bí mật Init- Secret vào cơ sở dữ liệu tự động nhưng không truyền qua Internet mà lưu tự động trực tiếp từ phía server.
- ✓ Áp dụng mã hóa hai chiều cho dữ liệu thông tin cá nhân của người dùng.