NGHIÊN CỨU CÁC GIẢI PHÁP CHỨNG THỰC TÀI KHOẢN TẬP TRUNG CHO CÁN BỘ GIẢNG VIÊN, CÔNG NHÂN VIÊN VÀ SINH VIÊN TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI THÀNH PHỐ HỒ CHÍ MINH

RESEARCH SOLUTIONS FOR AUTHORIZATION OF CONCENTRATED ACCOUNTS FOR EMPLOYEES, TEACHERS, AND STUDENTS IN THE HO CHI MINH CITY UNIVERSITY OF TRANSPORT

[1]Bùi Dương Thế, [2]Đặng Nhân Cách
[1,2]Trung tâm Dữ liệu và Công nghệ thông tin
Đại học Giao thông vận tải Thành phố Hồ Chí Minh

Tóm tắt*: Trong những năm gần đây, Trường Đại học Giao thông vận tải Thành phố Hồ Chí Minh đã tích cực triển khai và áp dụng Công nghệ thông tin trong mọi lĩnh vực quản lý, dạy học của Nhà trường. Mỗi sản phẩm công nghệ thông tin được đưa vào sử dụng trước đây thì cơ sở dữ liệu người dùng được lưu trữ độc lập, khi đó việc quản lý tài khoản người dùng khó khăn, người dùng phải nhớ nhiều tài khoản, mật khẩu khác nhau. Bài báo đề cập đến nghiên cứu giải pháp chứng thực tập trung, qua đó xây dựng hệ thống chứng thực tập trung thông qua Web API (Application Programming Interface) để xác thực tài khoản người dùng về một cơ sở dữ liệu nhất quán. Tất cả các ứng dụng công nghệ thông tin sau này khi triển khai sẽ được chứng thực qua hệ thống này, giúp cho Nhà trường quản lý tài khoản người dùng tập trung và cán bộ, giảng viên, sinh viên sẽ dùng một tài khoản duy nhất để truy cập vào ứng dụng mà Nhà trường cho phép.*

Từ khóa*: Chứng thực, chứng thực tập trung, quản lý tập trung.*

Chỉ số phân loại: *1.4*

Abstract*: In recent years, Ho Chi Minh City University of Transport has successfully implemented Information Technology in all areas of educational management and administration. The former IT products allowing user database separately stored have triggered diverse issues for user account management when the users have to remember different accounts and passwords simultaneously. Therefore, this article will focus on centralized authentication solution, thereby building a centralized authentication system through Web API (Application Programming Interface) to consolidate user accounts into a consistent database. In the future, all state of the art applications then will be examined and deployed by this system in order to manage user accounts attentively. Not only staff, lecturers but also students will use one unique account for accessibility to any school applications allowed..*

Keywords*: Authentication, centralized certification, centralized management.*

Classification number: *1.4*

1. Giới thiệu

Hiện nay, Trường Đại học Giao thông vận tải Thành phố Hồ Chí Minh (ĐH GTVT TP.HCM) đã áp dụng nhiều hệ thống thông tin vào quản lý, đào tạo và học tập. Nhưng phần nhiều các ứng dụng đều có cơ sở dữ liệu quản lý tài khoản người dùng riêng biệt. Vì vậy sẽ rất khó khăn trong công tác quản lý và sử dụng như: Bộ phận quản trị phải mất nhiều thời gian tạo tài khoản và quản trị trên từng hệ thống; người dùng phải nhớ rất nhiều tài khoản với mỗi hệ thống khác nhau thuộc Trường.

Trong nghiên cứu này nhóm khai thác các vấn đề sau:

- Nghiên cứu các giải pháp chứng thực tập trung tài khoản người dùng;
- Đồng bộ tài khoản người dùng về một cơ sở dữ liệu chung;
- Xây dựng hệ thống chứng thực cho phép các phần mềm, ứng dụng kết nối để xác thực tài khoản người dùng tập trung về một đầu mối duy nhất.

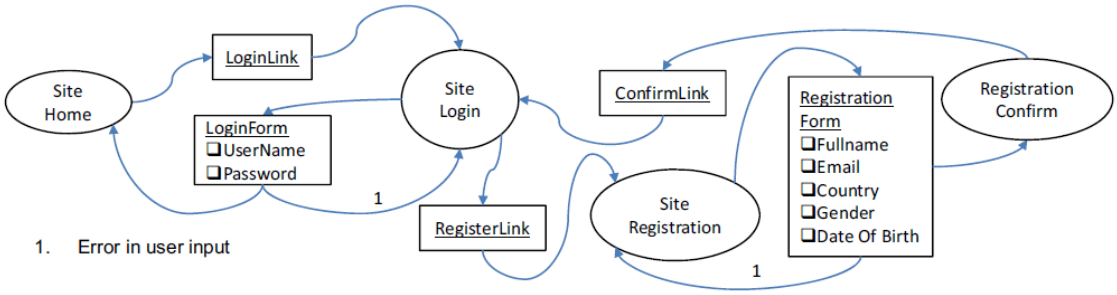
Mục tiêu nghiên cứu đưa ra là mỗi người dùng chỉ cần một tài khoản (username và password) duy nhất, có thể truy cập vào bất kỳ ứng dụng nào được cho phép và trên mỗi ứng dụng phần mềm người dùng sẽ được phân quyền theo nhu cầu riêng.

Khi hệ thống được vận hành, thì người quản lý tài khoản người dùng một trên một hệ thống duy nhất, đối với người dùng chỉ cần nhớ một tài khoản duy nhất có thể truy cập vào bất cứ hệ thống nào được cho phép. Khi cập nhật thông tin người dùng thì tất cả ứng dụng liên quan đều được cập nhật, hoặc khi khóa một tài khoản nào đó, hệ thống chỉ cần khóa một lần thì khi đó tài khoản bị khóa sẽ khóa lại trên tất các ứng dụng còn lại, hệ thống lúc này sẽ an toàn, tránh thiếu xót trong việc quản lý.

2. Các nghiên cứu liên quan

Ngày nay, có rất nhiều hệ thống chứng thực, giải pháp và phương thức xác thực tài khoản người dùng tập trung đang được sử dụng phổ biến. Từ đó xây dựng một hệ thống chứng thực phù hợp với hệ thống nội bộ và cơ sở hạ tầng hiện tại để triển khai thử nghiệm, đánh giá độ ổn định, độ tin cậy và khả năng mở rộng cao. Dưới đây là những mô tả về các phương pháp đã được sử dụng phổ biến:

OpenID [1] là một tiêu chuẩn chứng thực tập trung, cho phép các đối tác, website, tổ chức muốn sử dụng để chứng thực người dùng. Các nhà phát triển website không cần phải xây dựng phần đăng ký đăng nhập trên hệ thống của họ. Từ OpenID người dùng có thể chứng thực nhiều website khác nhau mà chỉ cần một tài khoản, một mật khẩu để sử dụng.



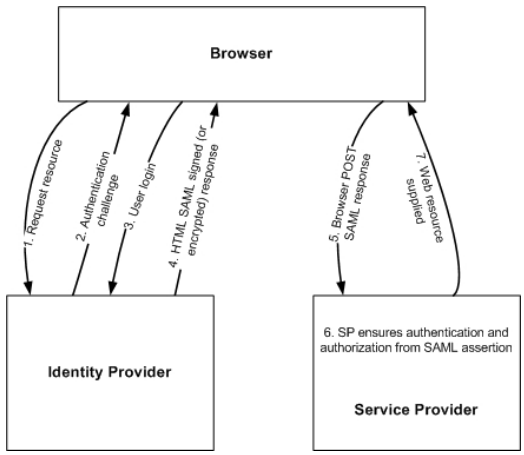
Hình 1. *Mô hình chứng thực OpenID.*

OAuth2 [2] là một phương thức chứng thực tập trung, giúp cho các ứng dụng, website có thể chia sẻ thông tin với nhau mà không cần cung cấp thông tin username và password. Tuy nhiên thông tin người dùng chỉ được cung cấp một số thông tin ở mức hạn chế nhất định. Trong đó:

- Authentication: Xác thực người dùng thông qua việc đăng nhập;

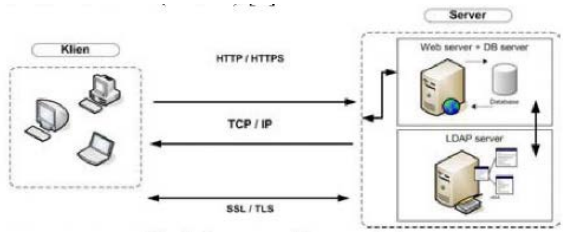
- Authorization: Cấp quyền truy cập vào các thông tin của người dùng.

SAML [3] (Security Assertion Markup Language) xuất hiện từ lâu đời, là một tiêu chuẩn mở để trao đổi dữ liệu xác thực và ủy quyền giữa các bên, đặc biệt giữa nhà cung cấp nhận dạng và nhà cung cấp dịch vụ. Khi đó người dùng có thể truy cập những thông tin ở các nhà cung cấp dịch vụ khác nhau được liên kết.



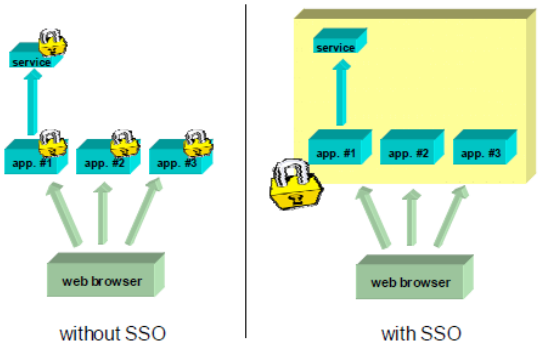
Hình 2*. Mô hình chứng thực SAML.*

LDAP [4] (Lightweight Directory Access Protocol) là một giao thức dựa trên mô hình Client Server, cho phép Client chứng thực, kết nối truy cập tài nguyên theo phân quyền từ Server. Một số ứng dụng và website ứng dụng cũng dùng giao thức này để chứng thực người dùng, chia sẻ tài nguyên thông tin thông qua Server Active Directory.



Hình 3. *Mô hình chứng thực LDAP.*

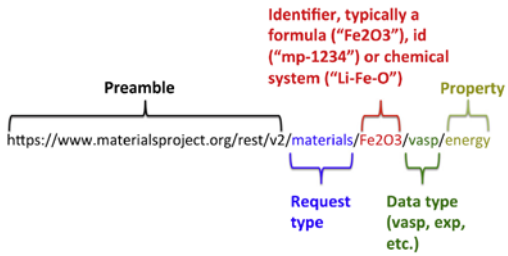
SSO [3] Single Sign On là một cơ chế xác thực yêu cầu người dùng đăng nhập chỉ một lần với một tài khoản và mật khẩu để truy cập vào nhiều ứng dụng trong một phiên làm việc.



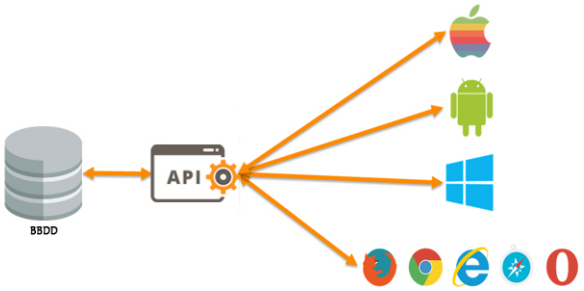
Hình 4. *Mô hình chứng thực SSO.*

Trên đây là những phương pháp chứng thực đã được sử dụng rộng rãi cho đến ngày nay. Trong bài báo này, qua việc tiến hành phân tích cách vận hành của các hệ thống chứng thực trên, từ đó lựa chọn những điểm tiện dụng và phù hợp để xây dựng cho Trường ĐH GTVT TPHCM một hệ thống chứng thực riêng biệt phù hợp với nhu cầu thực tế.

API [5] được viết tắt từ Application Programming Interface (giao diện lập trình ứng dụng) là các phương thức, giao thức kết nối với các thư viện và ứng dụng khác. API cung cấp khả năng cung truy xuất đến một tập các hàm hay dùng. Và từ đó có thể trao đổi dữ liệu giữa các ứng dụng.



Hình 5.*Ví dụ về cấu trúc API.*



Hình 6. *API cho phép hầu hết các ứng dụng kết nối.*

Web API hỗ trợ restful đầy đủ các phương thức như :get/post/put/delete dữ liệu giúp cho xây dựng các HTTP service một cách rất đơn giản và nhanh chóng. Ngoài ra cũng có khả năng hỗ trợ đầy đủ các thành phần HTTP: URI, request /response headers, caching, versioning, content forma. Khi xây dựng API thì URL API có thể để bên thứ ba dễ dàng gửi request dữ liệu đến máy chủ cung cấp nội dung thông qua giao thức HTTP hoặc HTTPS. Tại web server cung cấp nội dung, các ứng dụng nguồn sẽ thực hiện kiểm tra xác thực nếu có và tìm đến tài nguyên thích hợp để tạo nội dung trả về kết quả.

Server trả về kết quả theo định dạng JSON hoặc XML thông qua giao thức HTTP/HTTPS. Tại nơi yêu cầu ban đầu là ứng dụng web hoặc ứng dụng di động, dữ liệu JSON/XML sẽ được đọc để lấy dữ liệu. Sau khi có được dữ liệu thì thực hiện tiếp các hoạt động như lưu dữ liệu đến cơ sở dữ liệu, hiển thị dữ liệu…

3. Thực trạng hệ thống

Trong phần này nhằm mô tả lại thực trạng hệ thống đang gặp nhiều vấn đề gây khó khăn cho người quản lý và người dùng trong quá trình sử dụng.

DB1

id	user	name
1	the.bui	Bui Duong The

DB2

id	username	HovaTen
10	duongthe	Bui Duong The

DB3

id	username	fullname
1656	the.bd	Bui Duong The

DB4

id	username	ho	ten
1356	the_ditc	Bui Duong	The

Hình 7. *Mô tả cấu trúc lưu tài khoản người dùng.*

Hình 7 mô tả lại cách xây dựng, quản lý tài khoản người dùng ở các ứng dụng phần mềm cũ trong đó:

- Người viết ứng dụng phần mềm không nhất quán cấu trúc bảng dữ liệu tài khoản;

- Mỗi quản trị viên khởi tạo tài khoản theo ý muốn của mình, không tuân thủ quy luật hay chính sách nội bộ.

Như vậy, người dùng buộc phải nhớ các tài khoản của mình, mỗi khi đổi mật khẩu phải đổi mật khẩu trên từng hệ thống phần mềm.

4. Phương pháp đồng bộ hóa tài khoản

Trong nghiên cứu này sẽ tiến hành đồng bộ tài khoản người dùng về một mối duy nhất, là nơi lưu trữ tài khoản tập trung, xác thực tập trung, quản lý người dùng tập trung.

Với phương pháp này sẽ xem xét nhu cầu thực tế và tương lai, như vậy cần xác định xây dựng hạ tầng mạnh mẽ, ổn định, khả năng mở rộng cao để đáp ứng nhu cầu cho cả thực tế và các ứng dụng tiếp theo có thể tích hợp để cùng phát triển.

DB New

id	username	hoten	ten	alias
10	102103104	Bui Duong	The	the.bui

DB1

id	user	name	mans
1	the.bui	Bui Duong The	102103104

DB2

id	username	HovaTen	mans
10	duongthe	Bui Duong The	102103104

DB3

id	username	fullname	mans
1656	the.bd	Bui Duong The	102103104

DB4

id	username	ho	ten	mans
1356	the_ditc	Bui Duong	The	102103104

Hình 8. *Phương pháp đồng bộ tài khoản.*

4.1. Phương pháp đồng bộ

- Xây dựng một cơ sở dữ liệu mới (**DB New**) đó là mô hình dữ liệu quan hệ, đủ lớn, để có khả năng mở rộng, liên kết với thông tin nhân sự (**HR**);

- Trên các cơ sở dữ liệu cũ tạo thêm một trường (**mans**) có dữ liệu trùng với cơ sở dữ liệu mới (**username**).

4.2. Phương pháp thực hiện

- Nếu tài khoản nào đã biết rõ thông tin thì tiến hành cập nhật thêm trường (**mans**) cho tài khoản đó;

- Các tài khoản chưa rõ thông tin sẽ cho người dùng tự cập nhật trường (**mans**);

- Trên cơ sở dữ liệu mới (**DB New**) sẽ chọn một cách đặt tên tài khoản người dùng có quy tắc, nhằm gợi nhớ cho người dùng.

5. Hệ thống chứng thực tập trung

Đề tài nghiên cứu đã xây dựng quy trình vận hành hệ thống chứng thực tập dựa trên kiến trúc API bởi vì đơn giản, dễ triển khai, phù hợp với cơ sở hạ tầng sẵn có của Nhà trường, đáp ứng được đa nền tảng kết nối truy xuất dữ liệu.

Hình 9. *Mô hình xử lý chứng thực tập trung.*
AC: Authenticate Center;
DB New: Cơ sở dữ liệu tài khoản người dùng đã đồng bộ.

Quy trình xử lý như sau:

- Người dùng login vào ứng dụng;
- Ứng dụng sẽ kết nối với AC;
- AC kết nối với DB New;
- DB New trả kết quả về cho AC;
- Ứng dụng nhận được kết quả trả về cho người dùng thông qua các trạng thái sau:

+ 200: Đăng nhập thành công và có đủ thông tin đăng nhập;

+ 404: Thông báo không tìm thấy tài khoản;

+ 401: Thông báo đăng nhập không thành công;

+ 403: Không có quyền truy cập;

+ 500: Các lỗi khác.

Trong trường hợp kết quả đăng nhập có mã trạng thái là 200 thì tại ứng dụng sẽ kiểm tra tài khoản có tồn tại trong cở sở dữ liệu hay không, nếu chưa, hệ thống sẽ tạo tài khoản mới để truy cập ứng dụng, trường hợp tài khoản đã tồn tại thì cho phép truy cập ứng dụng và cập nhật các thông tin cần thiết khác.

6. Bảo mật thông tin

An toàn và bảo mật thông tin người dùng là một vấn đề quan trọng. Bởi vì các ứng dụng được phép kết nối lấy thông tin tài khoản để xác thực cho người dùng, vì thế nghiên cứu đã đưa ra các chính sách bảo mật kết nối, truy xuất thông tin như sau:

- Ứng với mỗi tài khoản, khi khởi tạo trên hệ thống, người quản trị sẽ cấp cho tài khoản này dùng những dịch vụ được phép sử dụng;

- Đối với ứng dụng được kết nối, hệ thống sẽ tạo một khóa (key), thông qua đó ứng dụng có thể truy xuất thông tin tài khoản người dùng;

- Những ứng dụng và dịch vụ chứng thực chỉ được sử dụng khi kết nối nội bộ hoặc kết nối thông qua Access list, Iptables, Firewall;

- Đối với tài khoản người dùng, hệ thống mã hóa thông tin trước khi gửi đi xác thực và kèm theo dịch vụ SSL.

7. Kết luận

7.1. Kết quả đạt được

Trong nghiên cứu này, đưa ra các giải pháp chứng thực tập trung đồng thời phối hợp với nhu cầu thực tế, cơ sở hạ tầng, mục đích sử dụng, từ đó xây dựng cho Nhà trường một dịch vụ chứng thực tập trung, đem lại sự thuận tiện cho người quản lý cũng như người dùng đó là cán bộ, giảng viên, sinh viên. Như vậy, chỉ với một tài khoản người dùng có thể truy cập vào những dịch vụ được cấp phép, qua đó cũng đã triển khai dịch vụ chứng thực tập trung cho các ứng dụng thuộc quản lý của Nhà trường để đánh giá tính hiệu quả, ổn định của hệ thống đã xây dựng.

Các dịch vụ đã triển khai:

- Hệ thống đào tạo trực tuyến;
- Hệ thống thi ngoại ngữ đầu vào;
- Hệ thống SMS;
- Hệ thống hỗ trợ trực tuyến;
- Hệ thống wifi;
- Hệ thống tin nội bộ giảng viên;
- Hệ thống thư viện trực tuyến.

Trong quá trình triển khai từ ngày 15/6/2017, nghiên cứu đã đạt được kết quả rất khả quan, hệ thống đã và đang hoạt động ổn định. Từ đó cho thấy, các ứng dụng được phát triển sau này có thể sử dụng dịch vụ chứng thực tập trung. Trung bình một ngày hệ thống xử lý 4000 đến 5000 lượt chứng thực.

7.2. Hướng phát triển

Đề tài nghiên cứu này cũng rất hữu ích cho các Trường, công ty doanh nghiệp lớn muốn phát triển hệ thống chứng thực tập trung cho đa nền tảng ứng dụng, nhằm quản lý tài khoản người dùng và thuận tiện cho người sử dụng❑

Lời cảm ơn

Đề tài nghiên cứu này được hỗ trợ từ nguồn kinh phí nghiên cứu khoa học của Trường Đại học Giao thông vận tải TP. HCM (**MS KH1633**).

Tài liệu tham khảo

[1] J. Bellamy-McIntyre, C. Luterroth, và G. Weber, "*OpenID and the enterprise: A model-based analysis of single sign-on authentication*", Proc. - IEEE Int. Enterp. Distrib. Object Comput. Work. *EDOC*, tr 129–138, 2011.

[2] M. Jones, B. Campbell, P. Identity, và C. Mortimore, "*JSON Web Token (JWT) Profile for OAuth 2 . 0 Client Authentication and Authorization Grants*", 2014.

[3] K. D. L. andjames E. Lewis, "*Web Single Sign-On Authentication using SAML*", 2009.

[4] R. F. Sari và S. Hidayat, "*Integrating web server applications with LDAP authentication: Case study on human resources information system of UI*", 2006 Int. Symp. Commun. Inf. Technol. Isc., tr 307–312, 2006.

[5] G. C. c Shyue Ping Ong a,⇑, Shreyas Cholia b, Anubhav Jain b, Miriam Brafman b, Dan Gunter b và K. A. P. B, "*The Materials Application Programming Interface (API): A simple, flexible and efficient API for materials data based on REpresentational State Transfer (REST) principles*", *Comput. Mater. Sci. 97*, tr 209–215, 2015.

Ngày nhận bài: 7/2/2020
Ngày chuyển phản biện: 12/2/2020
Ngày hoàn thành sửa bài: 4/3/2020
Ngày chấp nhận đăng: 11/3/2020