GIẢI PHÁP TÍCH HỢP ĐĂNG NHẬP NHIỀU HỆ THỐNG DỰA TRÊN NỀN TẢNG WEB SERVICE

NGUYỄN MINH KHA[*], NGUYỄN THỊ THÙY LINH[**],
NGUYỄN HỮU DUYỆT[**], LƯƠNG THÁI NGỌC[**]

TÓM TẮT

Bài báo này phân tích các bất lợi khi đăng nhập trên nhiều hệ thống khác nhau. Qua đó, tác giả trình bày một số giải pháp tích hợp đăng nhập đã công bố trước đây, đồng thời đề xuất mô hình thống nhất đăng nhập ULM (Unified Login Model) trên nền tảng dịch vụ web (Web Service – WS). Để đánh giá kết quả nghiên cứu, chúng tôi đã cài đặt thực nghiệm tích hợp đăng nhập trên một số hệ thống website đang hoạt động tại Trường Đại học Đồng Tháp.

Từ khóa: ULM, dịch vụ web, tích hợp đăng nhập, xác thực.

ABSTRACT

An integrated login solution for web applications based on Web Service

In this article, we analyse the inconvenience users may encounter when logging in many different systems. Furthermore, we discuss some intergrated login solutions which were introduced previously. We also propose a new solution calling ULM (Unified Login Model) based on WS (Web Service). To examine the results of the study, we have implemented the integration login system for three operating websites at Dong Thap University.

Keywords: ULM, authentication, unified login model, Web Service.

1. Giới thiệu

Ngày nay, công nghệ thông tin đã được ứng dụng rộng rãi trong các tổ chức, doanh nghiệp. Để đáp ứng nhu cầu chuyên môn nghiệp vụ, các tổ chức, doanh nghiệp thường phải vận hành đồng thời nhiều hệ thống độc lập với nhau, có thể dựa trên các nền tảng khác nhau. Mỗi hệ thống sở hữu một danh mục tài khoản với các chính sách bảo mật riêng, nên việc quản lí người dùng trở nên phức tạp. Điều quan trọng là người dùng gặp nhiều khó khăn khi sử dụng, vì phải ghi nhớ nhiều thông tin tài khoản tương ứng với mỗi hệ thống. Vì vậy, vấn đề thống nhất đăng nhập một lần trên nhiều hệ thống đã được nhiều tác giả nghiên cứu, và đã có một số giải pháp đề xuất trong thời gian qua, các giải pháp này tập trung phát triển cho các ứng dụng web dựa trên một số nền tảng khác nhau.

Trong thời gian qua đã có một số nghiên cứu nhằm giải quyết vấn đề thống nhất đăng nhập. Tiêu biểu là Li cùng các cộng sự đã đề xuất giải pháp chứng thực thống nhất dựa trên LDAP [7]. Tác giả Liang đã thiết kế và cài đặt hệ thống đăng nhập một lần (Single Sign-on) bằng cách kết hợp các công nghệ Web Service, Applet và Reverse Proxy

[*] Kĩ sư, Trường Đại học Đồng Tháp; *Email: nmkha@dthu.edu.vn*
[**] ThS, Trường Đại học Đồng Tháp

[8]. Wang cũng đã đề xuất và cài đặt giải pháp thống nhất đăng nhập (Unified Identity Authentication) dựa trên LDAP và RBAC [9]. Tuy nhiên, các nghiên cứu này chưa đưa ra được giải pháp đồng bộ các tài khoản trên nhiều hệ thống. Chúng tôi nhận thấy rằng các giải pháp đã công bố chỉ phù hợp ở giai đoạn bắt đầu phát triển ứng dụng, mà chưa đề cập đến khả năng tích hợp đăng nhập cho các hệ thống đang hoạt động. Trong bài báo [9], tác giả đề ra hai giải pháp tích hợp đăng nhập cho các hệ thống đang hoạt động và hệ thống được phát triển mới. Tuy nhiên, vấn đề đồng bộ hóa tài khoản giữa các hệ thống chưa được giải quyết triệt để vì việc đồng bộ hóa phải tiến hành một cách thủ công.

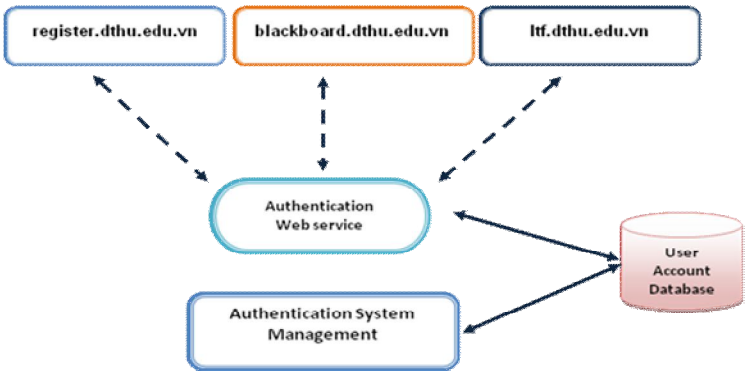
Ngoài ra, SAML (Security Assertion Markup Language) được OASIS phát triển trong [1, 4], đây là chuẩn mở dựa trên cấu trúc XML dùng để đóng gói dữ liệu truyền thông giữa các ứng dụng web. SAML cũng được ứng dụng trong việc xây dựng hệ thống tích hợp đăng nhập. Tuy nhiên, SAML vẫn còn một số hạn chế như vấn đề an ninh và khả năng thích ứng kịp thời của hệ thống. Tác giả [5, 6] trình bày giao thức OpenID là giao thức cung cấp cơ chế chứng thực người dùng theo giải pháp phân tán. Giao thức này được sử dụng rộng rãi nhưng vẫn còn một số hạn chế, nên nó trở thành mục tiêu của các cuộc tấn công giả danh, ngoài ra giao thức này tồn lại lỗ hổng cho phép khai thác thông tin cá nhân của người dùng. Tác giả [2] đề xuất CAS (Central Authentication Service), đây là giao thức cho phép xây dựng hệ thống đăng nhập một lần. CAS có độ bảo mật và tính linh động cao, ngoài ra CAS được hỗ trợ nhiều thư viện tương thích với nhiều nền tảng khác nhau. Tuy nhiên, CAS vẫn tồn tại một số hạn chế về bảo mật và hiệu năng. Tác giả [3], trình bày giải pháp đăng nhập một lần (SSO) trên nền tảng web với ưu điểm là đơn giản và dễ triển khai, tuy nhiên hạn chế là tồn tại nhiều lỗ hổng mà hacker có thể khai thác để đánh cắp thông tin tài khoản.

Trong nghiên cứu này, chúng tôi sẽ trình bày mô hình ULM nhằm thống nhất tài khoản đăng nhập cho các website đang hoạt động một cách tự động. Trong phần tiếp theo chúng tôi sẽ trình bày chi tiết mô hình ULM, giải pháp xây dựng hệ thống đăng nhập một lần ở Trường Đại học Đồng Tháp và cuối cùng là kết luận.

2. Mô hình thống nhất đăng nhập - ULM

Ý tưởng chính của mô hình ULM là cho phép quản lí người dùng một cách tập trung, nó cung cấp dịch vụ chứng thực chung cho nhiều hệ thống. Tài khoản người dùng được đồng bộ, điều này cho phép tài khoản xác thực trên hệ thống A sẽ có thể truy cập vào các hệ thống khác mà không phải tiến hành đăng nhập lại, người dùng có thể sử dụng một tài khoản đăng nhập vào nhiều hệ thống khác nhau. Ngoài ra, việc đăng xuất trên hệ thống A sẽ được tự động đăng xuất trên các hệ thống khác.

Trong mô hình ULM (Hình 1) có 3 thành phần chính: Thứ nhất, *Authentication System Management* là công cụ quản trị, cho phép quản trị tài khoản, quản lí danh mục các hệ thống website cần thống nhất đăng nhập; Thứ hai, *Authentication Web service* (Auth-WS) được chúng tôi xây dựng dựa trên nền tảng WS, nó cung cấp chức năng chứng thực người dùng cho các hệ thống khác, ngoài ra Auth-WS còn cung cấp chức năng cập nhật, quản trị tài khoản; Thứ ba, *User Account Database* là cơ sở dữ liệu lưu trữ thông tin người dùng của các hệ thống đang hoạt động.

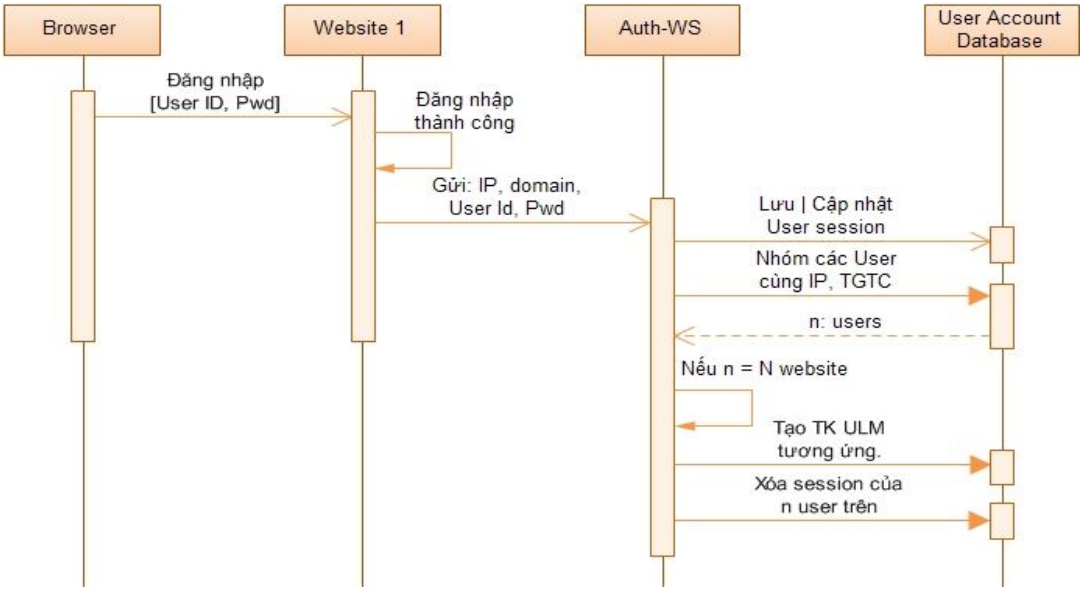


Hình 1. *Mô hình thống nhất đăng nhập ULM*

Để thực hiện thống nhất đăng nhập, giải pháp ULM phải giải quyết một số vấn đề cốt lõi như: Thứ nhất, việc đồng bộ tài khoản người dùng trên các hệ thống phải được thực hiện tự động; Thứ hai, việc đăng nhập trên một hệ thống nào đó người dùng sẽ được tự động đăng nhập trên hệ thống khác; Thứ ba, việc đăng xuất trên hệ thống này cũng sẽ đăng xuất trên hệ thống khác.

2.1. Vấn đề đồng bộ tài khoản trong mô hình ULM

Danh sách các tài khoản người dùng từ nhiều hệ thống phải được đồng bộ thành danh sách tài khoản chung trong mô hình ULM. Quá trình đồng bộ được diễn ra mỗi khi người dùng đăng nhập vào hệ thống bằng tài khoản nào đó. Sau khi đăng nhập, hệ thống sẽ thu thập thông tin gồm địa chỉ máy trạm, tên miền, tên đăng nhập và mật khẩu gửi đến ULM, và được ULM kiểm tra thông tin tài khoản và lưu vào cơ sở dữ liệu nếu tài khoản không tồn tại.



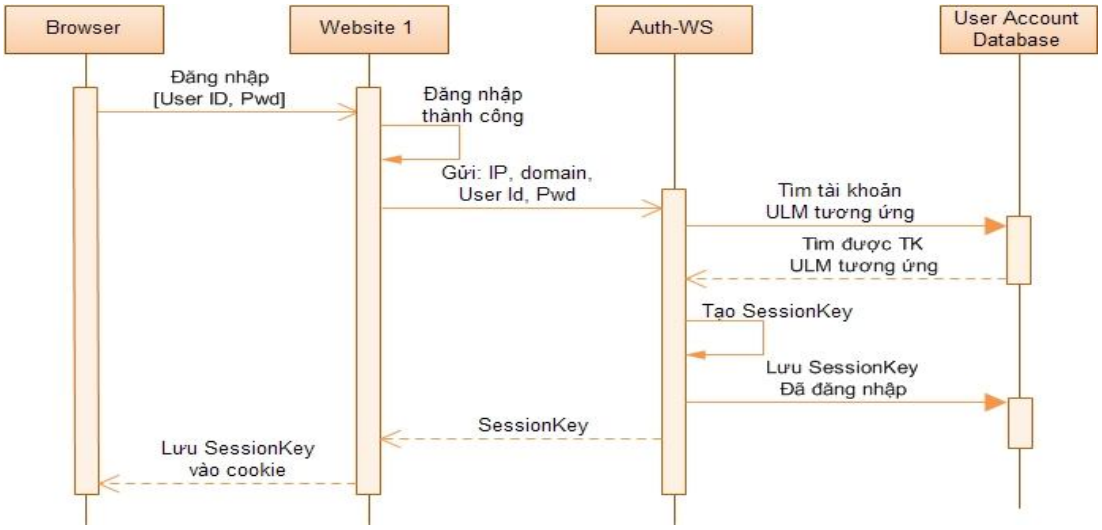
Hình 2. *Sơ đồ đồng bộ tài khoản người dùng*

Hệ thống ULM có thể truy vấn các tài khoản cùng một chủ sở hữu bằng cách đọc nhật kí truy cập theo địa chỉ IP và thời gian truy cập. Nhờ vậy mà nó có thể gom nhóm các tài khoản, sau đó tạo một tài khoản ULM đại diện cho nhóm. Hay nói cách khác, sau khi quá trình đồng bộ diễn ra, một người dùng sẽ có một tài khoản ULM sử dụng chung trên tất cả các hệ thống.

2.2. Vấn đề đăng nhập và tự động đăng nhập trên hệ thống khác

a) Đăng nhập

Sau khi hoàn thành quá trình đồng bộ tài khoản, ta cần kích hoạt hệ thống đăng nhập một lần, qua đó cho phép các ứng dụng được phép chứng thực dựa vào các dịch vụ của hệ thống trong ULM. Khi người dùng đăng nhập thành công vào một ứng dụng bất kì, ứng dụng sẽ gửi thông tin gồm địa chỉ IP, tên đăng nhập, mật khẩu và tên miền đến hệ thống ULM. Hệ thống ULM sẽ tự động tạo một khóa tương ứng với phiên làm việc. Hệ thống sẽ tìm được tài khoản trong ULM tương ứng và lưu trạng thái phiên làm việc vào cơ sở dữ liệu. Đồng thời gửi SessionKey về cho ứng dụng, SessionKey được ứng dụng lưu vào cookie của trình duyệt và được chia sẽ cho các ứng dụng khác.



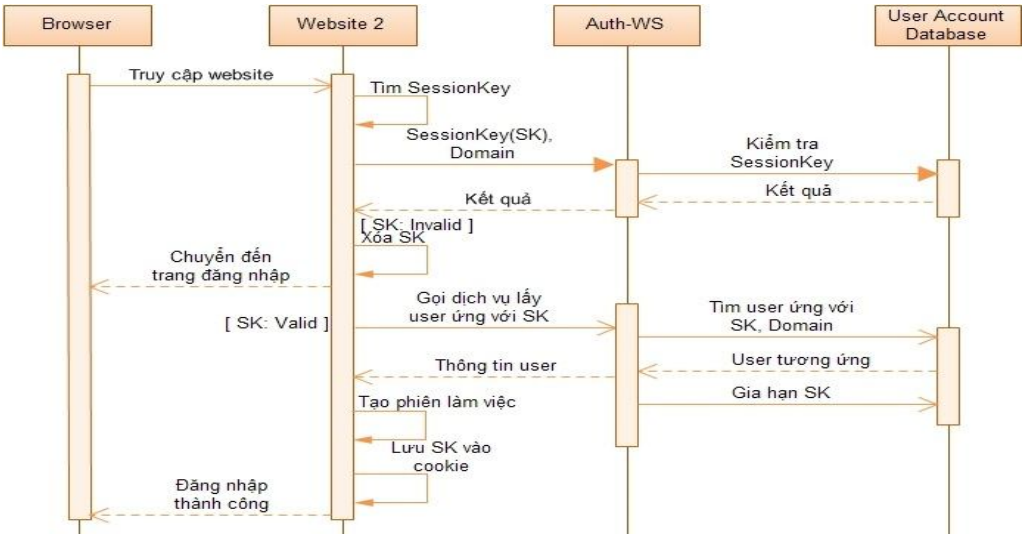
Hình 3. *Sơ đồ đăng nhập trên website 1*

b) Tự động đăng nhập trên hệ thống khác

Sau khi đã đăng nhập một hệ thống, thông tin về phiên làm việc trước đó đã được lưu vào cookie của trình duyệt. Khi người dùng truy cập vào ứng dụng khác, người dùng sẽ được tự động đăng nhập vào hệ thống mà không cần biết tài khoản. Quá trình này được tiến hành như sau:

Khi truy cập vào hệ thống khác, nó sẽ đọc cookie và tìm thông tin về phiên làm việc trước đó. Nếu không tìm được SessionKey hoặc SessionKey hết hạn, người dùng phải đăng nhập lại bằng một tài khoản người dùng.

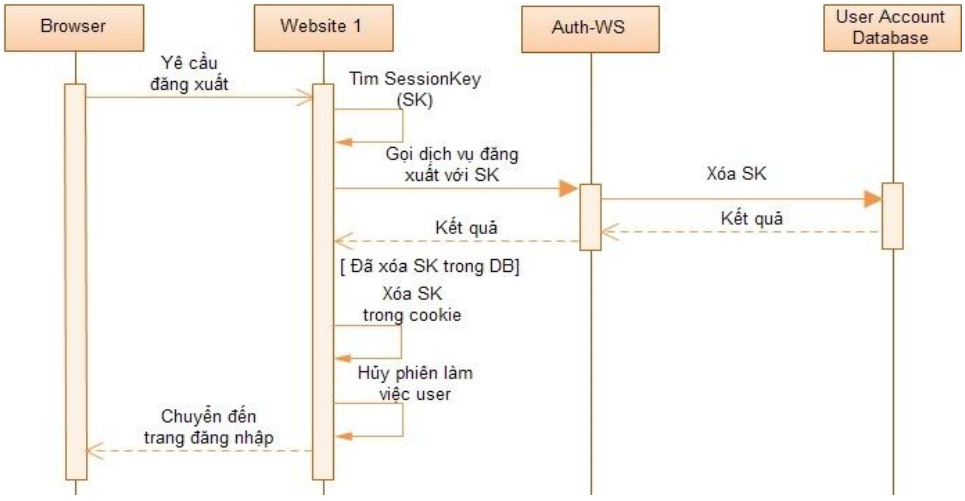
Ngược lại, SessionKey sẽ được gửi đến hệ thống ULM để gia hạn phiên làm việc. Dựa vào nhật kí truy cập và danh sách tài khoản ULM, hệ thống ULM biết được tài khoản người dùng đang truy cập. Thông tin tài khoản này sẽ được gửi ngược lại ứng dụng, ứng dụng tạo phiên làm việc cho người dùng và cập nhật lại SessionKey trong cookie.



Hình 4. *Sơ đồ tự động đăng nhập trên website 2*

2.3. Vấn đề đăng xuất và tự động đăng xuất trên các hệ thống

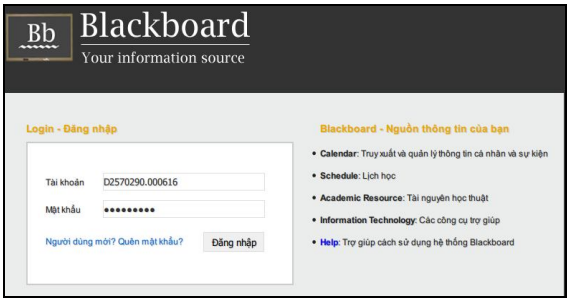
Khi người dùng đăng xuất từ một hệ thống nào đó, SessionKey sẽ được gửi đến ULM. ULM sẽ xóa SessionKey trong cơ sở dữ liệu, đồng thời hệ thống cũng xóa phiên làm việc và thông tin SessionKey trong cookie. Điều này đảm bảo có thể đăng xuất trên toàn bộ các hệ thống.



Hình 5. *Sơ đồ đăng xuất một lần*

3. Thực nghiệm

Để kiểm chứng kết quả nghiên cứu, chúng tôi đã tiến hành cài đặt thực nghiệm thống nhất đăng nhập trên một số hệ thống website đang hoạt động tại Trường Đại học Đồng Tháp. Chúng tôi sử dụng ngôn ngữ lập trình C#, Web Service [10, 11] để xây dựng ULM gồm các mô-đun thống nhất đăng nhập, mô-đun quản trị hệ thống, mô-đun Auth-WS cho phép chứng thực tài khoản.



a) Giao diện học liệu

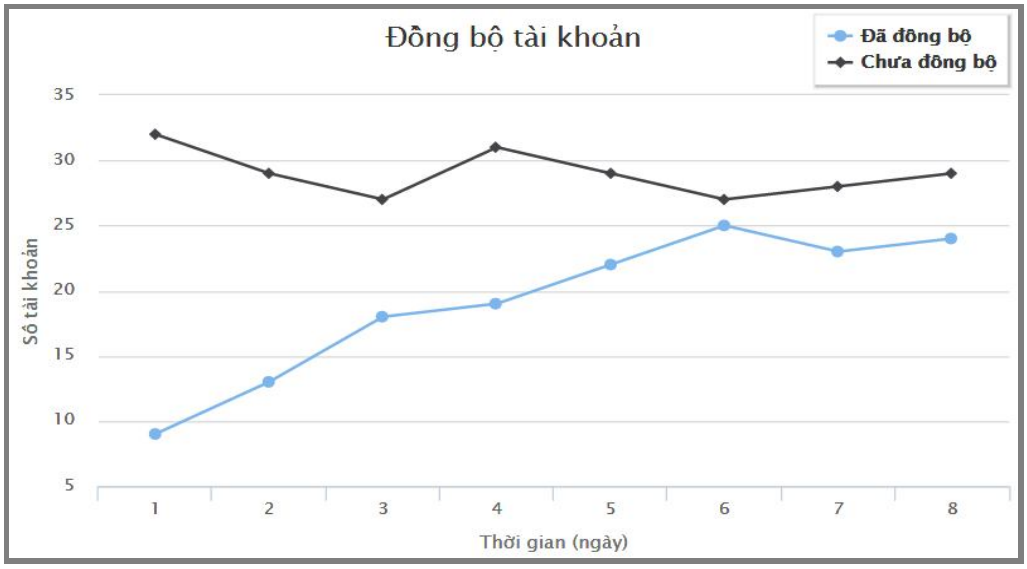
b) Giao diện xem thời khóa biểu

c) Giao diện quản lí đồ án môn học

d) Giao diện quản lí chứng thực

Hình 6. *Giao diện thực nghiệm thống nhất đăng nhập*

Trong giai đoạn đồng bộ hóa tài khoản, chúng tôi can thiệp vào chức năng đăng nhập của các hệ thống blackboard.dthu.edu.vn (Hình 6.a), register.dthu.edu.vn (Hình 6.b) và itf.dthu.edu.vn (Hình 6.c), nhằm thu thập dữ liệu về tài khoản người dùng thông qua Web Service. Thông tin tài khoản người dùng được mô-đun Auth-WS lưu trữ, xử lí để tạo ra các tài khoản thống nhất. Kết quả thực nghiệm trong 8 ngày (Hình 7), tổng số tài khoản được đồng bộ là 153, trung bình mỗi ngày có hơn 19 tài khoản UML được tạo ra.



Hình 7. *Số lượng tài khoản được đồng bộ theo thời gian*

Trong giai đoạn vận hành, các ứng dụng trên đã được đồng bộ tài khoản. Do vậy, người dùng chỉ cần đăng nhập vào một trong 3 ứng dụng, khi truy cập vào 2 ứng dụng còn lại người dùng được đăng nhập một cách tự động. Tuy nhiên, giải pháp này có một số nhược điểm là kết quả của quá trình thống nhất tài khoản cần có thời gian thu thập thông tin và phụ thuộc vào tần suất đăng nhập của người dùng, khó khăn khi can thiệp vào quá trình xác thực của các hệ thống đóng.

4. Kết luận

Như vậy, bài báo đã trình bày một giải pháp thống nhất đăng nhập ULM dựa trên nền tảng WS, giải pháp của chúng tôi bước đầu đã mang lại hiệu quả, với ưu điểm là thống nhất quá trình đăng nhập và chứng thực người dùng trên các hệ thống, quản lí người dùng tập trung giúp giảm chi phí quản trị. Chúng tôi đã cài đặt ULM cho phép thống nhất đăng nhập trên một số website tại Trường Đại học Đồng Tháp và bước đầu mang lại hiệu quả. Giải pháp chúng tôi đảm bảo sự vận hành liên tục của các hệ thống; quá trình đồng bộ hóa diễn ra một cách tự động; không sinh ra một hệ thống chứng thực mới mà chỉ thống nhất việc đăng nhập từ các hệ thống đã có. Tuy nhiên, vấn đề đảm bảo an ninh, hiệu năng và tính ổn định của hệ thống sẽ được chúng tôi tiếp tục nghiên cứu hoàn thiện.

TÀI LIỆU THAM KHẢO

1. Armando, A., Carbone, R., Compagna, L., Cuellar, J., & Tobarra, L. (2008), "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps", *In Proceedings of The 6th ACM workshop on Formal methods in security engineering*, 1-10.
2. Aubry, P., Mathieu, V., & Marchal, J. (2004), "ESUP-Portail: open source Single Sign-On with CAS", *Proceedings of EUNIS04-IT Innovation in a Changing World*.
3. Cao, Y., Shoshitaishvili, Y., Borgolte, K., Kruegel, C., Vigna, G., & Chen, Y. (2014), "Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel", *In Research in Attacks, Intrusions and Defense, Springer*, 276-298.
4. Groß, T. (2003), "Security analysis of the SAML single sign-on browser/artifact profile", *In Computer Security Applications Conference*, IEEE, 298-307.
5. Ionita, M. G. (2012), "Secure Single Sign-On using CAS and OpenID", *Journal of Mobile*, Embedded and Distributed Systems, Vol 4(3), 159-167.
6. Urueña, M., Muñoz, A., & Larrabeiti, D. (2014), "Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites", *Multimedia Tools and Applications*, Vol 68(1), 159-176.
7. Li, Xiang, Ai-nong Chao, and Meng-qiang LIU (2008), "Research and application of LDAP in uniform identity authentication", *Journal of Computer Application*, S1.
8. Liang, Zhigang, and Yuhai Chen (2012), "The Design and Implementation of Single Sign-on Based on Hybrid Architecture", *Journal of Networks 7.1*, 165-172.
9. Wang, Guowei, Guangming Xu, and Manjun Xue (2014), "Unified identity authentication between heterogeneous systems based on LDAP and RBAC", *Journal of Networks 9.10*, 2858-2865.
10. W3C, Web Service Activity (2015), www.w3.org/2002/ws/.
11. W3Schools, XML Web Services (2015), *www.w3schools.com/xml/xml_services.asp*.

(Ngày Tòa soạn nhận được bài: 14-10-2015; ngày phản biện đánh giá: 01-4-2016; ngày chấp nhận đăng: 13-6-2016)