

建構以代理人為基礎之雲端運算服務的單一登入機制

許育魁、曹偉駿

E-mail: 364846@mail.dyu.edu.tw

摘要

目前，雲端服務已有數百個，而使用者只須要註冊一組帳號密碼，就能隨時隨地透過瀏覽器，在各雲端服務平台存取服務。雲端雖然帶來諸多好處，然而，讓使用者擔心的，就是如何確保資料的安全性與機密性。由國際聯盟OASIS制定的安全宣告標記語言 (Security Assertion Markup Language, SAML) 標準，結合了雲端服務單一登入的功能，系統利用重新導向到認證伺服器的方法來達到認證的目的，其做法除了增加主機端之負載以及網路的流量與頻寬的浪費外，在安全上容易遭受重送攻擊及中間人攻擊之風險，因此，很容易造成機密資料與個人隱私的曝露。本論文之主要目的在於透過安全代理人平台與雲端服務進行整合，並建置出在信任模式下之單一登入系統。透過行動代理人本身之自發性攜帶使用者的資訊，讓使用者與主機間的溝通次數減少，以避免遭受駭客及其他惡意攻擊，提高在雲端服務環境之單一登入安全性並保護使用者的帳戶隱私內容，減少分散式環境中網路流量，進而使得整體服務及效能更加流暢。

關鍵詞：雲端運算、行動代理人、單一登入、資訊安全

目錄

內容目錄 中文摘要	iii 英文摘要	
iv 致謝辭	vi 內容目錄	
vii 表目錄	ix 圖目錄	
x 第一章 緒論	第一節 研究背景與動機 1	
第二節 雲端單一登入	第二節 研究目的 2	
第三章 研究方法	第三節 研究流程 2	
第一節 系統架構	第四節 研究架構 5	
第二節 效能比較	第一節 雲端運算安全 12	
第三節 系統實作與模擬	第二節 行動代理人 21	
第一節 硬體架構	第三節 系統流程 26	
第二節 系統設計流程	第一節 安全性分析 34	
第三節 結論與未來發展方向	第二節 綜合比較 36	
第一節 結論	第三節 工具軟體架構 36	
第二節 未來發展方向	第四節 程式執行畫面 36	
	第五章 參考文獻 57	
		59

參考文獻

- 1.M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, " Cloud Computing Security: From Single to Multi-Clouds, " in Proceedings of 2012 45th Hawaii International Conference on System Science (HICSS), pp. 5490-5499, 2012.
- 2.A. Armando, R. Carbone, Luca Compagna, J. Cuellar and Llanos Tobarra, " 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, 2008.
- 3.R. Aversa, B. D. Martino, M. Rak and S. Venticinque, " Cloud Agency: A Mobile Agent Based Cloud System, " in Proceedings of 2010 International Conference on Complex, Intelligent and Software Intensive Systems, pp. 132-137, 2010.
- 4.J. Bellamy-McIntyre, C. Luterroth and G. Weber, " OpenID and the Enterprise:A Model-based Analysis of Single Sign-On Authentication, " in Proceedings of 2011 15th IEEE International Enterprise Distributed Object Computing Conference, pp. 129-138, 2011.
- 5.A. Boldyreva and V. Kumar " Provable-security Analysis of Authenticated Encryption in Kerberos, " IET Information Security, vol. 5, pp. 207-219, 2011.
- 6.A. Celesti, F. Tusa, M. Villari and A. Puliafito, " Federation Establishment Between CLEVER Clouds Through a SAML SSO Authentication Profile, " International Journal on Advances in Internet Technology, vol 4, pp. 14-27, 2011.
- 7.A. Celesti, F. Tusa, M. Villari and A. Puliafito, " Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication, " 2010 Second International Conference on Advances in Future Internet, pp. 94-101, 2010.
- 8.C. C. Chang and C. Y. Lee, " A Secure Single Sign-on Mechanism for Distributed Computer Networks, " IEEE Transactions on Industrial Electronics, Vol. 59, No. 1, PP. 629-637, 2012.
- 9.G. Chen, J. Lu, J. Huang and Z. Wu, " SaaS - The Mobile Agent based Service for Cloud Computing in Internet Environment, " in Proceedings of 2010 Sixth International Conference on Natural Computation (ICNC 2010), pp. 2935-2939, 2010.
- 10.C. T. Fan, W. J. Wang and Y. S. Chang, " Agent-Based Service Migration

Framework in Hybrid Cloud, ” in Proceedings of 2011 IEEE 13th International Conference on High Performance Computing and Communications (HPCC), pp. 887-892, 2011. 11.J. Fang and X. Meng “ Application Investigation on Private Cloud in the Field of Group Company Financial Information Management, ” in Proceedings of 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, pp. 1926-1929, 2011. 12.N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund and M. Pourzandi, “ A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing, ” in Proceedings of 2011 Third IEEE International Conference on Cloud Computing Technology and Science, pp. 231-238, 2011. 13.B. Grobauer, T. Walloschek and E. Stocker, “ Understanding Cloud Computing Vulnerabilities, ” IEEE Security & Privacy, vol. 9, pp. 50-57, 2011. 14.I. Moise, M. Hurfin, L. Zeghache and B. Nadjib, “ Cloud-Based Support for Transactional Mobile Agents, ” in Proceedings of 2011 Workshops of International Conference on Advanced Information Networking and Applications, pp. 190-197, 2011. 15.K. Mukherjee and G. Sahoo “ A Secure Cloud Computing, ” in Proceedings of 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), pp. 269-271, 2010. 16.H. K. Oh and S. H. Jin “ The Security Limitations of SSO in OpenID, ” in Proceedings of ICACT 2008. 10th International Conference on Advanced Communication Technology, vol. 3, pp. 1608-1611, 2008. 17.T. Orawiattanakul, K. Yamaji, M. Nakamura, T. Kataoka and N. Sonehara, “ User-controlled Privacy Protection with Attribute-filter Mechanism for a Federated SSO Environment using Shibboleth, ” in Proceedings of 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 243-249, 2010. 18.G. Papuzzo and G. Spezzano “ Autonomic Management of Workflows on Hybrid Grid-Cloud Infrastructure, ” in Proceedings of 2011 7th International Conference on Network and Service Management (CNSM), pp. 1-4, 2011. 19.S. K. Pippal, A. Kumari and D. S. Kushwaha, “ CTES based Secure approach for Authentication and Authorization of Resource and Service in Clouds, ” in Proceedings of 2011 2nd International Conference on Computer & Communication Technology (IC CCT), pp. 444-449, 2011. 20.L. N. G. Paredes and S. D. Zorzo, “ Privacy Mechanism for Applications in Cloud Computing, ” IEEE Latin America Transactions, Vol. 10, No. 1, pp. 1402-1407, 2012. 21.A. Ramaswamy, A. Balasubramanian, P. Vijaykumar, V. P, “ A Mobile Agent based Approach of Ensuring Trustworthiness in the Cloud, ” in Proceedings of 2011 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 678-682, 2011. 22.A. G. Revar and M. D. Bhavsar “ Securing User Authentication using Single Sign-On in Cloud Computing, ” in Proceedings of 2011 Nirma University International Conference on Engineering (NUiCONE), pp. 1-4, 2011. 23.F. Rocha, S. Abreu and M. Correia, “ The Final Frontier: Confidentiality and Privacy in the Cloud, ” IEEE Computer Society, Vol. 44, pp. 40-50, 2011. 24.K. Sim, “ Agent-based Cloud Computing, ” IEEE Transactions on Services Computing, 2011. 25.S. Subashini and V. Kavitha, “ A Survey on Security Issues in Service Delivery Models of Cloud Computing, ” Journal of Network and Computer Applications, Vol. 34, pp. 1-11, 2011. 26.A. Tripathi and A. Mishra, “ Cloud Computing Security Considerations, ” in Proceedings of 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), pp. 1-5, 2011. 27.W. J. Tsaur, “ Secure Communication for Electronic Business Applications in Mobile Agent Networks, ” Expert Systems With Applications, Vol. 39, No. 1, pp. 1047-1055, 2012. 28.W. J. Tsaur and L. Y. Yeh, “ A Novel Mobile Agent Authentication Scheme for Multi-host Environments Using Self-certified Pairing-based Public Key Cryptosystem, ” International Journal of Innovative Computing, Information and Control, Vol. 7, No. 5(A), pp. 2389-2404, 2011. 29.W. J. Tsaur and Y. M. Lin, “ An Agent-based Single Sign-On Scheme for Web Services Environments, ” in Proceedings of the 2009 International Conference on Security and Management (SAM '09), Vol. I, pp. 220-226, 2009. 30.P. Zhang, H. Sun and Z. Yan, “ Building up Trusted Identity Management in Mobile Heterogeneous Environment, ” in Proceedings of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 873-877, 2011. 31.M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, “ Security and Privacy in Cloud Computing: A Survey, ” in Proceedings of 2010 Sixth International Conference on Semantics, Knowledge and Grids, pp. 105-112, 2010. 32.D. Zissis and D. Lekkas, “ Addressing Cloud Computing Security Issues, ” Future Generation Computer Systems, Vol. 28, pp. 583-592, 2012.