# Survei Tingkat Penggunaan Single Sign On pada 500 Situs Peringkat Teratas Alexa.com

I Wayan Manik Suhartanta[1], Nyoman Putra Sastra[2]

***Abstract*—Advances in Internet technology has provided a new market for the growth of the service provider. New sites appear in large numbers every year. This gives a new problem for users of the service. Users are forced to memorize many username and password to access the service. Overcoming it is a new emerging technology, the technology called Single Sign On (SSO). SSO offers simple authentication process for users to access many services sites. But the level of confidence of users and service providers, in the use of SSO technology have not been investigated. In this research shows that the rate of utilizing the SSO technology of the top 500 sites on alexa.com by 31% (155 websites). And the level of utilization of the SSO more than one provider, by 41%. In studies it appears that the most used SSO services provider is google followed by facebook and twitter.**

***Intisari*— Kemajuan internet telah memberikan sebuah pasar baru bagi tumbuhnya penyedia layanan. Situs–situs baru muncul dalam jumlah besar setiap tahunnya. Hal ini memberikan sebuah permasalahan baru bagi pengguna layanan. Pengguna terpaksa menghafal banyak *username* dan *password* dalam mengakses layanan tersebut. Mengatasi hal tersebut sebuah teknologi baru muncul, teknologi tersebut bernama *Single Sign On* (SSO). SSO menawarkan kemudahan proses otentifikasi bagi pengguna dalam mengakses banyak situs layanan. Namun tingkat kepercayaan pengguna dan penyedia layanan terhadap SSO belum pernah diteliti. Dalam penelitian ini terlihat bahwa tingkat penggunaan SSO dari 500 situs teratas pada alexa.com sebesar 31% (155 situs). Dan tingkat penggunaan layanan SSO lebih dari satu penyedia, sebesar 41%. Dalam penelitian terlihat bahwa penyedia layanan SSO yang paling diminati adalah google diikuti oleh facebook dan twitter.**

***Kata Kunci*— Single Sign On (SSO), Computer Security, Authentication, Network Security;**

## I. PENDAHULUAN

Internet adalah entitas yang hidup, selalu berubah dan berkembang. Perubahan ini juga didukung oleh berkembangnya konektivitas broadband yang semakin murah dan mudah diakses. Peningkatan jumlah perangkat yang terhubung ke internet mengarah pada paradigma baru yaitu Internet of Things (IoT). Perkembangan IoT didorong oleh perluasan pemanfaatan internet melalui masuknya layanan baru yang memanfaatkan sistem-sistem yang terhubung dengan internet, sehingga layanan menjadi semakin cerdas. Semua sistem yang terhubung semakin mendapatkan keuntungan dari internet. Ada tantangan baru yang muncul berkaitan dengan IoT, yang paling terlihat di bagian keperca-yaan dan keamanan, standarisasi dan tata kelola yang diperlukan untuk memastikan Internet terbuka yang adil dan dapat dipercaya [1].

Kepercayaan akan layanan internet berdasar pada kepercayaan tingkat keamanan. Salah satu sisi keamanan yang paling awal adalah tahapan otentifikasi pengguna. Semakin banyaknya layanan internet, menuntut pengguna mengingat banyak password, yang cenderung mendorong penguna membuat password yang lemah. Hal ini tentunya semakin membuat sisi keamanan menjadi semakin lemah. Mengatasi hal tersebut muncul sebuah solusi layanan otentifikasi bernama Single Sign On (SSO) [2].

SSO memberikan sebuah solusi dalam mengatasi upaya otentifikasi dalam banyak layanan. Namun tingkat kepercayaan pengguna, tetap menjadi dasar dari sebuah sistem keamanan. Menyikapi hal tersebut, maka penulis berupaya melakukan sebuah survei sederhana untuk melihat fenomena yang terjadi. Seberapa banyak situs utama di dunia yang sudah memanfaatkan teknologi SSO, sehingga diharapkan dapat diperlihat seberapa tinggi tingkat kepercayaan terhadap teknologi SSO ini.

## II. STUDI LITERATUR

### A. *Otentifikasi*

Otentifikasi adalah sebuah proses pembentukan identitas seorang pengguna sehingga dapat diotorisasi berhak atau tidak mengakses sebuah sistem atau aplikasi. Proses otentifikasi bisa terdiri dari berbagai tipe tergantung dari tingkatan keamanan yang diterapkan [3].

Ada berbagai jenis sistem otentikasi yang telah diterima secara luas dan digunakan dalam perangkat lunak untuk melindungi sistem online. Salah satunya dapat dibagi menjadi tiga tipe yaitu [4] :

*1) Single-factor Authentification (SFA)* : SFA adalah teknik tradisional, yang hanya membutuhkan *username* dan *password* untuk login ke sebuah situs atau aplikasi. Keuntungan utama dari SFA adalah kemudahan dalam penerapan dan penggunaannya. Sedangkan kelemahan utamanya karena hanya terdiri dari 1 faktor maka hanya akan ada 1 tahapan pengamanan.

*2) Two-Factor Authentication (TFA)* : TFA merupakan pengembangan dari teknik SFA, TFA biasanya menggunakan bantuan *TFA device*. Biasanya *TFA device* akan membuat PIN atau token yang akan berguna sebagai tahapan kedua dari proses otentifikasi. TFA tidak menjamin sebuah *password* menjadi kuat, namun TFA akan memberikan sebuah tahapan pengamanan tambahan yang menjamin yang mengakses situs adalah orang yang berhak. Model pengamanan TFA sangat banyak diterapkan pada transaksi perbankan [4].

*3) Multi-Factor authentication (MFA)* : MFA dikembangkan untuk melengkapi proses TFA. MFA yang

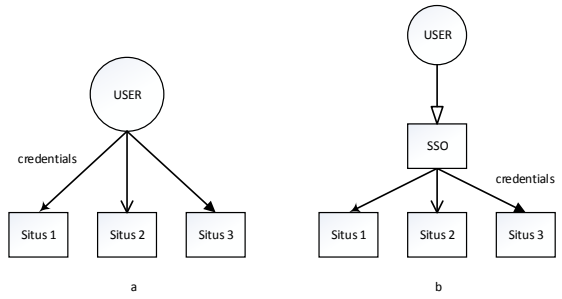
[1]*Magister Teknik Elektro dan Komputer Universitas Udayana, Kampus Sudirman, Denpasar Bali. Tel. 0361239599, fax: 0361239599; e-mail: manik095@gmail.com*

[2]*Magister Teknik Elektro dan Komputer Universitas Udayana, Kampus Sudirman, Denpasar Bali. Tel. 0361239599, fax: 0361239599, E-mail: putra.sastra@unud.ac.id*

dulunya hanya digunakan oleh instansi militer, mulai digunakan oleh perbankan dan keuangan. Pengunaan MFA secara umum didorong oleh kemajuan teknologi yang telah menekan keamanan TFA, sehingga pengamanan dengan TFA dirasa kurang memadai. Proses pengamanan MFA mempergunakan lebih dari dua tahap pengamanan, tahapan tersebut beragam dan terus dikembangkan sampai saat ini[4].

*B. Single Sign On*

Single Sign On adalah sebuah solusi yang membiarkan seorang pengguna mengotentifikasi dirinya sekali dan kemudian dapat mengakses beberapa layanan yang terkait tanpa perlu melakukan otentifikasi ulang [5]. Hal ini memberikan kemudahan bagi pengguna karena hanya perlu mengingat sebuah password untuk mengakses beberapa situs yang saling terkait [2]. Secara sederhana proses SSO dapat digambarkan pada Gambar 1.

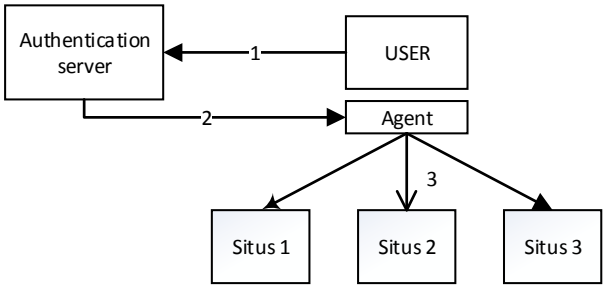



Gambar 1. Single Sign On

Gambar 1 memperlihatkan ilustrasi SSO. Pada bagian a terlihat bahwa user perlu proses otentifikasi tersendiri setiap berusaha mengakses sebuah situs. Sedangkan pada bagian b tahapan tersebut diambil alih oleh SSO, sehingga user cukup melakukan otentifikasi sekali saja ke SSO service [5].

Hal ini memberikan keuntungan berupa kemudahan bagi pengguna. Pengguna hanya perlu mengingat sebuah username dan password atau hanya perlu sebuah mekanisme otentifikasi [6],[7]. Disamping dari sisi pengguna, dari sisi penyedia layanan situs juga mendapatkan keuntungan. Perusahaan penyedia aplikasi dapat mengurangi pengeluaran untuk memelihara data user dan keamanannya [2].

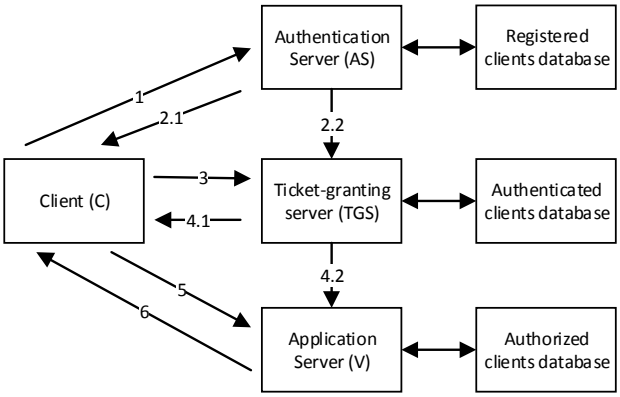
Secara garis besar tahapan otentifikasi melalui SSO dapat dilihat dari Gambar 2 [5].




Gambar 2. Arsitektur Tradisional Single Sign On

Pada Gambar 2 terlihat arsitektur dari SSO tradisional ketika diperkenalkan [5]. Tahapan dimulai ketika user ingin masuk ke situs-situs, terlebih dahulu user harus melalui tahap 1 yaitu proses otentifikasi ke server. Ketika Authentication server menyetujui proses otentifikasinya, pada tahap 2 Authentication server mengirimkan username dan password masing-masing situs ke agent yang menempel pada user. Agent kemudian membagi username dan password yang dibutuhkan oleh situs yang ingin dikunjungi oleh user dan melakukan login secara otomatis, seperti terlihat pada tahap 3. Hal ini menimbulkan sebuah permasalahan keamanan yang baru, agent berada pada computer user secara lokal dan menyimpan username dan password yang dimiliki oleh user, sehingga ketika agent bisa dibobol, maka password dan username dari user akan diketahui.

Menyikapi kelemahan arsitektur SSO tersebut, pengembangan SSO berikutnya terlihat pada Gambar 3 [8].




Gambar 3. Arsitektur Modern Single Sign On

Gambar 3 memperlihatkan ada sebuah tahapan baru (TGS) yang menggantikan peran agent. TGS memiliki peran memberikan informasi terotentifikasi kepada V (situs yang dituju) sehingga pengguna dapat menggunakannya. Yang berbeda disini informasi yang diberikan oleh TGS bukan username dan password melainkan sebuah tiket yang sama sekali tidak mengandung unsur username dan password dari pengguna. Prosesnya secara runut dimulai dari tahap 1, pengguna meminta proses otentifikasi dengan kepada AS. Setelah di otorisasi AS, pada tahap 2.1 memberikan flag kepada pengguna, yang kemudian dilanjutkan dengan tahap 3 dimana pengguna meminta tiket ke TGS. TGS menyimpan session pengguna dan membuat tiket sesuai session yang dipakai pengguna yang selanjutnya diberikan ke pengguna dengan tahap 4.1. Dengan tiket yang ada, pengguna kemudian masuk ke V menggunakan tiket tersebut dengan tahapan 5. V memberikan informasi / layanan kepada pengguna dengan tahap 6.

Dalam perkembangannya, hal ini masih dirasa terlalu banyak proses dalam jaringan. Sehingga tahap 2.1 dan 3 digantikan oleh tahap 2.2, dimana AS langsung

berkomunikasi dengan TGS tanpa melalui pengguna setelah proses otentifikasi. Kemudian tiket yang dibuat oleh TGS langsung diberikan ke V dengan tahap 4.2. Sehingga tahap 4.1 dan tahap 5 tidak diperlukan [8]. Hal ini dapat mereduksi proses komunikasi jaringan dan meningkatkan keamanan informasi sensitif dari pengguna.

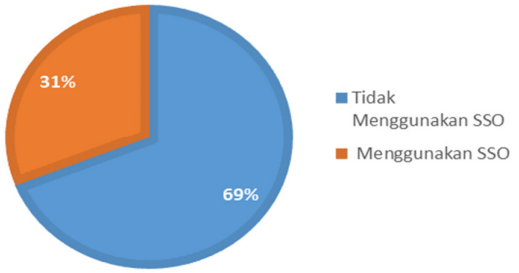
## III. ANALISA HASIL

Pengumpulan data dengan survei ke 500 situs teratas pada www.alexa.com dilakukan selama bulan April 2016. Sedangkan daftar situs diakses per tanggal 11 April 2016. Proses berikutnya adalah menelusuri setiap situs yang tertulis pada daftar tersebut, kemudian mencatat apabila situs tersebut menggunakan teknik SSO. Selain mencatat penggunaan teknik SSO, dalam penelusuran peneliti juga mencatat layanan SSO yang digunakan oleh situs yang bersangkutan. Hasil penelusuran terlihat seperti pada tabel 1.

TABEL 1. HASIL SURVEI PENGGUNAAN SSO PADA 500 SITUS TERATAS ALEXA.COM

| Jumlah Situs | Menggunakan SSO | Tidak Menggunakan SSO |
|---|---|---|
| 500 | 155 | 345 |

Dari Tabel 1 terlihat bahwa tingkat penggunaan SSO belum terlalu banyak diadopsi. Dari 500 situs yang disurvei terdapat 155 situs yang menggunakan SSO, sedangkan 345 lainnya belum menggunakan teknik SSO. Ilustrasi secara grafik hasilnya dapat dilihat pada Gambar 4.



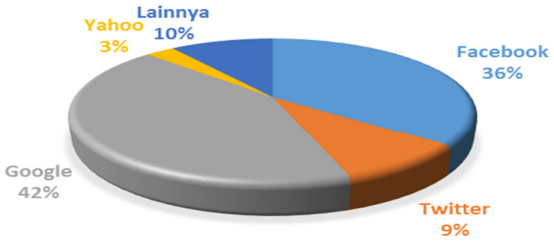

Gambar 4. Penggunaan SSO pada 500 Situs Teratas di Alexa.com

Gambar 5 memperlihatkan tingkat pengguna SSO sampai bulan April 2016 sebesar 31% sedangkan yang tidak menggunakan sebesar 69%. Di samping tingkat penggunaan teknik SSO, dari data hasil survei yang kami lakukan dapat dilihat komposisi penyedia layanan SSO yang digunakan. Data penyedia layanan SSO dapat dilihat pada Tabel 2.

TABEL 2. HASIL SURVEI PENYEDIA LAYANAN SSO YANG DIGUNAKAN

| Penyedia Layanan | | | | |
|---|---|---|---|---|
| Facebook | Twitter | Google | Yahoo | Lainnya |
| 89 | 23 | 106 | 7 | 25 |

Pencatatan penyedia layanan SSO dilakukan dengan cara mencoba masuk ke menu login yang tersedia pada situs yang di survei. Kemudian langkah berikutnya membaca profile penyedia layanan otentifikasi dan mencatat situs penyedianya. Hasil catatan kemudian dikelompokan. Hasil pengelompokan mendapatkan 5 kelompok besar yaitu facebook, twitter, google, yahoo dan lainnya. Kelompok lainnya adalah penyedia - penyedia layanan SSO dengan jumlah pengguna yang relatif kecil sehingga dikelompokkan menjadi satu. Ilustrasi secara grafik data penyedia layanan SSO dapat dilihat pada Gambar 5.




Gambar 5. Penyedia layanan SSO

Dari Gambar 5 dapat dilihat bahwa google menjadi penyedia layanan terbanyak digunakan. Sebanyak 106 situs (42%) menggunakan layanan google, diikuti oleh facebook sebanyak 89 situs(36%) dan twitter sebanyak 23 situs (23%). Hal yang menarik dari hasil survei, terlihat bahwa situs yang menggunakan teknik SSO tidak hanya menggunakan satu buah penyedia layanan SSO, tetapi menggunakan secara bersamaan beberapa penyedia layanan SSO. Data terlihat pada Tabel 3.

TABEL 3. HASIL SURVEI PENGGUNAAN PENYEDIA LAYANAN SSO

| 1 Layanan SSO | Lebih dari 1 layanan SSO | Jumlah |
|---|---|---|
| 92 | 63 | 155 |

Dari Tabel 3 terlihat dari 155 situs yang mempergunakan teknik SSO dalam proses otentifikasi penggunanya, 92 situs mempergunakan satu penyedia layanan SSO. Sedangankan 63 situs lainnya mempergunakan lebih dari satu penyedia layanan SSO. Ilustrasi secara grafik penggunaan penyedia layanan SSO dapat dilihat pada Gambar 6.


Gambar 6. Penggunaan Penyedia Layanan SSO

Gambar 6 mengilustrasikan 41% dari pengguna SSO mempergunakan lebih dari sebuah penyedia layanan SSO. Hal ini menunjukan bahwa tidak terjadi persaingan saling mematikan dalam penyediaan layaanan SSO. Penyedia layanan SSO dapat bersanding dengan penyedia lainnya.

## IV. KESIMPULAN

Dari penelitian dapat dilihat bahwa sampai bulan April 2016 tingkat penggunaan teknologi SSO hanya mencapai 31 % dari sampel survei yang dilakukan. Hal ini menunjukkan bahwa tingkat kepercayaan dari penyedia situs terhadap teknologi SSO belum penuh. Namun jika dilihat penyedia layanan SSO ternyata adalah pemain besar dalam pasar layanan di Internet memberikan harapan bahwa tingkat kepercayaan akan penggunaan SSO akan semakin meningkat.

Penelitian yang dilakukan kali ini hanya mempergunakan data per April 2016, hal ini tentunya tidak dapat memperlihatkan trend yang terjadi dalam penggunaan SSO. Diharapkan penelitian berikutnya akan melakukan penelitian terhadap penggunaan SSO dalam rentang waktu yang lebih panjang, sehingga didapatkan trend penggunaan dari layanan SSO itu sendiri.

## REFERENSI

[1] L. Coetzee and J. Eksteen, "The Internet of Things - promise for the future? An introduction," in *IST-Africa Conference Proceedings, 2011*, 2011, pp. 1–9.

[2] A. Nair, A. Madhu, and J. J. Kizhakkethottam, "Security issues of single sign on web services," in *Soft-Computing and Networks Security (ICSNS), 2015 International Conference on*, 2015, pp. 1–4.

[3] F. A. Alsulaiman and A. E. Saddik, "A novel 3D graphical password schema," in *Virtual Environments, Human-Computer Interfaces and Measurement Systems, Proceedings of 2006 IEEE International Conference on*, 2006, pp. 125–128.

[4] S. R. Basavala, N. Kumar, and A. Agarrwal, "Authentication: An overview, its types and integration with web and mobile applications," in *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*, 2012, pp. 398–401.

[5] A. Volchkov, "Revisiting single sign-on: a pragmatic approach in a new context," *IT Prof.*, vol. 3, no. 1, pp. 39–45, 2001.

[6] R. Malutan and C. Grosan, "Web authentication methods using single sign on method and virtual keyboard," in *Grid, Cloud & High Performance Computing in Science (ROLCG), 2015 Conference*, 2015, pp. 1–4.

[7] A. G. Revar and M. D. Bhavsar, "Securing user authentication using single sign-on in Cloud Computing," in *Engineering (NUiCONE), 2011 Nirma University International Conference on*, 2011, pp. 1–4.

[8] Y. Jian, "An Improved Scheme of Single Sign-on Protocol," 2009, pp. 495–498.