VISUALISASI SERANGAN *PORT SCANNING* DENGAN *CLUSTERING K-MEANS* PADA JARINGAN *INTERNET OF THINGS*

TUGAS AKHIR

MUHAMMAD RIFKI
09011181320049

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

VISUALISASI SERANGAN *PORT SCANNING* DENGAN *CLUSTERING K-MEANS* PADA JARINGAN *INTERNET OF THINGS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

MUHAMMAD RIFKI
09011181320049

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

HALAMAN PENGESAHAN

Visualization of Port Scanning Attack With Kmeans Clustering On The Internet Of Things Network

SKRIPSI

Submitted to Complete of the Term Obtaining Bachelor Of Computer Engineering

By:

Muhamad Rifki
09011181320049

Palembang, Juli 2020

Supervisor

Deris Stiawan, Ph. D

NIP: 197806172006041002

Head Of Departement
Computer Engineering

Dr. Ir. H. Sukemi, M.T

NIP: 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 04 Juni 2020

Tim Penguji :

1. Ketua : Huda Ubaya, M.T. (_____)
2. Anggota 1 : Ahmad Heryanto, M.T. (_____)
3. Anggota 2 : Samaryanta Sembiring, M.T. (_____)

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhamad Rifki
Nim : 09011181320049
Program Studi : Sistem Komputer
Judul Skripsi : Visualisasi Serangan Port Scanning Dengan Clustering Kmeans Pada Jaringan Internet Of Things
Hasil Pengecekan *Software iThenticate/Turnitin* : 13 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / *plagiat*. Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Juli 2020

Muhamad Rifki

09011181320049

HALAMAN PERSEMBAHAN

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

"Dengan menyebut Nama Allah yang maha pengasih lagi maha penyayang"

Seharusnya cumlaude, tapi……. Yasudahlah. Nasib dan takdir ditengah jalan nya perkuliahan yang berubah membuat saya akhirnya harus menekan diri untuk membiayai semua kebutuhan sendiri. Akhirnya saya lebih memilih untuk menunda gelar sarjana yang seharusnya cumlaude demi sesuap nasi. Terima kasih untuk allah zat yang maha pengasih lagi maha penyayang. Begitu pula dengan abah dan mama, terima kasih tak henti henti nya berjuang dan mendoakan, tidak ada yang lebih mabrur daripada doanya para orangtua. Sekali lagi terima kasih mama, sarang heo.

Terima kasih untuk semua perangkat kampus terkhusus dosen pembimbing yang sangat saya idolakan Prof. Deris Stiawan, Ph. D , karenanya saya menemui jalan penerangan.

Terima kasih untuk semua rekan rekan Angkatan 2013 jurusan system computer fakultas ilmu computer unsri.

Terima kasih untuk teman teman seperjuangan, rafdi mafazi serta semua anggota tongkrongan lain nya yang tidak henti nya memberikan support baik moral maupun finansial serta kehangatan yang membuat semakin erat nilai pertemanan.

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Allah SWT atas segala Rahmat dan Hidayah-Nya telah memberikan kemudahan dan kelancaran dalam menyelesaikan penulisan Tugas Akhir ini. Shalawat serta salam tidak lupa penulis ucapkan kepada suri tauladan yang baik bagi umat manusia Rasulullah Muhammad SAW.

Tugas Akhir ini dengan judul **" Visualisasi Serangan Port Scanning Dengan Clustering Kmeans Pada Jaringan Internet Of Things "** di buat berdasarkan tujuan untuk memenuhi persyaratan menyelesaikan pendidikan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada semua pihak atas bantuan dan kemudahannya dalam proses penulisan Tugas Akhir ini. Ucapan terina kasih penulis sampaikan kepada :

1. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Bapak Sukemi. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Rossi Passarella. selaku Pembimbing Akademik.
4. Bapak Prof Deris Stiawan. selaku Dosen Pembimbing Tugas Akhir. Terima kasih telah bersedia meluangkan waktu untuk membimbing penulis dalam menyelesaikan Tugas Akhir.
5. Bapak Ahmad Heryanto, M.T. dan Bapak Samaryanta Sembiring. selaku Dosen Penguji Sidang Tugas Akhir. Terima kasih telah memberikan banyak masukan untuk penulis dalam pembuatan Tugas Akhir ini.

Penulis berharap karya tulis ini bukanlah karya tulis terakhir dari penulis. Penulis berharap akan ada karya-karya tulis lainnya setelah ini. Penulis juga menyadari bahawa dalam penulisan Laporan Tugas Akhir masih banyak terdapat kekurangan. Oleh karena itu penulis menerima dengan senang hati kritik dan saran yang bersifat membangun dalam memperbaiki laporan ini. Di akhir pengantar penulis mengharapkan semoga Laporan Tugas Akhir ini dapat bermanfaat bagi pembaca dan terutama bagi penulis sendiri.

Indralaya,

Penulis

VISUALISASI SERANGAN *PORT SCANNING* DENGAN *CLUSTERING* KMEANS PADA JARINGAN *INTERNET OF THINGS*

Muhamad Rifki || 09011181320049
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : mail.muhammadrifki@gmail.com

Abstrak

Internet of things (IoT) muncul sebagai teknologi yang digunakan secara luas di beberapa bidang termasuk industri, transportasi, energi, pemantauan lingkungan, kesehatan, pertanian dan lain – lain. Pada penelitian ini penulis fokus terhadap pengenalan pola serangan *port scanning* dan menyajikan pola serangan tersebut kedalam bentuk visual. Penelitian dilakukan pada jaringan *internet of things* yang menggunakan *WiFi* dengan trafik normal, trafik serangan, dan trafik gabungan (normal – serangan). Dari skenario ini, dihasilkan tiga dataset berbeda, yang terdiri dari dataset normal, dataset serangan dan dataset normal – serangan. Pengujian dilakukan dengan dua tahapan : (i) pengujian dengan *Snort* sebagai *Intrusion detection System* (IDS), dan (ii) pengujian menggunakan metode *clustering k-means* untuk mendeteksi pola serangan *port scanning*. Evaluasi hasil deteksi menggunakan *confusion matrix detection rate* dengan metode *k-means* menunjukan tingkat akurasi deteksi sebesar 98.3%. Untuk menyajikan hasil visualisasi pola serangan *port scanning*, penulis menggunakan teknik visualisasi *andrew crews* dan *parallel coordinate* yang merupakan *library* yang disediakan pada bahasa pemrograman *python*, kedua teknik ini dapat mempresentasikan data multidimensional atau parameter yang lebih dari satu. Hasil dari visualisasi dapat menunjukkan grafik yang unik dimana setiap pola serangan membentuk garis dan warna yang berbeda dengan pola normal, yang mana dari setiap hasil yang disajikan memungkinkan *user* dapat dengan mudah mengenali pola serangan *port scanning*.

Kata Kunci : *Internet of Things, Port Scanning, Clustering K-means, Snort, Intrusion Detection System, Parallel Coordinate, Andrew Curves, Data Visualisation.*

VISUALIZATION OF PORT SCANNING ATTACK WITH KMEANS CLUSTERING ON THE INTERNET OF THINGS NETWORK

Muhamad Rifki || 09011181320049
Departement of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : mail.muhammadrifki@gmail.com

Abstract

Internet of things (IoT) emerged as a technology that is widely used in several fields including industry, transportation, energy, environmental monitoring, health, agriculture and others. In this study the author focuses on the introduction of port scanning patterns and presents the pattern into visual form. The research was conducted on the internet of things network that uses WiFi with normal traffic, attack traffic, and combined traffic (normal - attacks). From this scenario, three different datasets are generated, consisting of normal datasets, attack datasets and normal-attacks dataset. The testing was performanced on two stages, there are : (i) testing with Snort as an Intrusion detection System (IDS), and (ii) testing using the k-means clustering method to detect the port scanning pattern. In this research, measurment of detection results using the confusion matrix detection rate based on k-means method showing 98.3% as rate of detection accuracy values. To present the results of visualizing the port scanning attack, the author uses Andrew Crews and Parallel Coordinate visualization techniques, which are provided in the Python programming language. both of that techniques can present more than one multidimensional data and parameters. The results of visualization is showing an unique graph where each attack pattern showing different lines and colors with a normal pattern, which the result presented allows users to easily recognize the port scanning attack.

Keyword*: Internet of Things, Port Scanning, Clustering K-means, Snort, Intrusion Detection System, Parallel Coordinate, Andrew Curves, Data Visualisation.*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I. PENDAHULUAN

1.1 Latar Belakang

Internet of things (IoT) muncul sebagai teknologi yang digunakan secara luas di beberapa bidang termasuk industri, transportasi, energi, ramah, pemantauan lingkungan, kesehatan, pertanian dan lain – lain. Dengan memanfaatkan jaringan sensor nirkabel *(WSN)* untuk mengumpulkan serta memproses data dan menggunakan teknologi berbasis *cloud computing* sebagai penyedia layanan [1],[2]. *Internet of things (IoT)* diklasifikasikan menjadi lima layer, yaitu *application layer*, *perception layer, network layer, middleware layer* dan *business layer*. Masalah keamanan, seperti privasi, otorisasi, verifikasi, kontrol akses, konfigurasi sistem, penyimpanan informasi dan manajemen adalah tantangan utama dalam pengimplementasian *IoT* [3]. Dalam keamanan jaringan internet, terdapat sistem pendeteksi serangan yang disebut dengan *Intrusion Detection System*. *Intrusion detection system (IDS)* mempunyai peranan yang sangat penting untuk mendeteksi kemungkinan adanya serangan oleh *attacker* [4]. Teknik yang umum digunakan oleh IDS untuk mendeteksi serangan adalah *rule base signature analysis,* akan tetapi teknik ini masih memiliki kelemahan karena teknik ini seringkali tidak dapat mendeteksi tipe serangan baru yang tidak ada pada *database* serangan [5].

Visualisasi memberikan salah satu pendekatan alternatif yang dapat digunakan untuk mengatasi kelemahan tersebut. Dengan visualisasi kita dapat dengan mudah mengenali pola serangan tertentu dari gambar visual yang dihasilkan serta dapat mencari pola serangan yang baru [6]. Gambar visual didapat dari data mentah dengan teknik *clustering* [7]. Teknik *clustering* adalah pengukuran jarak yang dilakukan pada *object* dan mengelompokkan *object* pada *cluster.*

Salah satu algoritma yang sering digunakan untuk *clustering* adalah algoritma *clustering K-means. K-means* mengelompokkan data sesuai dengan nilai

nilai karakteristik mereka ke dalam sejumlah *cluster* tertentu yang ditentukan oleh pengguna [8].

Pada tugas akhir ini dengan menerapkan *clustering K-means* sebagai algoritma untuk dapat memvisualisasikan pola serangan *port scanning* pada jaringan *IoT*. Tujuan utama menggunakan clustering K-means adalah untuk membagi dan mengelompokkan data menjadi data normal dan data serangan. Metode pengelompokan K-means membagi input dari *dataset* kedalam *cluster* – *cluster* menurut nilai awal yang dikenal sebagai *centroid* [8].

1.2 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian tugas akhir ini adalah sebagai berikut :

1. Mengenali pola serangan *port scanning* pada jaringan *internet of things.*

2. Mengimplementasikan *cluster K-means* untuk membuat cluster pola serangan dan pola normal.

3. Menampilkan pola serangan dan pola normal kedalam bentuk visual.

4. Melakukan perhitungan, terkait akurasi dari penerapan *cluster K-means.*

1.3 Manfaat Penelitian

Adapun manfaat dari penelitian tugas akhir ini adalah sebagai berikut :

1. Dapat memberi kemudahan dalam mengenali pola serangan *port scanning*.

2. Dapat membedakan paket serangan *port scanning* dengan paket normal.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, maka didapatkan perumusan masalah yaitu :

1. Bagaimana mengidentifikasi pola serangan *port scanning* pada jaringan *internet of things (IoT).*

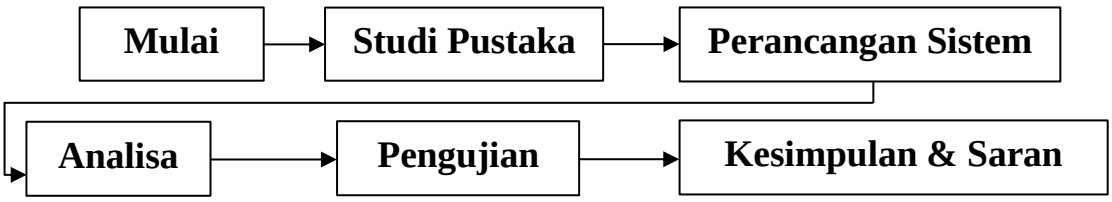
2. Bagaimana mengimplementasikan algoritma *clustering K-means* untuk membedakan pola serangan dan pola normal.
3. Memvisualisasikan serangan *port scanning* kedalam bentuk grafis.

1.5 Batasan Masalah

Selain perumusan masalah diatas, juga terdapat batasan masalah antara lain:

1. Pengujian dilakukan pada sistem jaringan *internet of things (IoT)* yang dibangun sendiri, terdiri dari *node* 1 – 4 (*WeMos D1*), *wireless router* dan *server monitoring.*
2. Menggunakan *dataset* yang sudah terekam (*tercapture*) berupa *network log connection* untuk lalu lintas data normal dan serangan *port scanning*.
3. Tidak membahas bagaimana cara pencegahan serangan tersebut.
4. Visualisasi serangan *port scanning* tidak diujikan pada lalu lintas jaringan *real – time.*
5. Tidak diujikan pada lalu lintas jaringan yang terenkripsi.

1.6 Metodelogi Penelitian



Gambar 1.1 Metodelogi Penelitian.

1. Tahap Pertama (Studi Pustaka)

   Tahap ini dilakukan dengan cara mengkaji dan mempelajari *literature* dan referensi berupa naskah ilmiah, buku, internet dan lain-lain yang dapat menunjang metodologi dan pendekatan yang akan diterapkan pada penelitian tugas akhir.

2. Tahap Kedua (Perancangan Sistem)

   Pada tahapan ini merupakan tahapan mengenai bagaimana membangun dan menerapkan metode pada sistem tugas akhir. Selain itu, apa saja yang digunakan pada penelitian ini seperti hardware maupun software, kemudian bagaimana proses konfigurasi ataupun menulis kode untuk penerapan metode pada tugas akhir.

3. Tahap Ketiga (Pengujian)

   Setelah semua sistem selesai dirancang, tahap selanjutnya adalah melakukan pengujian berdasarkan metodologi dan parameter pengujian yang telah ditentukan untuk medapatkan hasil yang sesuai dan tepat dengan algoritma yang digunakan.

4. Tahap Keempat (Analisa)

   Hasil dari pengujian pada tahap sebelumnya, selanjutnya akan dianalisa dengan tujuan untuk mengetahui kekurangan pada hasil perancangan dan faktor penyebabnya sehingga dapat dilakukan pengembangan pada penelitian selanjutnya.

5. Tahap Kelima (Kesimpulan dan Saran).

   Pada tahap ini akan dilakukan penarikan kesimpulan berdasarkan studi pustaka, hasil perancangan sistem dan hasil analisa sistem, kemudian dihadirkan pula beberapa poin saran dari penulis untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari setiap bab, maka dibuat suatu sistematika penulisan sebagai berikut :

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodelogi Penelitian, dan Sistematika Penelitian.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian tugas akhir terkait *Internet of things (IoT), Port scanning*, *Clustering Algorithm*, serta teori lainnya yang berkaitan dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISIS

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian berdasarkan parameter yang telah ditentukan sebelumnya.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang hasil penelitian yang dilakukan, serta menjawab setiap tujuan yang hendak dicapai seperti yang tercantum pada BAB I (Pendahuluan), serta saran untuk penelitian selanjutnya

DAFTAR PUSTAKA

[1] H. Hromic *et al.*, "Real time analysis of sensor data for the Internet of Things by means of clustering and event processing," *IEEE Int. Conf. Commun.*, vol. 2015–Septe, pp. 685–691, 2015.

[2] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the Internet of Things," *Proc. 2015 IEEE 8th Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS 2015*, vol. 1, no. October 2015, pp. 463–467, 2015.

[3] C. Tomastik, A. Schneider, S. Ilincic, and A. Pauschitz, "A Survey on the Internet of Things Security," *Galvanotechnik*, vol. 101, no. 2, pp. 288–295, 2010.

[4] A. H. Haneen Al-Alami and H. Al-Bahadil, "Vulnerability Scanning of IoT Devices in Jordan Using Shodan," *Cutis*, vol. 62, no. 5, pp. 227–230, 2000.

[5] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Comput. Secur.*, vol. 28, no. 5, pp. 276–288, 2009.

[6] H. Kim, I. Kang, and S. Bahk, "Real-time visualization of network attacks on high-speed links," *IEEE Netw.*, vol. 18, no. 5, pp. 30–39, 2004.

[7] M. Livny, "Visual exploration of large data sets," *Proc. SPIE*, vol. 2657, no. Apr, pp. 263–274, 1996.

[8] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "Intrusion detection based on K-means clustering and OneR classification," *Proc. 2011 7th Int. Conf. Inf. Assur. Secur. IAS 2011*, pp. 192–197, 2011.

[9] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things Routing Attacks and Countermeasures in the RPL-Based Internet of Things," no. August 2013, 2014.

[10] M. U. Farooq and M. Waseem, "A Critical Analysis on the Security

Concerns of Internet of Things (IoT),” vol. 111, no. 7, pp. 1–6, 2015.

[11] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future internet: The internet of things architecture, possible applications and key challenges,” in *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 2012, pp. 257–260.

[12] S. Anandita, Y. Rosmansyah, B. Dabarsyah, and J. U. Choi, “Implementation of dendritic cell algorithm as an anomaly detection method for port scanning attack,” *2015 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2015 - Proc.*, 2016.

[13] M. de Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, “A review of port scanning techniques,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 29, no. 2, p. 41, 1999.

[14] Stiawan Deris, Tasmi, and S. A. Valianta, “Identifikasi Serangan Port Scanning dengan Metode String Matching,” vol. 2, no. 1, pp. 466–471, 2016.

[15] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[16] S. Akbar, D. K. N. Rao, and D. J. A. Chandulal, “Intrusion Detection System Methodologies Based on Data Analysis,” *Int. J. Comput. Appl.*, vol. 5, no. 2, pp. 10–20, 2010.

[17] H. T. Elshoush and I. M. Osman, “Alert correlation in collaborative intelligent intrusion detection systems - A survey,” *Appl. Soft Comput. J.*, vol. 11, no. 7, pp. 4349–4365, 2011.

[18] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[19] S. Sandra, D. Stiawan, and A. Heryanto, “Visualisasi Serangan Brute Force

Menggunakan Metode K-Means dan Naïve Bayes," vol. 2, no. 1, pp. 315–320, 2016.

[20] M. E. Celebi, H. A. Kingravi, and P. A. Vela, "A comparative study of efficient initialization methods for the k-means clustering algorithm," *Expert Syst. Appl.*, vol. 40, no. 1, pp. 200–210, 2013.

[21] S. Rukhmode, G. Vyavhare, S. Banot, and A. Narad, "IOT Based Agriculture Monitoring System Using Wemos," *Int. Conf. Emanations Mod. Eng. Sci. Manag.*, no. March, pp. 14–19, 2017.

[22] M. Iftekharul Mobin, M. Abid-Ar-Rafi, M. Neamul Islam, M. Rifat Hasan, I. Professional Member, and I. Student Member, "An Intelligent Fire Detection and Mitigation System Safe from Fire (SFF)," *Int. J. Comput. Appl.*, vol. 133, no. 6, pp. 975–8887, 2016.

[23] A. Gaddam and W. F. Esmael, "Designing a Wireless Sensors Network for Monitoring and Predicting Droughts," pp. 2–4, 2014.

[24] J. G. Martin, C. L. Phillips, A. Schmidt, J. Irvine, and B. E. Law, "High-frequency analysis of the complex linkage between soil CO2fluxes, photosynthesis and environmental variables," *Tree Physiol.*, vol. 32, no. 1, pp. 49–64, 2012.

[25] J. Song, H. Takakura, and Y. Kwon, "A generalized feature extraction scheme to detect 0-day attacks via IDS alerts," *Proc. - 2008 Int. Symp. Appl. Internet, SAINT 2008*, pp. 55–61, 2008.

[26] X. Xu, "Adaptive intrusion detection based on machine learning: Extraction Data, classifier construction and sequential pattern prediction," *Int. J. Web Serv. Pract.*, vol. 2, no. 1, pp. 49–58, 2006.