Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway

Agus Tedyyana[1], Supria[2]
Teknik Informatika, Politeknik Negeri Bengkalis
Jl. Bathin Alam, Sei.Alam Bengkalis, RIAU, telp. 0766012021
Email : agustedyyana@polbeng.ac.id[1], phiya@polbeng.ac.id[2]

Abstrack *- Internet network is a media or technology that is very useful at this time. Almost everyone who uses electronics using internet network. With this internet network, humans can access the virtual world with ease, either in browsing, streaming, social media access and others. On the other hand there is a lack of Internet network technology. With the internet, computers can connect with other computers, so many cases of malware attacks through the internet network. Recently there has been a very dangerous malware attack. The malware is known as wannacry ransomware. Wannacry can attack computers that use windows operating system. Computers that have been infected wannacry will make all existing data in the computer hard drive becomes encrypted, so the user can not open the data that has been infected with the virus.To solve the problem then it is proposed Design of Malware Detection and Prevention System Using Unified Modeling Language (UML). This system is designed using Router, Server, and SMS Gateway. Router is used for network configuration. The server is used for WEB-based storage systems that serve to detect ports. SMS Gateway is used to send SMS to the network admins. With the proposed system is expected to help detect the presence of malware that goes through the router, so that the system will automatically send notification of malware via SMS.*

Keywords*: network, malware, wannacry, detection, sms gateway*

Intisari - Jaringan internet merupakan media atau teknologi yang sangat berguna pada masa ini. Hampir semua orang yang menggunakan elektronik mengunakan jaringan internet. Dengan adanya jaringan internet ini, manusia dapat mengakses dunia maya dengan mudah, baik dalam melakukan browsing, streaming, akses media sosial dan lain-lain. Disisi lain ada kekurangan pada teknologi jaringan internet. Dengan adanya internet, komputer dapat terhubung dengan komputer lainnya, sehingga banyak kasus terjadinya serangan malware melalui jaringan internet tersebut. Baru-baru ini telah terjadi serangan malware yang sangat berbahaya. Malware tersebut dikenal dengan nama wannacry ransomware. Wannacry dapat menyerang komputer yang menggunakan sistem operasi windows. Komputer yang telah terinveksi wannacry akan membuat semua data yang ada dalam hardisk komputer tersebut menjadi ter-enkripsi, sehingga pengguna tidak dapat membuka data yang telah terinveksi virus. Untuk mengatasi masalah tersebut maka diusulkan Perancangan Sistem Pendeteksi dan Pencegahan Malware Menggunakan Unified Modeling Language (UML). Sistem ini dirancang dengan menggunakan Router, Server, dan SMS Gateway. Router digunakan untuk konfigurasi jaringan. Server digunakan untuk tempat penyimpanan sistem yang berbasis WEB yang berfungsi untuk mendeteksi port. SMS Gateway digunakan untuk mengirim SMS ke admin jaringan. Dengan diusulkan sistem tersebut diharapkan dapat membantu mendeteksi adanya malware yang masuk melalui router, sehingga secara otomatis sistem akan mengirim notifikasi adanya malware melalui SMS.

Kata Kunci : Sistem pendeteksi, pencegahan penyebaran, malware, sms gateway

I. PENDAHULUAN

Hampir seluruh aspek kehidupan manusia saat ini tidak dapat dilepaskan dari teknologi, khususnya teknologi komputer, hal ini dapat dilihat dari penggunaan komputer yang semakin meluas, kemajuan teknologi komunikasi mempunyai pengaruh pada perkembangan pengolahan data, data

dari satu tempat dapat dikirim ke tempat lain dengan alat telekomunikasi. jaringan komputer bukanlah sesuatu yang baru saat ini, hampir di setiap perusahaan dan instansi pemerintahan terdapat jaringan komputer untuk memperlancar arus informasi. Internet yang mulai popular saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi, sehingga dalam beberapa tahun saja jumlah pengguna jaringan komputer yang tergabung dalam internet berlipat ganda.

Jaringan internet merupakan media atau teknologi yang sangat berguna pada masa ini. Hampir semua orang yang menggunakan elektronik mengunakan jaringan internet. Dengan adanya jaringan internet ini, manusia dapat mengakses dunia maya dengan mudah, baik dalam melakukan browsing, streaming, akses media sosial dan lain-lain.

Malware (*Malicious Software*) merupakan sebuah program yang dirancang dengan tujuan untuk masuk menyusup ke sebuah sistem komputer, yang akan merusak sistem komputer tersebut [1]. Malware dapat masuk ke banyak komputer melalui jaringan internet seperti email, *download* dari internet, atau melalui program yang terinfeksi. Malware bisa menyebabkan kerusakan pada sistem komputer, data dan memungkinkan juga terjadi pencurian data / informasi. Hal yang umum penyebab malware adalah mendownload software dari situs ilegal yang disisipkan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, ransomware dan lain-lain [2].

Baru-baru ini dunia telah terguncang dengan isu adanya virus wannacry [3] [4]. di mana 99 negara terkena dampak serangan *malware* ganas tersebut, termasuk Indonesia. Wannacry dapat menyusup masuk ke sebuah computer melalui internet. Direktur Jenderal Aplikasi Informatika, Semuel A Pangerapan mengatakan bahwa serangan siber ini bersifat tersebar dan masif serta menyerang *critical resource* (sumber daya sangat penting), maka serangan ini bisa dikategorikan sebagai teroris siber [5]. WannaCry (wcry) atau juga dikenal sebagai Wanna Decryptor adalah program ransomware spesifik yang mengunci semua data pada sistem komputer dan membiarkan korban hanya memiliki dua *file*: instruksi tentang apa yang harus dilakukan selanjutnya dan program *Wanna Decryptor* itu sendiri. Saat program itu dibuka, komputer akan memberitahukan kepada korban bahwa *file* mereka telah di-*encrypt*, dan memberikan mereka tenggat waktu untuk membayar, dengan memperingatkan bahwa *file* mereka akan dihapus [6].

Untuk mengatasi masalah tersebut maka diusulkan Perancangan Sistem Pendeteksi dan Pencegahan Malware Menggunakan Unified Modeling Language (UML). Sistem ini dirancang dengan menggunakan Router, Server, dan SMS Gateway. Router digunakan untuk konfigurasi jaringan. Server digunakan untuk tempat penyimpanan sistem yang berbasis WEB yang berfungsi untuk mendeteksi port. SMS Gateway digunakan untuk mengirim SMS ke admin jaringan. Dengan diusulkan sistem tersebut diharapkan dapat membantu mendeteksi adanya malware yang masuk melalui router, sehingga secara otomatis sistem akan mengirim notifikasi adanya *malware* melalui SMS.

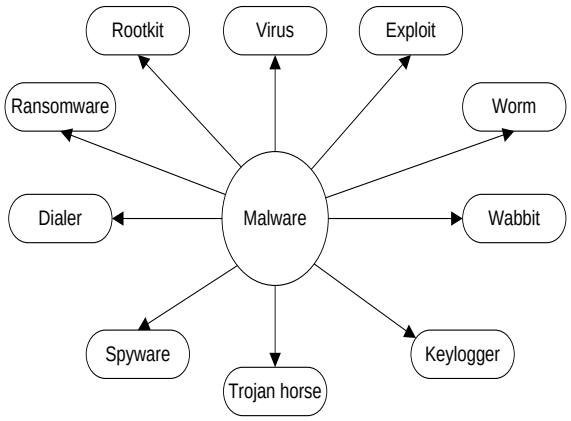
II. SIGNIFIKASI STUDI

A. Studi Literatur

1. Dasar Teori

Malware merupakan sejenis program komputer yang dimaksudkan untuk mencari kelemahan software sehingga pada perangkat akan terkena virus [7]. Malware (*Malicious Software*) merupakan sebuah program yang dirancang dengan tujuan untuk masuk menyusup ke sebuah sistem computer, yang akan merusak sistem computer tersebut [1]. Malware dapat masuk ke banyak komputer dengan cara masuk melalui jaringan internet seperti email, download dari internet, atau melalui

program yang terinfeksi. Malware bisa menyebabkan kerusakan pada sistem computer, data dan memungkinkan juga terjadi pencurian data / informasi. Hal yang pada umumnya terjadi penyebab malware adalah mendownload software dari situs ilegal yang disisipkan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, ransomware dan lain-lain [2].



Gambar 1. Malware (Qian Chen)

2. Mikrotik API

Application Programmable Interface (API) memungkinkan pengguna untuk membuat solusi perangkat lunak khusus untuk berkomunikasi dengan RouterOS untuk mengumpulkan informasi, menyesuaikan konfigurasi dan mengelola router. API umumnya menggunakan sintaks dari Command Line Interface (CLI). Ini dapat digunakan untuk membuat alat konfigurasi yang diterjemahkan atau kustom untuk membantu kemudahan penggunaan menjalankan dan mengelola router dengan RouterOS.

3. SMS Gateway

SMS Gateway adalah sebuah gerbang yang menghubungkan antara komputer dengan client melalui SMS, jadi secara garis besar, SMS Gateway dapat digambarkan seperti Gambar 2. Client secara tidak langsung berinteraksi dengan aplikasi / sistem melalui SMS Gateway. Saat melakukan SMS, maka informasi terpenting yang diperlukan adalah nomor tujuan dan pesan, maka itulah yang sebenarnya diolah oleh SMS Gateway [8] [9] [10].

Gambar 2. SMS Gateway (C.Taddia)

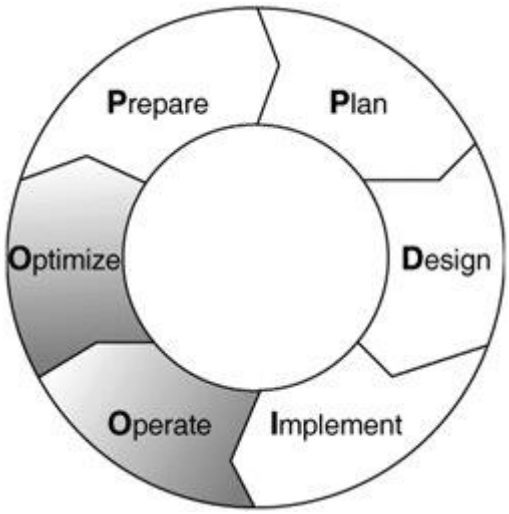
4. Unified Modeling Language (UML)

UML adalah sekumpulan alat yang digunakan untuk melakukan abstraksi terhadap sebuah sistem atau perangkat lunak berbasis objek. UML merupakan singkatan dari Unified Modeling Language. UML juga menjadi salah satu cara untuk mempermudah pengembangan aplikasi yang berkelanjutan. Aplikasi atau sistem yang tidak terdokumentasi biasanya dapat menghambat pengembangan dikarenakan *developer* harusmelakukan penelusuran dan mempelajari kode program. UML juga dapat menjadi alat bantu untuk *transfer* ilmu tentang sistem atau aplikasi yang akan dikembangkan dari satu *developer* ke *developer* lainya. Tidak hanya antar *developer* terhadap orang bisnis dan siapapun dapat memahami sebuah sistem dengan adanya UML. UML diciptakan oleh Object Management Group yang diawali dengan versi 1.0 pada Januari 1997. Dalam pengembangan berorientasi objek ada beberapa prinsip yang harus dikenal yaitu *Object, Class, Abstraction, Encapsulation, Inheritance* dan *Polymorphism*.

B. Metodologi Penelitian

Pada tahap ini akan dipaparkan tahapan-tahapan yang akan dilakukan dalam perancangan sistem. Adapun tahapan-tahapan dalam perancangan sistem ini yaitu tahap persiapan, perencanaan, desain, implementasi, operasional, dan

optimalisasi seperti yang ditunjukkan pada Gambar 3:



Gambar 3. Tahapan-tahapan pada perancangan sistem (Tedyyana)

1. Tahap Persiapan

Pada tahap ini akan dilakukan persiapan untuk menetapkan kebutuhan-kebutuhan atau data-data yang akan digunakan untuk merancang sistem yang diusulkan. Adapun persiapan yang akan dilakukan adalah :

a. Mengumpulkan data-data penelitian seperti port-port yang sering diakses oleh malware.
b. Menentukan software yang akan digunakan untuk merancang sistem.

2. Tahap Perencanaan

Fase Plan (perencanaan) mengidentifikasi persyaratan jaringan berdasarkan tujuan, fasilitas, dan kebutuhan pengguna. Fase ini mendeskripsikan karakteristik suatu jaringan, yang bertujuan untuk menilai jaringan tersebut, melakukan gap analisis pada perancangan terbaik sebuah arsitektur, dengan melihat perilaku dari lingkungan operasional. Sebuah perencanaan proyek dikembangkan untuk mengelola tugas-tugas (tasks), pihak-pihak yang bertanggung jawab, batu pijakan (*milestones*), dan semua sumber daya untuk melakukan desain dan implementasi. Perencanaan proyek harus sejalan dengan ruang lingkup (batasan), biaya dan parameter sumber daya yang disesuaikan dengan kebutuhan bisnis . Rencana proyek ini diikuti (dan diperbarui) selama fase-fase dalam siklus.

3. Tahap Desain

Desain jaringan dikembangkan berdasarkan persyaratan teknis, dan bisnis yang diperoleh dari kondisi sebelumnya. Spesifikasi desain jaringan adalah desain yang bersifat komprehensif dan terperinci, yang memenuhi persyaratan teknis dan bisnis saat ini. Jaringan tersebut haruslah menyediakan ketersediaan, kehandalan, keamanan, skalabilitas dan kinerja. Hasil desain termasuk diagram jaringan, dan daftar peralatan-peralatan. Rencana proyek harus terus diperbarui, dengan informasi yang lebih terperinci untuk diimplementasikan. Setelah tahap desain disetujui, fase implementasi dimulai.

4. Tahap Implementasi

Pada fase ini, peralatan-peralatan baru dilakukan instalasi dan di konfigurasi, sesuai spesifikasi desain. Perangkat-perangkat baru ini akan mengganti atau menambah infrastruktur yang ada. Perencanaan proyek juga harus diikuti selama fase ini, jika ada perubahan seharusnya disampaikan dalam pertemuan (meeting), dengan persetujuan yang diperlukan untuk dilanjutkan. Setiap langkah dalam implementasi, harus menyertakan deskripsi, rincian pedoman pelaksanaan, perkiraan waktu untuk penerapan, evaluasi (rollback) langkah-langkah jika terdapat kegagalan, dan informasi-informasi lainnya sebagai referensi tambahan. Seiring perubahan yang telah di implementasikan, tahapan ini juga menjadi langkah pengujian, sebelum pindah ke fase operasional (operate phase).

5. Tahap operasional

Fase operasional adalah mempertahankan ketahahan kegiatan sehari-hari jaringan. Operasional meliputi pengelolaan dan memonitor komponen-komponan jaringan, pemeliharaan routing, mengelola kegiatan upgrade, mengelola

kinerja, mengidentifikasi dan mengoreksi kesalahan jaringan. Tahapan ini adalah ujian akhir bagi tahapan desain. Selama operasi, manajemen jaringan harus memantau stabilitas dan kinerja jaringan, Deteksi kesalahan, koreksi konfigurasi, dan kegiatan-kegiatan pemantauan kinerja, yang menyediakan data awal untuk fase selanjutnya, yaitu fase optimalisasi (optimize phase).

6. Tahap Optimalisasi

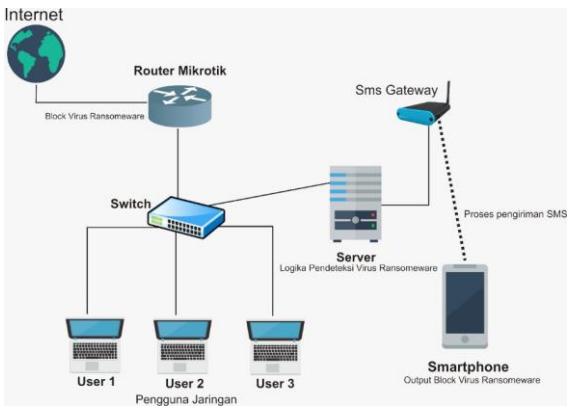
Fase optimalisasi, melibatkan kesadaran proaktif seorang manajemen jaringan dengan mengidentifikasi dan menyelesaikan masalah, sebelum persoalan tersebut mempengaruhi jaringan. Fase optimalisasi, memungkinkan untuk memodifikasi desain jaringan, jika terlalu banyak masalah jaringan yang timbul, kemudian juga untuk memperbaiki masalah kinerja, atau untuk menyelesaikan masalah-masalah pada aplikasi (*software*). Persyaratan-persayaratan untuk desain jaringan yang dimodifikasi mengarahkan perkembangan jaringan tersebut, kembali ke awal siklus hidup dalam model fase PPDIOO.

III. HASIL DAN PEMBAHASAN

Pada tahap ini akan dibahas tentang implementasi dari perancangan beserta pembahasannya.

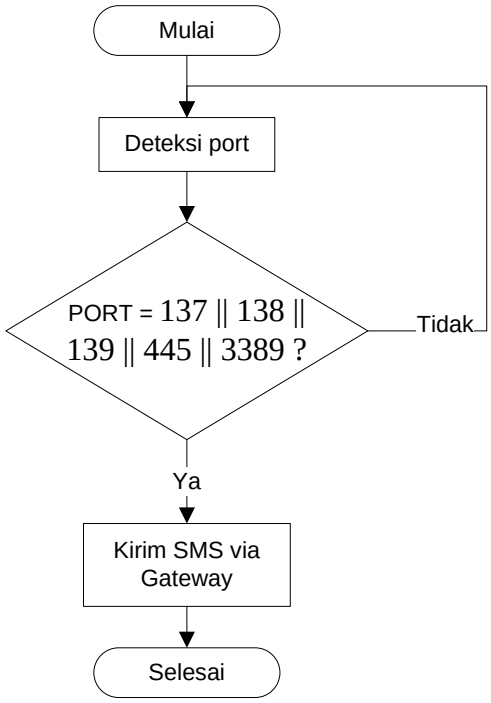
A. Implementasi

Hasil perancangan sistem yang diusulkan dapat dilihat pada Gambar 4.



Gambar 4. Hasil Perancangan Sistem.

Gambar 4. menunjukkan bahwa ada sebuah sistem yang dirancang untuk memonitoring aliran traffic jaringan yang terjadi di router. Adapun aliran traffic yang di monitoring adalah pada bagian aliran port. Sistem akan mendeteksi port-port yang lewat melalui router. Jadi ada beberapa port yang terindikasi sebagai port yang sering digunakan pada penyebaran malware seperti *wannacry*. Adapun port-port yang terindikasi sebagai port yang sering digunakan sebagai aliran malware adalah port 137, 138, 139, 445 dan 3389. Sehingga ketika ada aliran dari port-port tersebut, maka sistem akan melakukan aksi. Adapun aksi yang dilakukan adalah menutup port tersebut dan sekaligus mengirimkan informasi ada malware. Informasi tersebut dikirimkan melalui SMS Gateway. Pengguna akan menerima informasi dalam bentuk SMS.



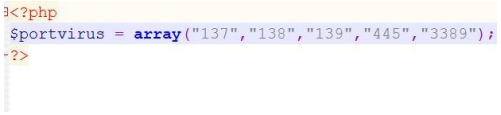
Gambar 5. Flowchart perancangan sistem.

Gambar 5 menunjukkan aliran proses yang diusulkan. Pada diagram tersebut menunjukkan beberapa proses yang digunakan yaitu dimulai dari deteksi port. Deteksi port digunakan untuk mendeteksi apakah ada jaringan yang melewati port-

port yang di seleksi. Jika ada jaringan yang melewati port-port yang diseleksi maka sistem akan mengirimkan informasi dalam bentuk SMS melalui SMS Gateway.

Gambar 6. Hasil Source Code dari sistem.

Gambar 6 menunjukkan hasil source code perancangan sistem yang diusulkan. Adapun port-port yang akan diidentifikasi sebagai port malware dapat dilihat pada Gambar 7.



Gambar 7. Hasil Source Code port virus.

Pada Gambar 7 menunjukkan port-port yang sering digunakan oleh malware seperti wannacry. Jadi port-port tersebut yang digunakan untuk mendeteksi malware.

B. Pembahasan

Dari perancangan sistem yang diusulkan menunjukkan bahwa sistem ini mampu mendeteksi malware yang menyusup masuk melalui router. Menurut mikrotik.com menjelaskan bahwa *malware* yang dikenal dengan wannacry masuk kejaringan melalui port. Adapun port-port yang sering dilewati *malware* yaitu 137, 138, 139, 445 dan 3389. Sehigga port-port tersebut digunakan untuk mendeteksi malware yang masuk melalui jaringan.

Sistem dirancang dengan membuat aplikasi berbasis web yang dibangun dengan menggunakan bahasa pemrograman web seperti html, php, css, dan lain-lain. Aplikasi web yang dibangun akan ditempatkan pada server atau hosting. Aplikasi tersebut akan digunakan untuk memonitoring sebuah router mikrotik. Sehingga ketika ada yang mengakses port-port (137, 138, 139, 445 dan 3389) pada router tersebut maka sistem akan melakukan aksi yaitu mengirim informasi kepada administrator atau pihak yang lain melalui SMS. SMS akan dikirim dengan memanfaatkan SMS Gateway.

Ada sisi kelemahan dari sistem yang diusulkan yaitu semua jaringan yang akan akses atau melewati port-port yang telah ditentukan (137, 138, 139, 445 dan 3389) maka akan dianggap sebagai aktivitas malware. Jadi sistem ini tidak bisa membedakan bahwa yang melewati port-port tersebut apakah malware atau bukan malware.

IV. KESIMPULAN

Berdasarkan penelitian dan perancangan sistem yang diusulkan menunjukkan bahwa sistem dirancang dengan cara mengindikasi port-port yang sering digunakan malware. Ketika ada malware yang melewati port-port yang ditentukan sebagai airan malware maka sistem akan mengirimkan informasi melalui SMS Gateway. Semua jaringan yang melewati port-port yang diindikasi sebagai aliran malware akan dianggap sebagai malware.

Dari analisa yang dilakukan terhadap perancangan sistem yang telah diusulkan maka ada beberapa saran untuk pengembangan kedepan dari sistem yang diusulkan seperti adanya penambahan port-port yang terindikasi sebagai aliran malware dan adanya seleksi jenis aliran malware atau bukan malware yang melewati port-port yang diindikasi sebagai port aliran malware.

REFERENSI

[1] M. Howard, A. Pfeffer, M. Dalal, and M. Reposa, “Predicting Signatures of Future Malware Variants,” 12th Int. Conf. Malicious Unwanted Softw.

(MALWARE 2017), pp. 126–132, 2017.

[2] M. Kalash, M. Rochan, N. Mohammed, N. D. B. Bruce, Y. Wang, and F. Iqbal, "Malware Classification with Deep Convolutional Neural Networks," 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur., pp. 1–5, 2018.

[3] S. Hsiao and D. Kao, "The Static Analysis of WannaCry ġ Ransomware," pp. 153–158, 2018.

[4] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry ransomware - IEEE Conference Publication," Int. Conf. Adv. Commun. Technolo gy(ICACT, pp. 159–166, 2018.

[5] N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," Aust. Inf. Secur. Manag. Conf., vol. 13, pp. 47–56, 2015.

[6] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware," pp. 454–460, 2017.

[7] S. Mohurle and M. Patil, "A brief study of Wannacry Threat : Ransomware Attack 2017," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 5, pp. 2016–2018, 2017.

[8] X. Lu, W. Lei, and W. Zhang, "The design and implementation of XMPP-based SMS gateway," Proc. - 2012 4th Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSyN 2012, pp. 145–148, 2012.

[9] C. Taddia and G. Mazzini, "Architectures for an efficient SMS Gateway service," 2015 23rd Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2015, pp. 254–258, 2015.

[10] M. Kashif, "Secure SMS communication using encryption gateway and digital signature," Proc. - 17th IEEE Int. Conf. Comput. Sci. Eng. CSE 2014, Jointly with 13th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC 2014, 13th Int. Symp. Pervasive Syst. Algorithms, Networks, I-SPAN 2014 8th Int. Conf. Front. Comput. Sci. Technol. FCST 2014, pp. 1430–1434, 2015.