

# PROTOTIPE SMS REPORT PORTABEL MENGUNAKAN RASPBERRY PI

Azmi Analisis Syuhada, Fakultas Ilmu Komputer Universitas Dian Nuswantoro Semarang

**Abstract:** Server log is a computer system that contain network traffic activities in router. Server log can be used as a reliable source when a network computer system has been attacked by hacker. Network administrator will able to know everything that the hackers do through these server log. Early detection system is a system that can notify any anomaly or interference in the system to the network administrator, so the network administrator can handle that interference immediately. It also make it easier for the network administrator to monitor the network when he's not in his working area. In this research, researcher aim to make a prototype of portable early detection system that will send through Short Message System (SMS) to network administrator when anomaly or interference happen in the network system that he handle. This system works by monitoring every server and router which connected in the network and then notify through SMS to network administrator when at least one or more server down all of sudden using ICMP protocol or PING so the network administrator can handle it immediately. This proposal will cover the method that will used in these prototype and the implementation. Things that has been done and things that haven't been done to create this prototype will be discussed in the end of this research.

**Index Terms**—*Gammu, Network Monitoring, Raspberry Pi, Rsyslog, Sms Report*

## I. PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi berkembang pesat saat ini, tuntutan akan kebutuhan akses informasi berupa data dalam kehidupan sehari-hari juga sangat meningkat. Begitu juga perkembangan teknologi pada sistem deteksi dini pada jaringan komputer baik itu internet maupun intranet ketika terjadi serangan oleh pihak yang tidak berwenang ataupun kerusakan perangkat keras dari infrastruktur yang telah dibangun.

Dalam perkembangan sistem deteksi dini, salah satu penelitian berjudul “*Design and Implementation of a Distributed Early Warning System Combined with Intrusion Detection System and Honeypot*” oleh (Pei-Sheng Huang, Chung-Huang Yang, Tae-Nam Ahn) menyatakan bahwa penggunaan *firewall* dan teknologi *intrusion detection* tradisional tidak bisa cocok dengan perubahan yang cepat ini. *Attacker* akan diberitahu bahwa *firewall* memungkinkan layanan yang ada dapat diakses dari luar sehingga *Attacker* dapat mengakses server internal tersebut untuk serangan berikutnya. Server merupakan sebuah sistem komputer yang menyediakan jenis layanan dalam sebuah jaringan komputer [1].

Kemampuan dalam pelaporan tentang terjadinya serangan pada jaringan dan infrastrukturnya sangat penting untuk seorang administrator dan pengelola infrastruktur jaringan tersebut. Dalam penelitian yang berjudul “*A DSL for Intrusion Detection Based on Constraint Programming*” oleh (Pedro D.Salgueiro, Salvador P.Abreu) menyatakan bahwa untuk mencegah degradasi jaringan komputer atau

bahkan kegagalan, jaringan terus menerus dipantau untuk mendiagnosa fungsi dan integritas. Sistem dan aplikasi monitor jaringan dirancang untuk melakukan tugas-tugas pemantauan jaringan pada jaringan komputer. *IDS* terus menerus memantau perangkat jaringan dan layanan dalam rangka untuk mendeteksi kemungkinan anomali. *IDS* (*Intrusion Detection System*) adalah aplikasi yang berfokus pada pemantauan lalu lintas dan memeriksa lalu lintas untuk mencari anomali atau komunikasi yang tidak diinginkan [2].

Portabilitas dan fleksibilitas sistem sangat penting karena dapat mengurangi biaya serta menambah efisiensi waktu, maka dalam penelitian yang berjudul “*Implementation of OpenWrt-based IP PnP Gateway*” oleh (Yun-Yu Lee, Ing-Yi Chen, Sy-Yen Kuo, Hsi-Hai Liu, Yuh-Rong Leu) menyatakan bahwa mengelola dan mengendalikan pengguna hotspot adalah masalah yang sangat penting dan membutuhkan biaya yang tidak sedikit, maka dari itu masalah tersebut dapat ditangani dengan menggunakan portabilitas platform open source yaitu OpenWRT dengan ChilliSpot Captive Portal yang berfungsi sebagai akses kontrol yang terintegrasi, Dynamic DNS Server dan Client yang berfungsi sebagai penyedia alamat IP yang dapat memperbarui secara otomatis ketika terjadi perubahan maka Dynamic DNS client akan mengirimkan permintaan pembaruan IP kepada Dynamic DNS Server. Dengan menambahkan fungsi diatas, gateway akan menjadi Network Access Control Gateway. Setelah menambahkan fitur tersebut, jalur access point umum dapat diubah ke dalam Network Access Control Gateway. Akhirnya, dalam rangka memberikan fleksibilitas untuk membiarkan gateway menjadi access point umum, IP PnP (Plug and Play) akan memberikan kenyamanan penggunaan. ChilliSpot Captive

Portal adalah captive portal open source atau LAN nirkabel jalur akses controller yang digunakan untuk otentikasi pengguna LAN nirkabel [3]. Kesimpulan dari ketiga penelitian tersebut terdapat teknik yang dapat digunakan untuk sistem deteksi dini pada layanan jaringan komputer yang fleksibel dan portabel.

Penerapan sistem deteksi dini melalui SMS pada *server* dan *router* yang terdapat pada infrastruktur jaringan komputer ini berguna jika sistem tersebut mati secara mendadak dapat segera ditangani dengan memanfaatkan informasi yang dikirimkan melalui sms dan Server log sebagai mesin pencatat aktivitas, namun sistem yang ada pada saat ini belum efisien karena sistem tersebut tidak portabel, mobilitasnya kurang dan pengaturannya tidak praktis karena sistem tersebut biasanya dipasang di satu mesin yang sama sehingga jika server tersebut rusak maka sistem sms report tersebut juga ikut rusak, dengan menggunakan raspberry pi yang dijadikan sebagai server log atau mesin pencatat aktivitas server lain dan apabila server tersebut rusak atau diserang oleh peretas maka server log tidak terpengaruh karena dipasang secara terpisah. Dibandingkan dengan server log yang digabung dengan satu layanan yang lain dalam satu mesin, maka sistem ini lebih efisien, tidak mengganggu layanan lain, hemat biaya dan tidak memakan tempat pada rak server. *Rsyslog* sebagai pencatat *system log* pada *server*, *gammu* dan *gammu-smsd* sebagai *sms gateway* untuk mengirimkan *sms* yang berupa informasi bahwa telah terjadi gangguan misalnya *router* ataupun *server* mati secara mendadak kepada administrator jaringan akan digunakan dalam penelitian ini.

## II. METODE YANG DIUSULKAN

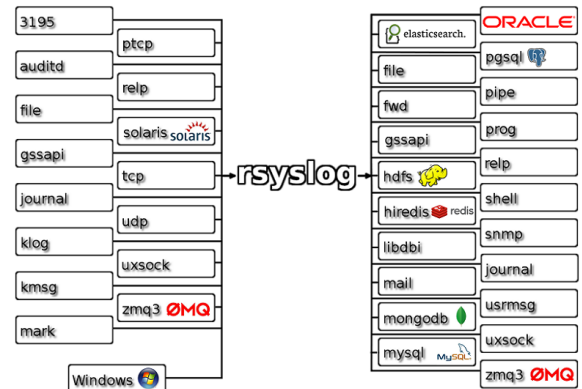
Model penelitian yang dilakukan oleh peneliti pada penelitian ini yaitu menggunakan model prototipe dan tahapan-tahapannya adalah sebagai berikut :

### A. Pengumpulan Kebutuhan

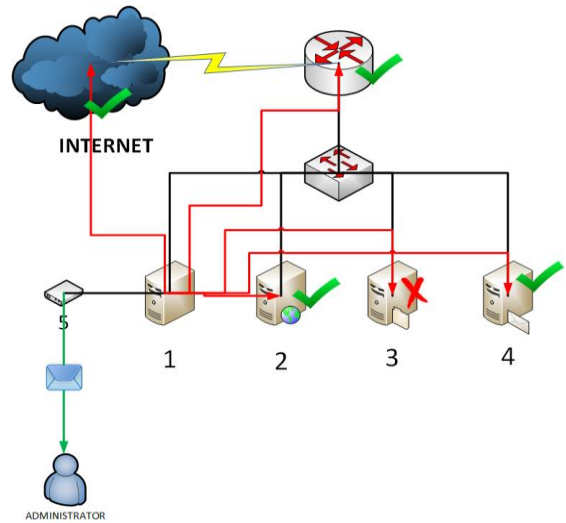
Pada tahapan ini peneliti mulai mengumpulkan kebutuhan-kebutuhan untuk membuat Prototipe yang diusulkan, dari pengumpulan hardware dan software seperti yang telah diulas pada instrumen penelitian.

### B. Merancang dan Membuat Prototipe

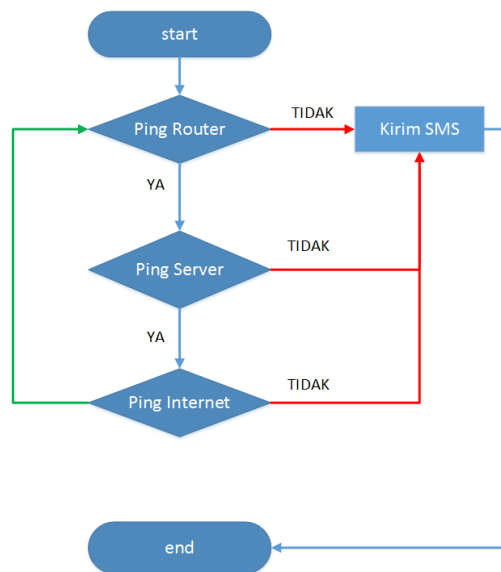
Pada tahap ini peneliti mulai merancang konsep prototipe yang diusulkan dan membuat prototipe dari konsep tersebut. Konsep prototipe dapat dilihat pada gambar dibawah ini :



Gambar 2.1. Konsep Rsyslog



Gambar 2.2. Perancangan Prototipe Sms Report



Gambar 2.3. Flowchart Perancangan Prototipe

### C. Uji Coba

Pada tahap ini peneliti mulai uji coba prototipe yang telah dibuat sebelumnya, kemudian mengevaluasi kerja prototipe.

### III. IMPLEMENTASI

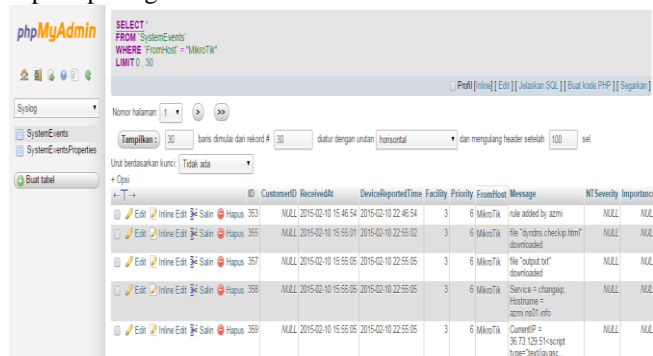
Dari metode atau model penelitian yang penulis gunakan maka cara pengujiannya dimulai dari tahap pertama yaitu pengumpulan kebutuhan perangkat keras dan perangkat lunak. Perangkat keras yang digunakan adalah Raspberry Pi Model B+ yang digunakan sebagai Server Log dan SMS Gateway, MikroTik Router sebagai Router, Modem Huawei Vodafone E220 sebagai pengirim SMS, dan Switch 8 Port sebagai penghubung semua perangkat jaringan. Sedangkan kebutuhan perangkat lunak antara lain Raspbian Wheezy sebagai Sistem Operasi Server Log dan SMS Gateway dan PuTTY sebagai aplikasi untuk remote server.

Tahap kedua yaitu perancangan konsep dan desain jaringan yang akan digunakan dalam model prototipe yang diusulkan. Tahap ketiga yaitu instalasi dan konfigurasi server sesuai dengan kebutuhan perangkat lunak. Tahap keempat yaitu uji coba model prototipe yang telah dibuat dan tahap terakhir yaitu mengevaluasi kerja model prototipe yang telah dibuat.

### IV. HASIL & PEMBAHASAN

#### A. Log Disimpan Dalam Database

Untuk pengujiannya bisa dilihat dari database mysql dengan melakukan penyaringan berdasarkan keyword, disini keyword yang dipakai adalah “MikroTik” (tanpa tanda kutip) yaitu dengan query mysql `SELECT * FROM SystemEvents WHERE `FromHost`="MikroTik"`; query tersebut berfungsi untuk mengambil semua record dengan keyword MikroTik dari tabel SystemEvents dan kolom FromHost pada database Syslog. Untuk lebih jelasnya seperti pada gambar dibawah ini :



The screenshot shows a MySQL query in phpMyAdmin: `SELECT * FROM SystemEvents WHERE `FromHost`="MikroTik" LIMIT 0, 30`. The results table contains the following data:

ID	CustomerID	ReceivedAt	DeviceReportedTime	Facility	Priority	FromHost	Message	NT Severity	Importance
353		2015-02-10 15:46:54	2015-02-10 22:46:54	3	6	MikroTik	rule added by azmi	NULL	NULL
355		2015-02-10 15:55:01	2015-02-10 22:55:02	3	6	MikroTik	file "syntax-checkip.htm" downloaded	NULL	NULL
357		2015-02-10 15:55:05	2015-02-10 22:55:05	3	6	MikroTik	file "output.txt" downloaded	NULL	NULL
358		2015-02-10 15:55:05	2015-02-10 22:55:05	3	6	MikroTik	Service = changep, Hostname = azmi.m01.info	NULL	NULL
359		2015-02-10 15:55:05	2015-02-10 22:55:05	3	6	MikroTik	CurrentIP = 28.73.129.51, receipt type="text/plain"	NULL	NULL

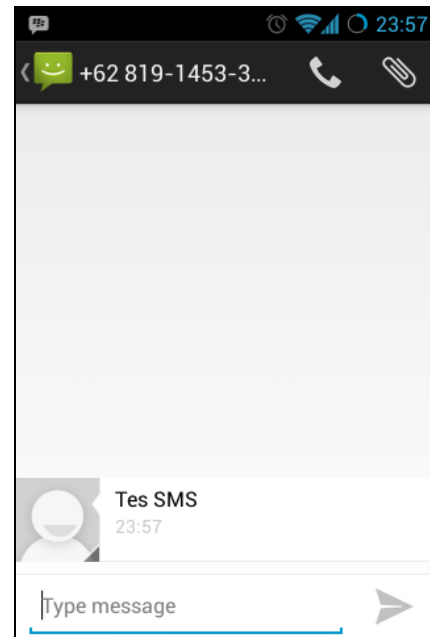
Gambar 4.1. Database Log Mikrotik

#### B. Pengujian Gammu Untuk Kirim SMS

Pengujian gammu sebagai mesin sms gateway dapat diuji dengan mengirimkan sms kepada nomor tujuan dengan perintah `gammu sendsms TEXT 085742147893 -text "Tes SMS"`.

```
root@raspberrypi:/home# gammu sendsms TEXT 085742147893 -text "Test SMS"
If you want break, press Ctrl+C...
Sending SMS 1/1...waiting for network answer..OK, message reference=17
root@raspberrypi:/home#
```

Gambar 4.2. Uji Coba Gammu Untuk Kirim SMS

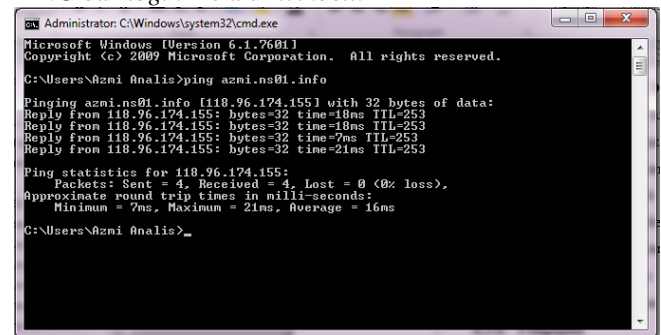


Gambar 4.3. Hasil Pengujian SMS Gateway

#### C. Pengujian Dynamic DNS

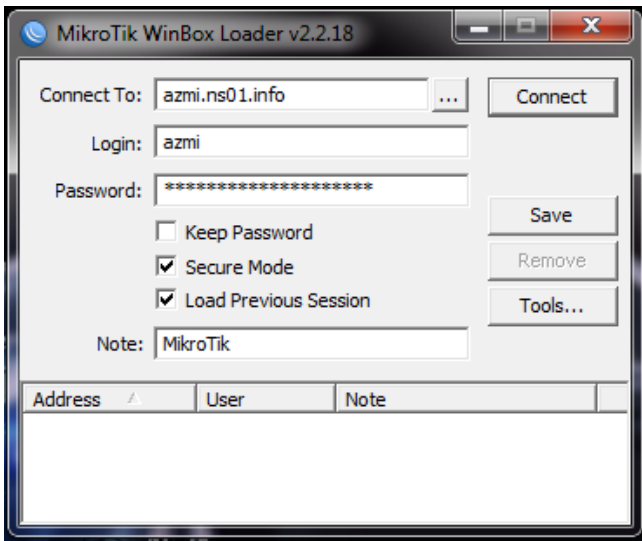
Dynamic DNS ini dipasang pada router MikroTik sehingga router tersebut dapat diakses melalui internet dengan hanya memanggil nama domain yang telah dibuat sebelumnya. Dalam pengujian ini peneliti menggunakan nama domain `azmi.ns01.info` yang telah dibuat sebelumnya.

Langkah-langkah pengujian dynamic dns pertama yaitu dengan memanggil nama domain tersebut dengan cara `PING` dan `login` melalui `Winbox`.

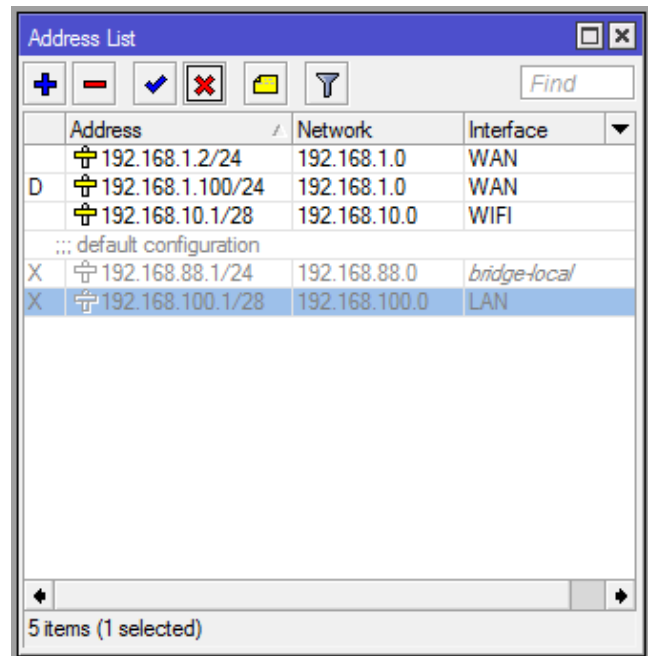


Gambar 4.4. Pengujian Ping Domain `azmi.ns01.info`

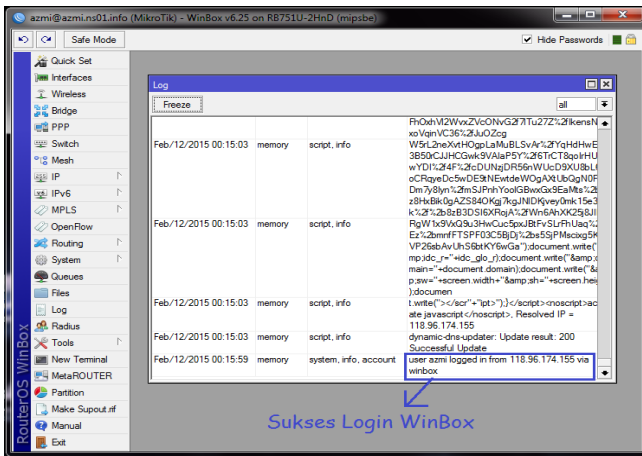
Langkah kedua dalam pengujian dynamic dns yaitu dengan `login` dengan aplikasi `Winbox` seperti gambar dibawah ini :



Gambar 4.5. Tampilan Winbox



Gambar 4.7. Salah Satu IP Di Non-Aktifkan



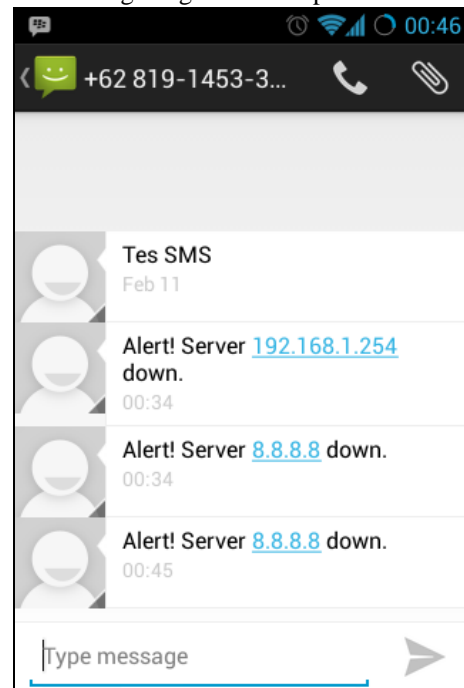
Gambar 4.6. Hasil Pengujian Dynamic DNS

#### D. Pengujian Script Monitoring Jaringan

Dalam pengujian ini salah satu alamat IP pada router MikroTik dinon-aktifkan sehingga ketika script ini akan melakukan ping satu-persatu terhadap alamat ip yang telah ditentukan akan secara otomatis mengirimkan SMS Report kepada Administrator Jaringan apabila salah satu atau lebih alamat ip yang *timeout* atau gagal dipanggil. Berikut adalah langkah-langkah pengujiannya :

- Login ke router MikroTik dengan Winbox kemudian non-aktifkan salah satu IP yang ada melalui menu *IP > Address*.

- Langkah kedua yaitu cek pesan masuk pada *Handphone*, apabila ada pesan masuk seperti gambar dibawah ini maka pengujian Script Monitoring dengan SMS Report berhasil.



Gambar 4.8. Hasil Pengujian Script Monitoring Jaringan dan SMS Report

Setelah dilakukan uji coba dengan menon-aktifkan salah satu alamat IP pada router MikroTik hasilnya adalah script tersebut melakukan pengecekan terhadap semua alamat IP yang telah ditentukan yaitu dengan keterangan alamat IP *192.168.1.254* adalah alamat IP modem bawaan dari ISP yang peneliti gunakan, sedangkan alamat IP *8.8.8.8* adalah alamat IP google sehingga server log tidak dapat terkoneksi

dengan internet karena alamat IP *192.168.100.1* adalah alamat IP Gateway yang berfungsi untuk menghubungkan server log dengan jaringan internet.

NO	PENGUJIAN	HASIL
1.	Server Log	Sesuai
2.	Dynamic DNS	Sesuai
3.	Monitoring Jaringan dan SMS Report	Sesuai

Tabel 4.1. Tabel Pengujian Prototipe SMS Report Portabel

## V. PENUTUP

Dari hasil pengujian Prototipe SMS Report Portabel Menggunakan Raspberry Pi dapat disimpulkan bahwa sistem dapat berjalan dengan baik namun ada kekurangan dalam sistem ini yaitu USB Modem yang digunakan kadang tidak terdeteksi oleh Gammu sehingga terjadi kendala ketika salah satu server mati maka Administrator Jaringan tidak mendapat SMS Report dari Sistem.

Karena selama proses pengujian terdapat masalah dan kekurangan pada prototipe ini maka ada beberapa saran untuk peneliti selanjutnya apabila ingin melakukan riset dengan topik yang sama tentang SMS Report Portabel Menggunakan Raspberry Pi yaitu :

1. Gunakan Modem USB yang stabil sehingga pengiriman SMS Report lancar.
2. Monitoring jaringan sebaiknya ditambahkan dengan protokol yang lain misalnya SNMP atau bila perlu tambahkan pendeteksi Intruder yang bisa dilaporkan melalui SMS Report.
3. Selain menggunakan PING, pemantauan jaringan juga bisa dilakukan berdasarkan layanan seperti layanan web server, mail server, ftp server, dan layanan yang lainnya.

## VI. DAFTAR PUSTAKA

- [1] M. B. Jan Bergstram, HANDBOOK OF NETWORK AND SYSTEM ADMINISTRATION, Amsterdam: Elsevier, 2007.
- [2] P. D. Salgueiro dan S. P. Abreu, "A DSL for Intrusion Detection Based on Constraint Programming," p. 224, 2010.
- [3] M. AB, "Chillispot," [Online]. Available: <http://www.chillispot.org>. [Diakses 08 Oktober 2014].
- [4] A. J. Alzahrani dan A. A. Ghorbani, "SMS Mobile Botnet Using A Multi-Agent System : Research In Progress," 2009.
- [5] Y.-y. Lee, I.-Y. Chen, S.-Y. Kuo, H.-H. Liu dan Y.-R. Leu, "Implementation of OpenWrt-based IP PnP Gateway".
- [6] Wagito, Jaringan Komputer, Teori dan Implementasi Berbasis Linux, Yogyakarta: Gaya Media, 2007.
- [7] R. Hertzog dan R. Mas, The Debian Administrator's Handbook, Frexian SARL, 2012.
- [8] I. Cartealy, Linux Networking : Ubuntu, Kubuntu, Debian, dll, Jasakom, 2013.
- [9] Hendriansyah, "Implementasi Polling Dengan SMS Gateway Berbasis Web," 2010.
- [10] M. Thompson, "Raspbian," [Online]. Available: <http://www.raspbian.org>. [Diakses 08 Oktober 2014].
- [11] Adiscon GmbH, "Rsyslog," [Online]. Available: <http://www.rsyslog.com>. [Diakses 08 Oktober 2014].
- [12] GNU Project - Free Software Foundation, "Bash - GNU Project - Free Software Foundation," [Online]. Available: <http://www.gnu.org/software/bash/>. [Diakses 20 Oktober 2014].
- [13] Oracle Corporation, MySQL 5.7 Reference Manual.
- [14] M. Cihar, Gammu Manual Release 1.28.96, 2011.
- [15] A. Murtino, "SMS Alert Dengan Memanfaatkan Remote Logging," pp. 3-16, 2013.
- [16] R. S. Pressman, Software Engineering : A Practitioner's Approach, 7th International Edition, New York: The McGraw-Hill Companies, 2010.
- [17] S. Parker, Shell Scripting : Expert Recipes for Linux, Bash and More, Wrox, 2011.