Implementasi *Failover* Pada Jaringan WAN Berbasis *VPN*

Siti Nur Khasanah[1], Liliyani Asri Utami[2]

Abstract*— Basically, data communication from one location to another has many ways, one of them is using Metronet Fiber Optic. For connections using Metronet Fiber Optics the most common problem is the breaking of the connection caused by external interference. At this time the existing network in PT. Micronics Internusa is a LAN (Local Area Network). The problem faced is the utilization of both ISP that are considered inefficient and ISP path switching methods are still done manually if the path used is disconnected contained at branch offices. Therefore, this research is proposed for the design of VPN-based WAN networks that use failover to connect a wide network with a relatively low cost.

***Intisari*— Pada dasarnya komunikasi data dari satu lokasi ke lokasi yang lain memiliki banyak cara, salah satunya adalah menggunakan Metronet Fiber Optik. Untuk koneksi menggunakan Metronet Fiber Optik permasalahan yang paling sering terjadi adalah putusnya koneksi disebabkan oleh gangguan *eksternal*. Pada saat ini jaringan yang ada di PT. Micronics Internusa adalah jaringan LAN (*Local Area Network)*. Permasalahan yang dihadapi adalah pemanfaatan kedua ISP yang dinilai tidak efisien dan metode pengalihan jalur ISP yang masih dilakukan secara *manual* apabila jalur yang digunakan terputus yang terdapat dikantor cabang. Oleh karena itu, pada penelitian ini diusulkan untuk perancangan jaringan Wide Area Network (WAN) Berbasis VPN yang menggunakan *failover* untuk menghubungkan jaringan yang luas dengan biaya yang relatif murah.**

Kata Kunci*— *Wide Area Network*, VPN, *failover

I. PENDAHULUAN

Jaringan komputer adalah gabungan dari dua komputer atau lebih yang telah didesain sedemikian rupa agar dapat saling terhubung satu sama lain untuk dapat melakukan komunikasi, berbagi sumber daya maupun berbagi informasi. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan *hardware* atau *software* yang terhubung dengan jaringan. Setiap komputer, printer yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan *node*.

Pada dasarnya komunikasi data dari satu lokasi ke lokasi yang lain memiliki banyak cara, salah satunya adalah menggunakan Metronet Fiber Optik. Untuk koneksi menggunakan Metronet Fiber Optik permasalahan yang paling sering terjadi adalah putusnya koneksi disebabkan oleh gangguan *eksternal*. Perkembangan teknologi *internet* yang semakin pesat membuatnya menjadi faktor yang sangat penting bagi banyak perusahaan. Salah satunya PT. Micronics Internusa menggunakan 2 (dua) *Internet Service Provider* (ISP), yaitu *Speedy* (8Mbps) dan *Biznet* (8Mbps).

Pada saat ini jaringan yang ada di PT. Micronics Internusa adalah jaringan LAN (*Local Area Network)*. Permasalahan yang dihadapi adalah pemanfaatan kedua ISP yang dinilai tidak efisien dan metode pengalihan jalur ISP yang masih dilakukan secara *manual* apabila jalur yang digunakan terputus yang terdapat dikantor cabang, sehingga membutuhkan waktu yang cukup lama untuk proses pengalihan jalur tersebut [1]

Keuntungan VPN adalah menghemat biaya dan dapat melakukan transfer data atau *remote view* untuk mengendalikan komputer di rumah atau kantor dan dimana saja, VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif murah, karena transmisi data teknologi VPN menggunakan media jaringan *public* yang sudah ada tanpa perlu membangun jaringan pribadi. Kelemahan VPN adalah jaringan publik *(internet)* yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.

II. KAJIAN LITERATUR

A. Konsep Dasar Jaringan

Secara sederhana jaringan komputer dapat diartikan sebagai kumpulan beberapa komputer dan peralatan lain yang saling terhubung menggunakan aturan-aturan tertentu. Apabila sebuah komputer dapat membuat komputer lainnya *restart*, *shutdown*, atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan *autonomous* (tidak melakukan kontrol terhadap komputer lain dengan akses penuh).

Secara umum jaringan komputer terbagi menjadi 3 jenis, yaitu:

1. *Local Area Network (LAN)*
2. *Metropolitan Area network (MAN)*
3. *Wide Area Network (WAN)*
4. *Internet*

[1] *Jurusan Sistem Informasi STMIK Nusa Mandiri Jakarta, Jalan Damai No 8 Warung Jati Barat Margasatwa, Jakarta Selatan 12510 (tlp: 021-78839502; fax : 021 78839421 e-mail: siti.skx@nusamandiri.ac.id)*

[2] *Jurusan Sistem Informasi STMIK Nusa Mandiri Jakarta, Jalan Damai No 8 Warung Jati Barat Margasatwa, Jakarta Selatan 12510 (tlp: 021-78839502; fax : 021 78839421 e-mail: lily.lau@nusamandiri.ac.id)*

B. Peralatan Pendukung

"GNS3 adalah *software* simulasi jaringan komputer berbasis GUI yang mirip dengan *Cisco Packet Tracer*. Namun pada GNS3 memungkinkan simulasi jaringan yang kompleks, karena menggunakan *operating system* asli dari perangkat jaringan seperti *cisco* dan *juniper*. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi *router* langsung dari pada di *Cisco Packet Tracer"*. [2]

Beberapa perangkat keras yang digunakan pada jaringan computer seperti *Ethernet Card, switch, Router dan Server.*

C. Topologi Jaringan

"Topologi jaringan adalah susunan atau pemetaan interkoneksi antara *node* dari suatu jaringan, baik secara fisik (*real*) dan logis (*virtual*)". Memilih jenis kabel yang digunakan untuk membangun jaringan tidak lepas dari jenis topologi yang kita gunakan, namun pada intinya, jaringan komputer adalah jaringan kabel, dimana bentuk dan fungsi dari jaringan tersebut menentukan pemilihan jenis kabel, demikian juga sebaliknya, ketersediaan kabel dan harga menjadi pertimbangan utama untuk membangun sebuah jaringan komputer (baik *home network*, ataupun *network* kelas raksasa seperti MAN-*metropolitan area network*)

D. *IP Address*

"TCP/IP *(Transmission Control Protocol/Internet Protocol)* adalah sekumpulan protokol yang terdapat di dalam jaringan komputer yang digunakan untuk berkomunikasi atau bertukar data antar computer [3]. TCP/IP secara umum berfungsi untuk memilih rute terbaik transmisi data, memilih rute alternative jika suatu rute tidak dapat digunakan, mengatur dan mengirimkan paket-paket pengiriman data dan lain – lain. TCP/IP merupakan protokol yang memungkinkan sistem di seluruh dunia berkomunikasi pada jaringan tunggal yang disebut Internet.

E. Manajemen Jaringan

Manajemen jaringan merupakan kemampuan untuk mengontrol dan *memonitor* sebuah jaringan komputer dari sebuah lokasi". *The International Organization for Standardization* (ISO) mendefinisikan sebuah model konseptual untuk menjelaskan fungsi manajemen jaringan yaitu:

1. Manajemen kesalahan (*Fault Management*), Menyediakan fasilitas yang memungkinkan *administrator* jaringan untuk mengetahaui kesalahan pada perangkat yang dikelola, jaringan, dan operasi jaringan, agar dapat segera menentukan apa penyebabnya dan dapat segera mengambil tindakan (perbaikan). Untuk itu manajemen kesalahan memiliki mekanisme untuk:
   a. Melaporkan terjadinya kesalahan
   b. Mencatat laporan kesalahan *(logging*)
   c. Melakukan diagnosis
   d. Mengoreksi kesalahan (dimungkinkan secara otomatis)
2. Manajemen konfigurasi (*Configuration Management*), memonitor informasi konfigurasi jaringan sehingga dampak dari perangkat keras atau pun lunak tertentu dapat dikelola dengan baik. Hal tersebut dapat dilakukan dengan kemampuan untuk inisialisasi, konfigurasi ulang, pengoperasian, dan mematikan perangkat yang dikelola.
3. Pelaporan (*Accounting*), mengukur utilisasi jaringan dari pengguna atau grup tertentu untuk:
   a. Menghasilkan informasi tagihan (*billing*)
   b. Mengatur pengguna atau grup
   c. Membantu dalam menjaga peforma jaringan pada *level* tertentu yang dapat diterima.
   d. Manajemen performa mengukur berbagai aspek dari performa jaringan termasuk pengumpulan dan analisis dari data statistik sistem sehingga dapat dikelola dan dipertahankan pada *level* tertentu yang dapat diterima.
   e. Memperoleh utilisasi dan tingkat kesalahan dari perangkat jaringan.
   f. Mempertahankan performa pada *level* tertentu dengan memastikan perangkat memiliki kapasitas yang mencukupi
4. Manajemen keamanan (*Security Management*) mengatur akses ke sumber data jaringan sehingga informasi tidak dapat diperoleh tanpa izin hal tersebut dilakukan dengan cara:
   a. Membatasi akses ke sumber daya jaringan
   b. Memberi pemberitahuan akan adanya usaha pelanggaran dan pelanggaran keamanan.

F. *Virtual Private Network (VPN)*

Virtual Private Network (VPN) adalah teknik pengaman jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet [4]

III. METODE PENELITIAN

Metode penelitian adalah suatu cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu.

A. Analisa Penelitian

Analisa penelitian dilakukan dengan beberapa tahapan yaitu:

1. Analisa Kebutuhan

   Didalam merancang sebuah jaringan alat-alat dan *software* yang dibutuhkan adalah kabel UTP CAT6, RJ-45, tang *crimping*, *router*, *switch*, komputer, laptop dan *Graphical Network Simulator (*GNS3) yang akan digunakan dalam merancang jaringan.
2. Desain

   Desain yang akan dirancang menggunakan *topologi star*, dimana semua koneksi kabel LAN terpusat pada *switch*, *router* berfungsi sebagai pemberi *ip address* kepada semua alat-alat yang terhubung dengan *switch* dan *Mikrotik Router OS* berfungsi sebagai pengaturan dan pengalihan jaringan *internet.*

3. Testing
   Testing menggunakan *software GNS3*, dengan menggunakan *software* tersebut penulis akan melakukan pengujian pada seluruh komputer yang terhubung ke jaringan agar dapat saling terhubung dan dapat mengetahui perpindahan jaringan secara otomatis
4. Implementasi
   Sistem jaringan yang sudah dirancang, didesain dan ditesting menggunakan *GNS3*, selanjutnya akan diimplementasikan pada PT. Micronics Internusa dengan harapan setelah terpasangnya sistem jaringan yang sudah dibuat dapat lebih membantu dalam proses bekerja pada PT. Micronics Internusa

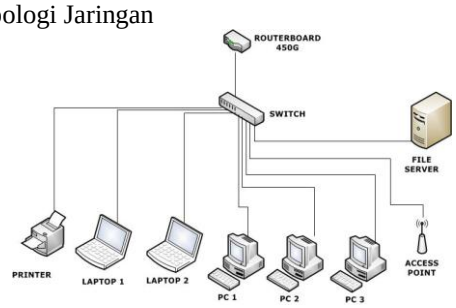
B. Metode Pengumpulan Data
1. Observasi
   Yaitu penulis melakukan pengamatan secara langsung pada sistem jaringan yang ada di PT. Micronics Internusa.
2. Wawancara
   Yaitu penulis melakukan wawancara langsung pada teknisi jaringan dan kepada pemakai komputer (*user*) dalam jaringan.
3. Studi Pustaka
   Untuk mengkaji masalah secara mendalam, penulis mengumpulkan data-data toritis dari refrensi buku-buku yang membahas mengenai jaringan komputer dan *Failover* pada WAN dengan Jaringan *Virtual Private Network* (VPN) dengan *Point to Point Tunnelling Protocol* (PPTP).

IV. HASIL DAN PEMBAHASAN

A. Jaringan Usulan

Kebutuhan akan aktifitas kantor dan tuntutan kerja yang semakin baik dan besar. Dengan adanya perubahan infrastruktur jaringan, perubahan skema jaringan yang berada di kantor cabang dan penggunaan *routerboard 450G* sebagai solusi pemindahan jaringan *internet* secara otomatis, yang terdapat di kantor cabang PT. Micronics Internusa menjadi lebih efisien, maka di perlukan adanya fasilitas yang baik pula untuk itu pembangunan jaringan VPN *(Virtual Private Network)* yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan *medium non* pribadi (misalnya internet) untuk menghubungkan antar *remote-site* secara aman.

B. Topologi Jaringan

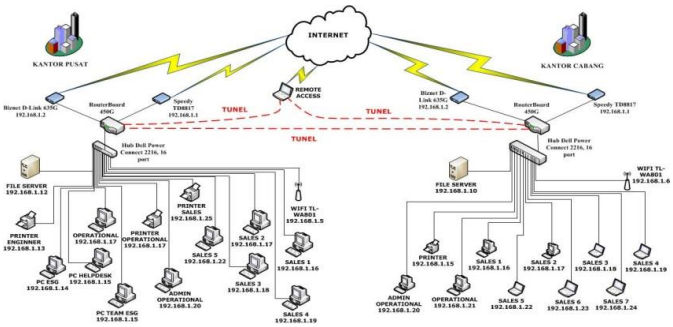


Sumber : Hasil Penelitian (2017)

Gbr. 1 Topologi Jaringan Usulan

Dari topologi jaringan usulan yang terdapat dikantor cabang PT. Micronics Internusa dapat dijelaskan menggunakan topologi star dimana semua komputer, laptop, *access point, file server, printer* dan semua peralatan terhubung dengan *switch*. Dalam topologi star terdapat *routerboard 450G* yang berfungsi sebagai *routing, firewall, bandwidth management* dan lain sebagainya. Dimana fungsi-fungsi utama *router* ini tidak membutuhkan *storage* yang besar.

C. Skema Jaringan



Sumber : Hasil Penelitian (2017)

Gbr. 2 Skema Jaringan Usulan

Berdasarkan hasil analisa yang dilakukan di PT. Micronics Internusa tidak merubah seluruh skema jaringan yang telah ada, hanya penambahan *routerboard 450G* dengan menggunakan *failover* berbasis VPN diperkirakan dapat menjadi solusi dalam melakukan pemindahan jaringan *internet speedy* ke jaringan *internet biznet* secara otomatis, tanpa petugas IT datang ke kantor cabang untuk melakukan pemindahan kabel *internet speedy* atau *biznet* yang menjadi masalah pada kantor cabang PT. Micronics Internusa. Pada skema jaringan usulan diatas jaringan WAN di kantor pusat dan kantor cabang PT. Micronics Internusa penulis memberikan usulan agar semua perangkat keras seperti: komputer, laptop, *access point, server, printer* berada dalam satu *switch* yang terhubung dengan *routerboard 450G*, artinya penambahan satu infrastruktur berupa *routerboard 450G* agar mempermudah dalam upaya perawatan *(maintenance)*. Dengan adanya penggunaan *Failover* dan VPN ini dapat dihubungkan melalui jaringan publik *(internet)* dengan dibuatkan jalur pribadi atau terowongan *(tunnel)* baik secara *site to site* maupun *remote site* dengan menerapkan *failover* dan *virtual private network* (VPN) menggunakan protokol PPTP *(Point to Point Tunneling Protocol)*, sehingga jaringan LAN antara kantor pusat dan cabang bisa saling terhubung dan jaringan internet secara otomatis akan berpindah jika jaringan internet terputus. selain itu juga bisa dilakukan melalui *remote access* dalam pengalihan jaringan *internet* baik di kantor pusat maupun di kantor cabang, jaringan perusahaan akan lebih efisien karena mampu menghindari adanya *collusion* atau tabrakan data dan pemindahan jaringan *internet* secara otomatis. Sedangkan pada kantor pusat, penulis tidak membahas jaringan *internet* karena dapat mengatasinya dengan kebutuhan jaringan yang ada.

D. Keamanan Jaringan

Untuk keamanan jaringan komputer yang diterapkan pada PT. Micronics Internusa adalah:

1) Pada sisi *router* keamanan yang diterapkan diantaranya:
   a. Membatasi Hak akses terhadap *router* dengan membatasi *ip address* yang bisa mengakses *router*, kemudian menutup atau menonaktifkan *port-port* yang tidak digunakan seperti halnya *port* 22 untuk *ssh*.
   b. Membuat *dhcp server* secara statik, hal ini bertujuan untuk memaksa *client* menggunakan ip yang diberikan oleh *dhcp server* sehingga *client* yang tidak terdaftar baik dari *ip address* maupun *mac address*nya tidak bisa masuk ke dalam jaringan tersebut.
   c. Mengaktifkan *transparent proxy* , yakni dengan memaksa setiap *client* yang akan terhubung ke jaringan luar (*internet*) harus melalui *proxy server*, hal ini bertujuan untuk meminimalisir serangan dari jaringan luar (*internet*) karena setiap *clien*t yang terhubung dengan jaringan luar *(internet*) sebenarnya tidak saling berhubungan secara langsung, melainkan melalui *proxy server*.

2) Pada sisi komputer *server* keamanan yang diterapkan diantaranya dengan membatasi hak akses ke *server* kepada tiap *client* sesuai dengan kewenangan masing-masing, kemudian untuk mengatasi serangan *virus* pada *server* yang sudah di *install* program anti *virus symantec* untuk *virus* internasional.
3) Pada sisi komputer *client* hampir sama dengan komputer *server* yakni dengan melakukan pembatasan hak akses ke komputer *client*, hanya *client* yang berhak dan terdaftar di *server* untuk menggunakan komputer tersebut, untuk mengatasi serangan *virus* pada tiap komputer *client* juga di *install* program anti *virus*, selain itu *service auto run* yang ada pada tiap komputer *client* dinonaktifkan, hal ini bertujuan jika ada *user* yang menggunakan *flash disk* dan di dalam *flash disk* tersebut terinfeksi *virus* dapat diminimalisir, karena biasanya *virus* di dalam *flash disk* bersifat *auto run*.

E. Manajemen Jaringan

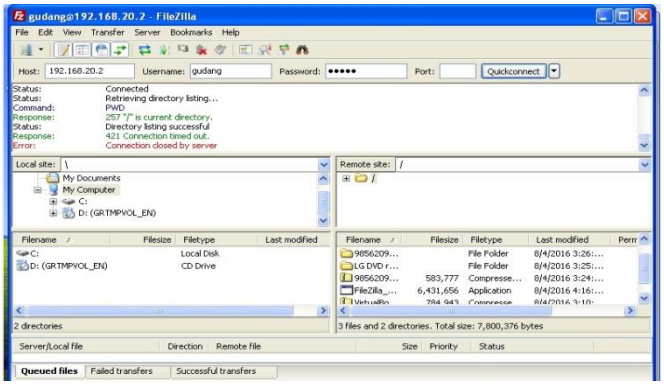
Sebuah fungsi pengawasan terhadap kinerja jaringan dan mengambil tindakan untuk mengendalikan aliran trafik agar kapasitas pengoperasian pada seluruh jaringan dapat dilakukan secara maksimal. Protokol yang sering digunakan dalam mengkontrol jarak jauh adalah *Virtual Private Network* (VPN). Manajemen atau pengelolaan, pada tahap ini meliputi aktifitas perawatan dan pemeliharaan dari keseluruhan sistem yang sudah dibangun. Tahap manajemen ini akan dilakukan setelah sistem ini berjalan dengan baik pada jaringan PT. Micronics Internusa.

Pada tahap ini penulis akan melakukan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yang diharapkan. Langkah-langkah yang dilakukan diantaranya:

1. Melakukan pengecekan rutin setiap satu bulan sekali ke semua alat yang berada di ruang server, mulai dari pengecekan suhu ruangan, listrik dan fisik dari alat tersebut.
2. Melakukan pembersihan setiap satu minggu sekali ke semua alat yang berada di ruang server.
3. Membuat laporan tertulis pada setiap pengecekan atau pembersihan yang di lakukan diruang server.
4. Membuat back up konfigurasi pada router, sehingga jika terjadi kerusakan pada router yang terpasang dapat langsung di ganti dengan router yang sudah di konfigurasi.
5. Melakukan *release IP address* di wifi setiap satu hari sekali, berfungsi agar tidak terjadinya konflik *IP address* pada *device* yang baru terkoneksi ke jaringan lokal.

F. Pengujian Jaringan Awal

Pengujian jaringan awal dengan membuka *Filezilla Client*. Pada kolom *hostname* isikan menggunakan *IP Address* PC Cabang (192.168.20.2), pada kolom *username* gudang dan *password* admin, menggunakan Port 21 kemudian klik *Connect.*



Sumber : Hasil Penelitian (2017)

Gbr. 3 Pengujian jaringan awal menggunakan *Filezilla Client*

G. Pengujian Jaringan Akhir

Beberapa cara untuk melakukan pengujian akhir jaringan sebagai berikut:

a. Mencoba melalui *browser* dengan cara ketik : *ftp://IP Address PC Cabang*, kemudian masukkan *user* dan *password*.

Sumber : Hasil Penelitian (2017)

Gbr. 4 Pengujian jaringan akhir menggunakan *IP Address PC* Cabang

b. Hasil pengujian jaringan akhir setelah isi pada kolom *username* dan *password.*

Sumber : Hasil Penelitian (2017)

Gbr. 5 Hasil pengujian jaringan akhir menggunakan jalur VPN

V. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan, hasil penelitian dapat disimpulkan sebagai berikut:

1. *Virtual Private Network* dapat mengefesiensikan waktu dalam pengiriman data yang diakses melalui jaringan lokal tanpa harus menunggu waktu yang cukup lama.
2. Model jaringan WAN dengan koneksi VPN menggunakan teknologi *tunneling* PPTP *(Point to Point Tunnelling Protocol).*
3. Dengan menggunakan konfigurasi *failover,* yang dikontrol oleh mikrotik, pertukaran data dari kantor pusat ke kantor cabang lebih cepat dan jika terdapat gangguan salah satu koneksi jaringan *internet* terputus dapat dibackup oleh koneksi yang lain.
4. Dengan menggunakan *Virtual Private Network,* seorang admin dapat melakukan kontrol data terhadap komputer *client* yang tersebar dibeberapa tempat.

Saran-saran yang dapat disampaikan dalam penelitian ini adalah:

1. Menggunakan jaringan VPN-PPTP dapat memberikan sebuah alternatif yang memiliki stabilitas kecepatan yang lebih baik dan layak digunakan untuk kepentingan *home small corporate* yang tidak membutuhkan enkripsi yang terlalu rumit.
2. Dalam penggunaan VPN dan *failover* agar dapat mendukung keakuratan dan kestabilan lebih baik dilakukan *upgrade bandwitch* menjadi 20 Mbps.
3. Menambahkan perangkat keras yaitu *Routerboard 450G.*

REFERENSI

[1] A. I. Harsapranata, "IMPLEMENTASI FAIL OVER Menggunakan Jaringan Vpn Dan Metronet Pada Astridogroup Indonesia," *Jurnal Teknik dan Ilmu Komputer*, Vols. Vol. 04 No. 13, Jan – Mar 2015, pp. 69-77, Desember 2014.

[2] I. Warman and A. Andrian, "Analisis Kinerja Load Balancing Dua Line Koneksi," *Jurnal TEKNOIF*, vol. Vol. 5 No. 1 April 2017, no. ISSN: 2338-2724, pp. 56-62, 2017.

[3] A. Widodo, "Implementasi Monitoring Jaringan Komputer," *Jurnal Teknologi Informasi*, Vols. Volume 11, Nomor 1, no. ISSN: 1979-1496, pp. 1-10, 2015.

[4] Y. Hendriana, "Evaluasi Implementasi Keamanan Jaringan Virtual Private," *Jurnal Teknologi*, vol. Volume 5 Nomor 2, pp. 132-142, 2012.

Siti Nur Khasanah, lahir di Tegal pada tanggal 25 November 1990. Menyelesaikan pendidikan S2 pada tahun 2016. Saat ini menjadi seorang dosen di STMIK Nusa Mandiri Jakarta. Tulisan jurnal yang pernah dipublikasikan adalah "Perancangan dan Implementasi Wide Area Network (WAN) dengan IP VPN" pada Jurnal Techno Tahun 2015, Keamanan Jaringan dengan *Packet Filtering* (Studi kasus: PT. Sukses Mandiri Jakarta) di tahun 2016 pada Jurnal Khatulistiwa dan pada Tahun 2017 menulis jurnal yang berjudul "Penerapan Algoritma C4.5 untuk Penentuan Kelayakan Kredit".

Lilyani Asri Utami, lahir di Bogor pada tanggal 15 November 1991, lulusan pendidikan Program S2 jurusan Ilmu Komputer – Pasca Sarjana STMIK Nusa Mandiri Jakarta tahun 2016. Bekerja sebagai instruktur di STMIK Nusa Mandiri Jakarta sejak tahun 2014. Sampai saat ini telah mengikuti beberapa kegiatan seminar nasional untuk menambah pengetahuan tentang menulis untuk menuangkan pemikiran dalam rangka melaksanakan Tri Dharma Perguruan Tinggi. Sebuah *prociding* berjudul "Sistem Informasi Administrasi Pasien Pada Klinik Keluarga Depok" pernah dimuat pada Konferensi Nasional Ilmu Pengetahuan dan Teknologi (KNIT) Nusa Mandiri pada tahun 2015.