

**PROSIDING KOMMIT 2012
(KOMPUTER DAN SISTEM INTELIJEN)
Volume 7 – 2012**

**TEKNOLOGI INFORMASI DAN KOMUNIKASI
(TIK) UNTUK KETAHANAN NASIONAL**

ISSN: 2302-3740

PENERBIT

Lembaga Penelitian Universitas Gunadarma

Alamat Editor:

Lembaga Penelitian Universitas Gunadarma
Jl. Margonda Raya 100 Pondok Cina
Depok, 16424
Telp. +62-21-78881112 ext. 455
Fax. +62-21-7872829
e-Mail: kommit@gunadarma.ac.id
Laman: <http://penelitian.gunadarma.ac.id/kommit>

Prosiding KOMMIT, Volume 7 - 2012

Editor:

Tety Elida, Moh. Okki Hardian, Wahyu Rahardjo, Fitriainingsih, Tri Wahyu Retno Ningsih

Disain sampul: Wira Catur

Penerbit: Lembaga Penelitian Universitas Gunadarma

Hak cipta © 2012 oleh Universitas Gunadarma. Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi prosiding ini dalam bentuk apapun, baik secara eletronis maupun mekanis, termasuk memfotocopy, merekam atau dengan sistem penyimpanan lainnya tanpa izin tertulis dari penerbit.

ISSN: 2302-3740

DEWAN REDAKSI

Penanggung Jawab:

Dr. Ir. Hotniar Siringoringo, MSc.

Ketua Dewan Editor:

Dr. Ir. Tety Elida Siregar, MM.

Editor Pelaksana:

Moh. Okki Hardian, ST., MT.

Wahyu Rahardjo, SPsi., MSi.

Fitrianingsih, SKom., MMSi.

Tri Wahyu Retno Ningsih, SSas., MM.

Reviewer:

Prof. Dr. I Wayan Simri Wicaksana, S.Si, M.Eng.

Prof. Dr.rer.nat. Achmad Benny Mutiara, SSI, SKom.

Prof. Dr. Busono Soerowirdjo

Prof. Dr. Sarifuddin Madenda

Prof. Dr. dr. Johan Harlan

Prof. Dr. Ir. Eriyatno MSAE.

Dr. Tb. Maulana Kusuma, SKom., MEngSc.

Dr.-Ing. Adang Suhendra, SSI,SKom,MSc.

Prof. Dr. Ir. Kudang Boro Seminar, MSc.

Drs. Agus Harjoko MSc., PhD.

Dr. Ir. Joko Lianto Buliali

PENERBIT

Lembaga Penelitian Universitas Gunadarma

Jl. Margonda Raya 100 Pondok Cina

Depok, 16424

Telp. +62-21-78881112 ext. 455

Fax. +62-21-7872829

e-Mail: kommit@gunadarma.ac.id

Laman: <http://penelitian.gunadarma.ac.id/kommit>

PANITIA PELAKSANA SEMINAR

Penasehat:

Prof. Dr. E.S. Margianti, S.E., MM.
Prof. Suryadi Harmanto, SSi., M.MS.I.
Agus Sumin, S.Si., MM.

Penanggung Jawab:

Prof. Dr. Yuhara Sukra, MSc.
Prof. Dr. Didin Mukodim, MM.

Ketua Pelaksana:

Dr. Ir. Hotniar Siringoringo, MSc.

Wakil Ketua Pelaksana:

Dr. Bertalya

Sekretariat:

Ida Ayu Ari Angreni, ST., MMT.
Dr. Jacobus Belida Blikololong
MS. Harlina, S.Kom., MM.

Sarana Prasarana:

Drs. Hardjanto Sutedjo, MM.
Rino Rinaldo, SE., MM
Riyanto, ST.

KATA PENGANTAR

Pertukaran informasi merupakan kebutuhan masyarakat modern, sehingga Teknologi Informasi dan Komunikasi (TIK) menjadi hal yang sangat penting. Secara kasat mata, setiap orang dapat menyaksikan perkembangan TIK yang sangat pesat. Perkembangan TIK sampai saat ini masih didominasi oleh negara-negara maju. Kondisi ini harus direposisi.

Indonesia memiliki sumber daya manusia yang handal dan banyak, di antaranya berada di perguruan tinggi. Sumber daya manusia ini terkesan bekerja masih sendiri-sendiri. Penelitian di lingkungan perguruan tinggi maupun litbang sering disalahartikan sebagai pemuas akademis, sementara di kalangan industri lebih tertarik pada penyelesaian ekonomis jangka pendek. Permasalahan ini dapat diatasi dengan memulai kolaborasi antara dunia pendidikan, litbang, industri dan pemerintah.

KOMMIT merupakan seminar nasional di bidang komputer dan teknik yang mendukung pengembangan teknologi komputer maupun aplikasi komputer dalam berbagai bidang. Seminar ini bertujuan menyediakan wadah bagi peneliti, akademisi dan praktisi untuk saling bertukar informasi, berdiskusi dan berkolaborasi sehingga dapat menghasilkan produk siap pakai di dalam bidang sistem informasi.

Topik yang menjadi pembahasan pada KOMMIT ke 7 ini adalah: sistem informasi manajemen, sistem informasi geografis, sistem informasi medis, *enterprise resource planning*, *information retrieval*, matematika aplikasi, sistem keamanan, aplikasi multimedia, pengolahan sinyal dan citra, *computer vision*, *open source & open content*, *e-government*, *e-business*, *e-education*, data semantik, *information system interoperability*, *distributed*, *parallel*, *grid*, *P2Pp*, *mobile information management*, *mobile technology*, *green computing*, telekomunikasi dan jaringan komputer, sistem kontrol, instrumentasi dan diagnosis, mekanika dan elektronika, energi terbarukan, *cognitive science*, *soft computing*, *perceptual science*, bioinformatika dan geoinformatika, *collaborative network*, dan *electron devices*.

Artikel yang disajikan pada seminar ini setelah melalui proses *peer review*, berjumlah seratus satu, yang berasal dari 15 Perguruan Tinggi di Indonesia. Beberapa artikel yang terpilih akan di publikasikan pada Jurnal Ilmiah yang diterbitkan oleh Universitas Gunadarma.

Semoga seminar ini dapat memberikan masukan bagi pengembangan teknologi informasi dan komunikasi di negara kita. Kami ucapkan terima kasih kepada para reviewer yang telah bersedia melakukan review, juga kepada pembicara tamu dan nara sumber yang telah berkontribusi pada acara ini, serta kepada semua pihak yang telah membantu proses produksi prosiding ini.

Ketua Pelaksana
Dr. Ir. Hotniar Siringoringo, MSc.

DAFTAR ISI

DEWAN REDAKSI.....	iii
PANITIA PELAKSANA SEMINAR	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vii
DAFTAR ARTIKEL:	
1. <i>Sistem Informasi Manajemen Penanggulangan Kemiskinan (Studi Kasus Kabupaten Ogan Komering Ilir Provinsi Sumatera Selatan)</i> Ahmad Haidar Mirza.....	1
2. <i>Optimasi Pencarian dengan Knowledge Graph</i> Abidin Ali, Dina Rifdalita, Juliana Putri Lestari, Lintang Yuniar Banowosari	11
3. <i>Analisis Teknik Reduksi Data dan Minimalisasi Ukuran File APK pada Mobile Application Pengenalan Budaya Indonesia Berbasis Android Serta Pengembangannya</i> Adhika Novandya, Debyo Saptono	18
4. <i>Aplikasi Manajemen File Berbasis Web untuk Monitoring Status Kegiatan</i> Akhmad Fauzi, Tri Sulistyorini.....	27
5. <i>Penerapan Metode Dijkstra dalam Pencarian Jalur Terpendek pada Perusahaan Distribusi Film</i> Albert Kurnia, Friska Angelina, Windy Dwiparaswati	36
6. <i>Penyembunyian Informasi (Steganography) Audio Menggunakan Metode LSB (Least Significant Bit) Menggunakan Matlab</i> Ari Santoso, Irfan, Nazori AZ.....	42
7. <i>Standardisasi Sistem Informasi Kesehatan Berjenjang Open E-Health Gunadarma Information System, Mewujudkan Layanan Kesehatan Prima</i> Aries Muslim, AB Mutiara, Teddy Oswari, Riyandari Auror, Irdiah Amsawati	51
8. <i>Pengembangan Web sebagai Upaya Penunjang Optimalisasi Produk Asuransi</i> Armaini Akhirson.....	59
9. <i>Protokol Autentikasi Berbasis One Time Password untuk Banyak Entitas</i> Avinanta Tarigan, D.L. Crispina Pardede	67
10. <i>Peningkatan Keamanan Kartu Kredit Menggunakan Sistem Verifikasi Sidik Jari di Indonesia</i> Bima Shakti Ramadhan Utomo, Denny Satria, Lulu Mawaddah Wisudawati.....	72
11. <i>Rancangan Aplikasi Pencarian Barang Pada Metro Pacific Place dengan Menggunakan Macromedia Dreamweaver 8</i> Triyanto, Bramantyo Sukarno, Miftah Andriansyah.....	78

12. <i>Sistem Pengambilan Keputusan Bela Negara Non-Fisik untuk Daerah Depok dengan Metode AHP (Analytic Hierarchy Process)</i> Damai Subimawanto, Surya Thiono Wijaya, Yusuf Triyuswoyo, I Wayan Simri Wicaksana, Detty Purnamasari.....	85
13. <i>Penerapan Teknologi Informasi dan Komunikasi (TIK) pada UMKM dengan Menggunakan Technology Acceptance Model (TAM) (Studi Kasus di Depok dan Qingdao)</i> Deboner Hillery, Dharma Tintri, Pandam R Wulandari.....	94
14. <i>Faktor Kunci Sukses dalam Pelaksanaan Sistem Enterprise Resource Planning</i> Delvita Dita Putri Anggrayni, Dewi Agushinta R.	101
15. <i>Model Penentuan Posisi Siaga Lift sebagai Pemanfaatan Penghematan Energi pada Sistem Kerja Lift</i> Denmas Muhammad Ridwan, Donny Ejje Baskoro, Faisal Yafi, Lily Wulandari.....	110
16. <i>Pemanfaatan Jaringan Akses Telepon sebagai Jaringan Broadband Layanan Internet dengan Teknologi Asymmetric Subscriber Line</i> Djasiodi Djasri.....	116
17. <i>Evaluasi Website JobsDBTM Mobile dengan Metode Usability Heuristic</i> Esty Purnamasari, Helen Wijayanti, Yosfik Alqadri, Dewi Agushinta Rahayu, Fani Yayuk Supomo	123
18. <i>Perancangan dan Implementasi Sistem Informasi Peralatan dengan Penerapan Konsep Three Tier (Studi Kasus: Gardu Induk Prabumulih UPT Palembang)</i> Evi Yulianingsih, Marlindawati	131
19. <i>Faktor-Faktor yang Mempengaruhi Minat Nasabah Menggunakan Internet Banking dengan Menggunakan Anjungan Tunai Mandiri (Studi Kasus pada Bank BCA, BRI dan Bank Syariah Mandiri)</i> Faramita Dwitama, Mohammad Abdul Mukhyi	139
20. <i>Enkripsi Informasi untuk Pengamanan Pesan Singkat pada Telepon Seluler Berbasis Java MIDP</i> Farid Thalib, Melba Mauludina Novalestari	148
21. <i>Desain Database e-Supermuseum Batik Indonesia</i> Fikri Budiman, Slamet Sudaryanto Nurhendratno	157
22. <i>Analisis Perbandingan Kinerja Search Engine Menggunakan Penelusuran Precision dan Recall untuk Informasi Ilmiah Bidang Ilmu Kedokteran</i> Sukei, Fitriainingsih.....	164
23. <i>Membandingkan Web Pengunduhan Perangkat Lunak</i> Fuji Ihsani, Istiana Idha Aulia, Melisa Chatrine Kamu, Anacostia Kowanda, Trini Saptariani.....	172
24. <i>Analisis dan Verifikasi Formal Protokol Non-Repudiasi Zhang-Shi dengan Logika SVO-CP</i> Hanum Putri Permatasari, Avinanta Tarigan, D. Lucia Crispina Pardede	178
25. <i>Implementasi Kebijakan E-Government pada Pemerintah Kota Palembang</i> Hardiyansyah.....	185

26.	<i>Aplikasi Pengingat Jadwal Imunisasi Berbasis Android</i> Hauliza Rindhayanti, Lintang Yuniar Banowosari	193
27.	<i>Model Berbasis Ekstraksi untuk Analisis Gaya Berjalan</i> Hustinawaty, Miftahul Jannah, Rd. Fazlur Rahman.....	201
28.	<i>Metoda Penumbuhan Kreativitas Berbasis Web: Studi Pengembangan Produk Kerajinan Tenun Ikat dalam Upaya Melestarikan dan Meningkatkan Nilai Tambah</i> Iman Murtono Soenhadji, Priyo Purwanto, Ida Astuti, Faisal Reza.....	209
29.	<i>Simulasi dan Optimasi Antrian Pelayanan Agen JNE Buaran</i> Isram Rasal, Hardimen Wahyudi, Nadia Rahmah Al Mukarromah, Yuhilza Nahum	218
30.	<i>Aplikasi Data Mining dengan Teknik Decision Tree untuk Mengklasifikasikan Data Pasien Rawat Inap</i> Julius Santony, Sumijan	226
31.	<i>Integrasi Sumber Data Heterogen Menggunakan Ontologi, Studi Kasus: Data Kependudukan Indonesia</i> Kemal Ade Sekarwati, I Wayan Simri Wicaksana.....	235
32.	<i>Pengenal Ucapan untuk Belajar Bahasa Menggunakan Perangkat Mobile</i> Kezia Velda Roberta, Raden Supriyanto.....	241
33.	<i>Sistem Pakar Pendeteksi Prediksi Kemungkinan Penyakit Stroke</i> Linda Atika.....	247
34.	<i>Analisis Sektor Unggulan dalam Perekonomian DKI Jakarta</i> Lita Praditha, Mohammad Abdul Mukhyi	254
35.	<i>Kapabilitas Proses Konstruksi Perangkat Lunak pada Perusahaan Pengembang Perangkat Lunak di Bali Menggunakan Kerangka Kerja ISO/IEC 15504</i> Luh Gede Surya Kartika, Kridanto Surendro	262
36.	<i>Sistem New Media pada Aplikasi Internet Radio Berbasis Android</i> Lulu Mawaddah Wisudawati, Avinanta Tarigan.....	269
37.	<i>Kajian Awal Hibridisasi Toyota Soluna dengan Konfigurasi Parallel HEV</i> Mohamad Yamin, Agung Dwi Sapto	276
38.	<i>Pemodelan dan Analisis Rem Cakram dan Rem Tromol dengan Software CATIA V5</i> Mohamad Yamin, Darmawan Sebayang.....	283
39.	<i>Deteksi Sonority Peak untuk Penderita Speech Delay Menggunakan Speech Filing System</i> Muhammad Subali, Tri Wahyu Retno Ningsih, M. Kholiq	289
40.	<i>Penerapan Periklanan di Internet dan Pemasaran Melalui E-Mail untuk Meningkatkan Pemasaran Produk UMKM di Wilayah Depok</i> Mujiyana, Lana Sularto, M. Abdul Mukhyi.....	296
41.	<i>Monitoring Sistem Pengendalian Suhu dan Saluran Irigasi Hydroponik pada Greenhouse Berbasis Web</i> Nia Maharani Raharja, Iswanto.....	303

42.	<i>Disain Rangkaian Detektor Mini Doppler</i> Nur Sultan Salahuddin, Paulus Jambormias, Erma Triawati.....	311
43.	<i>Prototipe Sistem Pemrosesan Limbah Medis</i> Nur Sultan Salahuddin, Adi Hermansyah, RR Sri Poenomo Sari	317
44.	<i>Audit TIK pada Sistem Penerbitan Surat Perjalanan Republik Indonesia (SPRI) di Kantor Imigrasi Bogor</i> Nurul Adhayanti, Karmilasari	323
45.	<i>Aplikasi Pencarian Lokasi Sekolah Menggunakan Telepon Selular Berbasis Android</i> Nuryuliani, Selvi Isni Hadisaputri, Miftah Andriansyah.....	331
46.	<i>Faktor Penentu Efektifitas IT Governance: Studi Kasus pada Perusahaan di DKI Jakarta</i> Pandam Rukmi Wulandari, Samuel David Lee, Renny Nur'ainy.....	340
47.	<i>Aplikasi Mobile Panduan Diet Berdasarkan Golongan Darah Berbasis Android</i> Parno, Swesti Mahardini.....	345
48.	<i>Studi Terhadap Konstruksi Model Pengklasifikasi Regresi Logistik</i> Retno Maharesi.....	352
49.	<i>Karakteristik dan Model Matematika Aliran Lumpur pada Pipa Spiral</i> Ridwan.....	360
50.	<i>Implementasi Mikrokontroler untuk Deteksi Drop Tegangan pada Instalasi Sederhana</i> Rif'an Tsaqif As Sadad, Iswanto.....	368
51.	<i>Analisis Pendeteksian Nodul Citra Sinar-X Paru</i> Rodiah, Sarifuddin Madenda, Dewi Agushinta Rahayu.....	377
52.	<i>Composite Range List Partitioning pada Very Large Database</i> Rosni Gonydjaja, Yuli Karyanti	384
53.	<i>Analisis Perbandingan Waktu untuk Layanan Email dan SMS pada Jaringan Interkoneksi untuk Kajian Efektivitas Dukungan Media Komunikasi Dosen-Mahasiswa</i> S N M P Simamora, Karina Datty Putri, Robbi Hendriyanto.....	389
54.	<i>Desain Prototipe Aplikasi Sistem Keamanan pada Rumah Berbasis Pengenalan Wajah dengan Algoritma Jaringan Saraf Tiruan dan Fitur Fft</i> Shinta Puspasari, Hendra.....	398
55.	<i>Analisis Implementasi Algoritma Propagasi Balik pada Aplikasi Identifikasi Wajah Secara Waktu Nyata</i> Shinta Puspasari, Alfian Sucipta.....	405
56.	<i>Sistem Pemantau Ruangan dengan Penangkapan Gambar Otomatis Menggunakan Sensor Infra Merah Pasif</i> Singgih Jatmiko, R. Supriyanto, R.N. Nasution	412

57.	<i>Sistem Pengenalan Ekspresi Wajah Berdasarkan Citra Wajah Menggunakan Metode Eigenface dan Nearest Feature Line</i> Sulistyo Puspitodjati, Tyas Arie Wirana	418
58.	<i>Ekstraksi Data pada Halaman Web Database Mining Akademik Menggunakan Simple Tree Matching (STM)</i> Sumijan, Julius Santony	426
59.	<i>Perancangan dan Implementasi Software Penyelesaian Persamaan Non Linier dengan Metode Fixed Point Iteration</i> Vivi Sahfitri.....	447
60.	<i>Perhitungan Panjang Janin pada Citra Ultrasonografi untuk Memprediksi Usia Kehamilan</i> Wahyu Supriyatin, Bertalya	456
61.	<i>Model Translator Notasi Algoritmik ke Bahasa C</i> Wijanarto, Achmad Wahid Kurniawan	464
62.	<i>Simulasi Dinamika Molekular Sistem Molekul Argon dan Graphene dengan Menggunakan Perangkat Lunak DL_Poly</i> Ahmad Rifqi Muchtar, Wisnu Hendradjit, Agus Samsi.....	473
63.	<i>Pengidentifikasian Otomatis Bentuk Kista Ovarium Menggunakan Deteksi Circle dan Deteksi Tepi Laplacian dan Prewitt.</i> Yenniwarti Rafsyam, Jonifan	482
64.	<i>Pengaruh Karakteristik, Sikap dan Pelatihan terhadap Penggunaan Teknologi Informasi dan Kinerja Pegawai untuk Penerapan Pemerintah Elektronik di Pedesaan</i> Yuventus Tyas Catur Pramudi, Karis Widyatmoko	489
65.	<i>Perancangan Sistem Informasi Alur Kerja (Work Flow) Dokumen Pengajuan Proposal Skripsi</i> Zulfandi, Sarip Hidayatullah, Wahyudianto	500
66.	<i>Aplikasi Pengenalan Budaya dari 33 Provinsi di Indonesia Berbasis Android</i> Adhika Novandya, Ajeng Kartika, Ari Wibowo, Yudhi Libriadiany	508
67.	<i>Sistem Informasi Geografis Bengkel Resmi Mercedes-Benz dan BMW di Kota Jakarta Menggunakan Quantum GIS</i> Agustini Dwi Setia Rahayu, Ana Rizki, Ria Awalliya.....	514
68.	<i>Studi Kasus Konflik PT.XXX dengan Pelanggan Kereta Kelas Ekonomi Berdasar Ilmu Teori Organsisasi Umum</i> Albert Kurnia Himawan, Juliana Putri Lestari, Aris Budi Setiawan.....	517
69.	<i>Aplikasi Pengenalan Dasar-Dasar Bahasa Inggris untuk Anak Usia Dini Menggunakan Adobe Flash CS 3 Professional</i> Alfa Marlin, Siti Andini, Sri Wahyuni	519
70.	<i>Eksplorasi Celah Keamanan Piranti Lunak Web Server Vertrigoserv pada Sistem Operasi Windows Melalui Jaringan Lokal</i> Andrias Suryo Widodo, Maria Magdalena Merry, Stefanus Dwi Putra Medisa	524

71.	<i>Sistem Pengambilan Keputusan Kelayakan Sekolah Mendapatkan Status RSBI Studi Kasus SMA RSBI Di DKI Jakarta</i> Ardhani Reswai Yudistari, Odheta, Tryono Taqwa	529
72.	<i>Penerapan Algoritma Kruskal dan Pengimplementasiannya dalam Kasus Pendistribusian Majalah "UG News" Antar Universitas Gunadarma</i> Ardisa Pramudhita, Mahisa Aji Kusuma, Nur Fisabilillah	535
73.	<i>Implementasi Algoritma Dijkstra untuk Menentukan Rute Terpendek Antar Museum di Yogyakarta Berbasis Web</i> Ardo Rama, Citra Ika Wibawati, Rizka Fajriah	538
74.	<i>Pembuatan Aplikasi Permainan Labirin 2D untuk Handphone</i> Aries Afriliansyah	542
75.	<i>Konfigurasi Trixbox Server Untuk VoIP pada Jaringan Peer to Peer</i> Arif Liberto Jacob, Muhammad Muhijar, Ferry Wisnuargo	547
76.	<i>Sistem Penunjang Keputusan Memilih Kriteria Lagu Pop Indonesia yang Baik</i> Ario Halik, Virgiawan Ananda Pratama.....	550
77.	<i>Evaluasi Algoritma Prim dan Kruskal Terhadap Pemasangan Kabel Telepon di DKI Jakarta</i> Atikah Luthfiyyah, Voni, Wahyu Pratama	553
78.	<i>Aplikasi Pemetaan Pusat Perbelanjaan Kota Bekasi Menggunakan Android</i> Awal Arifianto, Muhammad Yunus, Andrika Siman, Agung Rahmat Dwiardi, Deny Nugroho	556
79.	<i>Penerapan Algoritma Greedy pada Studi Kasus Pencarian Rumah Sakit Terdekat di Jakarta Selatan</i> Bagus Fitroh Alamsyah, Maulana Malik Ibrahim, Prakasita Wigati.....	559
80.	<i>Implementasi Algoritma Dijkstra Guna Optimasi Jalur Pendistribusian Produk Seluler</i> Banu Adi Witono, Dhita Angreny, Randy Aprianggi	561
81.	<i>Face Recognition Menggunakan Metode Linear Discriminant Analysis (LDA)</i> Bayu Adi Yudha Prasetya.....	563
82.	<i>Pembuatan Game Arasen untuk Latihan Soal Tes Potensi Akademik Menggunakan RPG Studio</i> Daisy Patria, Hayu Wasna Sari, Riyandari Asrita	570
83.	<i>Pemodelan Spasial Tingkat Kerawanan Kecelakaan Lalu Lintas di Kota Depok</i> Eriza Siti Mulyani, Muhammad Arsah Novel Simatupang	576
84.	<i>Sistem Log Monitoring Jaringan (LAN) Menggunakan Bahasa Pemrograman Pascal</i> Fendy Christian, Stefanus Goutama, Afrilia Nita Anjani.....	582
85.	<i>Website Surat Pembaca Sebagai Media Komunikasi dalam Penyampaian Aspirasi Masyarakat</i> Hamisati Muftia, Nabiurrahmah.....	584

86.	<i>Aplikasi Pendidikan Bagi Anak di Bawah Umur 7 Tahun</i> Helmi, Muhammad Subentra, Randy Aditiya Yusuf	586
87.	<i>Sistem Pencarian Fasilitas Umum Terdekat Menggunakan Augmented Reality dengan Minimum Spanning Tree</i> Hifshan Riesvicky, Prita Dessica, Tatang Fanji Permana	592
88.	<i>Aplikasi Multimedia Audio Video Player dengan Menggunakan Visual Basic .Net 2008</i> Inggrit Parnandes, Rias Astria, Meilisa Ndaru Hermiyanti.....	595
89.	<i>Aplikasi Energy Usage Calculator untuk Menghitung Penggunaan dan Biaya Energi Listrik Berbasis Python Versi 3.2.3</i> M Haidar Hanif, Herio Susanto.....	599
90.	<i>Implementasi Algoritma Kruskal untuk Optimasi Pengangkutan Sampah</i> Meilidyningtyas Cantika Ryadiani, Nurul Ardianingsih, Robby Matheus.....	602
91.	<i>Pemilihan Aplikasi Permainan untuk Perkembangan Motorik dan Simbolik Anak Usia 1 - 7 Tahun</i> Michael Satrio Prakoso, Detty Purnamasari.....	605
92.	<i>Sistem Informasi Geografis SMA di Bogor</i> Muhamad Ramadani Silatama, Narendra Paskarona, Ary Wahyudi.....	608
93.	<i>Pembuatan Website World Watch Shop Menggunakan Magento Commerce</i> Rahma Eka Putri, Septiana Dewi Saputri, Sheila Rizka	614
94.	<i>Pembuatan Aplikasi Pemetaan Tempat Usaha di Sekitar Kampus Depok Gunadarma Menggunakan Android 2.1</i> Rangga Adhitya Pradiptha, Titik Rahayu Mariani, Winda Utari	616
95.	<i>Aplikasi Penjualan Makanan Khas Garut pada Toko Aneka Sari dengan Menggunakan Visual Basic .Net</i> Rangga Septian Putra, Rion Saputra, Ryan Oktario.....	619
96.	<i>Pengembangan E-Government pada Layanan Informasi Publik Pemerintahan Daerah Sulawesi Barat Menuju Good Governance</i> Rizka Fajriah, Windy Dwiparaswati, Aris Budi Setyawan	625
97.	<i>Perlunya Penerapan Teknologi Web Semantik pada Situs Pencarian Lowongan Pekerjaan di DKI Jakarta</i> Robby Matheus Gultom, Tatang Fanji Permana, Aris Budi Setyawan	628
98.	<i>Program Aplikasi Enkripsi dan Dekripsi SMS pada Ponsel Berbasis Android dengan Algoritma DES</i> Rudy Hendrayanto, A. Ramadona Nilawati	631
99.	<i>Penentuan Keputusan untuk Membantu Program Genre Bagi Pasangan Muda</i> Sandi Agung Harseno, Moh. Ropiyudin, Dessy Wulandari.....	634
100.	<i>Pembuatan Aplikasi Pembelajaran Bahasa Jerman Berbasis Mobile Android</i> Satrio Wibisono, Lisda.....	638
101.	<i>Aplikasi Foodcourt Menggunakan Microsoft Visual Studio 2008</i> Tri Hardiyanti, Shelly Gustika Septiani	644

ANALISIS DAN VERIFIKASI FORMAL PROTOKOL NON-REPUDIASI ZHANG-SHI DENGAN LOGIKA SVO-CP

Hanum Putri Permatasari¹
Avinanta Tarigan²
D. Lucia Crispina Pardede³

¹Jurusan Sistem Informasi, ²Jurusan Teknik Informatika

³Jurusan Sistem Komputer
Universitas Gunadarma

Jl. Margonda Raya No. 100 Depok – 16424

^{1,2,3}{hanum, avinanta, pardede}@staff.gunadarma.ac.id

Abstrak

Protokol non-repudiasi adalah protokol keamanan yang memberikan layanan Non-Repudiation of Origin (NRO) dan Non-Repudiation of Receipt (NRR). Protokol non repudiasi yang memenuhi kedua layanan tersebut tanpa memberi keuntungan lebih kepada satu prinsipal daripada prinsipal lain merupakan protokol yang memenuhi aspek fairness. Protokol [Zhang and Shi, 1996] adalah protokol yang seharusnya mengamankan transaksi elektronik dalam konteks non-repudiasi. Berdasarkan penelitian terdahulu mengenai verifikasi protokol non-repudiasi dengan metode formal logika [Coffey and Saidha, 1997] yang dilakukan oleh [Ventuneac, 2004] menunjukkan bahwa hasil verifikasi protokol tidak dapat digunakan untuk menguji ketercapaian tujuan akhir (goal) serta tidak menguji fairness. Tujuan utama dari penelitian ini adalah melakukan analisis dan verifikasi formal terhadap protokol non-repudiasi Zhang-Shi dengan menggunakan logika SVO-CP untuk mengetahui kehandalan protokol tersebut dalam memenuhi sifat non-repudiasi, yaitu NRO, NRR, dan fairness. Prosedur penelitian dilakukan dalam empat tahap dan hasil menunjukkan bahwa protokol non-repudiasi Zhang-Shi mencapai kebenaran semua tujuannya (NRO dan NRR) serta penerapan logika SVO-CP kepada verifikasi protokol non-repudiasi Zhang-Shi menunjukkan protokol tersebut mencapai fairness.

Kata Kunci: non-repudiasi, fairness, logika SVO-CP

PENDAHULUAN

Peningkatan pemanfaatan layanan berbasis internet seperti e-mail bersertifikasi dan pembayaran elektronik dari suatu barang menjadikan non-repudiasi dituntut dalam pengembangan protokol keamanan sebagai pertukaran pesan yang adil (*fair*). Non-repudiasi adalah salah satu layanan keamanan yang mengawasi peristiwa penyangkalan (*repudiation*) oleh satu dari sejumlah pihak (entitas) yang terlibat dalam sebuah komunikasi, bahwa ia telah berpartisipasi dalam se-

mua atau sebagian komunikasi. Untuk menegakkan akuntabilitas setiap partisipan atas aksi yang dilakukan, dibutuhkan layanan *Non-repudiation of Origin* (NRO) dan *Non-repudiation of Receipt* (NRR). Secara formal, *fairness* dinyatakan sebagai keadaan dimana NRO dan NRR dipenuhi atau NRO dan NRR keduanya sama sekali tidak dipenuhi. Non-repudiasi dianalisis melalui tujuan NRO dan NRR. *Fairness* dianalisis dengan melakukan pemeriksaan tercapainya tujuan NRO dan NRR.

Protokol non-repudiasi yang ditawarkan

kan oleh (Zhang and Shi, 1996) dan (Zhou and Gollmann, 1996) merupakan protokol non-repudiasi yang menggunakan *online* TTP. Protokol Zhang-Shi (ZS) memiliki kelebihan dibanding protokol Zhou and Gollmann (ZG), yaitu menyediakan kerahasiaan ganda (*double confidentiality*) yang ditandai dengan pesan cipher di bawah kunci sesi serta pemanfaatan fungsi hash pada setiap transmisi pesan ke setiap partisipan.

Keamanan sebuah sistem tidak dapat hanya diukur melalui desainnya saja. Verifikasi atas implementasinya harus dilakukan juga. Verifikasi terhadap layanan non-repudiasi dapat dilakukan dengan menggunakan metode formal. Salah satu upaya pertama untuk menerapkan metode formal dalam verifikasi protokol non-repudiasi Zhang-Shi (Zhang and Shi, 1996) dengan menggunakan logika CS (Coffey and Saidha, 1997), yaitu oleh (Ventuneac, 2004). Verifikasi menggunakan logika CS menguji ketercapaian tujuan dari setiap langkah protokol dan tidak menguji ketercapaian tujuan akhir dari protokol non-repudiasi serta tidak menguji *fairness* dari protokol non-repudiasi yang diverifikasi.

Logika SVO yang merupakan unifikasi dari logika BAN, GNY, vO, dan AT telah digunakan untuk verifikasi protokol non-repudiasi (Zhou and Gollmann, 1998), namun pengujiannya dilakukan untuk membuktikan keyakinan hakim (*adjudicator*) yang merupakan pihak yang tidak terlibat dalam komunikasi yang diatur oleh protokol non-repudiasi. Pembuktian sifat *fairness* tidak hanya memeriksa bukti di akhir perjalanan protokol, melainkan harus memperhatikan tahap-tahap pengumpulan bukti oleh setiap prinsipal. Keterbatasan SVO membuatnya tidak dapat digunakan untuk membuktikan *fairness*.

Pembuktian *fairness* terhadap protokol non-repudiasi ZG tercapai oleh (Pardede, 2012) dalam penelitian disertasinya dengan menggunakan logika SVO

yang diperluas, yang kemudian disebut dengan logika SVO-CP. Dengan demikian dalam penelitian ini, penulis melakukan verifikasi terhadap protokol non-repudiasi ZS dengan menggunakan logika SVO-CP untuk mengetahui kehandalan protokol tersebut dalam memenuhi sifat non-repudiasi, yaitu *Non-Repudiation of Origin* (NRO), *Non-Repudiation of Receipt* (NRR) dan *fairness*.

Logika SVO

Logika SVO (Syverson and van Oorschot, 1994) mencakup empat logika pendahulunya, yaitu GNY, BAN, AT, dan vO. Logika GNY, AT dan vO merupakan perluasan dari logika BAN, dengan demikian logika SVO juga mencakup logika BAN.

Logika SVO mempunyai dua aturan inferensi, yaitu modus ponens dan *Necessitation*. Modus Ponens: Dari ϕ dan $\phi \supset \psi$ memberikan ψ . *Necessitation*: Dari $\vdash \phi$ memberikan $\vdash P$ belief ϕ . Logika SVO mengandung dua puluh aksioma :

Believing untuk sembarang prinsipal P dan formula ϕ dan ψ

AX1. $(P \text{ believes } \phi \wedge P \text{ believes } (\phi \supset \psi)) \supset P \text{ believes } \psi$.

AX2. $P \text{ believes } \phi \supset P \text{ believes } (P \text{ believes } \phi)$.

Source Association

AX3. $P \stackrel{K}{\leftrightarrow} Q \wedge R \text{ received } \{X^Q\}_K \supset (Q \text{ said } X \wedge Q \text{ sees } K)$

AX4. $PK_{\sigma}(Q, K) \wedge R \text{ received } X \wedge SV(X, K, Y) \supset Q \text{ said } Y$, dimana $PK_{\sigma}(Q, K)$ berarti K merupakan kunci verifikasi *public signature* bagi prinsipal Q. $SV(X, K, Y)$ berarti bahwa jika diberikan pesan X yang ditandatangani, dengan menerapkan kepadanya kunci verifikasi tandatangan K maka terbukti bahwa Y adalah pesan yang ditandatangani dengan kunci privat yang sesuai.

Key Agreement

AX5. $((PK_{\delta}(P, K_p)) \wedge (PK_{\delta}(Q, K_q))) \supset P \stackrel{FO(K_p, K_q)}{\leftrightarrow} Q$

AX6. $\phi \equiv \phi [F_0(K, K') / F_0(K', K)]$

Receiving

AX7. $P \text{ received } (X_1, \dots, X_n) \supset P \text{ received } X_i$

AX8. $(P \text{ received } \{X\}_K \wedge P \text{ sees } K) \supset P \text{ received } X$

AX9. $P \text{ received } [X]_K \supset P \text{ received } X$

Seeing

AX10. $P \text{ received } X \supset P \text{ sees } X$

AX11. $P \text{ sees } (X_1, \dots, X_n) \supset P \text{ sees } X_i$

AX12. $(P \text{ sees } X_1 \wedge \dots \wedge P \text{ sees } X_n) \supset P \text{ sees } F(X_1, \dots, X_n)$

Comprehending

AX13. $P \text{ believes } (P \text{ sees } F(X)) \supset P \text{ believes } (P \text{ sees } X)$

Saying

AX14. $P \text{ said } (X_1, \dots, X_n) \supset (P \text{ said } X_i \wedge P \text{ sees } X_i)$

AX15. $P \text{ says } (X_1, \dots, X_n) \supset (P \text{ said } X_1, \dots, X_n \wedge P \text{ says } X_i)$

Jurisdiction

AX16. $(P \text{ controls } \phi \wedge P \text{ says } \phi) \supset \phi$

Prinsipal P mengatakan formula ϕ dimana P memiliki wewenang atas ϕ , maka ϕ benar adanya.

Freshness

AX17. $\text{fresh}(X_i) \supset \text{fresh}(X_1, \dots, X_n)$

AX18. $\text{fresh}(X_1, \dots, X_n) \supset \text{fresh}(F(X_1, \dots, X_n))$

Nonce-verification

AX19. $(\text{fresh}(X) \wedge P \text{ said } X) \supset P \text{ says } X$

Freshness mengubah pesan yang pernah dikatakan pada waktu lampau menjadi pesan yang segar yang baru saja dikatakan.

Symmetric Goodness of Shared Key

AX20. $P \stackrel{K}{\leftrightarrow} Q \equiv Q \stackrel{K}{\leftrightarrow} P$

Logika SVO-CP

Penelitian yang dilakukan oleh (Pardede, 2012) dalam disertasinya yakni memperluas logika SVO agar dapat digunakan untuk verifikasi sifat *fairness* dari sebuah protokol non-repudiasi. CP melakukan perluasan terhadap logika SVO dengan menambahkan notasi dan

aksioma yang dibutuhkan untuk verifikasi protokol non-repudiasi.

Notasi yang diajukan untuk perluasan logika SVO adalah:

1. MR(P, L, X): Pesan X ditujukan bagi prinsipal P pada sesi L.
2. P knows X: Prinsipal P mengetahui pesan X. Pengetahuan P akan X dapat diperoleh melalui pesan yang diterima oleh P atau pesan yang memang berasal dari P.

Aksioma yang diajukan adalah:

1. $P \text{ says } X \supset P \text{ knows } X.$
2. $P \text{ knows } (x_1, x_2, \dots, x_n) \supset P \text{ knows } x_i.$
3. $P \text{ believes } Q \text{ said } X \text{ and } P \text{ believes } MR(Q, L, X) \supset P \text{ believes } Q \text{ knows } X.$
4. $P \text{ believes } (Q \text{ controls } \phi) \wedge P \text{ believes } (Q \text{ said } \phi) \supset P \text{ believes } \phi.$
5. $P \text{ believes } PK_{\psi}(Q, K) \wedge P \text{ receives } \{X\}_K \supset P \text{ believes } Q \text{ said } X.$

METODE PENELITIAN

Pada tahap awal yaitu melakukan identifikasi terhadap bukti NRO dan NRR dari protokol Zhang-Shi. Penelitian ini dilakukan dalam empat tahap utama, yaitu (1) tahap pertama, spesifikasi langkah-langkah protokol. Pada langkah pertama ini dilakukan spesifikasi protokol dalam bahasa logika dengan mengekspresikan setiap pesan di dalam protokol sebagai sebuah formula logika. Langkah pertama ini dikenal sebagai formalisasi protokol, (2) tahap kedua, spesifikasi asumsi-asumsi awal. Asumsi-asumsi yang diterapkan mencerminkan keyakinan (*belief*) dan milik (*possession*) dari setiap prinsipal, di awal perjalanan protokol, (3) tahap ketiga, tujuan yang diinginkan oleh protokol dinyatakan dalam bahasa logika. Tujuan-tujuan tersebut dinyatakan dalam hal keyakinan dan milik dari setiap prinsipal, di akhir perjalanan protokol. Verifikasi protokol keamanan dilakukan untuk memeriksa apakah tujuan-tujuan tersebut tercapai, dan (4) tahap keempat, langkah akhir verifikasi adalah penerapan

postulat-postulat logika. Penerapan postulat-postulat logika dilakukan untuk menurunkan keyakinan dan milik prinsipal-prinsipal, dari keyakinan awal (asumsi-asumsi) hingga mencapai tujuan protokol.

HASIL DAN PEMBAHASAN

Langkah-langkah dalam protokol Non-Repudiasi Zhang-Shi adalah

- (T1) $A \rightarrow B$: $\{PC_A \parallel \{M\}K_{AB}\}PK_B \parallel S_A(H(\{M\}K_{AB}) \parallel N_A)$
 (T2) $B \rightarrow A$: $S_B(H(\{M\}K_{AB}) \parallel N_A \parallel N_B \parallel t_B)$
 (T3) $A \rightarrow SS$: $\{PC_A \parallel \text{Label} \parallel t_B\}PK_{SS} \parallel S_A(H(\{M\}K_{AB}) \parallel K_{AB} \parallel t_B)$
 (T4) $B \leftrightarrow SS$: Label, I_A
 (T5) $A \leftrightarrow SS$: Label, I_A

Dimana

$\text{Label} = f(N_A, N_B, t_B)$ dan
 $I_A = \text{Label} \parallel PC_{SS} \parallel S_{SS}(\text{Label} \parallel S_A(H(\{M\}K_{AB}) \parallel K_{AB} \parallel t_B))$

Untuk kelengkapan, daftar item data dari setiap prinsipal A, B dan SS yang harus disimpan dalam basis data untuk keberhasilan kelengkapan protokol, yang dirangkum sebagai berikut

- A menyimpan: $S_B(H(\{M\}K_{AB}) \parallel N_A \parallel N_B \parallel t_B), I_A, M$ (atau $\{M\}K_{AB}, PC_B$, yang kemudian disebut bukti *NRR*,
- B menyimpan: $S_A(H(\{M\}K_{AB} \parallel N_A), N_B, t_B, I_A, M$ (atau $\{M\}K_{AB}, PC_A$, yang kemudian disebut bukti *NRO*,
- SS menyimpan: $\{PC_A \parallel \text{Label} \parallel t_B\}PK_{SS}, S_{SS}(t_{SS}), S_{SS}(\text{Label} \parallel S_A(H(\{M\}K_{AB}) \parallel K_{AB} \parallel t_B))$, yang kemudian disebut bukti *NRD*.

Analisis Protokol Zhang-Shi

Pada bagian ini diaplikasikan logika

SVO-CP (Pardede, 2012) untuk verifikasi protokol non-repudiasi Zhang-Shi (ZS). Protokol ZS dianalisis untuk verifikasi apakah tujuan akhir (*goal*) serta *fairness* tercapai. Langkah pertama adalah menetapkan spesifikasi protokol non-repudiasi ZS secara formal.

Spesifikasi Protokol Secara Formal

- (T1) $A \rightarrow B$: $\{PC_A, \{M\}K_{AB}\}PK_B, S_A(H(\{M\}K_{AB}), N_A)$
- (T2) $B \rightarrow A$: $S_B(H(\{M\}K_{AB}), N_A, N_B, t_B)$
- (T3) $A \rightarrow SS$: $\{PC_A, \text{Label}, t_B\}PK_{SS}, S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$
- (T4) $B \leftrightarrow SS$: $S_{SS}(\text{Label}, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$
- (T5) $A \leftrightarrow SS$: $S_{SS}(\text{Label}, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

Spesifikasi Asumsi Awal

- P1 A believes $PK_{\sigma}(B, S_B)$
 P5 A believes $PK_{\sigma}(SS, S_{ss})$
 P2 B believes $PK_{\sigma}(A, S_A)$
 P6 B believes $PK_{\sigma}(B, PK_B)$
 P3 SS believes $PK_{\sigma}(A, S_A)$
 P7 B believes $A \xleftrightarrow{K_{AB}} B$
 P4 B believes $PK_{\sigma}(SS, S_{ss})$
 P8 B believes fresh (N_A)
 P9 A believes fresh (t_B, N_B)

Asumsi P1 sampai dengan P5 menyatakan bahwa prinsipal yakin akan kunci verifikasi tanda tangan publik dari prinsipal lain yang mengirimkan pesan kepadanya. Sebagai contoh: *A believes* $PK_{sv}(B, S_B)$ berarti prinsipal A yakin bahwa S_B adalah kunci publik untuk verifikasi tanda tangan B. Asumsi-asumsi ini bersama dengan aksioma yang relevan digunakan untuk menunjukkan asal-usul pesan yang dikirimkan kepada resipien, juga untuk menunjukkan keyakinan resipien atas prinsipal yang mengatakan pesan.

P10 A believes $MR(B, L, H\{M\}K_{AB})$

P11 A believes $MR(SS, L, K_{AB})$

Asumsi P10 menyatakan bahwa prinsipal A sebagai originator pesan M yakin bahwa pesan M ditujukan bagi prinsipal B pada sesi L. Asumsi P11 menyatakan bahwa prinsipal A sebagai originator pesan K yakin bahwa pesan K ditujukan bagi SS pada sesi L.

P12 A believes $SV(S_B(H(\{M\}K_{AB})), N_B, t_B), S_B, (H(\{M\}K_{AB}))$

P13 B believes $SV(S_A(H(\{M\}K_{AB}))), S_A, (H(\{M\}K_{AB}))$

P14 SS believes $SV(S_A(H(\{M\}K_{AB})), K_{AB}, t_B), S_A, (H(\{M\}K_{AB}))$

P15 B believes $SV(S_{SS}(L, S_A(H(\{M\}K_{AB})), K_{AB}, t_B)), S_{SS}, (H(\{M\}K_{AB}, K_{AB}, t_B))$

P16 A believes $SV(S_{SS}(L, S_A(H(\{M\}K_{AB})), K_{AB}, t_B)), S_{SS}, (H(\{M\}K_{AB}, K_{AB}, t_B))$

Asumsi P12 sampai dengan P16 mengasumsikan keyakinan prinsipal akan kunci verifikasi tanda tangan publik dari prinsipal yang berkomunikasi dengannya.

P17 B believes SS controls $PK_{\psi}(A, K_{AB})$

P18 SS said $(A, B, L, K_{AB}) \supset A$ said $(A, B, L, K_{AB}) \wedge B$ receives (A, B, L, K_{AB})

Asumsi P17 menyatakan bahwa prinsipal B sebagai resipien pesan dari A yakin bahwa SS mempunyai wewenang atas kunci publik K_{AB} yang dimiliki oleh A. Asumsi P18 menyatakan bahwa bila SS said (A, B, L, K_{AB}) maka sebelumnya A mengatakan (A, B, L, K_{AB}) dan prinsipal B menerima (A, B, L, K_{AB})

Spesifikasi Tujuan

P19 B receives $\{PC_A, \{M\}K_{AB}\}PK_B, S_A(H(\{M\}K_{AB}), N_A)$

P20 A receives $S_B(H(\{M\}K_{AB}), N_A, N_B, t_B)$

P21 SS receives $\{PC_A, Label, t_B\}PK_{SS},$

$(S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

P22 B receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

P23 A receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

Premis P19 sampai dengan P23 adalah anotasi langkah-langkah spesifikasi tujuan dalam protokol ZS. Pada setiap langkah, prinsipal diasumsikan menerima pesan yang ditujukan kepadanya sesuai protokol.

Asumsi Pemahaman Penerimaan Pesan

P24 B believes B receives $\{PC_A,$

$\{M\}K_{AB}\}PK_B, S_A(H(\{M\}K_{AB}), N_A)$

P25 A believes A receives

$S_B(H(\{M\}K_{AB}), N_A, N_B, t_B)$

P26 SS believes SS receives $\{PC_A, L, t_B\}PK_{SS}, (S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

P27 B believes B receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

P28 A believes A receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

Keyakinan setiap prinsipal bahwa ia menerima pesan perlu diasumsikan untuk dapat menurunkan keyakinan prinsipal akan pesan yang ia yakin diterimanya.

Tujuan Fairness

Protokol dianalisis untuk melihat apakah protokol menjamin *fairness*. Protokol dikatakan mencapai *fairness* bila memenuhi B believes A said M (NRO) and A believes (B said NRR and SS said NRD).

Penerapan Postulat Logika

Sebagai langkah akhir dari verifikasi protokol keamanan, dilakukan penerapan aksioma-aksioma dan aturan inferensi secara berulang untuk memperoleh hasil yang diharapkan.

Berangkat dari premis [P20] dan dengan menerapkan aksioma [AX7] diperoleh [R4]. A receives $S_B(H(\{M\}K_{AB}),$

$N_A, N_B, t_B) \supset A$ receives $S_B(H(\{M\}K_{AB}))$. Dengan penerapan MP pada [P25] dan [R4] diperoleh [R5]. A believes A receives $S_B(H(\{M\}K_{AB}))$. Penerapan MP dan [AX4] kepada premis [P1], [P12], dan hasil [R5] memberikan [R6]. A believes B said $(H(\{M\}K_{AB}))$. [R6] menyatakan bahwa prinsipal A yakin bahwa pesan $(H(\{M\}K_{AB}))$ yang diterima berasal dari prinsipal B . $(H(\{M\}K_{AB}))$ adalah tanda terima pesan (NRR) yang merupakan bukti bahwa B telah menerima pesan yang sebelumnya dikirimkan oleh A .

Penerapan aksioma [AX7] pada [P22] diperoleh [R11]. B receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B)) \supset B$ receives $S_{SS}(L, S_A(H(\{M\}K_{AB})))$. Dengan penerapan MP pada [P27] dan [R11] diperoleh [R12]. B believes B receives $S_{SS}(L, S_A(H(\{M\}K_{AB})))$. Penerapan [MP] dan [AX4] kepada premis [P4], [P15] dan hasil [R12] memberikan [R13]. B believes SS said $(L, S_A(H(\{M\}K_{AB})))$ yang menyatakan B yakin bahwa pesan $(L, S_A(H(\{M\}K_{AB})))$ berasal dari SS . Pesan tersebut merupakan tanda konfirmasi dari SS bahwa ia telah menyediakan kunci K_{AB} untuk dapat diakses secara bebas oleh B .

Hasil penerapan MP pada [R13] dan premis [P18] memberikan [R14]. B believes A said (A, B, L, K_{AB}) yang menyatakan bahwa prinsipal B yakin bahwa (A, B, L, K_{AB}) yang memuat kunci K_{AB} berasal dari A . Hasil penerapan MP pada AX15 kepada [R13] memberikan [R15]. B believes SS said K_{AB} , dimana $K_{AB} = PK_{\psi}(A, K_{AB})$. Dengan memperhatikan [P17] dan [R15], aksioma [AT4] memberikan [R16]. B believes $PK_{\psi}(A, K_{AB})$. Penerapan aksioma [AT5] pada [R2a] dan [R16], dimana $M = \{M\}K_{AB}$, $K_{AB} = PK_{\psi}(A, K_{AB})$ memberikan [R17]. B believes A said M . Prinsipal B telah menerima $\{M\}K_{AB}$ dan yakin bahwa K_{AB} adalah kunci publik dari A , yakin bahwa

pesan M berasal dari A . Prinsipal B dapat membuka pesan M menggunakan kunci K_{AB} .

Berangkat dari premis [P23] dan dengan menerapkan aksioma [AX7] pada [P23] diperoleh [R18]. A receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B)) \supset A$ receives $S_{SS}(L, S_A(H(\{M\}K_{AB})))$. Penerapan MP pada [P28] dan [R18] memberikan [R19]. A believes A receives $S_{SS}(L, S_A(H(\{M\}K_{AB})))$. Penerapan [MP] dan [AX4] kepada premis [P5], [P16] dan hasil [R19] memberikan [R20]. A believes SS said $(L, S_A(H(\{M\}K_{AB})))$. Prinsipal A yakin bahwa SS telah meletakkan kunci K_{AB} pada direktori yang bisa diakses oleh B . Hal tersebut ditunjukkan oleh keyakinan A bahwa pesan $(L, S_A(H(\{M\}K_{AB})))$ berasal dari SS . Pesan tersebut merupakan bukti konfirmasi (NRD) bahwa SS telah menerima K_{AB} dari A dan telah menyediakannya untuk dapat diakses oleh B .

Diskusi

Berdasarkan analisis dengan penerapan logika SVO-CP pada protokol Zhang-Shi menunjukkan resipien B yakin pesan M berasal dari originator A . Hal tersebut ditunjukkan oleh [R17] B believes A said M . Keyakinan originator A bahwa pesan telah diterima oleh resipien B dan SS telah menyediakan kunci K_{AB} di sebuah tempat yang bisa diakses oleh B tercapai dan ditunjukkan oleh [R6] A believes B said $(H(\{M\}K_{AB}))$ dan [R20] A believes SS said $(L, S_A(H(\{M\}K_{AB})))$. $(H(\{M\}K_{AB}))$ adalah tanda terima pesan (NRR). $(L, S_A(H(\{M\}K_{AB})))$ adalah konfirmasi bahwa SS menyediakan kunci K_{AB} untuk dapat diakses oleh B (NRD). Kedua hal tersebut di atas menunjukkan dipenuhinya B believes A said M and A believes $(B$ said $(H(\{M\}K_{AB}))$ and A believes SS said $(L, S_A(H(\{M\}K_{AB})))$). Dengan demikian, analisis protokol menggunakan logi-

ka SVO-CP menunjukkan bahwa tujuan *fairness* *B believes A said M and A believes (B said NRR and SS said NRD)* dipenuhi.

SIMPULAN

Penerapan metode formal logika SVO-CP dalam analisis dan verifikasi protokol non-repudiasi Zhang-Shi menunjukkan bahwa protokol tersebut memiliki kehandalan yang dipenuhinya kebenaran atas semua tujuannya (*Non-Repudiation of Origin* (NRO) dan *Non-Repudiation of Receipt* (NRR)).

Tujuan *fairness* dalam penelitian ini adalah *B believes A said M and A believes (B said NRR and SS said NRD)*. Penerapan logika SVO-CP kepada verifikasi protokol non-repudiasi Zhang-Shi menunjukkan protokol tersebut mencapai *fairness*.

DAFTAR PUSTAKA

- Coffey, T. and Dojen, R. 2009 “A Formal Verification Centred Development Process for Security Protocols” chapter XIV, pages 165-178. IGI Global.
- Coffey, T. and Saidha, P. 1997 “Logic for verifying public-key cryptographic protocols” *IEEE Proceedings Computer Digital Technology*, 144(1):28 –32.
- Pardede, D. L. C. 2012 *Perluasan Logika SVO Untuk Analisis Dan Verifikasi Formal Protokol Non-Repudiasi* PhD thesis of Information Technology Gunadarma University Depok.
- Syverson, P. F. and Van Oorschot, P. C. 1994 “On unifying some cryptographic protocol logics” *IEEE Symposium on Research in Security and Privacy* pages 14-28.
- Tarigan, A., Rechneretze, A., Systeme, V., and Bielefeld, U. 2002 *Survey in formal analysis of security properties of cryptographic protocol*.
- Ventuneac, M., C. T. N. T. 2004 “Reasoning on properties of non-repudiation security protocols” *WSEAS Transactions on Information Science and Applications*, 1(5):1262–1267.
- Zhang, N. and Shi, Q. 1996 “Achieving non-repudiation of receipt” *The Computer Journal* 39(10):844–853.
- Zhou, J. and Gollmann, D. 1996 “A fair non-repudiation protocol” In *IEEE Symposium on Security and Privacy Research in Security and Privacy* pages 55–61 IEEE Computer Society Press.
- Zhou, J. and Gollmann, D. 1998 “Towards verification of non-repudiation protocols” In *Proceedings of 1998 International Refinement Workshop and Formal Methods Pacific* pages 370–380 Springer-Verlag