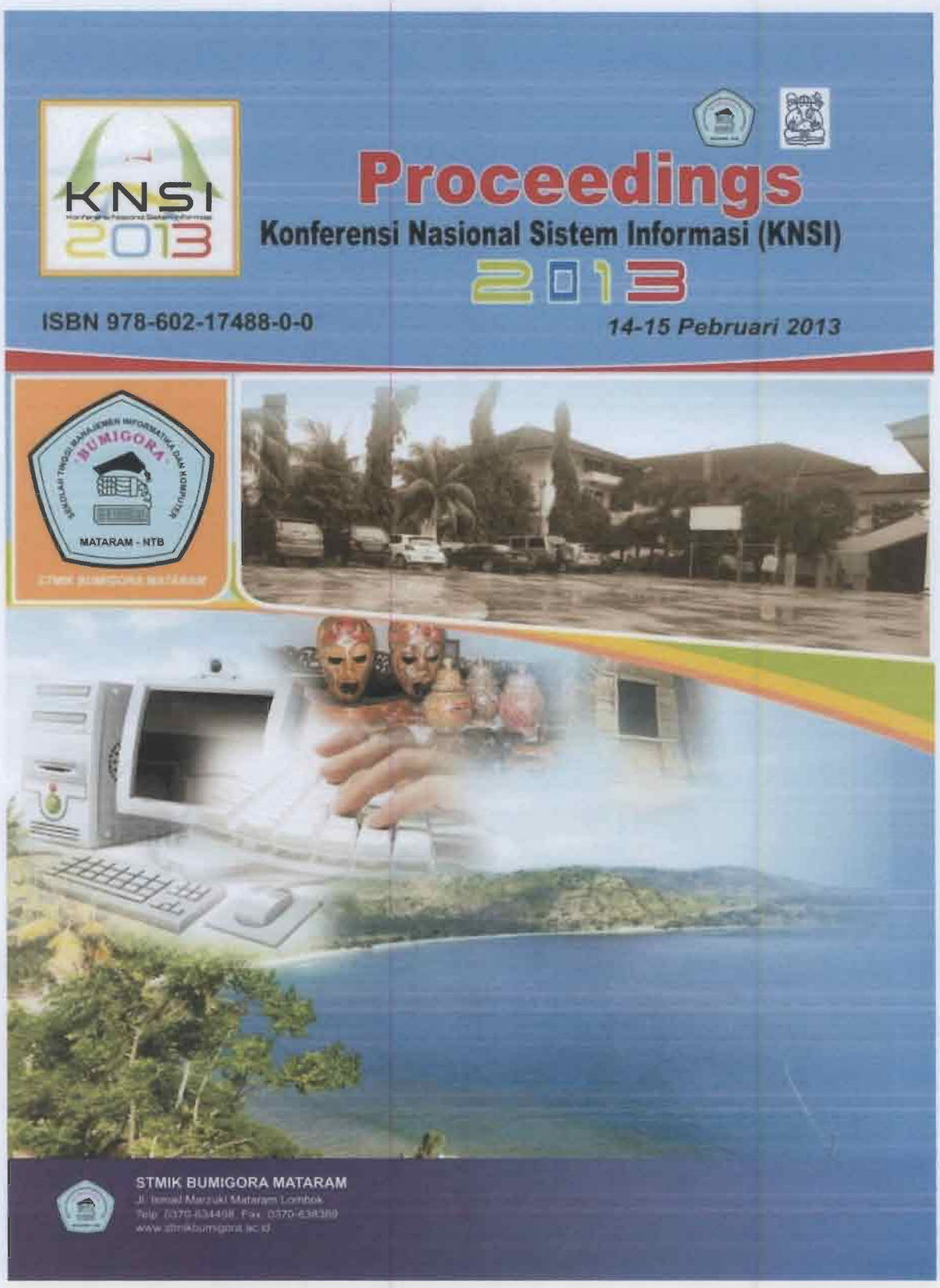


Dipublikasikan Tahun 2013 oleh :

STMIK BUMIGORA MATARAM
Mataram-Indonesia

ISBN : 978-602-17488-0-0

PROCEEDINGS
KONFERENSI NASIONAL SISTEM INFORMASI 2013

Ketua Editor
Agus Pribadi, S.T., M.Sc

Sekretaris Editor
Ir. Bambang Krismono Triwijoyo, M.Kom.

Anggota Editor
M.Yunus,S.Kom.
Ahmad Asril Rizal, S.Si.

KOMITE KNSI 2013

STEERING COMMITEE

- Kridanto Surendro, Ph.D
- Dr. Rila Mandala
- Dr. Husni S Sastramihardja
- Prof. Iping Supriana
- Dr. Ing. M. Sukrisno
- Dyah Susilowati, M.Kom.

PROGRAM COMMITTEE

- Kridanto Surendro, Ph.D (ITB)
- Dr. Rila Mandala (ITB)
- Dr. Husni Setiawan Sastramihardja (ITB)
- Prof. Jazi Eko Istiyanto, Ph.D (UGM)
- Prof. Dr. Beny A Mutiara (Univ. Gunadarma)
- Retantyo Wardoyo, Ph.D (UGM)
- Agus Harjoko, Ph.D (UGM)
- Dra. Sri Hartati, M.Sc, Ph.D (UGM)
- Prof. Zainal A. Hasibuan, Ph.D (Univ. Indonesia)
- Dr. Djoko Soetarno (Univ. BINUS)
- Prof. Ir. Arief Djunaedi, M.Sc.,PhD (ITS)
- Prof. Dr. Ir. Joko Lianto Buliali, MSc (ITS)
- Dr. Ir. Agus Buono, M.Si., M.Kom (IPB)
- Dr. Ir. Sri Nurdiati, M.Sc (IPB)
- Prof. Dr. M. Zarlis, M.Sc (USU)
- Dr. Masayu Leylia Khodra (ITB)

TECHNICAL COMMITTEE

- Agus Pribadi, S.T., M.Sc
- Ria Rosmalasari Safitri, M.M.
- Ni Ketut Sriwinarti, S.E, M.Ak.
- Ir. Bambang Krismono Triwijoyo, M.Kom.
- Dadang Priyanto, M.Kom.
- Muhammad Nur, M.Hum.
- Raisul Azhar, S.T., M.T.
- Kartarina, S.Kom.
- Husain, S.Kom

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa, atas perkenan-Nya, Konferensi Nasional Sistem Informasi (KNSI) tahun 2013 ini dapat diselenggarakan. KNSI 2013 merupakan event nasional tahunan yang diselenggarakan pertamakalinya pada tahun 2005 di Institut Teknologi Bandung (ITB). KNSI 2013 merupakan event ke sembilan yang diselenggarakan di Kampus STMIK Bumigora Mataram Lombok Nusa Tenggara Barat. Penyelenggaraan KNSI merupakan media para praktisi dan akademisi saling berbagi ide dan pengalaman baru tentang disiplin ilmu Sistem Informasi dan Teknologi Informasi. Topik-topik yang dibahas dalam konferensi digaharapkan dapat membentuk masyarakat yang dapat menuntun perwujudan Sistem Informasi sebagai salah satu solusi memajukan Bangsa Indonesia. Kemajuan yang duharapkan mampu meningkatkan daya saing bangsa Indonesia di tingkat dunia.

KNSI 2013 diselenggarakan sebagaimana dua hal dasar penyelenggaraan, yaitu pertemuan ilmiah yang dipadukan dengan kegiatan pengenalan budaya dan wisata Indonesia. Penyelenggaraan KNSI yang digelar tahunan dan secara safari akan mampu untuk lebih mengenalkan aneka regam khas, budaya dan wisata Indonesia utamanya kepada bangsa sendiri. Disamping merupakan media bertemunya para akademisi dan praktisi bidang Teknologi Informasi, KNSI juga mendukung program pemerintah dalam meningkatkan pengenalan dan kunjungan wisata Indonesia. Bangsa Indonesia harus mampu menjadi tuan rumah di negerinya sendiri dalam bidang wisata dan budaya.

Penyelenggaraan KNSI 2013 ini cukup diminati dari berbagai kalangan. Tentunya media temu ilmiah KNSI semakin diminati, dengan dijumpainya tidak sedikit peserta baru yang berbondong menghadiri temu ilmiah ini sebagai konferensi pertama yang peserta ikuti. Mengikuti KNSI dapat dipergunakan sebagai pengalaman untuk menapak dan sebagai pintu masuk untuk mengikuti konferensi atau temu ilmiah berikutnya. Peserta yang telah biasa mengikuti temu ilmiah serupa lain ataupun peserta KNSI yang menjadi langganan pada KNSI semuanya dapat berinteraksi dan berbagi pada *event* KNSI 2013 ini.

Akhirnya kami seluruh panitia konferensi berharap koleksi abstrak paper yang dimuat dalam proceedings KNSI 2013 ini akan dapat bermanfaat bagi semua mansyarakat ilmiah maupun praktisi dalam pengembangan ilmu pengetahuan di bidang Sistem Informasi. Tidak lupa kami juga menyampaikan ucapan terima ksih kepada semua pihak yang telah membantu terlaksananya KNSI 2013 kali ini serta diterbitkannya proceedings KNSI 2013.

Mataram, 22 januari 2013
Ketua Panitia Pelaksana

Agus Pribadi,S.T,M.Sc

SAMBUTAN KETUA STMIK BUMIGORA MATARAM

Yang terhormat para undangan, pembicara utama, pemakalah dan peserta Konferensi Nasional Sistem Informasi tahun 2013. Puji syukur kita panjatkan kepada Tuhan Yang Maha Esa, karena pada hari ini kita dapat berkumpul untuk bisa mengikuti acara pembukaan serta pemaparan ilmiah sebagai rangkaian kegiatan Konferensi kali ini, yang merupakan hasil kerjasama antara STMIK Bumigora Mataram dengan Departemen Teknik Informatika, Institut Teknologi Bandung selaku penggagas KNSI yang telah dirintis dan dilaksanakan untuk pertama kalinya pada tahun 2005 di ITB Bandung.

STMIK Bumigora merupakan perguruan tinggi komputer pertama di NTB yang berdiri pada tanggal 26 September 1987. STMIK Bumigora menyelenggarakan tiga program studi yaitu S1 Teknik Informatika, D3 Teknik Informatika dan D3 Manajemen Informatika. Seluruh program studi terakreditasi oleh BAN-PT. Pada tahun 2009 STMIK Bumigora telah memperoleh sertifikat ISO 9001:2008 untuk Penyelenggaraan Akademik Perguruan Tinggi.

Pada pelaksanaan konferensi kali ini dihadiri oleh lebih dari 350 peserta, baik peserta pemakalah maupun non pemakalah. Sebagian besar peserta pemakalah adalah akademisi dan praktisi, sementara non pemakalah terdiri dari kalangan birokrat dan pemerhati Sistem Informasi serta mahasiswa. Peserta berasalah dari berbagai perguruan tinggi di Indonesia mulai dari kota di pulau Sumatra sampai kota di pulau Papua. Harapan kami, konferensi ini dapat menjadi ajang kegiatan pendalaman di bidang Sistem Informasi guna menunjang pembangunan bangsa Indonesia. Saya selaku Ketua STMIK Bumigora Mataram menyampaikan banyak terimakasih kepada semua pihak yang telah bekerja keras merencanakan dan melaksanakan konferensi kali ini, saya juga mohon maaf apabila di dalam persiapan maupun pelaksanaan rangkaian acara konferensi ini terdapat kekurangan.

Akhirnya kami mengucapkan selamat mengikuti konferensi semoga konferensi kali ini dapat berjalan dengan lancar, dan bagi peserta yang akan mengikuti paket wisata kami menyampaikan selamat datang di pulau Lombok, dan selamat menikmati keindahan alam budaya, tradisi serta kuliner khas Lombok.

Mataram, 22 Januari 2012
Ketua STMIK Bumigora Mataram

Dyah Susilowati,M.Kom

JADWAL ACARA KNSI 2013

HARI PERTAMA
Hari : Kamis, Tanggal : 14 February 2013

No	Waktu (WITA)	Acara			
1	08.00-08.30	Registration Peserta			
2	08.30-08.35	Pembukaan MC			
3	08.35-08.45	Tarian Pembukaan			
4	08.45-09.00	Sambutan Ketua Pelaksana KNSI 2013 (Agus Pribadi,S.T,M.Sc)			
	09.00-09.15	Sambutan Steering Committee KNSI			
5	09.15-09.30	Sambutan Ketua STMIK Bumigora Mataram (Dyah Susilowati,M.Kom)			
6	09.30-09.45	Opening spech, Walikota Mataram sekaligus membuka acara KNSI 2013.			
7	09.45-09.50	Doa			
8	09.50-10.30	Keynote Speaker Prof. Ir. Zainal Hasibuan, MLS, Ph.D (UI)			
9	10.30-11.00	Persiapan Parallel Session I			
10	11.00-12.45	**Kelp. I** R.Aula	**Kelp. II** R.Seminar	**Kelp. III** R.TC	**Kelp. IV** R.1TC
		Kelp. V R.LAB.JAR	**Kelp. VI** R.1TB	**Kelp. VII** R.1T	**Kelp. VIII** R.1M
		Kelp. IX R.1TA	**Kelp. X** R.2T	**Kelp. XI** R.2MA	**Kelp. XII** R.2MB
11	12.45-14.00	Ishoma /Persiapan Parallel Session II			
12	14.00-16.00	**Kelp. I** R.Aula	**Kelp. II** R.Seminar	**Kelp. III** R.TC	**Kelp. IV** R.1TC
		Kelp. V R.LAB.JAR	**Kelp. VI** R.1TB	**Kelp. VII** R.1T	**Kelp. VIII** R.1M
		Kelp. IX R.1TA	**Kelp. X** R.2T	**Kelp. XI** R.2MA	**Kelp. XII** R.2MB
13	16.00-16.30	Coffee Break / Persiapan Parallel Session III			
14	16.30-17.30	**Kelp. I** R.Aula	**Kelp. II** R.Seminar	**Kelp. III** R.TC	**Kelp. IV** R.1TC
		Kelp. V R.LAB.JAR	**Kelp. VI** R.1TB	**Kelp. VII** R.1T	**Kelp. VIII** R.1M
		Kelp. IX R.1TA	**Kelp. X** R.2T	**Kelp. XI** R.2MA	**Kelp. XII** R.2MB

Keterangan: Masing-masing peserta dialokasikan 15 menit untuk presentasi dan Tanya jawab.

HARI KEDUA

Hari : Jum'at, Tanggal : 15 February 2013

No	Waktu (WITA)	Acara			
1	08.00-08.30	Registration Peserta, Persiapan Parallel Session IV			
2	08.30-10.15	**Kelp. I** R.Aula	**Kelp. II** R.Seminar	**Kelp. III** R.TC	**Kelp. IV** R.1TC
		Kelp. V R.LAB.JAR	**Kelp. VI** R.1TB	**Kelp. VII** R.1T	**Kelp. VIII** R.1M
		Kelp. IX R.1TA	**Kelp. X** R.2T	**Kelp. XI** R.2MA	**Kelp. XII** R.2MB
3	10.15-10.30	Coffee Break /Persiapan Penutupan			
4	10.30-11.30	Penutupan			

Keterangan
Masing-masing peserta dialokasikan 15 menit untuk presentasi dan Tanya jawab.

HARI KETIGA
Hari : Sabtu, Tanggal : 16 February 2013

Pelaksanaan Paket Wisata One Day Tour

PANDUAN UNTUK PRESENTASI PEMBICARA

1. Presentasi dalam bahasa Indonesia.
2. Pembicara harus menyiapkan presentasinya dalam format Microsoft Power Point file (*.ppt or *.pptx).
3. File presentasi harus diserahkan pada Organizing Committee sebelum dimulainya presentasi.
4. Tiap paper hanya bisa dipresentasikan oleh satu orang pembicara. Jika pembicara ingin mewakilkan pada orang lain resentasinya, maka harus menghubungi panitia terlebih dahulu.
5. Pembicara harus menggunakan laptop yang disediakan oleh panitia.
6. Tiap pembicara mempunyai waktu 15 menit untuk mempresentasikan papernya termasuk waktu diskusi/Tanya jawab.
7. Panitia berhak mengakhiri waktu presentasi apabila sudah melebihi 15 menit.

Jadwal Presentasi

3	KNSI-401	MEMAKSIMALKAN KEMANAN SISTEM DENGAN KONSEP ENCRYPTION DAN DEMILITARIES ZONE	RITA RIJAYANTI
4	KNSI-402	KOLABORASI PENGEMBANGAN PERANGKAT LUNAK : FAKTOR PERILAKU MANUSIA	TIEN FABRIANTI KUSUMASARI[1] , HUSNI SASTRAMIHARDJA[3], KRIDANTO SURENDRO[2] , IPING SUPRIANA[4]
5	KNSI-403	PERENCANAAN PENGOLAHAN DATA SPASIAL UNTUK MENDUGA KECUKUPAN DAYA TAMPUNG SEKOLAH MENENGAH ATAS BERDASAR LULUSAN SEKOLAH MENENGAH PERTAMA	AGUS PRIBADI[1], AHMAT ADIL[2]
6	KNSI-404	PERHITUNGAN TCO (TOTAL COST OF OWNERSHIP) UNTUK RANCANGAN DATA CENTER SPTIK UNPAS YANG BERBASIS TEKNOLOGI VIRTUALISASI	SANSAN MAULANA[1], RIRIN DWI AGUSTIN[2], SALI ALAS M [3]
7	KNSI-190	PERAMALAN CUACA MENGGUNAKAN GABUNGAN METODE ANFIS DAN MOVING AVERAGE	CANDRA DEWI[1]
SESI IV, KELOMPOK III, RUANG TRAINING CENTER (TC)			
NO	**NO.REG**	**JUDUL MAKALAH**	**PENULIS**
1	KNSI-406	SISTEM PENDUKUNG KEPUTUSAN PENENTUAN PROGRAM STUDI BAGI SISWA SMA	SRI EKAWATI[1], HEROE SANTOSO[2]
2	KNSI-407	KERANGKA KERJA PROSES PERLUASAN KUERI BERBASIS TESAURUS	LILY WULANDARI
3	KNSI-408	RANCANGAN SISTEM INFORMASI PERENCANAAN PRODUKSI PADA PT. ZEBRA ASABA INDUSTRIES	ATIK ARIESTA, NAOMI CHRISTY NOVEMBER, ADITYAS YUNITA GUSTAMI, AHMAD BAHRUL ULUM
4	KNSI-411	INFORMASI DAERAH WISATA MELALUI PEMANFAATAN TEKNOLOGI MOBILE PHONE BERBASIS ANDROID	SHERLY PERMATASARI WOLLAH [1], ANITA WASUTININGSIH [2], MARIA Y. ARYATI [3]
5	KNSI-412	SISTEM INFORMASI PELAYANAN CUSTOMER DI PT. XXX	SANDI YUDHA[1], SUCI RAHMADAYANI[2], RAHMAN P RAMDANI [3],CACA E.SUPRIANA,S.SI [4], MUHAMMAD WILDAN [5]
6	KNSI-413	ANALISIS OPINION SPAM PADA PRODUCT REVIEW DENGAN MENGGUNAKAN METODE LOGISTIC REGRESSION	AMITA DESMARANI1[1], WARIH MAHARANI [2], EMA RACHMAWATI[3]
7	KNSI-327	SISTEM REKOMENDASI TAG PADA DOKUMEN BLOG MENGGUNAKAN LATENT SEMANTIC INDEXING	LAILIL MUFLIKHAH[1], NURUL FADILAH[2], ACHMAD RIDOK[3]
SESI IV, KELOMPOK IV, RUANG 1TC			
NO	**NO.REG**	**JUDUL MAKALAH**	**PENULIS**
1	KNSI-414	PEMETAAN KONSEP LEARNING ORGANIZATION DAN INTERAKSI	NURUL MUTIAH[1], SITI SARAH ABDULLAH[2], ROSALINA NATALYA REVASSI[3]
2	KNSI-415	APLIKASI DESAIN KREATIF UNTUK MENINGKATKAN DAYA INOVASI PERAJIN SEPATU SKALA KECIL	ROMDONI SUSILOATMADJA[1], SEPTI MARIANI[2], IDA ASTUTI[3], IMAN MURTONO SOENHADJI[4]
3	KNSI-416	MODEL SISTEM INTERAKSI: KOLABORASI SEKTOR TENAGA KERJA DAN PENDIDIKAN UNTUK MENDUKUNG KKNI	DINY SYARIFAH SANY[1], MEITA NOVIA[2], SITI SARAH ABDULLAH[3]
4	KNSI-417	ANALISIS DAN IMPLEMENTASI CHANGE DATA CAPTURE DENGAN METODE ASYNCHRONOUS DISTRIBUTED HOTLOG PADA DATA WAREHOUSE	SHAFNIATI[1], WARIH MAHARANI, ST.MT.[2], KUSUMA AYU L, ST.MT.[3]
5	KNSI-418	ANIMASI TEX DAN ANGKA DENGAN TRANSFORMASI SINUSOIDAL MENGGUNAKAN OPENGL	ROMDHONI SUSILOATMADJA

Makalah Nomor: KNSI-390
PERANCANGAN KNOWLEDGE MANAGEMENT SYSTEM (KMS) PROSES AKADEMIK PADA STMIK SYAIKH ZAINUDDIN NAHDLATUL WATHAN ANJANI LOMBOK TIMUR
Marwan Hakim, Siti Ruja'ah

Nomor Makalah: KNSI-391
PENERAPAN FUZZY MULTI ATTRIBUT DECISION MAKING (FMACM) UNTUK PEMILIHAN PEJABAT FUNGSIONARIS DI LINGKUNGAN PERGURUAN TINGGI
Alfonsus Situmorang

Makalah Nomor: KNSI-392
SISTEM PENENTUAN METODE FORECAST DAN PERHITUNGAN FORECAST PENJUALAN
Dara Kusumawati

Makalah Nomor: KNSI-395
PEMODELAN PROSES BISNIS B2C DENGAN BPMN (STUDI KASUS: KONFEKSI PADA BARZAS CLOTHING)
Suryatiningsih

Makalah Nomor: KNSI-396
PENGEMBANGAN FRAMEWORK PEMBANGKITAN PETA PENELITIAN UNTUK MENGGAMBARKAN POSITIONING RESEARCH SECARA OTOMATIS
Afrida Helen, Ayu Purwarianti, Dwi Hedratmo Widyantoro

Makalah Nomor: KNSI-397
EVALUASI PROSES PEMBELAJARAN BERBASIS ANDROID UNTUK MATA KULIAH FISIKA DASAR
Mukhammad Ramdlan Kirom

Makalah Nomor: KNSI-398
ADOPSI E-COMMERCE UNTUK KEBERLANJUTAN BISNIS DI SENTRA KAOS SURAPATI BANDUNG
Yuhana Astuti

Makalah Nomor: KNSI-399
PEMODELAN SISTEM IMUN DENGAN PENDEKATAN BERBASIS AGEN
Ayi Purbasari, Iping Supriana S, Oerip S Santoso3

Makalah Nomor: KNSI-400
PEMILIHAN TESAURUS ONLINE BERBAHASA INDONESIA UNTUK TEMU KEMBALI INFORMASI
Ahmad Thantawi, Detty Purnamasari, Lily Wulandari

Makalah Nomor: KNSI-401
MEMAKSIMALKAN KEMANAN SISTEM DENGAN KONSEP ENCRYPTION DAN DEMILITARIES ZONE

Rita Rijayanti

Makalah Nomor: KNSI-402
FAKTOR PERILAKU MANUSIA DALAM KOLABORASI PENGEMBANGAN PERANGKAT LUNAK
Tien Fabrianti Kusumasari , Husni Sastramihardja, Kridanto Surendro , Iping Supriana

Makalah Nomor: KNSI-403
PERENCANAAN OLAH DATA SPASIAL SEKOLAH UNTUK MENDUGA KECUKUPAN DAYA TAMPUNG SEKOLAH MENENGAH ATAS BERDASAR LULUSAN SEKOLAH MENENGAH PERTAMA DI PULAU LOMBOK
Agus Pribadi, Ahmat Adil

Makalah Nomor: KNSI-404
PERHITUNGAN TCO (Total Cost of Ownership) UNTUK RANCANGAN DATA CENTER SPTIK UNPAS yang BERBASIS TEKNOLOGI VIRTUALISASI
Sansan Maulana, Ririn Dwi Agustin, Sali Alas M

Makalah Nomor: KNSI-406
SISTEM PENDUKUNG KEPUTUSAN PENENTUAN PROGRAM STUDI BAGI SISWA SMA
Sri Ekawati, Heroe Santoso

Makalah Nomor: KNSI-407
KERANGKA KERJA PROSES PERLUASAN KUERI BERBASIS TESAURUS
Lily Wulandari

Makalah Nomor: KNSI-408
RANCANGAN SISTEM INFORMASI PERENCANAAN PRODUKSI PADA PT. ZEBRA ASABA INDUSTRIES
Atik Ariesta, Naomi Christy November, Adityas Yunita Gustami, Ahmad Bahrul Ulum

Makalah Nomor: KNSI-411
INFORMASI DAERAH WISATA MELALUI PEMANFAATAN TEKNOLOGI MOBILE PHONE BERBASIS ANDROID
Sherly Permatasari Wollah, Anita Wasutiningsih, Maria Y. Aryati

Makalah Nomor: KNSI-412
SISTEM INFORMASI PELAYANAN CUSTOMER DI PT. XXX
Sandi Yudha, Suci Rahmadayani, Rahman P Ramdani, Caca E.Supriana,S.Si, Muhammad Wildan

Makalah Nomor: KNSI-413
ANALISIS OPINION SPAM PADA PRODUCT REVIEW DENGAN MENGGUNAKAN METODE LOGISTIC REGRESSION
Amita Desmarani1, Warih Maharani , Ema Rachmawati]

Makalah Nomor: KNSI-414
PEMETAAN KONSEP LEARNING ORGANIZATION DAN INTERAKSI

Makalah Nomor: KNSI-401

MEMAKSIMALKAN KEAMANAN SISTEM DENGAN KONSEP *ENCRYPTION* DAN *DEMILITARIES ZONE*

Rita Rijayanti

Jurusan Teknik Informatika, Universitas Pasundan
Jalan Doktor Setiabudi 193 (0)22 2013090
ritarijayanti@yahoo.com

Abstrak

Kompleksitas sistem dan luasnya jangakauan akses serta pesatnya perkembangan teknologi jaringan/komunikasi sekarang ini memaksa kita untuk mengoptimalkan pengamanan data dan informasi. Cukup beresiko bila sebuah sistem tidak memfasilitasi diri dengan *security* yag baik, apakah dari sisi sistem, basisdata termasuk infrastruktur jaringan komputernya. Saat ini paling tidak ada tiga tipe dasar dari enkripsi, yaitu manual, *semi-transparent* dan *transparent*. *Transparent data Encription* adalah salah satu jenis enkripsi yang mempunyai keuntungan dalam kemudahan dari sisi pengelola atau pengguna, karena pengelola tidak perlu melakukan proses manajeman enkripsi dan deskripsi data secara manual, tetapi telah otomatis disertakan pada paket sistem basisdata yang digunakan. Konsep dasar keamanan Demilitaries Zone (DMZ) merupakan mekanisme untuk melindungi *system* internal dari serangan hacker atau pihak-pihak lain yang tidak mempunyai akses.

Jurnal ini akan membahas cara kerja dari *transparent data encryption* dan *Demilitaries Zone* serta keunggulannya dalam penerapan pada sebuah sistem. Dari pembahasan ini dapat dikatehui performansi pengamanan sebuah sistem jika menggunakan kedua konsep tersebut, seperti para penyusup akan lebih sulit melakukan pencurian/perusakan data karena sudah dilakukan pengaman secara berlapis dari sisi infrastruktur jaringan dan data.

Kata kunci : *Security, Database, Jaringan, Encryption, DMZ*

1. Pendahuluan

Perkembangan jaman saat ini mulai menuntut berbagai kalangan untuk menggunakan teknologi jaringan (ex: internet) tidak hanya dunia bisnis saja bahkan sekarang sudah merambah kedunia sosialisasi.

Dengan semakin terbukanya fasilitas tersebut maka keamanan dan kerahasian data juga menjadi sorrotan penting dari sebuah system. Gangguan pada sebuah sistem tidak dapat dihindari dan hal tersebut dapat mengakibatkan kerugian baik materi/imateril. Maka untuk mencegah berbagai ancaman tersebut diperlukan pengamanan.

Beberapa aspek yang harus diperhatikan dalam kemanan sebuah sistem, yaitu dari sisi keamanan data/informasi dan dari sisi ancaman yang mungkin timbul baik itu dari sisi perangkat computer, jaringan atau sisi sistem nya sendiri. Karena tidak jarang penyerangan-penyerangan terhadap sebuah sistem bisa berawal dari sistem jaringan yang kurang reliable atau bisa saja penyerangan langsung pada data sarver.

Dalam jurnal ini akan dibahas mengenai pengamanan dari sisi jaringan dan aliran data/informasi (merupakan layer keamanan level 1 – 3).

1.1 Aspek Keamanan Sistem Informasi

1. ***Authentication***
   Penerima informasi dapat memastikan keaslian pesan yang didapat tersebut berasal dari orang yang seharusnya.
2. ***Integrity***
   Pesan yang diterima melalui sebuah jaringan dapat terjamin keasliannya (informasi yang diterima tidak dimodifikasi oleh orang yang tidak berhak).
3. ***Authority***
   Informasi yang melalui sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak (penyusup).
4. ***Confidentiality***
   Sebuah usaha untuk menjaga informasi dari pengaksesan orang yang tidak berhak.

5. ***Privacy***
   Sifatnya lebih ke arah data-data yang privat (pribadi) dari user. [2]

1.2 Aspek ancaman keamanan komputer atau keamanan sistem

1. ***Interruption***
   Informasi dan data yang ada dalam sistem komputer dirusak dan dihapus.
2. ***Interception***
   Informasi yang ada disadap atau orang yang tidak berhak mendapatkan akses ke komputer dimana informasi tersebut disimpan.
3. ***Modifikasi***
   Perubahan data oleh orang yang tidak berhak dengan cara menyadap lalu lintas informasi yang sedang dikirim.
4. ***Fabrication***
   Membuat sebuah informasi tampak seperti aslinya (meniru) sehingga orang yang menerima informasi menyangka informasi tersebut berasal dari orang yang seharusnya. [2]

1.3 Metodologi Keamanan Sistem

1. ***Keamanan level 0***
   keamanan fisik, merupakan keamanan tahap awal dari komputer security. Jika keamanan fisik tidak terjaga dengan baik, maka data-data bahkan hardware komputer sendiri tidak dapat diamankan.
2. ***Keamanan level 1***
   Terdiri dari database, data security, keamanan dari PC itu sendiri, device, dan application. Contohnya : jika kita ingin database aman, maka kita harus memperhatikan dahulu apakah application yang dipakai untuk membuat desain database tersebut merupakan application yang sudah diakui keamanannya seperti oracle. Selain itu kita harus memperhatikan sisi lain yaitu data security. Data security adalah cara mendesain database tersebut. Device security adalah alat-alat apa yang dipakai supaya keamanan dari komputer terjaga. Computer security adalah keamanan fisik dari orang-orang yang tidak berhak mengakses komputer tempat datadase tersebut disimpan.
3. ***Keamanan level 2***
   Network security. Komputer yang terhubung dengan jaringan sangat rawan dalam masalah keamanan, oleh karena itu keamanan level 2 harus dirancang supaya tidak terjadi kebocoran jaringan, akses ilegal yang dapat merusak keamanan data tersebut.
4. ***Keamanan level 3***
   Information security. Keamanan informasi yang kadang kala tidak begitu dipedulikan oleh administrator seperti memberikan password ke teman, atau menuliskannya dikertas, maka bisa menjadi sesuatu yang fatal jika informasi tersebut diketahui oleh orang yang tidak bertanggung jawab.
5. ***Keamanan level 4***
   merupakan keamanan secara keseluruhan dari komputer. Jika level 1-3 sudah dapat dikerjakan dengan baik maka otomatis keamanan untuk level 4 sudah terwakili.

2. Metodologi

Metodologi yang diterapkan adalah pengamatan secara langsung pada sistem runtime di sebuah perusahaan, dipusatkan pada sisi keamanan jaringan dan data dengan dilakukan pengkajian teknik pengamanan sehingga didapatkan hasil yang maksimal/sesuai dengan kebutuhan keamanan di diperusahaan tersebut untuk saat ini.

Setiap perusahaan akan memiliki nilai maksimal yang berbeda tergantung strategi dan kebutuhan perusahaan tersebut, dimana suatu teknik bisa dikatakan baik untuk suatu sistem tertentu namun belum tentu akan baik juga jika diterapkan ditempat lain [1]. Sekala kemanan diperusahaan yang diamati adalah sistem dapat berjalan dengan baik tanpa disusupi berbagai script titipan sehingga aplikasi dapat berjalan dengan baik dan kerahasian data yang dimiliki perusahaan dapat terjaga.

3. Konsep De-Militarized Zone (DMZ)

Konsep dari DMZ adalah untuk melindungi sistem internal dari serangan haker atau pihak-pihak yang tidak berkepentingan yang ingin memasuki sistem tanpa mempunyai hak akses dengan tujuan menggagu jalannya aktifitas sistem.

Penerapan DMZ yaitu dengan memindahkan semua layanan suatu jaringan ke jaringan lain yang berbeda dengan cara pemotongan jalur komunikasi pada jaringan internal sehingga jika hacker menyerang dan melakukang craking pada server yang mempunyai DMZ, haker tersebut dapat mengakses host yang berada pada DMZ tapi tidak bisa masuk pada jaringan internal.

Adapun konsep yang harus dipahami dalam pemasangan DMZ ini yaitu, konsep yang di build oleh DNS yang disebut dengan There fruit concept (NAT, PAT, dan Daftar Akses Network Address Translation(NAT) berfungsi untuk

mengarahkan alamat riil, seperti alamat internet, ke bentuk alamat internal). [5]

Analisis dan Perancangan DMZ :

1. Sebaran IP Baru dan Firewall dan memindahkan Layanan Web,
2. Menentukan perangkat keras pendukung, meliputi koneksi ADSL, implementasi Firewall, dan implementasi DMZ.
3. Implementai jalur ADSL dan Firewall PIX, Setelah perangkat keras tersedia, maka berikutnya adalah melakukan pemetaan alamat perangkat keras, misalnya: o ADSL – 209.15.20.34 o Ethernet0 pada ADSL – 192.1.10.5/30 (255.255.255.252) o Ethernet0 pada firewall PIX. Berikutnya dibangun translasi NAT untuk melakukan panggilan forward ke 192.168.10.6. Biarkan router menjadi data route, dan biarkan Firewall menentukan konfigurasi yang diperlukan untuk pengelolaan resiko
4. Instalasi dan konfigurasi pada DMZ,
5. Konfigurasi Chaining/PassThrough,
6. Alarm dan Tripwire,
7. Aktifkan Sistem. [5]

3.1 Proses De-Militarized Zone (DMZ)

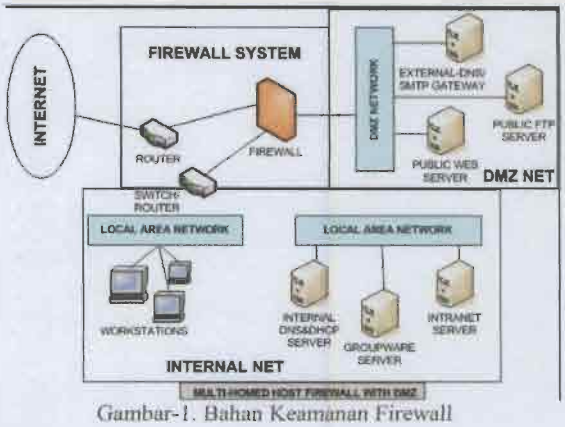
Proses dari De-Militariez Zone data dapat dijelaskan sebagai berikut :

1. Penetapan model keamanan firewall

Firewall adalah suatu sistem perangkat lunak yang menyediakan konektifitas dan mengimplementasikan aturan-aturan pada lalu lintas antar jaringan komputer baik internal maupun eksternal dengan tujuan mengamankan sistem.

Penerapan firewall untuk konsep DMZ dengan cara router atau komputer yang dilengkapi dengan NIC (Network Interface Card) membandingkan alamat sumber dari paket-paket yang masuk dengan aturan-aturan (kebijakan) yang sudah dibuat sebelumnya. Melakukan pengujian terhadap alamat IP atau nama domain yang menjadi sumber paket dan menentukan apakah hendak meneruskan atau menolak paket tersebut. Biarkan router menjadi data route, dan biarkan Firewall menentukan konfigurasi yang diperlukan. [5]

Selengkapnya dapat dilihat pada gambar 1



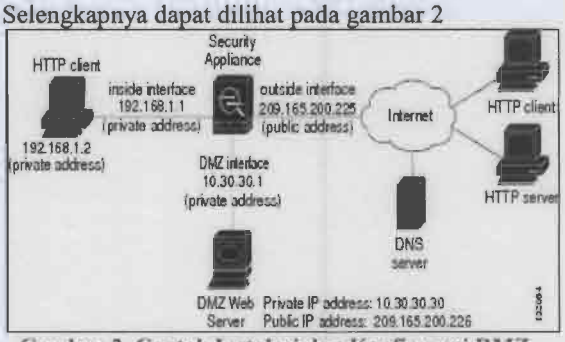
Gambar-1. Bahan Keamanan Firewall

2. Instalasi dan Konfigurasi

Konsep instalasi dan konfigurasi DMZ adalah sebagai berikut:

1. Tentukan subnet yang akan digunakan.
2. Tetapkan alamat-alamat IP sebaran yang akan digunakan (Firewall PIX : Konfigurasi dengan berbagai spesifikasi keamanan)
3. Lakukan redicate layanan DNS dari koneksi ADSL.
4. Lakukan konfigurasi antarmuka ethernet pada firewall PIX didalam jaringan internal.[5]

Selengkapnya dapat dilihat pada gambar 2



Gambar-2. Contoh Instalasi dan Konfigurasi DMZ

4. Konsep Enkripsi

Enkripsi merupakan sebuah cara untuk menjadikan data-data atau informasi tidak dapat dibaca oleh orang-orang yang tidak berhak. Data disandikan (encripted) dengan menggunakan sebuah kunci (key) dan untuk membuka (decrypt) data tersebut digunakan sebuah kunci yang sama dengan kunci untuk mengenskripsi (kasus private key cryptography) atau dengan kunci berbeda (kasus public key cryptography). Tujuan utama dari enkripsi adalah selain menyembunyikan data/informasi yang terkandung didalamnya juga untuk menjaga intergritas data/informasi pada saat ditransmisikan.

Type dasar dari enkripsi dapat dibagi menjadi :

1. Enkripsi Manual

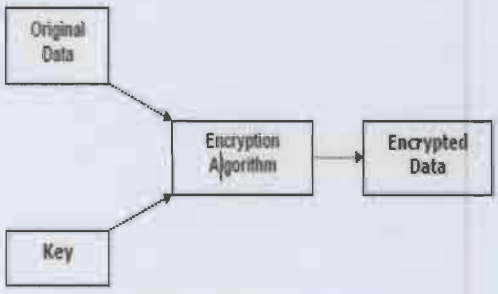
Enkripsi tipe ini sepenuhnya dilakukan oleh user dimana user harus memilih secara manual objek mana yang akan di enkripsi dan kemudian menjalankan command khusus untuk melakukan enkripsi dan deskripsi object tersebut.

2. **Enkripsi Semi-Transparant**
   Enkripsi jenis ini disebut juga enkripsi 'On-the-fly'. Enkripsi ini beroperasi tidak secara permanen, tapi sebelum dan sesudah akses dilakukan pada object-object rahasia atau ketika operasi read/write.
3. **Enkripsi Transparent**
   Enkripsi ini bisa dikatakan sebagai kebalikan dari enkripsi manual. Proses enkripsi dan deskripsi dilakukan pada level rendah, secara permanen, kertika semua operasi read/write, sehingga data yang dienkripsi selalu disimpan dalam bentuk enkripsi. Dari sisi prinsip-prinsip umum keamanan enkripsi jenis ini adalah tipe yang paling aman dan mudah. [3]

4.1 Proses Enkripsi

Cara kerja enkripsi dilakukan dengan menambahkan kode karakter teks sumber dengan teks kunci (script sorce code/algoritma). Membandingkan kunci/key yang sudah kita tentukan dengan data sumber dan lakukan perubahan.

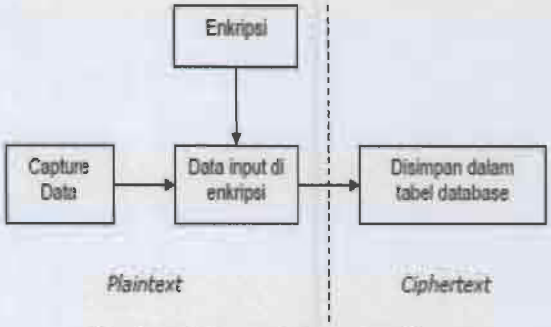
Proses dari sebuah enkripsi data dapat dilihat pada gambar 3.



Gambar-3. Proses Encryption Data

Dekripsi adalah kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (ciphertext) dikembalikan ke bentuk aslinya (Original Plaintext) sehingga dapat dibaca/ dimengerti kembali.

Proses dari sebuah dekripsi data dapat dilihat pada gambar 4.



Gambar-4. Process Decryption Data

4.2 Mekanisme Enkripsi Transparan

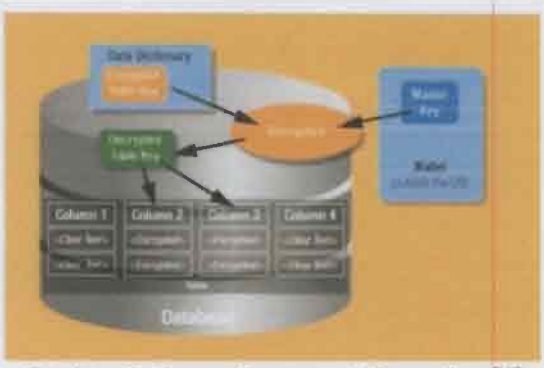
Transparent Data Encription adalah salah satu jenis enkripsi yang mempunyai keuntungan dalam kemudahan dari sisi pengelola atau pengguna, karena pengelola tidak perlu melakukan proses manajeman enkripsi dan deskripsi data secara manual, tetapi telah otomatis disertakan pada paket sistem basisdata yang digunakan.

Dengan data yang terenkripsi ini, jika data dalam disk dicuri, maka data yang terenkripsi ini tidak bisa diambil tanpa master key, yang berada didalam wallet dan bukan bagian dari data yang dicuri. Bahkan jika wallet nya dicuri, master key nya tidak bisa diambil dari wallet tanpa wallet password (mengenkripsi data sensitif dalam database dan menyimpan encription key nya dilokasi yang berbeda). Oleh karena itu, pencurinya tidak bisa mendekripsikan data, bahkan jika dia mencuri disk nya atau melakukan copy pada file data.

Untuk penerapannya diawali dengan proses pendefinisian sebuah kolom yang akan dienkripsi, setelah itu sistem database membuat sebuah encryption key yang aman secara kriptografikal untuk table yang berisi kolum tersebut dan mengenkripsi data input clear-text yang berada didalamnya, menggunakan suatu algoritma enkripsi yang akan digunakan. Menjaga table key ini sangat penting karena sistem database mengenkripsinya menggunakan sebuah master key dan menyimpannya disebuah lokasi yang aman, yang disebut dengan wallet, yang bisa berupa sebuah file pada database server.

Table key yang telah dienkripsi tersebut diletakkan disebuah data dictionary. Ketika seorang user memasukkan data ke sebuah kolom yang didefinisikan sebagai terenkripsi, sistem database mengambil master key dari wallet, mendekripsi encryption key untuk table tersebut dari data dictionary, menggunakan encryption key pada nilai input dan menyimpan data yang dienkripsi pada
database. [4]

Proses dari sebuah Tranparent Encription data dapat dilihat pada gambar 5.



Gambar -5. Konsep Transparent Encryption. [4]

4.3 Persamaan Matematika Enkripsi

Secara matematis proses atau fungsi enkripsi dapat dirumuskan sebagai berikut :

E(M) = C

Sedangkan untuk proses atau fungsi deskripsi dapat dirumuskan sebagai berikut :

D(C) =M

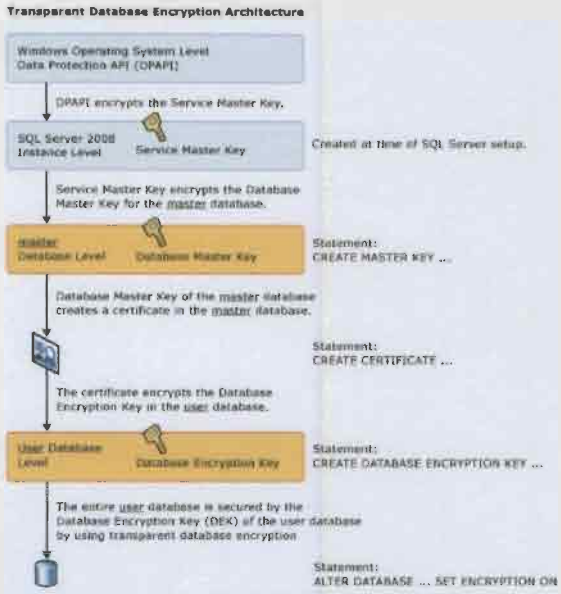
Keterangan:

E = Encription
D = Decription
M = Plain text
C = Chiper text

5. Penggabungan Konsep Enkripsi dan DMZ

Diawali dengan pengembangan keamanan disisi jaringan dengan menerapkan konsep DMZ yang merupakan penerapan keamanan level-2, sebenarnya dengan penerapan konsep DMZ ini keamanan sudah dibuat cukup aman dari sisi lalulintas data pada sistem jaringan karena penyusup dibuat hanya akan dapat masuk ke jalur bayangan, namun dikarenakan keamanan itu tidak hanya bisa dari sisi jaringan saja dibutuhkan keamanan secara berlapis, maka dari itu konsep selanjutnya adalah pengamanan dari sisi database dengan menggunakan konsep enkripsi transparent, keamanan type ini jika dilihat dari metodologi merupakan konsep keamanan level-1 (keamanan dari sisi database). Model kemanan transparan enkripsi diterapkan setelah melalui tahapan pengkajian beberapa metode keamanan dilihat dari kemudahan, keunggulan dan kesesuaian dengan sistem yang berjalan, maka ditetapkan model kemanan transparan enkripsi yang paling sesuai untuk sistem yang berjalan saat ini.

Untuk penerapan enkripsi transparansi disini menggunakan SQL server. Proses Transparansi Encription dari sebuah Tranparent Encription data dapat dilihat pada gambar 6.

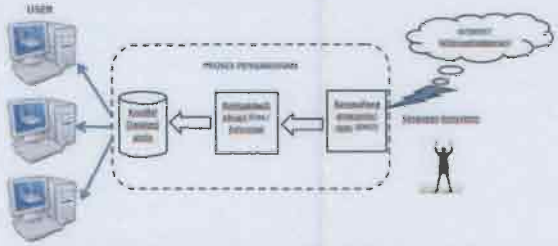


Gambar -6. Transparent Database Encryption Architecture (SQL Server 2008)

Konsep DMZ dan transparan enkripsi selanjutnya dapat dipandang sebagai gabungan proses-proses yang saling melengkapi dan berjalan bersamaan, DMZ dari sisi jaringan dan transparan enkripsi dari segi keamanan data pada database.

Secara metodologi keamanan sistem, ada beberapa aspek yang wajib diamankan yaitu aspek keamanan data/informasi dan lalulintas data nya, dan dengan menggabungkan kedua kosep Encripsi dan pengamanan jaringan dengan konsep DMZ keamanan telah dibuat berlapis. Pengembangan dilakukan pada level-1 dan level-2 yang secara otomatis keamanan di level-3 akan terpenuhi. Jika kita mengacu pada metodologi keamanan maka bisa dikatakan sudah baik karena keamanan level-0 sampai dengan level-4 telah terpenuhi.

Pada akhirnya konsep menyeluruh dari enkripsi data DMZ (keamanan Level 0-4) dapat digambarkan dengan gambar 7.



Gambar-7. Konsep Keamanan Sistem DMZ dan Enkripsi Data

6. Kesimpulan

DMZ adalah konsep untuk keamanan dari sisi jaringan dalam sebuah sistem, tugasnya adalah melindungi aliran data/infomasi pada sistem agar

tidak terganggu dan tidak disusupi oleh pihak-pihak yang tidak berkepentingan / tidak bertanggung jawab atau menggunakan resource bandwid yang dimiliki sehingga kondisi aliran data menjadi lambat. konsep DMZ dapat memblokir semua serangan yang masuk kedalam sistem dengan cara memotong jalur komunikasi pada jaringan internal. Sehingga jika penyerang bermaksud menyerang dan melakukang penyusupan/perusakan pada server yang mempunyai DMZ, haker tersebut dapat mengakses host yang berada pada DMZ tapi tidak bisa masuk pada jaringan internal.

Apabila dengan konsep DMZ tetap dapat ditembus maka data yang berjalan didalam sistem sudah terenkripsi sehingga data/informasi dapat terlindungi karena tidak mungkin bisa terbaca oleh pihak-pihak yang tidak berkepentingan, dan kelebihan dari transparent enkripsi ini adalah jika media fisik tercuri pun maka pencuri mungkin mendapatkan fisiknya namun data tetap tidak bisa terbaca tanpa adanya key.

Sehingga sudah bisa dikatakan performansi dari sistem dapat berjalan dengan baik jika kita menggunakan penggabugan kedua konsep diatas karena secara metodologi konsep keamanan sistem informasi yang diutamakan adalah level 1-3 yaitu dari sisi database, keamanan data, keamanan jaringan dan keamanan informasi-nya dimana ke ketiga level ini sudah mengcover dua level lainnya (level 0 dan 4) sehingga dengan penggabungan kedua konsep tersebut sudah dapat mengcover hal-hal tersebut. Karena Dengan diterapkannya kedua konsep tersebut (Encriptyon dan DMZ) kita dapat meminimalisasi dari segi kebocoran data/infomasi dan menjaga agar lalu lintas data berjalan tetap stabil dan performansi dari sistem dapat terjamin karena pergerakan para pihak-pihak yang tidak berkempentingan seperti Hacker/Craker pun dapat dihambat.

Performansi sebuah keaman system memang bisa kita modifikasi namun perlu menjadi catatan tidak ada semuah keamanan yang benar-benar fix dan menjamin untuk mengamankan suatu jaringan atau data. Keamanan adalah suatu proses, bukan produk. Jika kita memasang firewall, IDSes (intrusion detection system), router, honeypots (system untuk jebakan) dan enkripsi data mungkin dapat menyediakan lapisan-lapisan untuk bertahan, tetapi sekali lagi peralatan paling canggih pun tidak akan menolong suatu organisasi sampai organisasi tersebut mempunyai proses untuk mengupgrade sistem, mengecek security pada sistem sendiri.

Jalan terbaik untuk melindungi data/informasi maupun jaringan dari serangan adalah dengan melakukan pendekatan dan menjadikan keamanan sebagai tantangan terhadap pengembangan dari sistem yang berjalan.

7. Acknowledgements

Saya ucapkan terima kasih kepada semua pihak yang telah membantu dan memberikan dukungan selama ini sehingga saya dapat menyelesaikan paper dengan judul 'Memaksimalkan Kemanan Sistem dengan Konsep Encription dan Demilitaries Zone (DMZ)", khususnya kepada Jurusan Teknik Informatika UNPAS dan umumnya kepada semua rekan-rekan seperjuangan yang sudah memberikan masukan-masukan dan untuk semua para penulis yang tertera di daftar pustaka yang telah berbagi ilmu dengan menguplod apa yang mereka pahami diinternet sehingga dapat membantu saya dalam membuat paper ini.

Daftar Pustaka:

[1] Indrajit, R.E., 2000, Pengantar Konsep Dasar Manajemen Sistem Informasi dan Teknologi Informasi,
[2] Mesran S.Kom, Diktat:KBMI3523-Keamanan Komputer.
[3] Antonius QWahyu Sudrajat, 2006, Implementasi Enkripsi data base Menggunakan Transparant Data Encription pada Database Engine Oracle
[4] khafit fauzika, 2011, http://ndolietz.blogspot.com/2011/12/enkripsi-database-menggunakan.html
[5] http://artikel-jaringan.blogspot.com/2011/12/konsep-dasar-demilitarised-zone-dmz.html