JOURNAL
TICOM
TECHNOLOGY OF INFORMATION AND COMMUNICATION

Vol. 8 No. 3, Mei 2020 ISSN : 2302-3252

ASOSIASI PERGURUAN TINGGI INFORMATIKA & ILMU KOMPUTER
(APTIKOM) WILAYAH 3

Sekretariat Redaksi :
Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp. 021.5853753 Fax .021.5869225

JURNAL ILMIAH
TICOM

Jurnal TICOM adalah jurnal ilmiah dalam bidang teknologi informasi dan komunikasi (TIK) yang diterbitkan oleh Asosiasi Perguruan Tinggi Informatika dan Ilmu Komputer (Aptikom) wilayah 3. *Jurnal TICOM* terbit 3 kali dalam satu tahun yaitu: September, Januari dan Mei

Pelindung:
Ketua APTIKOM Wilayah 3:
Mochamad Wahyudi, M.M., M.Kom., M.Pd.
(STIMIK Nusa Mandiri)

Ketua Dewan Redaksi:
Dr. Ir. Nazori AZ, MT (Universitas Budi Luhur)

Redaksi Pelaksana:
Dra. Andiani, M.Kom (Universitas Pancasila)
Ina Agustina, S.Si, S.Kom, MMSI (Universitas Nasional)
Dwiza Riana, S.Si, MM, M.Kom (STMIK Nusa Mandiri)
Nani Tachjar, S.Kom, MT (ABFI Institute Perbanas)
I.G.N. Mantra, M.Kom (ABFI Institute Perbanas)
Muhaemin, MM, M.Kom (STMIK Indonesia)

Mitra Bestari:
Prof. Jazi Eko Istiyanto, Ph.D (Universitas Gadjah Mada)
Prof. Iping Supriana Suwardi (Institut Teknologi Bandung)
Prof. Dr. Ir. Richardus Eko Indrajit, M.Sc (ABFI Institute Perbanas)
Prof. Dr. Djoko Lianto Buliani (ITS Surabaya)
Prof. Dr. Zainal Hasibuan (Universitas Indonesia)

Dewan Editor:
Benfano Soewito, ST, M.Sc, Ph.D (Universitas Bakrie)
Dr. Iskandar Fitri, ST, MT (Universitas Nasional)
Muhammad Agni Catur Bhakti, ST, MSc, Ph.D (Universitas Pancasila)
Dr. Manik Haspara, M.Kom (Universitas Bakrie)
Prof. Marsudi Wahyu Kisworo, Ph.D (ABFI Institute Perbanas)
Prof. Dr. Ir. Kaman Nainggolan, MS (STMIK Nusa Mandiri)
Dr. Rusdah, S.Kom, M.Kom (Universitas Budi Luhur)

Sekretariat Redaksi:
Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Email: jurnalticom@yahoo.co.id
nazori@budiluhur.ac.id

JURNAL ILMIAH
TICOM

Editorial

Puji dan syukur kehadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya jurnal ilmiah "TICOM" ini dapat diterbitkan. Penerbitan jurnal ilmiah ini diharapkan dapat menjadi wadah bagi akademisi dan praktisi untuk menuangkan ide-ide dan pembahasan seputar isu-isu di bidang Teknologi Informasi dan Komunikasi (TIK).

Penerbitan jurnal TICOM edisi ini adalah merupakan penerbitan Vol. 8 No. 3 Mei 2020, yang memuat 7 paper dari berbagai perguruan tinggi yang merupakan hasil penelitian dan kajian ilmiah. Topik jurnal edisi ini memuat:

1. Implementasi Sensor Fingerprint Smartphone Android dan Mikrokontroler NODE MCU dalam Mengamankan Kendaraan
2. Perencanaan Strategis Sistem Informasi Studi Kasus Politeknik LP3i Kampus Pasar Minggu
3. Rivest Code 4 dan Kompresi Huffman Pada Aplikasi Pengamanan Data Berbasis Web
4. Pemodelan dan Estimasi Cadangan Klaim Menggunakan Metode GEE (Generalized Estimazing Equations) Pada Perusahaan Asuransi PT XYZ
5. Penerapan Algoritma RC6 dan Vigenere pada Aplikasi SMS berbasis Android
6. Aplikasi Penerimaan Karyawan Dengan Metode Analitycal Hierarchy Process (AHP) Berbasis Web Pada PT Kinarya Alihdaya Mandiri
7. Implementasi Algoritma Vigenere Cipher dan Steganografi Least Significant Bit Untuk Mengamankan File Vigenere Chiper Algorithm and Least Significant Bit Steganography Implementation for Securing File

Sebagai penutup, kami selaku tim redaksi ingin mengucapkan terima kasih kepada berbagai pihak yang banyak membantu sehingga terbitnya jurnal TICOM Vol. 8 No. 3, Mei 2020 ini. Tak lupa pula kami mengucapkan terima kasih kepada para penulis yang telah bersedia menyumbangkan karya tulisnya dari mulai tahapan *reviewer*, *editing* sehingga "*camera ready paper*" sesuai dengan aturan yang telah ditetapkan jurnal TICOM.

Jakarta, Mei 2020

Tim Redaksi

JURNAL ILMIAH
TICOM

Daftar Isi

Implementasi Sensor Fingerprint Smartphone Android dan Mikrokontroler NODE MCU dalam Mengamankan Kendaraan

Rizky Tahara Shita[1)], Lauw Li Hin[2)]

[1,2)] Universitas Budi Luhur, Fakultas Teknologi Informasi,
Jl. Ciledug Raya. Petukangan Utara. Jakarta Selatan, Jakarta, 12260
Telp: (021) 5853753, HP: +6285716483190 [1)], +628129743900 [2)]
rizky.taharashita@budiluhur.ac.id [1)], lihin@budiluhur.ac.id [2)]

ABSTRAK — Kendaraan bermotor merupakan sebuah alat transportasi yang banyak dibutuhkan setiap orang, dimana dengan menggunakan kendaraan bermotor kita dapat menuju suatu tempat atau lokasi dengan cepat. Pada saat ini sistem keamanan kendaraan yang diberikan oleh perusahaan masih dirasa belum cukup untuk membuat kendaraan menjadi aman, sehingga masih banyak tindakan kriminal seperti pencurian kendaraan bermotor. Dibutuhkan sebuah cara agar pemilik dapat mengetahui kondisi dan keberadaan kendaraannya dengan mudah dan hal ini dapat dibantu dengan adanya penerapan teknologi yang dapat disematkan pada kendaraan dan aplikasi yang dipasang pada Smartphone, sehingga kemudahan bagi pemilik kendaraan untuk dapat mengetahui informasi dan keberadaan kendaraannya dapat menjadi salah satu tambahan tingkat keamanan yang dapat diimplementasikan agar pemilik dapat merasa lebih tenang saat meninggalkan kendaraannya karena dapat dipantau secara realtime. Pemanfaatan sensor fingerprint dapat juga digunakan untuk menambah tingkat keamanan dengan menerapkannya pada saat menyalakan maupun mematikan mesin kendaraan, sehingga tingkat keamanan tidak saja hanya menggunakan kunci kendaraan yang biasa digunakan pada umumnya.

Kata kunci: keamanan, internet of things, fingerprint

ABSTRACT — Motorized vehicle is a transportation tool that is needed by everyone, where by using motorized vehicles we can go to a place or location quickly. At this time the vehicle safety system provided by the company is still considered insufficient to make the vehicle safe, so there are still many criminal acts such as motor vehicle theft. A way is needed so that the owner can know the condition and whereabouts of his vehicle easily and this can be helped by the application of technology that can be embedded in the vehicle and the application installed on the Smartphone, so that the ease for the vehicle owner to be able to know the information and the whereabouts of his vehicle can be one an additional level of security that can be implemented so that the owner can feel calmer when leaving his vehicle because it can be monitored in real time. Utilization of a fingerprint sensor can also be used to increase the level of security by applying it when turning on or turning off a vehicle's engine, so the level of security does not only use vehicle keys that are commonly used in general.

Keywords: security, internet of things, fingerprint

I. PENDAHULUAN

I.1. Latar Belakang

Pada saat sekarang ini kendaraan bermotor merupakan sebuah alat transportasi yang banyak dibutuhkan setiap orang, dimana dengan menggunakan kendaraan bermotor kita dapat menuju suatu tempat atau lokasi dengan cepat. Di Indonesia sendiri pembelian kendaraan bermotor setiap tahunnya mengalami kenaikan. Berdasarkan surat berita elektronik kompas.com tanggal 28/04/2018, penjualan di pasar wholesaler industri otomotif roda empat, menuai hasil positif 2,87 persen di kuartal pertama 2018; ketika membandingkannya dengan perolehan periode yang sama pada tahun lalu. Dari data Gabungan Industri Kendaraan Bermotor Indonesia (Gaikindo), total perolehan pada tiga bulan pertama 2018 ini mencapai 291.912 unit. Sementara tahun lalu hanya mencapai 283.760 unit saja. (https://otomotif.kompas.com). [12]

Salah satu dealer yang mendukung meningkatnya pemasaran kendaraan bermotor adalah PT. Astrido Daihatsu cabang Kebon Jeruk yang merupakan sebuah dealer tempat penjualan dan service kendaraan bermotor khususnya roda empat. Pada saat ini, sistem keamanan kendaraan yang diberikan oleh perusahaan kendaraan bermotor masih dirasa belum cukup untuk membuat kendaraan menjadi aman; dapat terlihat dari banyaknya kasus pencurian kendaraan bermotor khususnya daerah DKI Jakarta membuat banyak pemilik kendaraan merasa takut atau was-was untuk meninggalkan kendaraannya dimana saja. Kehilangan kendaraan terjadi disebabkan karena

pemilik kendaraan tidak memiliki sistem keamanan kendaraan tambahan yang dapat menjaga kendaraan dari aksi pencurian, selain tidak memiliki sistem keamanan kendaraan tambahan, pemilik kendaraan juga tidak memiliki sebuah informasi yang diterima mengenai kondisi kendaraan sebelum kendaraan miliknya hilang dicuri, dan pemilik kendaraan juga tidak memiliki sebuah alat yang dapat mendeteksi keberadaan kendaraan setelah hilang dicuri yang menyebabkan kendaraan sulit ditemukan.

I.2. Masalah

Dari latar belakang tersebut, terdapat masalah yang terjadi; yaitu:

- Dibutuhkan cara agar dapat mencegah terjadinya aksi pencurian kendaraan bermotor.
- Dibutuhkan sebuah cara agar pemilik kendaraan dapat mengetahui jika terjadi indikasi pencurian pada kendaraan miliknya.
- Dibutuhkan oleh pemilik kendaraan untuk dapat mengetahui lokasi kendaraan secara realtime dengan mudah.
- Bagaimana cara memberikan tambahan keamanan pada kendaraan bermotor agar dapat mengatasi permasalahan yang dipaparkan sebelumnya.

I.3. Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

- Agar dapat meminimalisir terjadinya aksi pencurian kendaraan bermotor dengan memberikan informasi kepada pemilik kendaraan terhadap kendaraannya jika terindikasi aksi pencurian.
- Informasi yang disajikan memudahkan pemilik hanya melalui aplikasi pada Smartphone, baik dalam hal pemantauan lokasi kendaraannya secara realtime maupun informasi lainnya terkait dengan keamanan tambahan pada kendaraannya.
- Menyediakan tambahan pengamanan berupa pemanfaatan sidik jari melalui aplikasi yang dapat diakses melalui Smartphone.

I.4. Batasan Masalah

Agar penelitian ini tidak keluar dari pembahasan maka diperlukan ruang lingkup masalah, yaitu:

- Penambahan keamanan pada kendaraan bermotor memanfaatkan sensor sidik jari (fingerprint) yang ada pada Smartphone melalui mikrokontroler NodeMCU dan GPS untuk memantau lokasi kendaraan secara realtime serta sensor SW-420 untuk pendeteksi getar yang berfungsi sebagai pendeteksi dini terhadap aksi pencurian.
- Pemanfaatan internet sebagai media penyaluran informasi terhadap kendaraan yang dipantau agar pemilik dapat mengetahui informasi tentang kondisi kendaraannya melalui aplikasi pada Smartphone nya.

II. Landasan Teori

II.1. Kendaraan Bermotor

Kendaraan bermotor adalah kendaraan yang digerakkan oleh peralatan teknik untuk pergerakannya, dan digunakan untuk transportasi darat. Umumnya kendaraan bermotor menggunakan mesin pembakaran dalam (perkakas atau alat untuk menggerakkan atau membuat sesuatu yg dijalankan dengan roda, digerakkan oleh tenaga manusia atau motor penggerak, menggunakan bahan bakar minyak atau tenaga alam). Kendaraan bermotor memiliki roda, dan biasanya berjalan di atas jalanan. [7]

II.2. Internet of Things

Internet of Things, atau dikenal juga dengan singkatan IoT; merupakan sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus-menerus. Secara singkat Internet of Things dapat dikatakan sebagai sebuah konsep dari benda – benda disekitar yang mampu berkomunikasi dan berbagi data antara satu sama lain melalui sebuah jaringan seperti internet. [3]

II.3. Fingerprint (Sidik Jari)

Secara umum sidik jari (fingerprint) adalah hasil reproduksi tapak jari baik yang sengaja diambil, dicapkan dengan tinta, maupun bekas yang ditinggalkan pada benda karena pernah tersentuh kulit telapak tangan atau kaki. [1]

Pola sidik jari selalu ada dalam setiap tangan dan bersifat permanen, pola sidik jari yang dimiliki mulai dari bayi hingga orang dewasa tidak akan pernah berubah. Setiap jari memiliki pola sidik jari yang berbeda. Bentuk Pokok Sidik ada tiga bentuk sidik jari yaitu busur (arch), sangkutan (loop), dan lingkaran (whorl). [9]

Gambar 1: Bentuk Pokok Sidik Jari

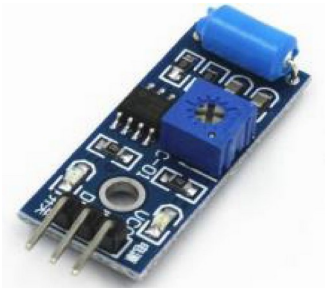
II.4. NodeMCU

NodeMCU pada dasarnya adalah pengembangan dari ESP8266 dengan firmware berbasis e-Lua. Pada NodeMCU dilengkapi dengan micro usb port yang berfungsi untuk pemrograman maupun power supply. Selain itu juga pada NodeMCU dilengkapi dengan tombol push button yaitu tombol reset dan flash. NodeMCU menggunakan bahasa pemrograman Lua yang merupakan package dari esp8266. Bahasa Lua memiliki logika dan susunan pemrograman yang sama dengan bahasa pemprograman C, hanya berbeda syntax nya saja. [13]

Gambar 2: NodeMCU Esp8266 v3

II.5. Sensor Getar

Modul sensor digital ini akan menghasilkan keluaran logika high pada saat mendeteksi getaran, dapat diaplikasikan pada sistem keamanan,deteksi gempa, pendeteksi malfungsi pada sistem mekanik, analisa struktur konstruksi berdasarkan vibrasi, pengukuran kekuatan tumbukan secara tidak langsung, dsb. [8]



Gambar 3: Sensor Getar SW-420

II.6. GPS Neo 6MV2

GPS adalah sistem navigasi yang menggunakan satelit yang didesain agar dapat menyediakan posisi secara instan, kecepatan dan informasi waktu di hampir semua tempat di muka bumi, setiap saat dan dalam kondisi cuaca apapun. [4]

Sedangkan alat untuk menerima sinyal satelit yang dapat digunakan oleh pengguna secara umum dinamakan GPS Tracker atau GPS Tracking, dengan menggunakan alat ini maka dimungkinkan user dapat melacak posisi kendaraan, armada ataupun mobil dalam keadaan Real-Time. [9]

Gambar 4: Modul GPS Neo 6v M2

II.7. Android

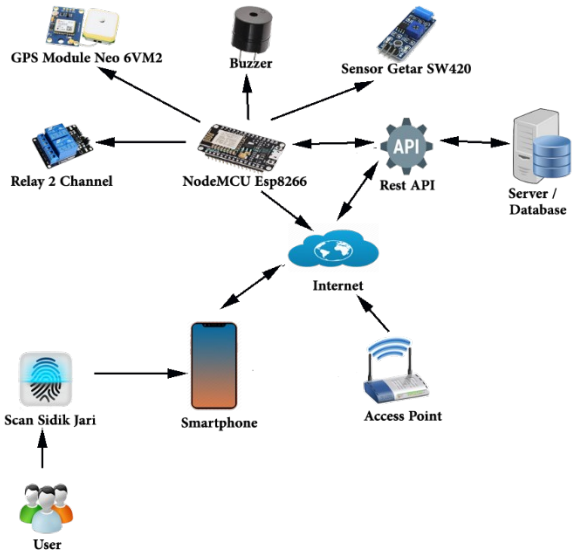
Menurut Safaat (2012:1), Android adalah sistem operasi berbasis Linux bagi telepon seluler seperti telepon pintar dan komputer tablet. Android juga menyediakan platform terbuka (open source) bagi para pengembang untuk menciptakan aplikasi mereka sendiri yang akan digunakan untuk berbagai macam piranti gerak.

III. Perancangan Aplikasi

III.1. Rancangan Aplikasi

III.1.1. Prinsip Kerja

Prinsip kerja dari aplikasi keamanan kendaraan dengan menggunakan sidik jari dengan android berbasis IoT (Internet of Things) ini, dapat bekerja jika rangkaian elektronik yang dibuat dengan menggunakan mikrokontroler NodeMCU Esp8266 ini terhubung dengan jaringan internet, kemudian rangkaian elektronik tersebut berkomunikasi dengan server atau database melalui ReST API, komunikasi ini bertujuan untuk menyimpan data dari sensor dan membaca data dari database atau server sebagai inputan untuk mikrokontroler NodeMCU Esp8266 agar dapat memberi perintah kepada komponen atau sensor yang terhubung dengan mikrokontroler untuk proses keamanan pada kendaraan.



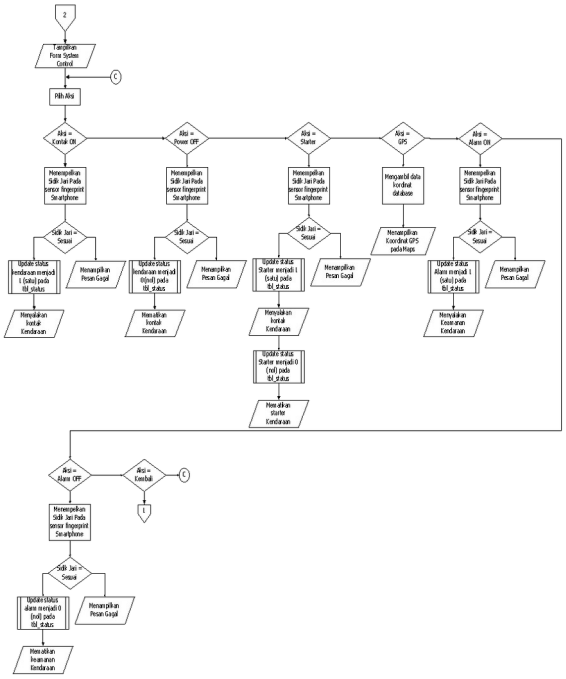
Gambar 5: Arsitektur Rancangan Aplikasi

III.1.2. Cara Kerja

Aplikasi keamanan kendaraan bermotor menggunakan sidik jari dengan konsep IoT (Internet of Things) ini dapat dijalankan dengan menggunakan sebuah perangkat smartphone android. Agar dapat menggunakan aplikasi keamanan kendaraan ini, perangkat smartphone harus terhubung dengan jaringan internet, jaringan internet diperlukan untuk menghubungkan atau untuk saling berkomunikasi dengan server, begitu pula dengan rangkaian alat yang telah dibuat rangkaian tersebut harus terhubung dengan jaringan internet agar data yang diperoleh mikrokontroler dari sensor yang terpasang dapat disimpan terutama untuk sensor GPS. Aplikasi keamanan kendaraan menggunakan sidik jari ini juga dapat memberikan sebuah notifikasi melalui email kepada pemilik kendaraan apabila kendaraan tersebut terjadi sesuatu pada saat keamanan kendaraan diaktifkan. Aplikasi keamanan kendaraan ini memiliki 3 buah menu utama yaitu menu system control, menu setting email dan terakhir adalah menu setting wifi. Untuk menggunakan aplikasi keamanan kendaraan ini pada tahap pertama user atau pengguna aplikasi harus menghubungkan terlebih dahulu rangkaian elektronik dengan jaringan internet yaitu dengan cara menghubungkan rangkaian elektronik dengan perangkat smartphone android melalui USB OTG, kemudian masuk kedalam menu setting wifi, selanjutnya masukkan nama wifi yang tersedia berikut dengan passwordnya kemudian simpan, jika berhasil terhubung maka rangkaian elektronik akan menampilkan IP Address pada perangkat smartphone. Setelah itu setting alamat email user atau pengguna aplikasi sebagai pemilik kendaraan pada menu setting email, alamat email ini berfungsi untuk mengirimkan notifikasi keamanan kendaraan kepada pemilik kendaraan. Dan yang terakhir adalah menu system control dimana pada menu ini seluruh kendali kendaraan dapat dilakukan seperti menghidupkan kontak kendaraan, mematikan kontak kendaraan, menghidupkan starter kendaraan, serta menghidupkan dan mematikan alarm sebagai sistem keamanan kendaraan. Pada menu system control ini juga terdapat menu GPS, menu GPS ini berfungsi untuk menampilkan letak lokasi kendaraan berdasarkan koordinat GPS yang ditampilkan pada sebuah maps.

III.1.3. Flowchart System Control

Flowchart Sistem Kontrol menggambarkan alur proses yang menampilkan sebuah form yang digunakan untuk mengendalikan atau mengontrol sistem kelistrikan kendaraan dengan menggunakan smartphone android. Adapun sistem yang dapat dikendalikan adalah untuk menghidupkan kelistrikan kendaraan, menghidupkan mesin kendaraan, dan menghidupkan alarm kendaraan dengan menggunakan fingerprint dari pemilik smartphone.



Gambar 6: Flowchart System Control

IV. Hasil Implementasi dan Analisa Program

IV.1. Implementasi

IV.1.1. Pemasangan Rangkaian Alat

Untuk pemasangan rangkaian alat yang telah dibuat pada sebuah kendaraan yaitu dengan cara menyambungkan atau

menghubungkan NodeMCU Esp8266 dengan sumber daya 5V yang berasal dari sebuah AKI yang telah diturunkan tegangannya terlebih dahulu untuk menjadi 5V DC, ini berfungsi untuk memberikan sumber listrik yang digunakan oleh mikrokontroler NodeMCU Esp8266, setelah itu hubungkan kabel kontak dan starter kendaraan pada relay yang tersedia. Berikuti ini adalah gambar dari pemasangan rangkaian alat pada sebuah prototipe kendaraan.

Gambar 7: Prototype Kendaraan

IV.1.2. Tampilan Layar Aplikasi pada Smartphone Android

Tampilan layar merupakan sebuah tampilan dari sebuah aplikasi yang telah dibuat, pada tampilan layar aplikasi ini, akan dijelaskan tentang semua proses tampilan layar dari sebuah aplikasi keamanan kendaraan menggunakan sidik jari berbasis android yang dijalankan dari awal aplikasi dibuka sampai dengan aplikasi selesai dijalankan.

Gambar 8: Menu pada Aplikasi

IV.1.3. Uji Kasus

Pengujian aplikasi merupakan sebuah tahap terakhir dalam pembuatan aplikasi, sebelum aplikasi benar-benar dirilis dan dapat digunakan oleh setiap orang. Pengujian aplikasi ini dilakukan untuk melihat apakah aplikasi masih terdapat kesalahan pada saat dijalankan dan melihat apakah aplikasi dapat berjalan dengan baik. Serta pada pengujian aplikasi ini bertujuan untuk melihat rangkaian alat apakah rangkaian alat yang telah dibuat dengan sensor-senor dapat menerima perintah dengan baik dari aplikasi, dan melihat apakah aplikasi dan rangkaian alat menghasilkan output yang sesuai dengan apa yang diharapkan. Berikut ini adalah proses-proses dari pengujian aplikasi sistem keamanan kendaraan dengan menggunakan sidik jari berbasis android yang telah dibuat.

IV.1.4. Kelebihan dan Kekurangan Program

IV.1.4.1. Kelebihan Program

- Aplikasi yang dibuat berbasis android atau mobile sehingga dapat digunakan dengan efisien tanpa perlu menggunakan laptop atau komputer.
- Aplikasi sudah berkonsep dengan IoT (Internet of Things) sehingga dapat di akses dari mana saja.
- Aplikasi keamanan kendaraan dengan menggunakan sidik jari.
- Rangkaian alat dapat memberikan notifikasi kepada pemilik kendaraan jika terjadi sesuatu pada kendaraan.
- Tampilan aplikasi mudah dipergunakan oleh user atau pengguna aplikasi.
- Dapat mengetahui lokasi kendaraan secara realtime.

IV.1.4.2. Kekurangan Program

- Untuk menghubungkan rangkaian alat dengan jaringan internet masih dengan menggunakan komunikasi serial.
- Belum dapat mengirim email notifikasi lebih dari satu penerima.
- Aplikasi belum mampu mendeteksi kerusakan pada sensor.
- Belum dapat menyimpan rute perjalanan kendaraan.
- Sidik jari yang dibaca masih pada database perangkat smartphone.

V. PENUTUP

V.1. Kesimpulan

Kesimpulan yang dapat ditarik dari adanya permasalahan hingga solusi yang diberikan antara lain adalah:

- Aplikasi dapat dijalankan pada smartphone yang memiliki operating system android yang memiliki sensor sidik jari.
- Dapat mengontrol sistem kendaraan dari jarak yang jauh.
- Aplikasi dapat menampilkan koordinat GPS secara realtime.
- Sistem keamanan pada aplikasi dilakukan dengan menggunakan sidik jari.
- Prototype kendaraan menggunakan mobilan remote control.
- Letak koordinat kendaraan didapat dari modul GPS Neo VM2, yang terhubung dengan satelit.
- Aplikasi dapat mendeteksi getaran dengan menggunakan sensor getaran SW 420.
- Untuk simulasi menghidupkan dan mematikan kendaraan serta mengaktifkan sistem dan mematikan sistem keamanan menggunakan Lampu LED.
- Relay digunakan untuk mengontrol kelistrikan dari kendaraan.
- Sensor sidik jari memanfaatkan dari smartphone android.
- Rangkaian alat dapat memberikan notifikasi kepada pemilik kendaraan melalui sebuah email.

V.2. Saran

Dengan keterbatasan yang ada dalam mengembangkan aplikasi, maka beberapa saran untuk pengembangan berikutnya adalah:

- Aplikasi dapat dijalankan pada perangkat smartphone yang memiliki operating system android.
- Diharapkan pengembang selanjutnya dapat menampilkan rute dari perjalanan kendaraan.
- Diharapkan pengembangan selanjutnya sidik jari dapat tersimpan pada database.
- Rangkaian alat dapat diperkecil sehingga memudahkan untuk pemasangan di tempat yang tersembunyi.
- Diharapkan Aplikasi dapat menampilkan indikator kerusakkan sensor yang digunakan.

DAFTAR PUSTAKA

[1] Belsazar Elgiborado Giovani Djoedir, dkk. (2018) Pengembangan Teknologi Informasi dan Ilmu Komputer, Implementasi Low Power Mode Pada Sistem Keamanan Ignition Coil Breaker Sepeda Motor dengan Pengenalan Sidik Jari, Jurnal: Vol. 2, No. 11

[2] Eni Yuliza, dan Toibah Umi Kalsum(2015) Media Infotama, ALAT KEAMANAN PINTU BRANKAS BERBASIS SENSOR SIDIK JARI DAN PASSWORD DIGITAL DENGAN MENGGUNAKAN MIKROKONTROLER ATMEGA 16, Jurnal: Vol. 11 No. 1

[3] Erwan Eko Prasetiyo. (2017) Teknika STTKD, APLIKASI INTERNET OF THINGS (IoT) UNTUK PEMANTAUAN DAN PENGENDALIAN BEBAN LISTRIK DI RUANGAN, Jurnal: Vol.4, No. 2

[4] Fatmah Rizkidiniah, dkk. (2016) semanTIK, PERANCANGAN DAN IMPLEMENTASI PROTOTYPE SISTEM GPS (GLOBAL POSITIONING SYSTEM) DAN SMS GATEWAY PADA PENCARIAN KENDARAAN BERMOTOR BERBASIS ARDUINO UNO , Jurnal: Vol.2, No.2

[5] Hariandi Maulid dan Entik Insanudin, (2018) e-Proceeding of Applied Science, “DyD (Don’t You Dare) : Perangkat yang Berfungsi Sebagai Alat Pencegah Tindak Pencurian Berbasis IoT ”, Jurnal: Vol.4, No.3

[6] Joyner R. Oroh, dkk. (2014) e-Journal Teknik Elektro dan Komputer, Rancang Bangun Sistem Keamanan Motor Dengan Pengenalan Sidik Jari.

[7] Muhammad Yusuf Afandi, dkk. (2017) Prosiding SNATIF, MINIMUM SYSTEM BERBASIS MIKROKONTROLER ATMEGA32 BERBANTUAN SENSOR PASSIVE INFRARED RECEIVER DAN FINGERPRINT UNTUK SISTEM PENGAMANAN KENDARAAN BERMOTOR RODA EMPAT ATAU LEBIH.

[8] Mohammad Hafiz Hersyah, dkk. (2018) TEKNOIF, Penerapan Face Recognition Pada Sistem Starter Mobil Otomatis Menggunakan Metode Eigenface Berbasis Mini PC, Jurnal: Vol. 6 No. 2

[9] Riyan Rahardi, dkk. (2018) PERANCANGAN SISTEM KEAMANAN SEPEDA MOTOR DENGAN SENSOR FINGERPRINT, SMS GATEWAY, DAN GPS TRACKER

BERBASIS ARDUINO DENGAN INTERFACE WEBSITE, Jurnal: Volume 06, No. 03

[10] Suharijanto dan Affan Bachri. (2018) Rancang Bangun Sistem Keamanan Sepeda Motor Dengan Fingerprint Berbasis Telephone,

[11] Muhammad Yusuf Afandi, dkk. (2017) Prosiding SNATIF, MINIMUM SYSTEM BERBASIS MIKROKONTROLER ATMEGA32 BERBANTUAN SENSOR PASSIVE INFRARED RECEIVER DAN FINGERPRINT UNTUK SISTEM PENGAMANAN KENDARAAN BERMOTOR RODA EMPAT ATAU LEBIH , JE-Unisla, Vol 3 No 2 83

[12] Sumantri K. Risandriya dan Alan Burhannudin (2017) OF APPLIED ELECTRICAL ENGINEERING, Optimalisasi Identifikasi Sidik Jari Menggunakan Metode Neural network pada Sistem Keamanan Sepeda Motor. Journal: Vol. 1, No. 1

[13] https://otomotif.kompas.com/read/ 2018/08/31/072200015/rapor-wholesales-mobil-di-januari-juli-2018. (diakses 12 oktober 2018)

[14] https://escapequotes.net/esp8266-wemos-d1-mini-pins-and-diagram/. (diakses, 12 oktober 2018)

[15] https://www.bc-robotics.com/shop/peltier-thermo-electric-cooler-module-12v-5a/ (diakses, 19 desember 2018)

Perencanaan Strategis Sistem Informasi Studi Kasus Politeknik LP3i Kampus Pasar Minggu

Marini

Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
marini@budiluhur.ac.id

ABSTRAK — Di Jakarta pada khususnya, banyak lembaga pendidikan vokasi yang menawarkan program studi unggulan guna menarik calon mahasiswa agar masuk ke dalam lembaga pendidikannya. Politeknik LP3I Kampus Pasar Minggu, salah satu lembaga pendidikan vokasi yang memiliki moto " Link and Match " yang mana mensinergikan antara pendidikan dan perusahaan, dimana kelulusan dari Politeknik LP3I Kampus Pasar Minggu nantinya sesuai dengan kebutuhan yang diinginkan perusahaan. Untuk mencapai tujuan tersebut maka diperlukannya perencanaan strategis yang dapat memenangkan persaingan yang ada dengan memperbaiki daya saing atau meningkatkan keunggulan kompetitif Politeknik LP3I Kampus Pasar Minggu. Pokok dari penelitian ini dilakukan dengan pendekatan model Ward and Peppard dan metode analisa strategisnya menggunakan analisis Five Force Model's, analisis Value Chain, Analisis McFarlan Strategic Grid . Hasil dari penelitian ini merupakan suatu kerangka kerja perencanaan strategis sistem informasi yang terintegrasi dalam memanajemen sumber daya untuk menghasilkan informasi yang dibutuhkan, akurat, dan dapat digunakan secara bersama. Kesimpulan dari hasil penelitian ini merupakan kerangka kerja perancangan strategis sistem informasi yang dapat diimplementasikan di Politeknik LP3I Kampus Pasar Minggu.

Kata Kunci : Perencanaan Strategis Sistem Informasi dan Teknologi (SI / TI), Model Ward dan Peppard, Five Force Model's, Value Chain, McFarlan Strategic Grid.

ABSTRACT — In Jakarta in particular, many vocational education institutions offer superior study programs to attract prospective students to enter their educational institutions. LP3I Polytechnic Pasar Minggu Campus, one of the vocational education institutions that has a motto "Link and Match" which synergizes education and companies, where graduation from Polytechnic LP3I, Pasar Minggu Campus, will be in accordance with the needs of the company. To achieve this goal, a strategic plan is needed that can win the existing competition by improving competitiveness or increasing the competitive advantage of the Polytechnic LP3I, Pasar Minggu Campus. The main point of this research is the Ward and Peppard model approach and the strategic analysis method uses the Five Force Model's analysis, Value Chain analysis, McFarlan Strategic Grid Analysis. The result of this research is an integrated information system strategic planning framework in managing resources to produce the information needed, accurate, and can be used together. The conclusion from the results of this study is a strategic design framework for information systems that can be implemented in the LP3I Polytechnic Pasar Minggu Campus.

Keywords: Information Systems and Technology (IS / IT) Strategic Planning, Ward and Peppard's Model, Five Force Model's, Value Chain, McFarlan Strategic Grid.

I. PENDAHULUAN

Di Jakarta pada khusunya, banyak lembaga pendidikan vokasi yang menawarkan program studi unggulan guna menarik calon mahasiswa agar masuk ke dalam lembaga pendidikanya. Persaingan yang ketat membuat sejumlah lembaga pendidikan lain harus membuat perencanaan strategis dalam menghadapinya. Politeknik LP3I salah satu lembaga pendidikan yang berfokus pada vokasi perlu membuat perencanaan strategis dengan melakukan perbaikan dan peningkatan di bidang sistem informasi dan teknologi, yang diharapkan dapat meningkatkan keunggulan kompetensi.

Perencanaan strategis sistem informasi dilakukan dengan pendekatan konsep pemikiran John Ward dan Joe Peppard yang menjadi dasar kerangka kerja perencanaan strategis sistem informasi yang digunakan Politeknik LP3I Kampus Pasar Minggu.

Politeknik LP3I memiliki 48 kampus cabang, salah satu diantaranya : Kampus LP3I Pasar Minggu. Dengan banyaknya kampus cabang dipastikan ada permasalahan pada sistem informasi dan teknologi.

Saat ini sistem informasi antara kampus pusat dan kampus cabang masih berbasis desktop dan tidak terintegrasi, akibatnya banyak sekali permasalahan terutama data yang tidak sama, kebutuhan informasi yang dibutuhkan oleh mahasiswa baik itu di Akademik dan Kemahasiswaan sering terlambat.

Dalam penelitian ini, permasalahan akan dibatasi pada hal – hal berikut ini :

1. Pada penelitian ini studi kasus yang diambil hanya pada lingkup Politeknik LP3I Kampus Pasar Minggu.
2. Masalah yang dibahas dalam penelitian ini dibatasi dengan perancangan model Perencanaan Strategis SI berdasarkan kerangka kerja John Ward dan Joe Peppard.

Rumusan yang digunakan adalah merancang sebuah model kerangka kerja Perencanaan Strategi Sistem Informasi yang sesuai dengan strategi bisnis Politeknik LP3I Kampus Pasar Minggu dan nantinya dapat memberikan kontribusi dalam pencapaiannya.

II. TINJAUAN PUSTAKA

II.1. Perencanaan Strategis

Seperti yang dikutip dari [3] bahwa perencanaan strategis adalah suatu rencana jangka panjang yang bersifat menyeluruh, memberikan rumusan terhadap suatu organisasi mengenai arahan dan bagaimana sumber daya dialokasikan untuk mencapai tujuan selama jangka waktu tertentu dalam berbagai kemungkinan keadaan lingkungan.

Menurut Umar, yang dikutip dari [3], mendefinisikan strategi sebagai suatu proses penentuan rencana para pemimpin puncak yang berfokus pada tujuan jangka panjang organisasi, disertai penyusunan suatu cara atau upaya bagaimana agar tujuan tersebut dapat dicapai.

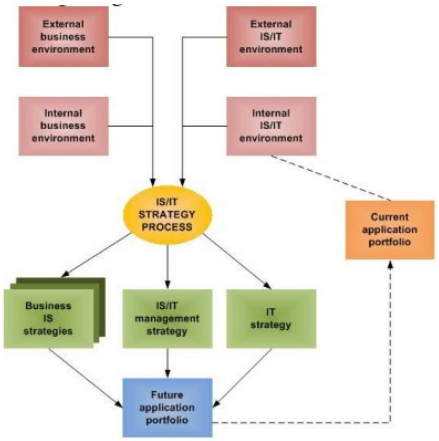
II.2. Strategi Sistem Informasi

Menurut (Kurniadi dan Mulyani) yang dikutip dari [3], bahwa strategi sistem informasi diartikan sebagai suatu sistem yang membantu suatu perusahaan meningkatkan kinerja jangka panjangnya dengan secara langsung meningkatkan kontribusi pertambahan nilainya ke rantai nilai industri. Strategi sistem informasi sebagai suatu penggunaan teknologi informasi untuk mendukung atau menerapkan strategi kompetisi dari perusahaan dan pemanfaatannya dapat meningkatkan daya saing.

Menurut Ward dan Peppard seperti yang dikutip dari [2], strategi dapat didefinisikan sebagai suatu rangkaian tindakan – tindakan terpadu yang menjadi alat untuk meningkatkan keberhasilan dan kekuatan jangka panjang sebuah perusahaan dalam mencapai keunggulan dalam bersaing.

II.3. Model Strategis Sistem Informasi

Pendekatan model yang digunakan dalam penelitian ini menggunakan model Ward and Peppard, yang mana diharapkan nantinya akan menghasilkan perencanaan portfolio sistem informasi ke depannya dapat memberikan kontribusi nyata bagi portofolio sistem informasi yang ada sekarang. [1].



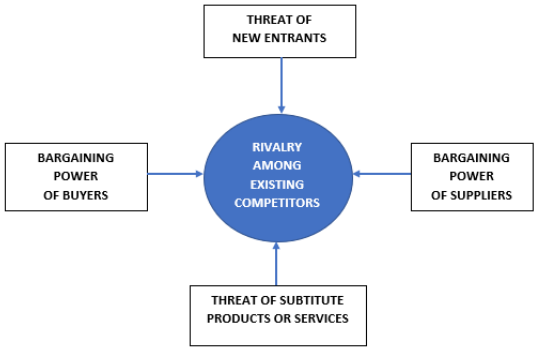
Gambar 1. Model Perencanaan Strategis Sistem Informasi (Ward and Peppard)

Untuk membuat perencanaan sistem informasi yang baik dapat dilakukan dengan beberapa metode antara lain :

II.3.1. Five Force

Dikutip dari [2] untuk menganalisa dan memahami faktor eksternal organisasi dari ancaman maupun peluang maka dapat menggunakan Five Forces Model.

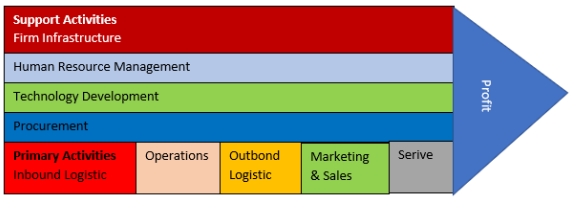
Model ini dapat mengetahui dan mengevaluasi struktur lingkungan industri bisnis serta ancaman dari persaingan. Penggunaan five forces model pada penelitian ini digunakan untuk membangun analisis sistem informasi dalam persaingan, dan juga untuk mengetahui posisi bisnis dalam persaingan.



Gambar 2. Five Forces Model

II.3.2. Value chain

Analisis value chain seperti yang dikutip dari [2] merupakan kegiatan menganalisis dari kumpulan aktivitas yang dilakukan untuk merancang, memproduksi, memasarkan, mengantarkan dan mendukung produk dan jasa.



Gambar 3. Value Chain

II.3.3. McFarlan Strategic Grid

Analisis McFarlan Strategic Grid seperti yang dikutip dari [2] merupakan pemetaan aplikasi sistem informasi berdasarkan kontribusinya terhadap perusahaan. McFarlan Strategic Grid terdiri dari (strategic, high potential, key operation, and support). Dari pemetaan tersebut dapat dilihat sebuah aplikasi sistem informasi terhadap organisasi dan pengembangannya di masa depan.

STRATEGIC	HIGH POTENTIAL
Applications that are critical to sustaining future business strategy	*Applicatios that may be important in achieving future success*
Applications on which the organization currently depends for success	*Applications that are valuable but not critical to success*
KEY OPERATIONAL	**SUPPORT**

Gambar 4. McFarlan Strategic Grid

III. Metode Penelitian

Metode penelitian ini menggunakan beberapa pendekatan John Ward and Joe Peppard yaitu Five Force Model's, Value Chain, dan McFarlan Strategic Grid.

Adapun Five Force Model's menitik beratkan pada 5 kekuatan eksternal yang dapat menjadi sebuah ancaman.

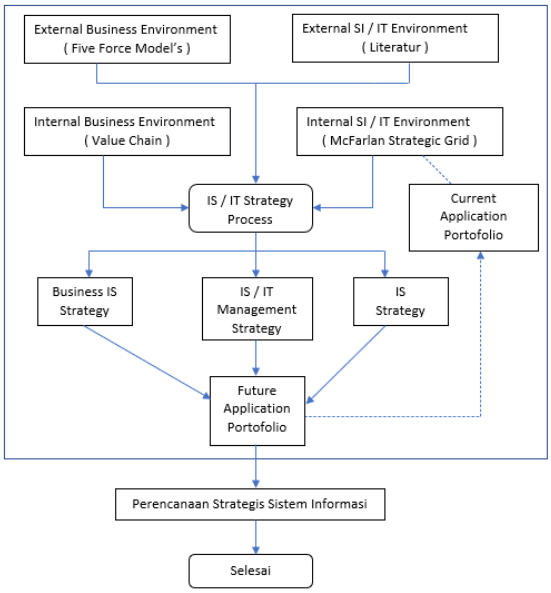
Value Chain sendiri merupakan kumpulan aktivitas organisasi yang dilakukan untuk mendesain, memproduksi, memasarkan, mengirimkan serta mensupport kegiatan yang ada.

Sedangkan McFarlan Strategic Grid itu sendiri merupakan penganalisaan sistem informasi saat ini, dengan keadaan perencanaan sistem informasi yang akan datang.

Metodologi penelitian yang digunakan adalah metodologi kualitatif. Adapun teknik pengumpulan datanya yaitu :

1. Observasi, kegiatan penelitian yang dilakukan secara langsung terhadap obyek penelitian dalam hal ini Politeknik LP3I Kampus Pasar Minggu.
2. Studi Kepustakaan, menggunakan referensi yang berkaitan dengan perencanaan stategis SI / TI berupa buku sumber, jurnal ilmiah dan penelitian – penelitian terdahulu mengenai perencanaan strategis SI / TI.

Perencanaan strategis sistem informasi yang dilakukan dengan pendekatan konsep pemikiran John Ward dan Joe Peppard yang menjadi dasar kerangka kerja perencanaan strategis sistem informasi dan teknologi pada obyek penelitian.



Gambar 5. Kerangka Pemikiran Penelitian

Model ini terdiri dari beberapa inputan :

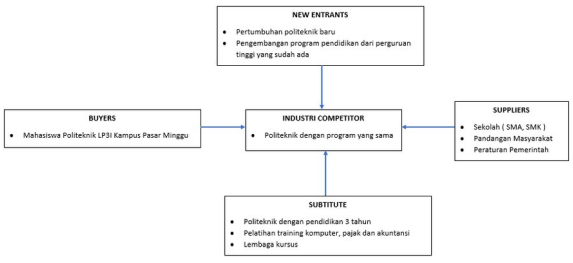
1. Lingkungan Bisnis Eksternal : strategi bisnis sekarang, tujuan (objektif), sumber daya, proses, kebudayaan serta nilai dari suatu bisnis dijelaskan dengan Five Force Model's.
2. Lingkungan Eksternal IS / IT : di dapatkan dari berbagai sumber literatur yang ada untuk menunjang dari sistem perencanaan SI / IT yang ada.
3. Lingkungan Bisnis Internal : ekonomi, lingkungan kampus, serta iklim persaingan dimana kampus beroperasi, dijelaskan dengan Value Chain.
4. Lingkungan Internal IS / IT : perspektif SI / IT sekarang di bisnis dan kematangannya, dijelaskan dengan McFarlan Strategic Grid.

Output dari model ini :

1. Strategi Bisnis SI : bagaimana setiap unit dapat mengembangkan SI / IT dalam mencapai tujuan (objektif) bisnisnya.
2. Strategi Manajemen SI / IT : elemen – elemen yang lazim dari strategi yang diterapkan di kampus secara keseluruhan, menjamin kebijakan yang konsisten.
3. Strategi IS : kebijakan dan strategi dalam memanajemen sistem informasi yang ada.

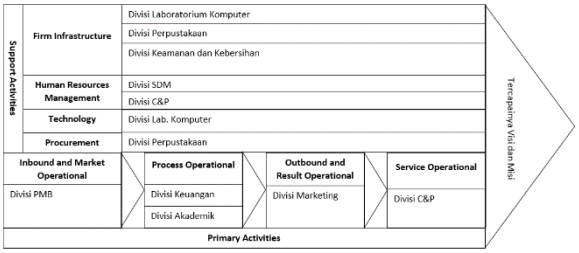
IV. HASIL DAN PEMBAHASAN

Metode yang digunakan pada lingkungan bisnis eksternal menggunakan analisis Five Forces Model yang berguna untuk menentukan posisi Politeknik LP3I Kampus Pasar Minggu terhadap lingkungan eksternal yang dapat mempengaruhi jalannya proses bisnis yang ada. Berikut ini adalah hasil analisis Five Forces Model :



Gambar 6. Hasil Analisis Five Forces Model

Pada lingkungan bisnis internal menggunakan analisis Value Chain yang berguna untuk pembagian aktifitas pada tiap unit :



Gambar 7. Pembagian Aktifitas Setiap Unit

Adapun sistem informasi yang ada saat ini di Politeknik LP3I Kampus Pasar Minggu dapat dilihat pada tabel dibawah ini :

Tabel 1. Sistem Informasi Politeknik LP3I Pasar Minggu

Nama Sistem Informasi	Keterangan
SI Akademik	Data Matakuliah
	Data Nilai Mahasiswa
SI Penggajian	Data Perhitungan Gaji Dosen dan Karyawan
	Pencetakan Slip Gaji Pembayaran Dosen dan Karyawan
SI Perpustakaan	Transaksi Peminjaman Buku
	Transaksi Pengembalian Buku
SI Presensi Karyawan	Pencatat Kehadiran Karyawan
	Perhitungan Data Kehadiran Karyawan

Dari tabel diatas sistem informasi yang digunakan Politeknik LP3I Pasar Minggu, maka untuk lingkungan bisnis internal SI / IT dapat menggunakan analisis McFarlan Strategic Grid yang gunanya untuk memetakan bisnis sistem informasi yang ada, seperti dibawah ini :

Tabel 2. Current Application Portofolio

Strategic	High Potential
SI Akademik	
SI Penggajian SI Keuangan SI Perpustakaan SI Presensi Karyawan	Jaringan LAN
Key Operational	**Support**

Perencanaan strategis sistem informasi disusun berdasarkan analisa lingkungan bisnis internal / eksternal serta lingkungan

bisnis internal / eksternal SI / TI pada Politeknik LP3I Kampus Pasar Minggu.

Dari hasil analisa tersebut maka perencanaan strategis sistem informasi yang akan dibuat diawali dengan penentuan strategi bisnis sistem informasi, penentuan strategi manajemen SI / TI, dan strategi SI Politeknik LP3I Pasar Minggu.

Visi dan misi Politeknik LP3I Kampus Pasar Minggu merupakan awal penentu strategi bisnis. Adapun visi dan misi Politeknik LP3I Kampus Pasar Minggu yaitu :

1. Visi
    1. Menjadi Perguruan Tinggi vokasi yang unggul dan inovatif dengan orientasi kerja dan wirausaha pada tahun 2020.
2. Misi
    1. Menyelenggarakan dan mengembangkan pendidikan vokasi yang berkualitas, bermoral, kompeten dan berjiwa wirausaha.
    2. Mengembangkan kurikulum untuk mengantisipasi kebutuhan dunia kerja dalam bidang manajemen, bisnis dan teknologi.
    3. Mengembangkan dan meningkatkan mutu pengelolaan pendidika berdasarkan prinsip – prinsip tata pamong yang baik.
    4. Menyelenggarakan penelitian dan pengabdian kepada masyarakat bagi pengembangan ilmu pengetahuan dan keterampilan untuk kesejahteraan masyarakat.
    5. Melakukan pengembangan dan pengokohan jejaring dan kemitraan pada tingkat nasional, regional dan internasional.
    6. Mengembangkan kualitas sumber daya manusia untuk memberikan layanan prima.
    7. Meningkatkan kuantitas dan kualitas sarana dan prasarana untuk mendukung proses pembelajaran yang unggul di bidang manajemen, bisnis dan teknologi.

Strategi yang baik dalam pengelolaan SI / TI sangat diperlukan agar pelaksanaan SI / TI berhasil dengan baik, maka proses bisnis kampus dapat berjalan secara efektif dan efisien sehingga strategi bisnis dapat dilaksanakan.

Strategi manajemen SI / TI didapatkan dari hasil analisis perencanaan strategis sistem informasi berupa kebijakan kampus serhingga dalam penerapan strategi SI / TI sesuai dengan kondisi manajemen Politeknik LP3I Kampus Pasar Minggu. Adapun strategi manajemen SI / TI meliputi pengembangan kompetensi SDM tentang SI / TI serta pembuatan kebijakan SI / TI.

Pada divisi Laboratorium Komputer yang menangani hal yang berkaitan dengan SI / TI, maka akan lebih maksimal lagi untuk pelayanan SI / TI nantinya agar dibuatkan unit tersendiri sehingga pengembangan SI / TI akan menjadi maksimal.

Tujuan dari strategi SI adalah mengumpulkan dan mengidentifikasi kebutuhan – kebutuhan strategi bisnis organisasi yang diterjemahkan dalam bentuk solusi SI yang dapat mendukung strategi bisnis yang ada.

Berdasarkan identifikasi kebutuhan SI dari hasil analisa value chain Politeknik LP3I Kampus Pasar Minggu, maka dapat disusun Future Application Portfolio menggunakan McFarlan's Strategic Grid seperti terlihat pada Tabel 3.

Tabel 3. Future Application Portofolio

Strategic	**High Potential**
SI Akademik SI Keuangan Website Kampus SI Alumni SI Kerjasama	SI Pendaftaran Mahasiswa Baru SI Manajemen Data Mahasiswa SI Manajemen Data Dosen SI Manajemen Data Karyawan
SI Penggajian SI Perpustakaan SI Presensi Karyawan SI Inventaris	Jaringan LAN Internet
Key Operational	**Support**

Untuk dapat membandingkan sistem informasi yang ada saat ini dengan sistem informasi yang akan dibangun dengan menggunakan perencanaan strategis sistem informasi, peneliti menggunakan analisis GAP seperti dibawah ini.

IS Existing / *IS Need*	SI Akademik	SI Keuangan	SI Penggajian	SI Perpustakaan	SI Presensi Karyawan	Future SI
SI Akademik	Tetap					
SI Keuangan		Kembangkan				
SI Alumni						Baru
SI Kerjasama						Baru
SI Pendaftaran Mahasiswa Baru						Baru
SI Manajemen Data Mahasiswa Baru						Baru
SI Manajemen Data Dosen						Baru
SI Manajemen Data Karyawan						Baru
SI Penggajian			Tetap			
SI Perpustakaan				Tetap		
SI Presensi Karyawan					Tetap	
SI Inventaris						Baru

Gambar 8. Gap analisis Sistem Informasi

Dari tabel gap analisis diatas, terdapat tiga kriteria tindakan yang harus dilakukan terhadap sistem informasi yang sudah ada maupun yang akan diajukan. Adapun penjelasannya sebagai berikut :

1. Kembangkan

   Kriteria ini yang artinya bahwa sistem informasi perlu dikembangkan fiturnya sehingga dapat memenuhi fungsi – fungsi yang diperlukan dari sistem informasi tersebut terhadap kebutuhan yang akan datang.

2. Tetap

   Kriteria ini berarti bahwa sistem informasi yang sudah ada tetap dapat digunakan karena sudah sesuai dengan kebutuhan yang akan datang.

3. Baru

   Kriteria ini yang artinya bahwa sistem informasi tersebut belum ada dan dibutuhkan untuk mendukung proses bisnis yang akan datang.

Implementasi dari perencanaan strategis sistem informasi ini setidaknya membutuhkan waktu sekitar 1 tahun. Adapun rekomendasi implementasinya dijelaskan pada Gambar 9.

Nama Kegiatan	Januari	Februari	Maret	April	Mei	Juni	Juli	Agustus	September	Oktober	November	Desember
Strategi Manajemen SI												
Perubahan Struktur Organisasi												
Pengembangan Kompetensi SDM SI/TI												
Sosialisasi Kebijakan SI / TI												
Perekrutan Staff SDM SI / TI Kompeten												
Strategi SI												
Pembuatan SI kategori *Strategic*												
Pembuatan SI kategori *Key Operational*												
Pembuatan SI kategori *High Potential*												
Pembuatan SI kategori *Support*												

Gambar 9. Jadwal Rencana Implementasi

V. KESIMPULAN

1. Visi dan misi Politeknik LP3I Kampus Pasar Minggu merupakan dasar awal terbentuknya strategi bisnis SI.
2. Sedangkan pada bagian strategi manajemen SI / TI, diperlukannya restrukturisasi organisasi yaitu penambahan divisi baru untuk menghandle SI / TI.
3. Untuk bagian strategi SI sendiri dibutuhkan sekitar 12 sistem informasi yang dipetakan dalam McFarlan Strategic Grid guna mendukung kegiatan bisnis berupa aktifitas utama dan aktifitas pendukung agar proses bisnisnya menjadi efisien.
4. Dan perbedaan sistem informasi saat ini dengan sistem informasi yang akan datang terlihat pada GAP analisis yang mana terdapat 7 sistem informasi baru yang dapat mendukung kinerja serta efisiensi bisnis proses yang ada.

DAFTAR PUSTAKA

[1] Ward, John, & Peppard, Joe. (2002). Strategic Planning for Information Systems. Baffins Lane, Chichester : John Wiley & Sons Ltd.

[2] Heriadi, Agustono. dan Suyanto, M. dan Sudarmawan. Perencanaan Strategis Sistem Informasi STMIK Cahaya Surya Kediri. Citec Journal, Vol.1, No. 1, November 2013 – Januari 2014.

[3] Septiana, Yosep. Perencanaan Strategis Sistem Informasi Dengan Pendekatan Ward And Peppard Model (Studi Kasus : Klinik Inti Garut). Jurnal Wawasan Ilmiah. Volume 8, Nomor 1 Tahun 2017

[4] Suryadi, Lis. Perencanaan Strategis Sistem Informasi Dan Teknologi Informasi (SI/TI) Studi Kasus Universitas Budi Luhur.

[5] Yudhistyra, Weeka Imam. dan Nugroho, Eko. Lima Metode Perencanaan Strategis Sistem Informasi Dan Teknologi Informasi Untuk Pengembangan E-Goverment. Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014).

Rivest Code 4 dan Kompresi Huffman Pada Aplikasi Pengamanan Data Berbasis Web

Dheni Dwi Wibowo [1)], Rizky Pradana [2)], Agnes Aryasanti [3)]

[1,2,3)] Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E- mail : 1511510677@student.budiluhur.ac.id [1)], rizky.pradana@budiluhur.ac.id [2)], agnes.aryasanti@budiluhur.ac.id [3)]

ABSTRAK — Perkembangan dan kemajuan teknologi komputer dan telekomunikasi saat ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi suatu kebutuhan yang penting . Setiap harinya terjadi pertukaran data melalui jalur komunikasi (Internet). Keamanan data merupakan salah satu faktor penting bagi sebuah perusahaan, terlebih perusahaan multi nasional. Salah satu langkah yang dapat dilakukan untuk mengamankan data adalah dengan menggunakan teknik kriptografi, dan untuk mempercepat daya transfer dapat mengandalkan teknik kpmpresi. Dalam penelitian ini untuk mengamankan data pada sebuah perusahaan multinasional yang bergerak di bidang otomotif adalah dengan kriptografi RC4 dan kompresi Huffman. Berdasarkan pada penelitian yang dilakukan, obek dalam penelitian ini adalah file dengan format dokumen dan perhitungan. Berdasarkan pada hasil yang di dapat, setelah di lakukan kriptografi dan kompresi, perbesaran data dapat ditekan menjadi 33%.

Kata kunci: Data, Huffman, Kompresi, Kriptografi,RC4.

ABSTRACT — The development and advancement of computer and telecommunications technology currently has experienced a rapid progress and has become an important requirement. Every day data exchange takes place via communication lines (the Internet). Data security is one important factor for a company, especially multinational companies. One step that can be taken to secure a data is to use cryptographic techniques, and to accelerate the transfer of power can rely on compression techniques. In this study, we used RC4 cryptography and Huffman compression to secure a data in a multinational company engaged in the automotive sector. Based on this study, the object in this study is a file which contained document and calculation format. Based on the results of this study, after diong the cryptography and copression, the increase of size can be pressed become 33%.

Keywords: Data, Huffman, Compression, Cryptography, RC4.

I. PENDAHULUAN

Perkembangan dan kemajuan teknologi komputer dan telekomunikasi saat ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi suatu kebutuhan yang penting bagi setiap orang. Semakin tinggi tingkat teknologi komputer, maka semakin tinggi pula tingkat ancaman yang dapat mengancam keamanan para pengguna komputer. Salah satu dampak negatif di dalam perkembangan teknologi adalah adanya pencurian data. Dengan adanya pencurian data maka aspek keamanan data dalam pertukaran informasi serta penyimpanan data dianggap sangat penting.

Perusahaan multinasional merupakan salah satu dari banyak jenis perusahaan yang mengandalkan penggunaan teknologi komputer dan telekomunikasi dalam melakukan pertukaran data-data yang ada di perusahaan. Data-data yang dikirim merupakan data pelanggan yang sangat rahasia dan penting. Untuk menghindari terjadinya hal seperti itu, maka sangat dibutuhkan suatu cara untuk mengamankan file yang akan dikirim dimana data yang dikirim akan diacak dengan suatu metode penyandian agar file tersebut hanya bisa dibaca oleh orang yang berhak. Oleh karena itu diperlakukan suatu sistem untuk melakukan untuk melakukan pengkodean pesan sebelum dilakukan proses pengiriman tersebut, sehingga pesan yang dikirim tetap terjaga kerahasiannya dan tidak dapat dengan mudah diubah.

Algoritme kriptografi yang akan digunakan adalah metode kriptografi simetris yaitu Rivest Code 4 (RC4) yang bersifat stream cipher serta menggunakan algoritme kompresi Huffman untuk mengkompresi file. Proses dimulai dengan mengenkripsi file dengan algoritme yang telah disebutkan diatas dengan cara file yang telah dienkripsi dengan satu algoritme kemudian diteruskan dengan dengan mengkompresikan file yang sudah dienkripsi tadi dengan algoritme kompresi Huffman. Teknik kriptografi ini dipilih karena diharapkan dengan algoritme ini proses enkripsi-dekripsi data dapat dilakukan dengan waktu yang lebih cepat.

II. LITERATURE REVIEW

Data atau file mempunyai peranan yang sangat penting [1]. Pengamanan untuk melindungi data yang memiliki file yang berformat Microsoft Word, Microsoft Excel, dan PDF dapat mencegah terjadinya pencurian, kerusakan dan penyalahgunaan data oleh pihak yang tidak bertanggung jawab[2]. Implementasi sistem kriptografi dapat dilakukan dengan memanfaatkan aplikasi berbasis web Tahapan kompresi dapat digunakan untuk proses pemampatan, dan tahapan dekompresi untuk proses pengembalian file ke bentuk dan ukuran yang semula[3]. Teknik kriptografi digunakan untuk merubah data atau informasi yang berbentuk plain-text menjadi cipher-taxt.Selanjumya [4]. Proses penyandian data dan algoritme Huffman dalam pengompresian data sehingga hanya orang tertentu yang dapat memahami file yang dikirimkan dan hal ini menghindari orang/ oknum yang mencoba mencuri file yang dikirim[5].

III. METODOLOGI

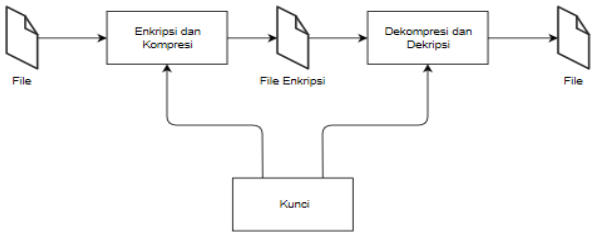
III.1. Identifikasi Masalah

Setiap instansi memiliki informasi yang sangat berharga yang tidak ingin diketahui oleh pihak yang tidak berwenang. Kerahasiaan suatu informasi tersebut selalu menjadi masalah tersendiri bagi setiap instansi. Data dan informasi yang dihasilkan instansi harus bisa diamankan. Tanpa pengamanan yang maksimal, maka kerugian akan dialami instansi tersebut manakala data yang sangat penting dan rahasia tersebut hilang atau dicuri oleh orang yang tidak bertanggung jawab. Seiring dengan kemajuan teknologi, banyak orang yang dapat mengakses segala bentuk data dan informasi dengan sangat mudahnya, baik data yang bersifat umum atau pribadi. Hal ini dapat menimbulkan masalah baru, terutama masalah pengiriman data atau informasi pada suatu instansi yang sebagian data dan informasinya merupakan rahasia aset instansi.

III.2. Perancangan Program

Tahap perancangan program dilakukan untuk mencari bentuk yang optimal dan program yang akan dibuat dengan mempertimbangkan faktor permasalahan dan kebutuhan yang telah dijelaskan sebelumnya. Upaya yang dilakukan adalah dengan berusaha mencari kombinasi penggunaan perangkat keras (hardware) dan perangkat lunak (software) yang tepat sehingga diperoleh hasil yang maksimal dan mudah untuk diimplementasikan.

Untuk melakukan enkripsi sekaligus kompresi file, user dapat memilih menu enkripsi. Pada menu ini, user diharuskan memilih file dokumen DOC, DOCX, XLSX, dan XLS terlebih dahulu, baru kemudian melakukan proses enkripsi sekaligus kompresi. Namun file dokumen DOC, DOCX, XLSX, dan XLS tidak boleh lebih besar dari ukuran file yang telah ditentukan yaitu 2 MB, selanjutnya akan tampil output berupa informasi hasil enkripsi sekaligus kompresi file tersebut.



III.3. Perancangan Uji Kasus Enkripsi dan Dekripsi

Uji kasus Enkripsi dan Dekripsi dilakukan untuk mengetahui besarnya ukuran file setelah melalui proses enkripsi sekaligus kompresi dan dekripsi sekaligus dekompresi. Juga untuk mengetahui lamanya waktu yang dibutuhkan dalam proses enkripsi sekaligus kompresi dan dekripsi sekaligus dekompresi.

III.4. Rancangan Layar Aplikasi

Salah satu hal penting yang dilakukan dalam pembuatan program ini adalah rancangan layar. Rancangan layar harus sesuai dengan fungsinya agar dapat memudahkan pengguna dalam penggunaannya, serta dapat memberikan rasa nyaman dalam menjalankan program. Berikut rancangan layar dalam program yang dibuat:

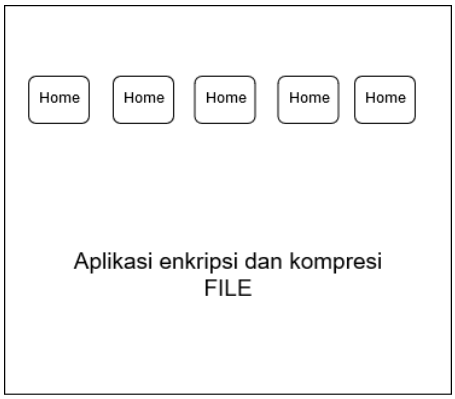
III.4.1. Rancangan Layar Form Login

Fungsi form login yaitu agar user dapat masuk dan dapat menggunakan program ini. Untuk login dengan memasukan username dan password yang telah terdaftar di database, maka user langsung masuk pada menu utama. Seperti gambar 1 berikut :

Gambar 1. Rancangan Layar Form Login

III.4.2. Rancangan Layar Menu Utama

Rancangan layar pada gambar 2 terdapat empat menu. Menu yang pertama adalah Menu home, kedua adalah menu Enkripsi, dimana user dapat mengenkripsi sekaligus mengkompresi file dokumen DOC, DOCX, XLSX, dan XLS. Menu yang ketiga adalah Dekripsi, pada menu ini user dapat mengembalikan file yang telah dienkripsi sekaligus dikompresi tadi menjadi file semula. Dan keempat menu Help untuk membantu user dalam menggunakan program ini. Untuk keluar dari program tekan tombol Logout.

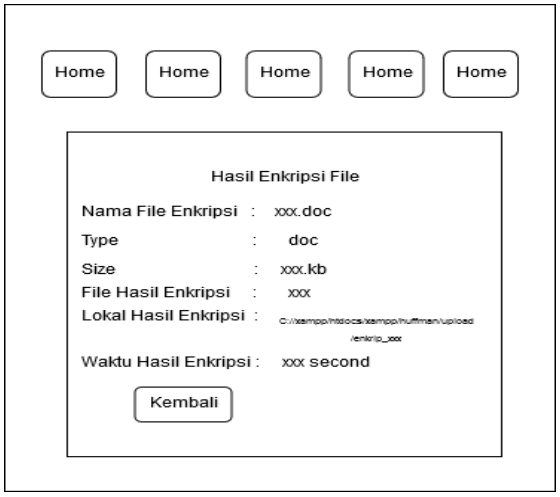


Gambar 2. Rancangan Layar Menu Utama

III.4.3. Rancangan Layar Form Enkripsi

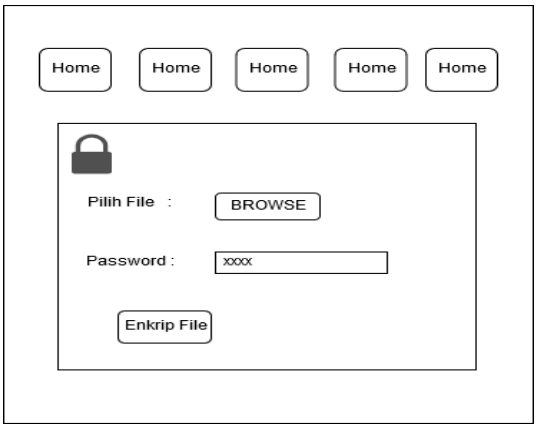
Gambar 3 berikut ini adalah rancangan layar pada Form Enkripsi. Untuk mengenkripsi sekaligus mengkompresi file dokumen DOC, DOCX, XLSX, dan XLS user terlebih dahulu memilih file yang akan dienkripsi sekaligus dikompresi.

Kemudian user harus memasukan password maksimal 8 karakter agar file dapat dienkripsi sekaligus dikompresi. Selanjutnya proses enkripsi siap dijalankan. Setelah dijalankan, user dapat melihat hasil dari proses tersebut.



Gambar 3. Rancangan Layar Form Enkripsi

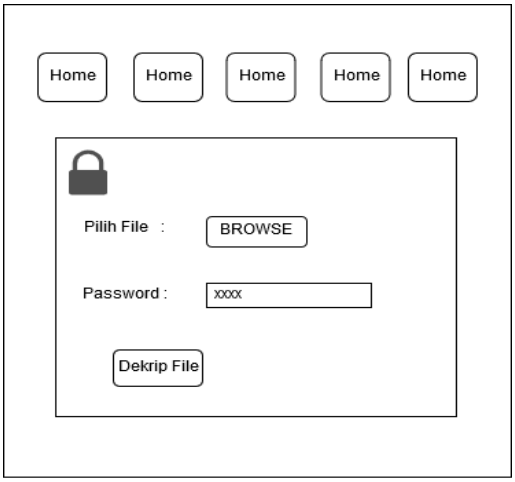
Apabila proses enkripsi sekaligus kompresi berhasil dijalankan, maka akan tampil form hasil enkripsi sekaligus kompresi seperti gambar 4 di bawah ini.



Gambar 4. Rancangan Hasil Enkripsi File

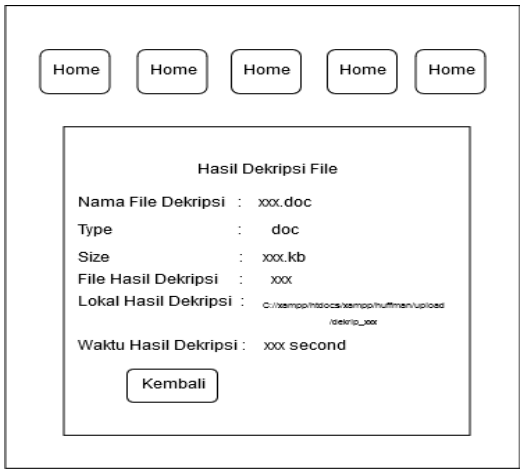
III.4.4. Rancangan Layar Form Dekripsi

Gambar 5 merupakan rancangan layar dari Form Dekripsi. Pada form ini, user terlebih dahulu memilih file yang telah dienkripsi sekaligus dikompresi sebelumnya. Setelah memilih file yang sudah dienkripsi sekaligus dikompresi, user harus memasukan password yang sama ketika melakukan proses enkripsi sekaligus kompresi tadi. Kemudian proses dekripsi sekaligus dekompresi file dijalankan.



Gambar 5. Rancangan Layar Form Dekripsi

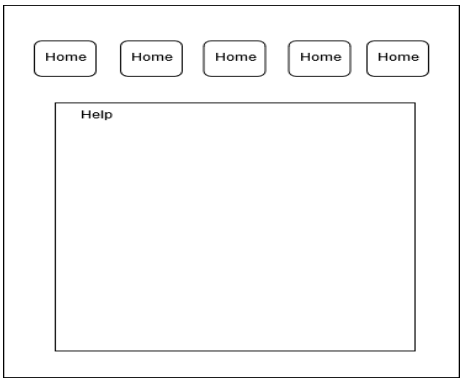
Setelah proses dekripsi dan dekompresi berhasil dijalankan, maka akan muncul hasil dari proses dekripsi sekaligus dekompresi seperti gambar 6 berikut ini.



Gambar 6. Rancangan Layar Hasil Dekripsi File

III.4.5. Rancangan Layar Layar Form Help

Pada rancangan layar form Help ini, user dapat melihat atau mengetahui informasi bantuan yang bisa digunakan untuk menggunakan aplikasi ini. Rancangan layar form Help seperti terlihat pada gambar 7 di bawah ini.



Gambar 7. Rancangan Layar Form Help

III.5. Algoritme Program

III.5.1. Enkripsi

1. Tampilkan Form Enkripsi
2. Pilih File Dokumen DOC, DOCX, XLSX, dan XLS
3. Input password
4. If Password Valid Then
5. Input Pilih
6. If Pilih = “Enkrip File” Then
7. Proses Enkripsi dan Kompresi
8. Tampil Form Hasil Enkripsi dan Kompresi
9. Input Pilih
10. If Pilih = “Kembali” Then
11. Kembali ke baris 1
12. Else
13. Kembali ke baris 8
14. End If
15. Else
16. Kembali ke Baris 5
17. End If
18. Else
19. Tampil Pesan Error
20. Kembali ke Baris 3
21. End If

III.5.2. Dekripsi

1. Tampil Form Dekripsi
2. Pilih File Enkrip
3. Input Password
4. If Password Dekrip = Password Enkrip Then
5. Input Pilih
6. If Pilih = “Dekrip File” Then
7. Proses Dekripsi dan Dekompresi
8. Tampil Form Hasil Dekripsi dan Dekompresi
9. Input Pilih
10. If Pilih = “Kembali”
11. Kembali ke Baris 1
12. Else
13. Kembali ke Baris 8
14. End If
15. Else
16. Kembali ke Baris 5
17. End If
18. Else
19. Tampil Pesan Error
20. Kembali ke Baris 1
21. End If

IV. IMPLEMENTASI DAN UJICOBA

IV.1. Implementasi Program

Agar aplikasi pengamanan data dengan algoritme Kriptografi Rivest Code 4 (RC4) dan Kompresi Huffman berbasis web dapat berjalan dengan baik, spesifikasi yang dipakai untuk implementasi sistem ini juga harus mendukung. Spesifikasi berikut bisa mendukung sistem saat ini, diantaranya adalah:

1. Perangkat Keras (Hardware)

   Perangkat keras (hardware) yang dipakai untuk implementasi aplikasi ini adalah sebagai berikut :

   1. Processor Intel Core i3-6006U cpu 2.0 Ghz
   2. RAM 4.00 GB
   3. Harddisk 1 TB
   4. VGA NVIDIA Geforce 920mx
   5. Keyboard dan Mouse

2. Perangkat lunak (Software)

   Perangkat lunak (software) yang dipakai untuk implementasi aplikasi ini adalah sebagai berikut :

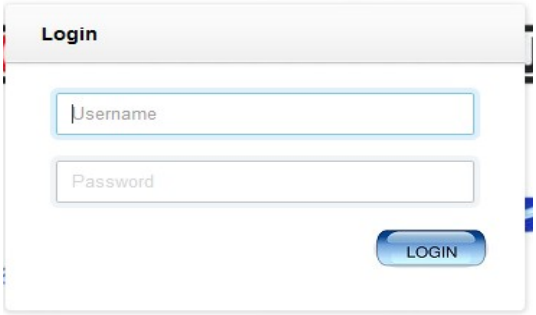
   1. Sistem Operasi Windows 10 64-Bit
   2. XAMPP v3.2.2
   3. Sublimte Text 3
   4. phpMyAdmin

IV.2. Data Masukan

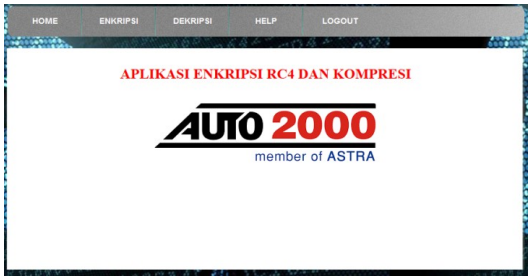
Dalam program ini data masukan yang digunakan berbentuk file dengan format .DOC, .DOCX, .XLS, dan .XLSX. Jumlah data yang dimasukan sesuai dengan kebutuhan yang diinginkan, jika semakin besar data yang diproses maka proses enkripsi dan dekripsi akan semakin lama.

IV.3. Tampilan Layar

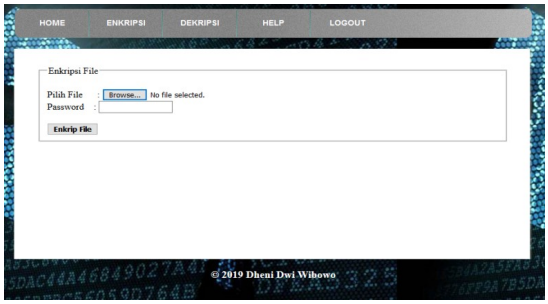
Tampilan layar menu login pada gambar 4.1 ini muncul pada saat aplikasi ini dijalankan. Didalam form login terdapat username dan password. User harus memasukkan username dan password agar terlebih dahulu agar dapat menggunakan aplikasi ini



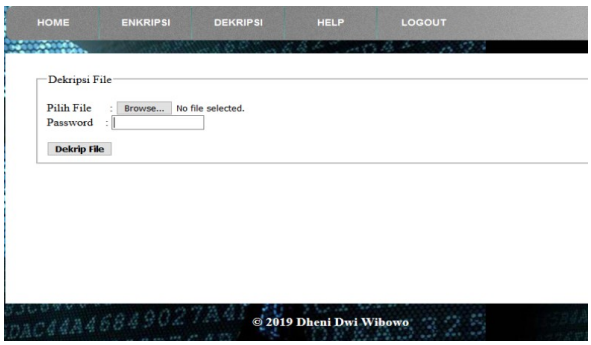
Gambar 8. Tampilan Layar Menu Login



Gambar 9. Tampilan Layar menu Utama



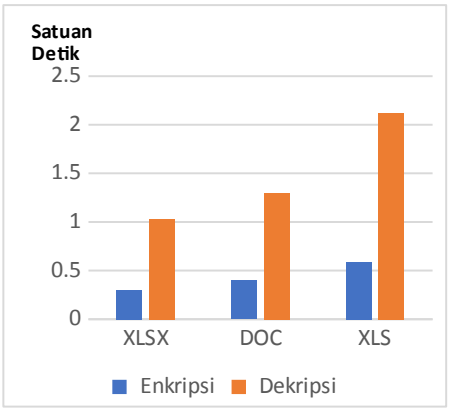
Gambar 10. Tampilan Layar Form Enkripsi



Gambar 11. Tampilan Layar Form Dekripsi

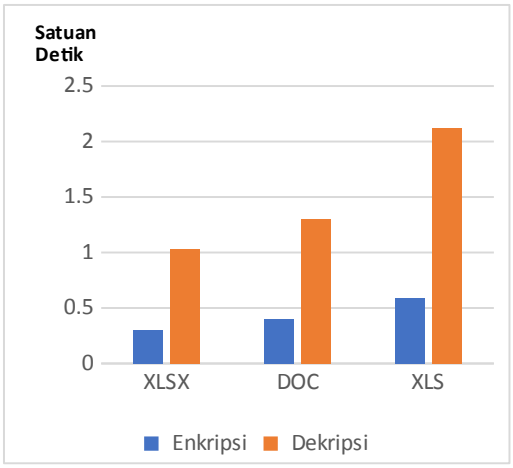
IV.4. Grafik Perbandingan Ukuran File

Berikut adalah grafik perbandingan dari pengujian aplikasi Keamanan File. File yang di Enkripsi dan kompresi

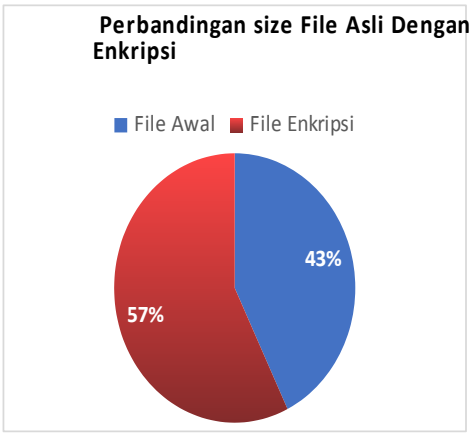


Gambar 12. Grafik Perbandingan Ukuran File

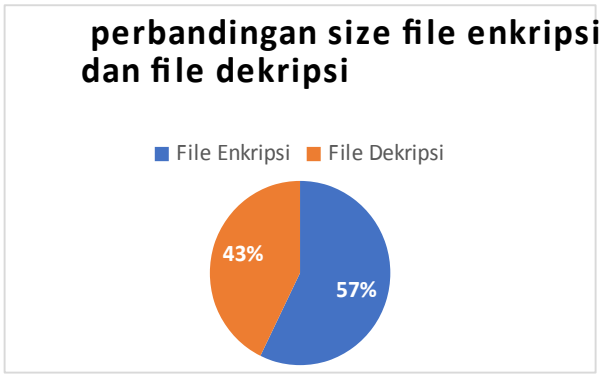
File awal yang dienkripsi rata-rata naik sebesar 33% namun pada saat file enkripsi didekripsi, size dari file dekripsi akan mendekati size dari file awal.



Gambar 13. Grafik Perbandingan Waktu Enkripsi dan Dekripsi File



Gambar 14. Perbandingan Size File Asli dan File Enkripsi



Gambar 15. Perbandingan Size File Enkripsi dan File Dekripsi

V. KESIMPULAN DAN SARAN

V.1. KESIMPULAN

Dari hasil pengujian dan analisa yang telah dilakukan dapat disimpulkan bahwa:

1. Aplikasi ini menggunakan algoritme Rivest code 4 untuk Enkripsi. Dibangun untuk dapat mengamankan jenis file dokumen DOC, DOCX, XLSX, dan XLS
2. Aplikasi ini juga menggunakan algoritme Huffman. Algoritme Kompresi Huffman digunakan bertujuan untuk memperkecil ukuran setelah dienkripsi dengan algoritme RC4.
3. File yang telah dienkripsi tidak akan dapat dibuka kembali tanpa melalui proses dekripsi.
4. Dari pengujian enkripsi dan dekripsi dapat disimpulkan file awal yang setelah dienkripsi akan naik sebesar 33% sebaliknya file enkripsi yang telah didekripsi ukurannya sama dengan file awal

V.2. SARAN

Aplikasi kriptografi menggunakan algoritme RC4 dan Kompresi Huffman ini belum sempurna dan masih memerlukan banyak perbaikan untuk meningkatkan efektifitas pekerjaan. Untuk meningkatkan kinerja aplikasi ini maka diusulkan beberapa saran yang dapat menjadi pertimbangan, antara lain:

1. Program dapat mengenkripsi berbagai macam jenis file.
2. Kunci sandi (password) yang digunakan sebaiknya hanya diketahui oleh seorang pengirim dan penerima informasi saja.

3. Sebaiknya program dioperasikan dengan minimal processor Intel Core i3.
4. Agar bisa mengkompres dan mengenkripsi file lainnya selain bertipe DOC, DOCX, XLSX, dan XLS

DAFTAR PUSTAKA

[1] Handayani, Fitri. (2017). Implementasi Teknik Kompresi File Teks Dengan algoritma Huffman Dan Mengamankan File Teks Dengan algoritma ADVANCED ENCRYPTION STANDARD (AES), Medan, STMIK Budidarma Medan

[2] Setiawan, Okie., Fiati, Rina., Listyorini, Tri. (2014). Algoritme Enkripsi RC4 Sebagai Metode Obfuscation Source Code PHP. Kudus, Universitas Muria Kudus.

[3] Himawan, Imam. (2018). Steganografi Untuk Keaslian Tanda Tangan Yang Terdigitalisasi algoritme RC4. Jakarta, Universitas Indraprasta PGRI.

[4] Imelda, Imelda, & Prawira, Ega. (2018). Pengamanan Disposisi Dokumen Secara Online Menggunakan Kriptografi Twofish dan Kompresi HUFFMAN pada CV. TMU. Jakarta, Universitas Budi Luhur.

[5] Darwis, Dedi., Prabowo, Rizky., Hotimah, Nurul,. (2018). Kombinasi Gifshuffle, Enkripsi AES dan Kompresi data HUFFMAN Untuk meningkatkan Keamanan Data. Lampung, Universitas Lampung.

Pemodelan dan Estimasi Cadangan Klaim Menggunakan Metode GEE (Generalized Estimazing Equations) Pada Perusahaan Asuransi PT XYZ

Dwi Achadiani [1)], Ririt Roeswidiah [2)]

[1,2)] Program Studi Sistem Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl.Ciledug Raya, Petukangan Utara Pesanggrahan, Jakarta Selatan 12260.
dwi.achadiani@budiluhur.ac.id [1)], ririt.roeswidiah@budiluhur.ac.id [2)]

ABSTRAK — Penelitian ini berisi tentang pemodelan dan estimasi cadangan klaim perusahaan asuransi umum dengan menggunakan metode Generalized Estimating Equations (GEE) , data yang digunakan adalah klaim asuransi PT XYZ yang termasuk bisnis short-tail. Berdasarkan hasil penelitian potensi masalah yang akan muncul adalah akan terjadi gagal bayar yang disebabkan kurangnya cadangan klaim pada bulan tertentu dalam setahun. Telah dilakukan estimasi perhitungan cadangan klaim dengan metode GEE, terjadinya klaim selama tahun 2016, nilai estimasi yang dihasilkan metode ini memiliki kesalahan berkisar 55% sampai dengan 60%. pada Mean Absolute Percentage Error (MAPE).

Kata Kunci : Asuransi Umum, Cadangan Klaim, Generalize Estimating Equations (GEE).

Abstract — This study contains modeling and estimating claims reserves of general insurance companies using the Generalized Estimating Equations (GEE) method, the data used are PT XYZ insurance claims which are included in the short-tail business. Based on the results of the study the potential problems that will arise are defaults due to lack of reserve claims in certain months of the year. Estimation of claims reserve calculations using the GEE method has been carried out, claims occurred during 2016, the estimated value generated by this method has an error ranging from 55% to 60%. in Mean Absolute Percentage Error (MAPE).

Keyword : General Insurance, Claim Reserving, Chain-Ladder, Generalize Estimating Equations

I. PENDAHULUAN

Persoalan yang paling penting dari suatu perusahan asuransi adalah perhitungan cadangan klaim. Cadangan klaim yang harus disiapkan oleh suatu perusahaan asuransi minimum sebesar penjumlahan nilai estimasi klaim yang masih dalam proses penyelesaian (Reported But Not Settled/RBNS) dan nilai estimasi klaim yang terjadi tetapi belum dilaporkan (Incurred But Not Reported/IBNR).

Perusahaan asuransi PT XYZ (bukan nama sebenarnya) harus dapat memperhitungkan besar cadangan klaim agar dapat memenuhi kewajiban perusahan asuransi tersebut terhadap pemegang polis, karena waktu terjadinya klaim tidak pasti.

Ketidakpastian terhadap waktu terjadinya klain dan kerugian yang wajib ditanggung perusahaan asuransi sangat berkaitan dengan penetapan atau estimasi suatu cadangan klaim perusahaan. Berdasarkan hal di atas maka potensi masalah yang akan muncul adalah akan terjadi gagal bayar yang disebabkan kurangnya cadangan klaim.

Banyak metode dalam estimasi pecadangan klaim telah dikembangkan, England dan Verrall (2002) atau Wüthrich dan Merz (2008) menentukan pencadangan klaim menggunakan model-model linear umum atau generalized linear models (GLM). Model GLM ini merupakan model yang fleksibel, model ini memungkinkan merespon segala bentuk variabel yang tergolong dalam keluarga eksponensial. Semua pendekatan klasik adalah berdasarkan asumsi bahwa jumlah klaim pada tahun-tahun yang berbeda merupakan variabel bebas. Akan tetapi, asumsi ini terkadang tidak sesuai dengan kejadian yang sebenarnya.

Salah satu perluasan dari model GLM adalah model Generalized Linear Mixed Model (GLMM). Menurut Antonio dan Beirlant (2007) GLMM dapat menangani kemungkinan ketergantungan di antara klaim inkremental pada tahun-tahun perkembangan berturut-turut. Pendekatan ini memperluas GLM klasik dan sering digunakan pada analisa-analisa data longitudinal. Pendekatan GLMM diusulkan dengan lebih banyak data granular yang dibutuhkan (misalnya data klaim-per-klaim).

Pengembangan model GLM adalah Generalized Estimating Equations (GEE). Model GEE merepesentasikan pendekatan

alternatif dari modelling data yang terkorelasi. Berbeda dari GLMM dan GLM, GEE tidak membutuhkan informasi dari distribusi klaim, pada GEE diasumsikan bahwa distribusi ini termasuk keluarga eksponensial. Struktur mean, relasi variance terhadap mean yang disebut working correlations structure cukup untuk melakukan GEE.

Pada penelitian ini akan digunakan metode Generalized Estimating Equations dalam mengestimasi cadangan klaim pada PT XYZ.

II. LANDASAN TEORI

II.1. Cadangan Klaim

BerdasarkanPeraturanKetuaBadanPengawasPasar Modal dan Lembaga Keuangan Nomor: PER-09/BL/2012, tentang Pedoman Pembentukan Cadangan Teknis Bagi Perusahaan Asuransi Dan Perusahaan Reasuransi. Cadangan teknis dalam bentuk Cadangan Klaim harus memenuhi:

- Cadangan Klaim paling sedikit dihitung sebesar
  - Penjumlahan nilai estimasi klaim yang masih dalam proses penyelesaian (*Reported But Not Settled* /RBNS); dan
  - Nilaiestimasiklaim yang terjaditetapibelumdilaporkan (*Incurred ButNot Report/IBNR*)
- Nilai klaim untuk produksi asuransi dan atau reasuransi yang masih dalam proses penyelesaian paling sedikit dihitung berdasarkan estimasi sentral atau estimasi terbaik (*best estimate*) atas klaim yang sudah terjadi dan sudah dilaporkan tetapi masih dalam proses penyelesaian, berikut biaya jasa penilai kerugian asuransi, biaya penyelesaian hukum dan biaya-biaya lain yang terkait dengan penyelesaian klaim.
- Nilai klaim yang sudah terjadi tetapi belum dilaporkan (*Incurred But Not Reported*) dihitung berdasarkan estimasi sentral atau estimasi terbaik (*best estimated*) atas klaim yang sudah terjadi tetapi belum dilaporkan dengan menggunakan metode rasio klaim atau salah satu dari metode segitiga (*triangle method*), berikut biaya jasa penilai kerugian asuransi.
- Dalam hal cadangan klaim RBNS belum dapat diestimasi, jumlah yang dicadangkan adalah presentase rata-rata klaim dibayar terhadap uang pertanggungan untuk jenis usaha yang sama pada tahun buku terakhir dikalikan dengan uang pertanggungan dari klaim tersebut.

Agar perusahaan asuransi tetap berjalan dengan baik, maka harus selalu dapat mengevaluasi cadangan klaimnya.Estimasi cadangan klaim yang akurat akan berpengaruh pada penetapan nilai premi yang tepat dan stabil. Apabila estimasi tidak akurat maka perusahaan akan tidak memiliki dana yang cukup untuk pembayaran klaim.Selain hal tersebut diatas apabila estimasi cadangan klaim tidak akurat, maka perusahaan akan salah dalam melaporkan keuangan

II.2. *Generalized Estimating Equations* (*GEE*)

Metode GEE merupakan pengembangan dari metode GLM. Perbedaan pada Metode GEE dengan metode GLM adalah pada metode GEE tidak diperlukan informasi distribusi pada data. Pada metode GEE dilakukan pemodelan korelasi antara periode kejadian dan periode pengembangan pada data. Pada metode Generalizing Estimating Equationsjumlah klaim di periodekejadian yang sama memiliki keterkaitan. Hubungan pada periode kejadian dan periode pengembangan dianalisa melalui salah satu pilar pada kerangka kerja GEE yang disebut working correlations structure. Hal ini juga tidak terdapat pada metode GLM,

Menurut Hudecova dan Pesta (2013) Kerangka kerja dari GEE secara umum membutuhkan tiga pilar yang harus dipenuhi, yaitu:

1 Pilar 1: Fungsi Link

Fungsi link yang sesuai dibutuhkan untuk menghubungkan nilai variabel respon yang diharapkan, dalam hal ini $X_{i,j}$ dengan nilai estimasi. Menurut Hudecova dan Pesta (2013) ekspektasi dari X_i dinotasikan sebagai

$$E\,X_i = \mu_i = ¿$$

Misalkan periode kejadian$i$ dan periode development$j$ mempengaruhi ekspektasi melalui fungsi link$g$, maka

$$\mu_{i,j} = g^{-1}\left(\eta_{i,j}\right) = g^{-1}\left(z_{i,j}^{T}\theta\right)$$

dimana $z_{i,j}$ merupakan suatu vektor $p \times 1$ dari *dummy covariates* yang mengatur dampak dari periode kejadian dan periode development pada jumlah besaran klaim melalui parameter model $\theta \in R^{p\times 1}$. Prediktor linear $\eta_i = z_{i,j}^{T}\theta$ bersama dengan fungsi link$g$ sepenuhnya menentukan struktur rata-rata μ_i.

Setelah memahami pilar I, langkah selanjutnya adalah melakukan pemilihan struktur rata-rata. Struktur rata-rata digunakan untuk menunjukkan dasar dari GEE. Menurut Hudecova dan Pesta (2013) Logaritma fungsi link dengan struktur rata-rata adalah

$$\log\left(\mu_{i,j}\right) = \gamma + \alpha_i + \beta_j$$

Dimana γ merupakan parameter dasar (*baseline parameter*) lalu $\alpha_i$dan β_j merupakan parameter yang merepresentasikan pengaruh dari periode kejadian i (kecelakaan/ terjadi klaim) dan periode pengembangan j masing-masing. Baseline parameter digambarkan dengan $\alpha_1 = 0 = \beta_1$.

Parameter γ, α_idan β_j membentuk vektor

$\theta = ¿$

dan

$z_{i,j} = ¿$

2 **Pilar 2: Fungsi *Variance***

Asumsikan bahwa varians dari klaim *incremental* dapat dinyatakan sebagai fungsi varians h dari ekspektasinya

$$Var\, X_{i,j} = \phi h(\mu_{i,j})$$

Dimana $\phi > 0$ merupakan parameter dispersi (parameter skala).

Sehubungan dengan GLM, jika $X_{i,j}$ mengikuti distribusi gamma, maka $h(x) = x^2$. Pada kerangka kerja GEE, tidak diperlukan distribusi keseluruhan dari data, karena pada metode GEE menggunakan *quasi-likelihood.*

Langkah selanjutnya adalah dengan memilih Fungsi Varians. Pada GEE, fungsi varian yang sesuai untuk pencadangan klaim adalah fungsi varians linier dan fungsi varians kuadratik, dimana vektor *quasi-score* sesuai dengan vektor skor dari distribusi Poisson yang overdispersi dan fungsi varians kuadratik yang sesuai dengan distribusi gamma. Fungsi varians sebagai suatu kekuatan *non-integer* dari *mean* dapat menjadi pilihan jika diketahui konkordansi dengan ditribusi Tweedie.

3 Pilar 3: Struktur Korelasi

Dalam menentukan korelasi antara komponen dari X_i dimodelkan menggunakan matriks *working correlation*

$$C_i(\vartheta) \in R^{(n-i+1)\times(n-i+1)}$$

Bergantung hanya pada suatu vektor $s \times 1$ dari ϑ suatu *unknown* parameter , dimana sama pada setiap periode kejadian i. Hal ini berakibat, matriks *working correlation*dari klaim incremental menjadi

$$V_i = Cov\, X_i = \phi A_i^{\frac{1}{2}} C_i(\vartheta) A_i^{\frac{1}{2}}$$

dimana A_i merupakan suatu matriks diagonal $(n-1+1)\times(n-i+1)$ dengan $h(\mu_{i,j})$ sebagai elemen diagonal ke j. Kata "*working*" berasal dari fakta bahwa struktur dari C_i tidak perlu ditentukan secara spesifik.

Setelah memahami pilar III, maka langkah selanjutnya adalah memilih struktur korelasi yang dapat digunakan dalam mengestimasi cadangan klaim. Terdapat berbagai pilihan struktur korelasi yang dapat digunakan dalam mengestimasi cadangan klaim. Terdapat lima struktur korelasi pada GEE, yaitu

I **Struktur Korelasi *Independent* (*uncorrelated*)**, merupakan bentuk yang paling sederhana, yaitu jika klaim incremental tidak berkorelasi. Memiliki bentuk

$$C_i(\vartheta) = I_{n-i+1} = \{\delta_{j,k}\}_{j,k=1}^{n-i+1,n-i+1}$$

II **Struktur Korelasi *Unstructured***, merupakan suatu kasus ekstrem yang berlawanan dimana matriks korelasi yang tidak terstruktur

$$C_i(\vartheta) = \{\vartheta_{j,k}\}_{j,k=1}^{n-i+1,n-i+1}$$

Sehingga $\vartheta_{j,j} = 1$ dan $C_i(\vartheta)$ merupakan definit positif

III **Struktur Korelasi Exchangeable,** sebagai kompromi dari dua kasus ekstrem, memiliki bentuk

$$C_i(\vartheta) = \{\delta_{j,k} + (1-\delta_{j,k})\vartheta\}_{j,k=1}^{n-i+1,n+1}, ¿$$

IV **Struktur Korelasi *m-dependent,*** struktur ini memiliki bentuk

$$C_i(\vartheta) = \{C_{j,k}\}_{j,k=1}^{n-i+1,n+1}$$

dimana

$$C_{j,k} = \begin{cases} 1, & j = k \\ \vartheta_{|j-k|}, & 0 < |j-k| \le m, \vartheta = \{\vartheta_l\}_{l-1}^{m} \\ 0, & ¿\, j-k \vee ¿\, m \end{cases}$$

V **Struktur Korelasi Autoregressive AR (1)**, struktur korelasi ini memiliki bentuk

$$C_i(\vartheta) = \{\vartheta^{|j-k|}\}_{j,k=1}^{n-i+1,n+1}, \vartheta = ¿$$

Pada penelitian kali ini akan digunakan tiga struktur korelasi, yaitu struktur korelasi AR (1), *exchangeable*, dan *independent.*

Setelah dilakukan pemilihan terhadap elemen di dalam tiga pilar, langkah terakhir yang dikerjakan adalah menghitung nilai estimasi cadangan klaim. Estimasi Cadangan Klaim pada

metode GEE, persamaan estimasi umum dibentuk menggunakan persamaan

$$u(\theta)=\sum_{i=1}^{n} D_i^T V_i^{-1}(X_i-\mu_i)$$

dimana $D_i=\frac{\partial \mu_i}{\partial \theta}\equiv\left\{\frac{\partial \mu_{i,j}}{\partial \theta_k}\right\}_{j,k=1}^{n-i+i,\,p}$

Untuk suatu estimasi $(\hat{\phi},\hat{\vartheta})$ dari (ϕ,ϑ), estimasi parameter θ menyelesaikan persamaan

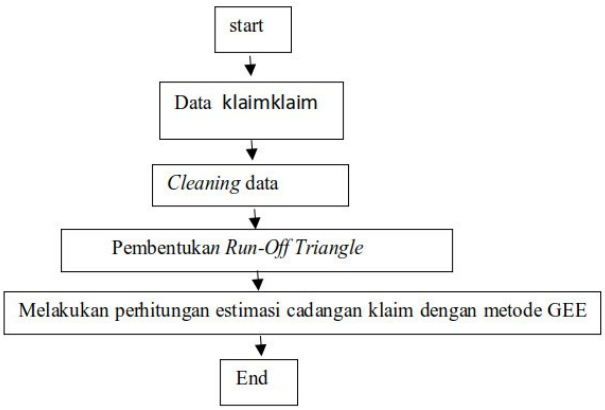
$$u(\hat{\theta})=0.$$

III. PERANCANGAN SISTEM

III.1.1. Data Penelitian

Data yang digunakan dalam penelitian ini adalah data *historical* pada lini bisnis asuransi kendaraan bermotor PT XYZ selama tahun 2015 dan 2016 (Januari 2015 sampai dengan Desember 2016). Penggunaan data 2015 dan 2016 bertujuan untuk melakukan estimasi besar klaim dengan menggunakan data 2015 lalu hasil estimasi yang didapat akan dibandingkan dengan data 2016.

III.1.1.1. Perancangan Sistem



1 Data klaim
Data yang didapat adalah data keseluruhan dari klaim yang terjadi pada PT XYZ
2 Proses *cleaning* data untuk merapikan data.
3 Pembentukan *Run-Off Triangle*
4 Setelah dilakukan proses cleaning data maka proses selanjutnya adalah pembentukan *Run-Off Triangle,* pembentukan *run-off triangle incrementatatil* menggunakan *R-Project*
5 Melakukan perhitungan estimasi cadangan klaim dengan metode GEE

IV. PEMBAHASAN

Dalam melakukan penilaian terhadap hasil estimasi cadangan klaim untuk tahun 2016 dengan metode *GEE.*. Berikut merupakan data klaim yang terjadi pada lini bisnis asuransi kendaraan bermotor PT XYZ pada awal hingga akhir tahun 2016 (setelah dilakukan proses *cleaning*)

Tabel 1 : Data Klaim PT XYZ

Periode Kecelakaan	Jumlah Klaim
2	-
3	-
4	6.500.000
5	4.500.000
6	4.000.000
7	74.500.000
8	85.397.097
9	22.350.000
10	261.500.000
11	82.010.000
12	502.003.240
Total	1.042.760.337

Pada tabel 1 di atas terlihat klaim yang terjadi setiap bulannya serta total klaim yang terjadi selama tahun 2016. pada asuransi kendaraan bermotor PT XYZ sebesar Rp 1,042,760,337.

Terdapat enam model lainnya berasal dari Metode GEE dimana struktur korelasi AR (1), exchangeable, dan independentdigabungkan dengan fungsi varians linier dan kuadrat.

Perhitungan Estimasi Cadangan Klaim dengan Metode GEE dapat dilihat pada tabel 2, dioleh dengan aplikasi R. Untuk perbandingan hasil maka digunakan metode Chain Leader untuk pembandingan hasil

Tabel 2 : Perhitungan Estimasi Cadangan Klaim dengan Metode GEE dan Chain Leader

Periode Kecelakaan	data 2016	Chain Ladder	GEE AR(1)		GEE Exchangeable		GEE Independent	
			Liniear Variance Function	Quadratic Variance Function	Liniear Variance Function	Quadratic Variance Function	Liniear Variance Function	Quadratic Variance Function
2	-	3,916,821.35	3,787,010	5,137,197	2,155,883	5,159,527	3,916,821	5,159,527
3	-	10,578,578.07	10,570,103	13,022,801	8,718,851	12,991,173	10,578,578	12,991,173
4	6,500,000.00	11,020,080.11	11,099,536	10,516,285	8,805,754	10,491,993	11,020,080	10,491,993
5	4,500,000.00	18,788,461.34	18,368,523	21,082,823	16,277,274	21,129,485	18,788,461	21,129,485
6	4,000,000.00	54,822,422.01	54,591,144	60,427,661	51,984,683	60,544,926	54,822,422	60,544,926
7	74,500,000.00	65,439,005.41	64,442,677	70,718,328	63,371,196	70,885,373	65,439,005	70,885,373
8	85,397,097.00	111,972,045.55	111,611,381	120,698,205	109,301,248	120,837,821	111,972,046	120,837,821
9	22,350,000.00	146,936,777.04	146,815,242	138,751,710	143,046,767	138,752,042	146,936,777	138,752,042
10	261,500,000.00	257,702,881.82	258,702,932	351,874,463	262,964,811	352,489,985	257,702,882	352,489,985
11	82,010,000.00	484,482,698.50	481,955,683	413,872,914	475,192,852	414,070,968	484,482,699	414,070,968
12	502,003,240.00	554,104,747.94	553,391,975	588,269,092	550,004,205	588,508,801	554,104,748	588,508,801
Total	1,042,760,337.00	1,719,764,519.14	1,715,336,206	1,794,371,479	1,691,823,524	1,795,862,094	1,719,764,519	1,795,862,094

Pada baris “data 2016” menunjukkan klaim yang terjadi pada tahun 2016 untuk tiap bulan serta total dari seluruh klaim, jumlah klaim pada baris ini menunjukkan jumlah dana yang seharusnya dicadangkan dan sebagai patokan penilaian terhadap prediksi dari model-model yang diterapkan.

Setiap estimasi yang dibuat oleh tiap model selalu lebih tinggi dibandingkan nilai aktual data 2016. Nilai estimasi yang dibentuk oleh model *Chain-Ladder* mempunyai beberapa nilai yang mendekati nilai aktual pada tahun 2016 yaitu pada bulan ke-7, ke-10, serta bulan ke-12. Untuk nilai pada bulan lainnya memiliki nilai yg terpaut cukup jauh. Sehingga perbedaan total klaim dibandingkan dengan data aktual adalah sebesar Rp 677,004,182.14. Sedangkan nilai estimasi yang dihasilkan model GEE tidak berbeda jauh dengan nilai estimasi yang dihasilkan oleh model *Chain-Ladder.* Nilai estimasi total cadangan klaim yang dihasilkan oleh ketiga struktur korelasi GEE berada pada kisaran Rp 1,7 M dengan nilai estimasi terendah berada pada Rp 1,691,823,524 yang didapat pada struktur korelasi *exchangeable* yang digabungkan dengan fungsi varians linier dan nilai estimasi tertinggi berada pada Rp 1,795,862,094, pada struktur korelasi *independent* yang digabungkan dengan fungsi varians kuadrat serta struktur korelasi *exchangeable* yang digabungkan dengan fungsi varian kuadrat (memiliki nilai yang sama) .

Nilai estimasi yang memiliki yang mendekati data aktual tahun 2016 adalah nilai estimasi yang dihasilkan oleh struktur korelasi exchangeable yang digabungkan dengan fungsi varians linier yaitu sebesar Rp 1,691,823,524 dengan perbedaan dengan data aktual 2016 sebesar Rp 649,063,187.

Untuk memperkuat perbandingan dan melihat seberapa besar kesalahan estimasi yang dihasilkan, digunakan MAPE (Mean Absolut Percentage Error) yang dihasilkan estimasi pada model GEE dan *Chain-Ladder*. MAPE merupakan rata-rata dari hasil keseluruhan persentase kesalahan antara data aktual dengan data hasil estimasi (Selisih). Ukuran akurasi ditunjukkan dalam bentuk persentase. Pada hasil estimasi dari metode GEE dan *Chain-Ladder* dilihat tidak terdapat nilai ekstrem, yaitu nol atau mendekati nol, sehingga metode MAPE dapat digunakan sebagai evaluasi dari nilai estimasi yang didapatkan.

Pada tabel 3 di bawah diperlihatkan kesalahan persen absolut untuk tiap bulan dengan dibandingkan dengan data akual 2016 dan MAPE dari hasil estimasi yang didapat dari tiap model. Mean Absolute Percentage Error hasil Estimasi Berdasarkan Data Aktual 2016 dapat dilihat pada tabel 3 di bawah ini

Tabel 3 : *Mean Absolute Percentage Error* Hasil Estimasi Berdasarkan Data Aktual 2016

Periode Kecelakaan	data 2016	Chain Ladder	GEE AR(1)		GEE Exchangeable		GEE Independent	
			Liniear Variance Function	Quadratic Variance Function	Liniear Variance Function	Quadratic Variance Function	Liniear Variance Function	Quadratic Variance Function
2	-	100%	100%	100%	100%	100%	100%	100%
3	-	100%	100%	100%	100%	100%	100%	100%
4	6,500,000	41%	41%	38%	26%	38%	41%	38%
5	4,500,000	76%	76%	79%	72%	79%	76%	79%
6	4,000,000	93%	93%	93%	92%	93%	93%	93%
7	74,500,000	14%	16%	5%	18%	5%	14%	5%
8	85,397,097	24%	23%	29%	22%	29%	24%	29%
9	22,350,000	85%	85%	84%	84%	84%	85%	84%
10	261,500,000	1%	1%	26%	1%	26%	1%	26%
11	82,010,000	83%	83%	80%	83%	80%	83%	80%
12	502,003,240	9%	9%	15%	9%	15%	9%	15%
MAPE		57%	57%	59%	55%	59%	57%	59%

Dapat dilihat bahwa MAPE dengan kesalahan terkecil terdapat pada nilai estimasi yang dihasilkan oleh struktur korelasi *exchangeable* yang digabungkan dengan fungsi varians linier yaitu dengan nilai kesalahan sebesar 55%.

V. KESIMPULAN

Berdasarkan hasil pembahasan dari penelitian ini dapat disimpulkan bahwa setiap estimasi yang dibuat oleh tiap model selalu lebih tinggi dibandingkan nilai aktual data 2016. Nilai estimasi yang dibentuk oleh model baik model GEE maupun *Chain-Ladder* mempunyai beberapa nilai yang mendekati nilai aktual pada tahun 2016 yaitu pada bulan ke-7, ke-10, serta bulan ke-12. Untuk nilai pada bulan lainnya memiliki nilai yg terpaut cukup jauh. Nilai estimasi yang memiliki yang mendekati data aktual tahun 2016 adalah nilai estimasi yang dihasilkan oleh struktur korelasi exchangeable yang digabungkan dengan fungsi varians linier yaitu sebesar Rp 1,691,823,524 dengan perbedaan dengan data aktual 2016 sebesar Rp 649,063,187. Untuk memperkuat perbandingan dan melihat seberapa besar kesalahan estimasi yang dihasilkan berdasarkan perhitungna dengan *Mean Absolute Percentage Error* Hasil Estimasi Berdasarkan Data Aktual 2016 nilai estimasi yang dihasilkan model GEE dan *Chain-Ladder* memiliki kesalahan berkisar pada 55% sampai dengan 60%.

VI. DAFTAR PUSTAKA

Antonio, K., Beirlant, J., Hoedemakers, T & Verlaak, R. (2006). Lognormal mixed models for reported claim reserve. *North American Actuarial Journal 10(1),30–48.*

Antonio, K & Beirlant, J.(2007). Actuarial statistics with generalized linear mixed models. *Insurance: Mathematics and Economics40,58–76.*

England, P.D & Verrall, R.J.(2002). Stochastic claims reserving in general insurance. *British Actuarial Journal 8,443–544.*

Gigante, P., Picech, L& Sigalotti, L. (2013). Prediction error for credible claims reserves: an h-likelihood approach. *European Actuarial Journal, 3(2),453-470.*

Hürlimann, W. (2009) Credible loss ratio claims reserves: The Benktander, Neuhaus and Mack methods revisited.*Astin Bulletin, 39(01)*.

Hudecová,Š& Pešta, M. (2013). Modeling dependencies in claims reserving with GEE. *Insurance: Mathematics and Economics 53(2013),786–794*

Kim, Sungil & Kim, Heeyoung. (2016). A New Metric od Absolute Percentage Error for Intermittent Demand Forecast. *International Journal of Forcasting 32,669-679*

Mack, T.(1993). Distribution-free calculation of the standard error of chain ladder reserve estimates. *Astin Bulletin 23(2),213–225.*

Peraturan Ketua Bapepam-LK Nomor: PER-09/BL/2012 tentang Pedoman Pembentukan Cadangan Teknis bagi Perusahaan Asuransi dan Perusahaan Reasuransi.

Peraturan Menteri Keuangan Nomor 53/PMK.010/2012 tentang Kesehatan Keuangan Perusahaan Asuransi dan Perusahaan Reasuransi.

Taylor, G., McGuire, G., & Greenfield, A. (2003). Loss Reserving: Past, Present and Future. *Casualty Actuarial Society*, 2003

Vladimirovich, M et al. (2013). A Survey of Forecast Error Measures. *World Applied Sciences Journal 24,171-176.*

Wüthrich, M.V& Merz, M.(2008). *Stochastic Claims Reserving Methods in Insurance*. In: Wiley Finance Series, John Wiley & Sons

Penerapan Algoritma RC6 dan Vigenere pada Aplikasi SMS berbasis Android

Fatmasari Tarigan[1)], Ahmad Pudoli[2)]

[1)] STMIK Antar Bangsa, Teknologi Informasi,
Jl. Raden Fatah No 70A. Pondok Aren. Ciledug. 10412
Telp: (021) 31908575
fsarie@gmail.com

[2)] Universitas Budi Luhur, Fakultas Teknologi Informasi,
Jl. Ciledug Raya. Petukangan Utara. Jakarta Selatan, Jakarta, 12260
Telp: (021) 5853753
ahmad.pudoli@budiluhur.ac.id

ABSTRAK — Keamanan pesan merupakan suatu hal yang sangat penting dan perlu dijaga kerahasiaannya agar pesan tidak dapat dibaca oleh orang lain, maka dari itu pada Kecamatan Pinang yang bergerak dalam sektor publik serta bekerja untuk memberikan layanan yang lebih baik kepada masyarakat. Untuk itu bapak Camat dan Kasubag masih menggunakan layanan SMS untuk memberikan informasi tentang kegiatan sehari-hari seperti, mengadakan rapat dinas antara kecamatan maupun kelurahan dan mengenai proyek lapangan yang sedang dibuat antara bapak camat (ketua kecamatan) dan bapak lurah (ketua kelurahan) yang tidak boleh diketahui oleh masyarakat dan sangat dirahasiakan. Maka tujuan dibuatnya aplikasi ini diharapkan bisa menimplementasikan algoritma RC6 (Rivest Code 6) dan Vigenere Cipher untuk mengamankan pesan yang berbentuk teks berbasis android. Dengan mengkombinasikan algoritma RC6 (Rivest Code 6) dan algoritma Vigenere Cipher dalam satu proses enkripsi dan dekripsi, proses enkripsi dilakukan melalui inputan plaintext (data asli atau data yang dapat dibaca) yang akan dienkripsi oleh algoritma RC6 (Rivest Code 6), kemudian hasil enkripsi melalui algoritma RC6 (Rivest Code 6) yang masih berbentuk Ciphertext (data yang tidak dapat dibaca) dijadikan proses masukan plaintext untuk enkripsi yang diproses algoritma Vigenere Cipher, kemudian dari proses enkripsi algoritma Vigenere Cipher didapat suatu Ciphertext kemudian menjadi hasil akhir. Dan untuk proses dekripsi menggunakan metode sebaliknya yaitu, Ciphertext yang merupakan hasil proses enkripsi yang dilakukan algoritma Vigenere Cipher menjadi masukan Plaintext untuk dilakukan proses dekripsi dengan algoritma Vigenere Cipher terlebih dahulu, setelah itu dilakukan proses dekripsi menjadi plaintext yang berbentuk Ciphertext kemudian dilakukan proses dekripsi lagi dengan algoritma RC6 (Rivest Code 6) dan didapatkan hasil keluaran Plaintext yang merupakan data awal. Hasil akhir yang didapat pada aplikasi ini adalah bisa mengimplementasikan algoritma RC6 (Rivest Code 6) dan Vigenere Cipher pada proses enkripsi dan dekripsi dalam satu proses. Maka dibuat kesimpulan yaitu diharapkan kepada bapak Camat dan Kasubag pada kantor Kecamatan Pinang Mempunyai aplikasi ini untuk memberikan informasi penting dan terjaga kerhasiaannya tanpa diketahui orang lain.

Kata kunci: kriptografi, rc6, vigenere

ABSTRACK — Message security is a very important matter and needs to be kept confidential so that messages cannot be read by others, therefore in Pinang District which is engaged in the public sector and works to provide better services to the community. For this reason, the head of the sub-district and the head of the sub-district still use the SMS service to provide information about daily activities such as holding official meetings between sub-districts and sub-districts and regarding field projects that are being made between the camat (head of the sub-district) and the village head (head of the village) who are not can be known by the public and very confidential. So the purpose of making this application is expected to be able to implement the RC6 (Rivest Code 6) and Vigenere Cipher algorithms to secure messages in the form of text based on android. By combining the RC6 algorithm (Rivest Code 6) and the Vigenere Cipher algorithm in one encryption and decryption process, the encryption process is carried out through plaintext input (original data or readable data) which will be encrypted by the RC6 algorithm (Rivest Code 6), then the encryption results through the RC6 (Rivest Code 6) algorithm which is still in the form of Ciphertext (unreadable data) it is used as a plaintext input process for encryption processed by the Vigenere Cipher algorithm, then from the encryption process the Vigenere Cipher algorithm is obtained a Ciphertext then becomes the final result. And for the decryption process using the opposite method, namely, Ciphertext which is the result of the encryption process carried out by the Vigenere Cipher algorithm becomes Plaintext input for the decryption process with the Vigenere Cipher algorithm first, after that the decryption process is carried out into plaintext in the

form of Ciphertext then the decryption process is carried out again with algorithm RC6 (Rivest Code 6) and the Plaintext output is the initial data. The final result obtained in this application is that it can implement the RC6 (Rivest Code 6) and Vigenere Cipher algorithms in the encryption and decryption processes in one process. So a conclusion is drawn, that is, it is hoped that the Head of Sub-District and the Head of Sub-Division at the Pinang District office. Having this application is to provide important information and keep its confidentiality without anyone knowing.

Keywords: cryptography, rc6, vigenere

I. PENDAHULUAN

I.1. Latar Belakang

Pada saat ini perkembangan teknologi menjadi bagian penting dan suatu kebutuhan pada instansi Kecamatan Pinang yang bergerak dalam sektor publik serta diiringi tuntunan untuk meningkatkan produktivitas untuk memberikan layanan yang lebih baik kepada masyarakat dan meningkatkan kinerja pada sebuah penerapan Teknologi Informasi dan Komunikasi (TIK) pada kecamatan Pinang, mengingat peran TIK yang sangat penting untuk peningkatan kualitas layanan sebagai salah satu realisasi yang baik. Dalam peningkatkan kualitas layanan, faktor keamanan informasi merupakan aspek yang penting untuk diperhatikan, mengingat kinerja pada sebuah Kecamatan Pinang dan kerahasiaannya.

Berkaitan dengan kerahasiaan, salah satu teknik pengamanan data adalah kriptografi yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan sebuah data. Pengiriman atau penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan kerahasiaan dari data yang di kirimkan. Data tersebut tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan ditujuan. Untuk memenuhi kebutuhan tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirim.

Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel masih banyak digunakan oleh masyarakat luas, dan bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi dengan baik. Selain itu, pengiriman SMS yang dilakukan tidak sampai ke penerima secara langsung, namun pengiriman SMS harus melewati Short Message Service Center (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima. Dengan tersimpannya SMS pada SMSC, seorang operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut.

Dengan demikian dibutuhkan suatu pengamanan pada aplikasi tersebut. Inilah kenapa metode dan aplikasi encrypted end to end dengan melakukan enkripsi terhadap pesan SMS dibutuhkan. Enkripsi adalah proses mengubah suatu pesan asli yang disebut plaintext menjadi sebuah sandi atau kode yang tidak terbaca yang disebut ciphertext yang tidak dapat dimengerti.

Pada perkembangan teknologi saat ini, telepon selular berbasis Android telah banyak dipakai oleh banyak pengguna telepon selular. Selain itu, Android bersifat terbuka, gratis, dan hampir setiap kode program Android diluncurkan berdasarkan lisensi open source Apache yang berarti bahwa setiap orang yang ingin menggunakan Android dapat mengunduh source code nya.

Pada penelitian ini dibuatlah sebuah aplikasi berbasis mobile Android dengan menggunakan metode algoritma Kriptografi RC6 (Rivest Code) dan VIGENERE CIPHER pada aplikasi SMS(Short Message Service) untuk pesan teks SMS. Perangkat lunak yang dibangun merupakan perangkat lunak yang diterapkan pada telepon selular yang bersistem operasi Android dan memiliki fungsi untuk melakukan enkripsi dan dekripsi pesan.

I.2. Masalah

Dari latar belakang tersebut, terdapat masalah yang terjadi; yaitu:

- Bagaimana mengimplementasikan aplikasi enkripsi SMS berbasis android dengan metode RC6 (Rivest Code) dan Vigenere cipher.
- Bagaimana cara mengembalikan data dan pesan yang sudah di enkripsi menjadi data yang asli tanpa mengalami perubahan sedikitpun.
- Bagaimana user bisa menggunakan pesan yang di kirim tetap terjamin privasinya.

I.2.1. Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

- Membuat sebuah aplikasi pengamanan SMS (short Message Service) berbasis android menggunakan algoritma RC6 (Rivest Code) dan Vigenere Cipher agar pesan yang dikirim tetap terjamin keamanannya`
- Mengamankan isi pesan SMS (Short Message Service) yang berupa teks.

- Pesan SMS (Short Message Service) akan dikirim setelah melakukan enkripsi dan pesan akan di dekripsi atau mengembalikan pesan seperti semula.

I.2.2. Batasan Masalah

Agar penelitian ini tidak keluar dari pembahasan maka diperlukan ruang lingkup masalah, yaitu:

- Algoritma Kriptografi yang digunakan untuk mengamankan pesan adalah algoritma RC6 (Rivest Code) dan vigenere cipher.
- Aplikasi yang digunakan berbasis android.
- Pesan yang dapat dienkripsi dan dekripsi berupa teks.
- Jenis perangkat mobile harus beroperasi sistem android minimal versi 4.4. (Kitkat)

II. LANDASAN TEORI

II.1. SMS

SMS (Short Message Service) merupakan sebuah layanan yang banyak di aplikasikan pada sistem komunikasi tanpa kabel, memungkinkan dilakukan pengiriman pesan dalam bentuk teks. SMS didukung oleh GSM (Global System for Mobile Communication), TDMA (Time Division Multiple Access), CDMA (Code Division Multiple Access) yang berbasis pada telepon seluler saat ini banyak digunakan. SMS (Short Message Service) adalah merupakan salah satu layanan pesan teks yang dikembangkan dan distandarisasi oleh suatu badan yang bernama ETSI (European Telecommunication Standards Institute) sebagian dari pengembangan GSM (Global System for Mobile Communication), yang terdapat pada dokumentasi GSM 03.40 dan GSM 03.38. Fitur SMS ini memungkinkan perangkat Stasiun Seluler Digital (Digital Cellular Terminal, seperti ponsel) untuk dapat mengirim dan menerima pesan-pesan teks dengan panjang sampai dengan 160 karakter melalui jaringan GSM. SMS dapat dikirimkan ke perangkat stasiun seluler digital lainnya hanya dalam beberapa detik selama berada pada jangkauan pelayanan GSM.

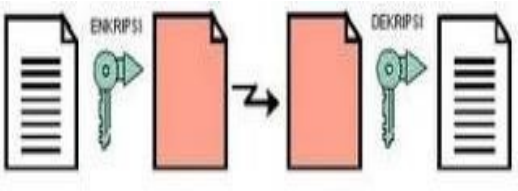
II.2. Kriptografi

Adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter.Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak dibeberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter.Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan(parameter menjadi ekuivalen dengan kunci).

Pengelompokan algoritma juga dilakukan berdasarkan kunci enkripsi – dekripsi yang digunakan, yaitu symmetric cryptosystem atau simetris (menggunakan kunci yang sama untuk proses enkripsi – dekripsi) dan Assymmetric cryptosystem atau asimetris (menggunakan kunci yang berbeda untuk proses enkripsi – dekripsi). [2]

II.2.1. Symetric Cryptosystem

Symmetric cryptosystem atau kriptografi simteris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Contoh algoritma kunci simetris yang terkenal adalah DES (Data EncryptionStandard) dan RC-4, sebagaimana ditunjukkan pada gambar 2 berikut :



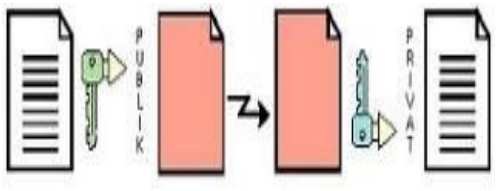
Gambar 1: Kunci Simetris

Ada beberapa kelebihan menggunakan kunci simetris yang sudah diketahui yaitu Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik walupun hal ini berbanding lurus dengan penambahan ukuran file, kecepatan proses enkripsi/dekripsi bergantung pada besarnya ukuran file, semakin besar ukuran file semakin banyak waktu yang dibutuhkan untuk enkripsi/dekripsi, selain itu Karena kecepatannya yang cukup tinggi, maka dapat digun akan pada sistem real-time. Namun terdapat pula kelemahannyya, yaitu Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut, dan Permasalahan dalam pengiriman kunci itu sendiri yang disebut “key distribution problem”. [2] Algoritma simetri terbagi menjadi dua jenis, yaitu adalah Stream Cipher dan Block Cipher.

II.2.2. Asymetric Cryptosystem

Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan

suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci private untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya. Sebagai contoh jika Anto mengirim pesan untuk Badu, Anto dapat merasa yakin bahwa pesan tersebut hanya dapat dibaca oleh Badu, karena hanya Badu yang bisa melakukan dekripsi dengan kunci privatnya. Tentunya Anto harus memiliki kunci publik Badu untuk melakukan enkripsi. Anto bisa mendapatkannya dari Badu, ataupun dari pihak ketiga seperti Tari.



Gambar 2: Kunci Asimetris

Teknik enkripsi asimetris ini jauh lebih lambat dibandingkan enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi. Contoh algoritma terkenal yang menggunakan kunci Asimetris adalah RSA (merupakan singkatan penemunya yakni Rivest, Shamir dan Adleman). [2]

II.3. Algoritma RC6

Algoritma RC6 merupakan salah satu kandidat Advanced Encryption Standard (AES) yang diajukan oleh RSA Laboratoriest kepada NIST. Dirancang oleh Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin, algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST. RC6 dirancang untuk menghilangkan segala ketidakamanan yang ditemukan pada RC5, karena analisis pada RC5 menunjukkan bahwa ternyata jumlah rotasi yang terjadi pada RC5 tidak sepenuhnya bergantung pada data yang terdapat dalam blok. Selain itu, serangan kriptanalisis diferensial juga ternyata dapat menembus keamanan yang ditawarkan RC5.

RC6 juga dirancang untuk memenuhi persyaratan AES yang diantaranya adalah kemampuan untuk beroperasi pada mode blok 128 bit. Jika besar blok 128 bit langsung dipaksakan untuk diimplementasikan dengan algoritma RC5, maka akan dibutuhkan register kerja 64 bit. Spesifikasi arsitektur dan bahasa yang menjadi tempat implementasi algoritma yang ditentukan oleh AES belum mendukung pengoperasian 64 bit yang efisien. Oleh karena itu, daripada menggunakan 2 register 64 bit seperti pada RC5, RC6 menggunakan 4 register 32 bit. Karena menggunakan 4 register maka akan terdapat 2 operasi rotasi pada setiap half-round yang ada, dan juga akan lebih banyak bit-bit yang akan digunakan untuk mempengaruhi banyaknya bit yang dirotasi. Algoritma RC6 adalah versi yang dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b, dimana parameter w merupakan ukuran kata dalam satuan bit, r adalah bilangan bulat bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi, dan b menunjukan ukuran kunci enkripsi dalam byte.

II.4. Algoritma Vigenere

Vigenere cipher adalah salah satu contoh metode kriptografi kunci simetris dengan tingkat keamanan kunci yang lebih sulit dipecahkan. Hal ini disebabkan algoritma dari vigenere cipher merupakan bentuk sederhana dari subtitusi polialfabetik dengan kunci enkripsi berupa huruf. Dengan adanya tingkat keamanan data yang rendah pada data berupa teks maka penelitian ini diharapkan dapat memberikan prosedur pengamanan pada data berupa teks dengan modifikasi vigenere cipher.

Tujuan utama dari Vigenere cipher ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.

III. Perancangan Aplikasi

III.1. Analisa Masalah

Pesan merupakan data yang sangat penting baik itu berupa pesan pribadi, perusahaan atau organisasi dan lain sebagainya. Oleh karena itu, sebuah pesan khusus seharusnya dijaga kerahasiaannya agar tidak di salahgunakan oleh orang yang tidak berhak dan bertanggung jawab. Di sini seringkali masalah keamanan menjadi urutan kedua atau bahkan urutan yang terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performa sistem, masalah keamanan ini sering dikurangi atau bahkan dihilangkan. Salah satu cara untuk mengamankan sebuah pesan yaitu dengan mengubah pesan asli menjadi pesan yang tidak bisa dibaca oleh orang lain atau sering disebut dengan enkripsi. Untuk mengimplementasikan enkripsi pesan dibutuhkan algoritma enkripsi agar dokumen tersebut bisa dienkripsi dan kemudian dikembalikan seperti semula atau dekripsi tanpa mengalami perubahan sehingga diperlukan suatu aplikasi yang dapat memberikan solusi dari permasalahan yang ada. Pada penulisan ini akan menggunakan algoritma RC6 (Rivest code 6) dan VIGENERE CIPHER. Pada Kecamatan Pinang ada berbagai macam data yang tidak diperkenankan oleh pihak yang tidak berkepentingan.

III.2. Spesifikasi Perangkat Keras

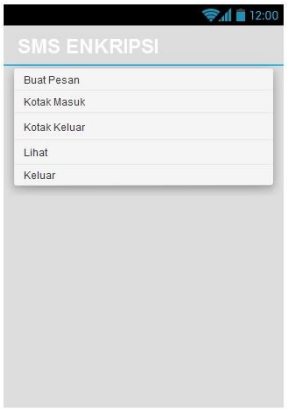
Perangkat keras yang dibutuhkan dalam membangun perangkat lunak ini memiliki spesifikasi, spesifikasi perangkat keras dapat dilihat sebagai berikut:

- Processor : Intel(R) Celeron(R) 2957U @ 1.40GHz
- Hardisk : 500 GB
- RAM : 2 GB

III.3. Rancangan Layar

III.3.1. Menu Utama

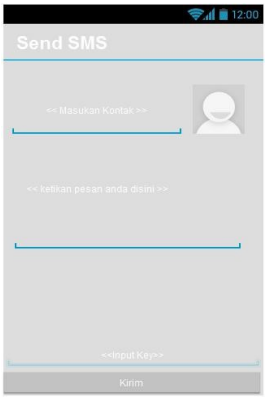
Pada rancangan menu utama tersedia beberapa menu yang dapat dipilih pengguna dan informasi yang dapat memudahkan pengguna dalam menjalakan aplikasi ini. Menu-menu yang tersedia pada aplikasi kriptografi ini.



Gambar 3: Menu Utama

III.3.2. Membuat Pesan

Memuat pesan SMS enkripsi yang akan dibuat dan dikirim oleh pengguna. Menu ini terdapat kotak untuk meng- input nomor tujuan, kotak untuk membuat teks pesan, kotak untuk meng- input key dalam enkripsi dan option kirim.



Gambar 4: Membuat Pesan

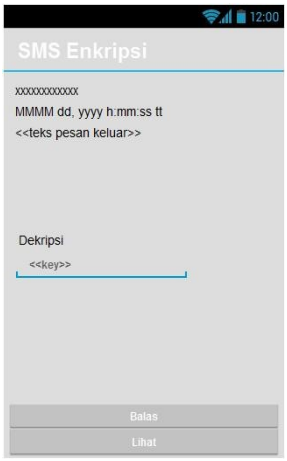
III.3.3. Inbox

Rancangan layar memuat pesan-pesan masuk yang menggunakan enkripsi ataupun pesan biasa.

Gambar 5: Inbox

III.3.4. Outbox

Rancangan ini memuat pesan-pesan keluar atau pesan terkirim yang menggunakan enkripsi ataupun pesan biasa.

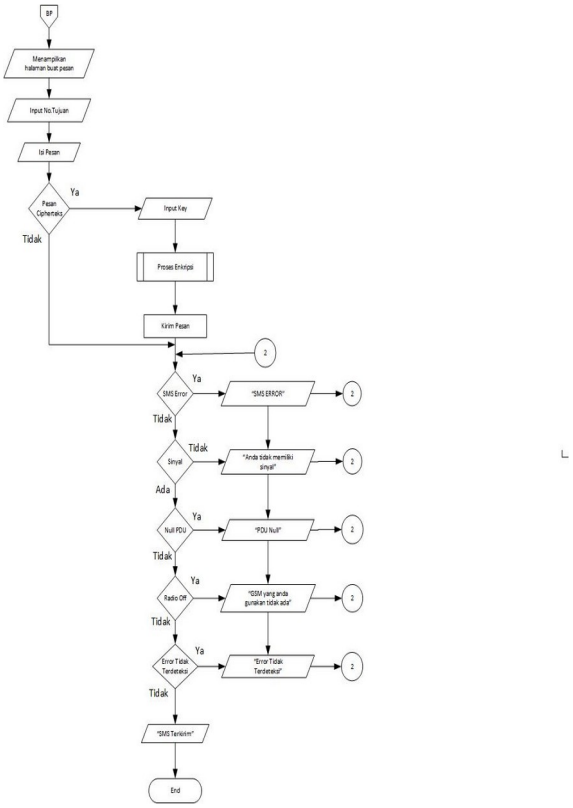


Gambar 6: Outbox

III.4. Flowchart

III.4.1. Membuat Pesan

Digunakan untuk membuat pesan baru, baik pesan biasa ataupun pesan enkripsi. Saat akan membuat pesan enkripsi, pengguna diharuskan mengisi key pada kolom yang tersedia.

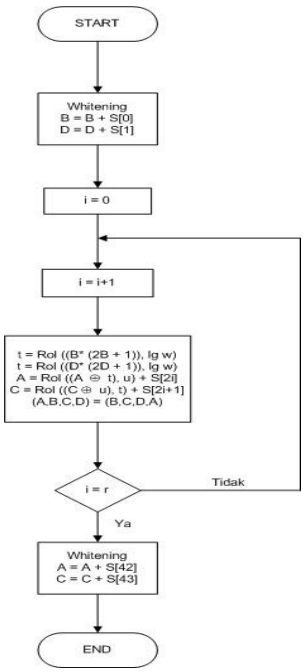


Gambar 7: Flowchart Membuat Pesan

III.4.2. RC6

III.4.2.1. Enkripsi

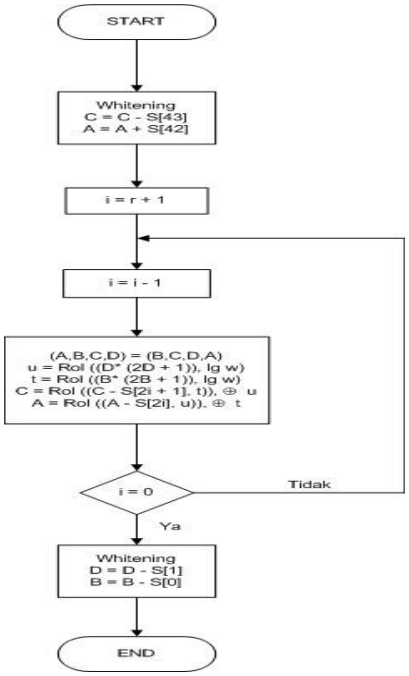
Flowchart ini akan menjelaskan proses enkripsi yang terjadi diprogram.



Gambar 8: Flowchart Enkripsi RC6

III.4.2.2. Dekripsi

Flowchart ini akan menjelaskan proses pengembalian pesan asli dari pesan enkripsi menjadi pesan asli.

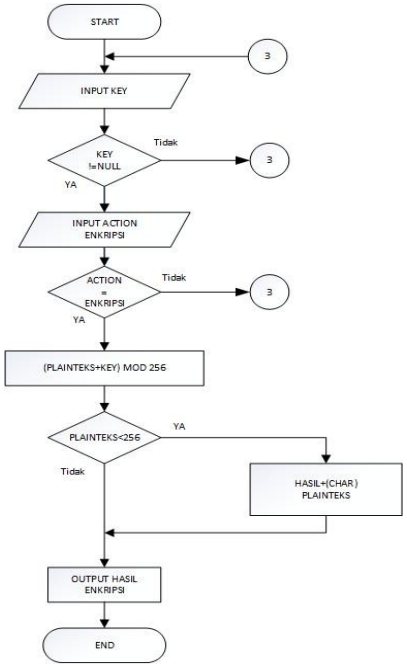


Gambar 9: Flowchart Dekripsi RC6

III.4.3. Vigenere

III.4.4. Enkripsi Vigenere

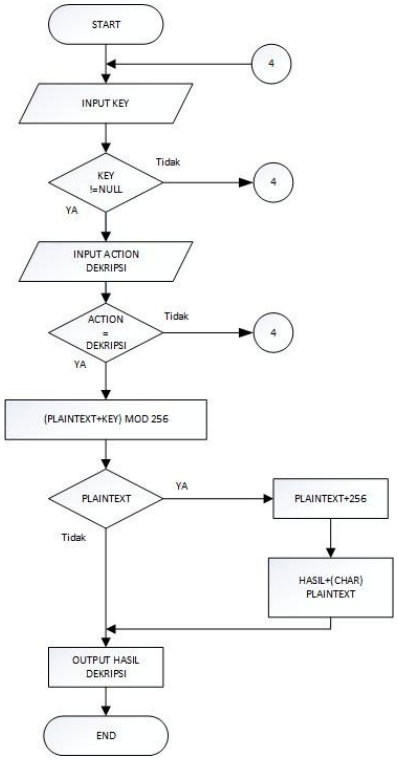
Flowchart ini akan menjelaskan proses pengembalian pesan asli dari pesan enkripsi menjadi pesan asli.



Gambar 10: Flowchart Enkripsi Vigenere

III.4.5. Dekripsi Vigenere

Flowchart ini akan menjelaskan proses pengembalian pesan asli dari pesan enkripsi menjadi pesan asli.



Gambar 11: Flowchart Dekripsi Vigenere

IV. Hasil Implementasi dan Analisa Program

IV.1. Implementasi

Agar aplikasi Enkripsi SMS berbasis android berjalan dengan baik, spesifikasi perangkat yang digunakan untuk implementasi aplikasi ini juga harus mendukung. Spesifikasi yang digunakan oleh pembuat aplikasi ini pada saat pembuatan aplikasi ini, diantaranya adalah:

- Perangkat keras

  Dalam pembuatan aplikasi ini requirement perangkat keras (hardware) yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

  - Laptop Acer One-4V57ETJL
  - Processor, Intel(R) Celeron(R) 2957U @1.40GHz (2CPUs),~1.4GHz
  - RAM (Random Access Memory) 2 GB
  - Smartphone Samsung Galaxy S8+
  - CPU, Samsung Exynos 2,31 GHz
  - RAM 4 GB

- Perangkat lunak

  Dalam pembuatan aplikasi enkripsi SMS, perangkat lunak yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

  - Sistem Operasi Android minimum 4.4. (kitkat)
  - Sistem Operasi Windows 10 64-bit
  - Eclipse

IV.2. Pengujian

Pengujian program merupakan salah satu hal yang perlu dilakukan dalam pembuatan perangkat lunak, untuk mengetahui hasil yang telah dicapai oleh aplikasi pengamanan pesan berbasis android yang telah dibuat dalam sebuah aplikasi. Pada aplikasi ini, penulis melakukan enkripsi dan dekripsi pesan SMS. Pengujian tersebut akan mendapatkan hasil perbandingan pesan asli dengan pesan yang telah dienkripsi. Selain uji coba enkripsi dan dekripsi.

IV.2.1. Proses Enkripsi

Berikut ini adalah tabel hasil pengujian proses enkripsi pada aplikasi yang dikembangkan:

Tabel 1: Pengujian Proses Enkripsi

Plaintext	**Kunci**	**Hasil enkripsi**
semoga berhasil	123	é.% á <ÕA'~ºkbÏ
semoga berhasil	abc	È_D Ñ'Þyz†Ÿ•)AÕ
semoga berhasil	ABC	T¶)Us w?; R$5
semoga berhasil	@1aB	ßK A÷8\t›B ¾~õ
semoga berhasil	+x&=$	Û¿ÔÄ Ú èÎºÎV® /

IV.2.2. Proses Dekripsi

Berikut ini adalah tabel hasil pengujian proses dekripsi pada aplikasi yang dikembangkan:

Tabel 2: Pengujian Proses Dekripsi

Ciphertext	**Kunci**	**Hasil dekripsi**
é.% á <ÕA'~ºkbÏ	123	semoga berhasil
È_D Ñ'Þyz†Ÿ•)AÕ	Abc	semoga berhasil
T¶)Us w?; R$5	ABC	semoga berhasil
ßK A÷8\t›B ¾~õ	@1aB	semoga berhasil
Û¿ÔÄ Ú èÎºÎV® /	+x&=$	semoga berhasil

IV.3. Evaluasi

Evaluasi program merupakan tahap terakhir yang perlu dilakukan dalam pengembangan suatu perangkat lunak. Evaluasi program bertujuan untuk mengetahui hasil yang telah dicapai oleh aplikasi dan menentukan kekurangan dan kelebihan aplikasi yang dibuat. Berdasarkan hasil uji coba program yang telah dilakukan, maka didapati beberapa kelebihan dan kekurangan pada aplikasi pengamanan pesan SMS berbasis Android adalah sebagai berikut :

IV.3.1. Kelebihan

1. Aplikasi dapat diakses dengan mudah menggunakan perangkat Android.
2. Aplikasi mudah dikelola dan digunakan.
3. Saat menekan tombol enkrip, pesan sudah otomatis terenkripsi.
4. Isi kotak masuk yang telah didekripsi akan kembali ke ciphertext setelah keluar dari kotak masuk.

IV.3.2. Kekurangan

1. Masih menggunakan code native belum menggunakan database.
2. Tidak semua hasil enkripsi dapat dibaca oleh sistem, karena program ASCII pada sistem perangkat android berbeda-beda.
3. Panjang pesan tidak terenkripsi hanya mencapai 160 karakter, jika lebih dari itu pesan tidak dapat dikirim.

V. Penutup

V.1. Kesimpulan

Kesimpulan yang dapat ditarik dari adanya permasalahan hingga solusi yang diberikan antara lain adalah:

- Dengan adanya aplikasi enkripsi, proses pengiriman pesan menjadi lebih aman dan tidak dapat dibaca oleh orang lain.
- Aplikasi enkripsi SMS dapat dibuat dengan perangkat, mobile berbasis android menggunakan Algoritma RC6 dan Vigenere Cipher.
- Menggabungkan algoritma RC6 dan Vigenere Cipher dalam satu proses.
- Aplikasi yang dihasilkan dapat mengenkripsi dan mendekripsi karakter text yang terdiri dari huruf besar, huruf kecil, angka, dan simbol.
- Aplikasi sangat membantu dalam proses pengiriman pesan menggunakan fitur enkripsi.
- Menurut responden hasil dari aplikasi enkripsi ini sangat baik dan membantu untuk keamanan dalam mengirim pesan.

V.2. Saran

Dengan keterbatasan yang ada dalam mengembangkan aplikasi, maka beberapa saran untuk pengembangan berikutnya adalah:

- Aplikasi dapat ditingkatkan lagi kinerjanya, dengan menggunakan database, serta tidak hanya mengirim pesan jenis teks namun dapat mengirim dan mengenkripsi dengan MMS (Multimedia Message) seperti gambar, dokumen dan lain-lain .
- Adanya fitur Hapus untuk menghapus pesan yg ada pada aplikasi ini.
- Adanya fitur draft untuk menyimpan pesan yang akan dikirim kemudian.
- Adanya fitur pin dan unpin untuk mengetahui pesan yang sudah dibaca dan belum dibaca.

VI. Daftar Pustaka

[1] Basri (2016) „Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi", Jurnal Ilmiah Ilmu Komputer, 2(2), pp. 17–23. Available at: http://ejournal.fikom-unasman.ac.id.

[2] Hendri (2016) „IMPLEMENTASI ALGORITMA COULUMNAR TRASPOSITION DAN ALGORITMA RC6 UNTUK MENGAMANKAN PESAN", 1(3), pp. 53–60.

[3] Jumrin, Sutardi and Subardin (2016) „Aplikasi sistem keamanan basis data dengan teknik kriptografi rc4", semanTIK, 2(1), pp. 59–64. Available at: http://ojs.uho.ac.id/index.php/semantik/article/view/715.

[4] Prabowo, H. E. and Hangga, A. (2015) „Enkripsi Data Berupa Teks Menggunakan Metode Modifikasi Vigenere Cipher", pp. 1–4.

[5] Purnama, B. (2014) „Pengamanan Pesan Rahasia Melalui Kriptografi Vigenere Cipher Dengan Kunci Berlapis", Media Processor, 9(3), pp. 1–8.

[6] Rionald Ricardo Mangundap, W. A. K. (2015) „Aplikasi secure message menggunakan algoritma rc6 berbasis android", e-Jurnal Spirit Pro Patria, 1(2), pp. 96–110.

[7] Sugiyanto and Hapsari (2016) „Pengembangan algoritma", Ultimatics, VIII(2), pp. 131– 138.

[8] Widi Puji Atmojo, R. Rizal Isnanto, R. K. (2016) „Implementasi Aplikasi Kriptografi Pada Layanan Pesan Singkat (SMS) Menggunakan Algoritma RC6 Berbasis Android", Jurnal Teknologi dan Sistem Komputer, 4(3), pp.450–453.doi:10.14710/jtsiskom.4.3.2016.450-453.

Aplikasi Penerimaan Karyawan Dengan Metode Analitycal Hierarchy Process (AHP) Berbasis Web Pada PT Kinarya Alihdaya Mandiri

Muhammad Husein[1)], Rizky Pradana[2)], Riri Irawati[3)]

[1, 2)] Teknologi Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[3)] Sistem Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
1511510578@student.budiluhur.ac.id [1)], rizky.pradana@budiluhur.ac.id [2)], riri.irawati@budiluhur.ac.id [3)]

ABSTRAK — Employees are one of the main assets of a company, therefore the process of receiving human resources receives professional and accurate ways to obtain human resources that can support the success of a company. In this case, objectivity is needed to support each decision for a long period of time. However, when it was approved, this matter was completed in contradiction with what was implemented in the field. Judgment based on subjectivity is one example of failure to make decisions in the recruitment process. Based on these problems, PT. Kinarya Alihdaya Mandiri requires a more efficient application in the selection of employee data and a decision-making system looking for the most appropriate employee for the selection of positions needed. The method used is the Analytical Hierarchy Process (AHP), with criteria consisting of education, performance, experience and performance in this study. The test results are 100% successful using the blackbox. The results of the UAT test concluded that 85.7% of the audience agreed, the system worked as expected, and 14.3% stated strongly agree. And, the results 71.7% of the audience agreed, the system agreed as expected and 28.6% agreed strongly agreed.

Kata Kunci: Penerimaan Karyawan , Analitycal Hierarchy Process (AHP), blackbox.

ABSTRACK — ***Karyawan merupakan salah satu aset terpenting sebuah perusahaan, oleh sebab itu proses penerimaan sumber daya manusia memerlukan cara yang profesional dan akurat agar mendapatkan sumber daya manusia yang dapat mendukung kesuksesan sebuah perusahaan. Dalam hal ini, obyektivitas sangat diperlukan untuk menunjang setiap keputusan untuk jangka waktu yang panjang. Namun pada kenyataannya, hal ini sangatlah kontradiktif dengan yang diimplementasikan di lapangan. Penilaian berdasarkan subyektivitas merupakan salah satu contoh dari kegagalan pengambilan keputusan dalam proses penerimaan karyawan. Berdasarkan masalah tersebut PT. Kinarya Alihdaya Mandiri membutuhkan aplikasi yang lebih efisien dalam pemilihan data karyawan dan sistem pengambilan keputusan mencari karyawan yang paling tepat untuk menduduki posisi yang dibutuhkan. Metode yang digunakan adalah Analitycal Hierarchy Process (AHP), dengan kriteria-kriteria yang terdiri dari pendidikan, performance, pengalaman dan penampilan pada penelitian ini. Hasil pengujian adalah sistem 100% behasil dengan menggunakan blackbox. Hasil dari pengujian UAT dapat disimpulkan bahwa 85,7% audience setuju, bahwa sistem bekerja sesuai dengan yang diharapkan, dan 14,3% menyatakan sangat setuju. Dan hasil pengujian untuk fungsi penilaian, sebanyak 71,4% audience setuju, bahwa sistem berfungsi sesuai dengan yang diharapkan dan sebanyak 28,6% menyatakan sangat setuju.***

Kata Kunci: Penerimaan Karyawan, Analitycal Hierarchy Process (AHP), blackbox.

I. PENDAHULUAN

Karyawan adalah salah satu aset terpenting bagi perusahaan. Dengan kepuasan dari karyawan terhadap perusahaan, tidak menutup kemungkinan bagi karyawan untuk memberikan yang terbaik bagi perusahaan. Tak hanya itu, karyawan juga memiliki peran penting dalam perkembangan bisnis perusahaan

Oleh karenanya obyektivitas sangat diperlukan untuk dapat menunjang setiap keputusan agar mendapatkan sumber daya manusia yang baik untuk jangka waktu yang panjang. Namun, hal ini sangatlah kontradiktif dengan yang diimplementasikan di lapangan. Seringnya penilaian yang berdasarkan subyektivitas merupakan salah satu contoh dari kegagalan pengambilan keputusan dalam proses penerimaan. Bila dibiarkan dalam waktu yang panjang hal tersebut dapat

mempengaruhi kinerja sebuah organisasi sehingga berakibat pada gagalnya sebuah organisasi dalam mencapai tujuan.

PT Kinarya Alihdaya Mandiri adalah perusahaan yang fokus pada pengelolaan jasa outsourcing yang berbasiskan penyedia tenaga kerja (*Labor Supply*). Perusahaan ini sudah berjalan dengan cukup baik namun dengan banyaknya jumlah pelamar, mulai dari penyortiran data calon karyawan yang masuk hingga penentuan karyawan mana yang cocok untuk dipekerjakan pada klien sesuai dengan posisi tertentu yang dibutuhkan oleh klien, membuat metode konfensional yang saat ini digunakan dirasa sudah tidak lagi efisien.

Berdasarkan masalah tersebut PT Kinarya Alihdaya Mandiri membutuhkan aplikasi yang lebih efisien dalam penyortiran data karyawan, dan sistem pengambilan keputusan yang bisa membantu klien dalam memutuskan karyawan yang paling tepat untuk menduduki posisi yang dibutuhkan klien.

Berdasarkan hal-hal diatas, maka metode *Analitycal Hierarchy Process* (*AHP*) dipilih untuk digunakan dalam penelitian untuk menentukan penerimaan karyawan dengan mempertimbangkan kriteria-kriteria yang telah ditentukan kriteria tersebut terdiri dari pendidikan, *performance*, pengalaman dan penampilan.

II. Literature Review

Sistem penunjang keputusan untuk penilaian kinerja pegawai menggunakan metode *AHP* pada proses penilaian kinerja pegawai lebih efisien sehingga pihak RSUD Serang lebih cepat dalam proses pengambilan keputusan yang bersifat objektif. Setelah dilakukan penilaian pada aplikasi SPK penilaian kinerja pegawai dengan 5 pegawai yaitu Ratnawati, Toni, Fuadi, Retno dan Nina didapat hasil nilai akhir dengan skor tertinggi 0,4481 yaitu Ratnawati [1]. Sistem pendukung keputusan yang dibangun dapat memberikan rekomendasi kepada manager HRD dalam pengambilan keputusan layak atau tidaknya calon karyawan berdasarkan hasil nilai yang objektif pada penilaian rekrutmen. Sistem pendukung keputusan yang dibangun dapat memudahkan manager HRD dalam menghasilkan nilai hasil seleksi sehingga mendapatkan calon karyawan yang tepat [2]. Sistem pemilihan karyawan menggunakan metode *AHP* dengan kriteria dan bobot yang telah ditentukan oleh PT. Noreen Surya Perdana yang diperoleh dari hasil wawancara kemudian diproses oleh sistem sehingga menghasilkan *output* perangkingan karyawan baru. Berdasarkan hasil pengujian sistem perhitungan metode *AHP* dengan perhitungan manual, maka didapatkan hasil akhir yang mendekati sama [3]. Penelitian ini membahas penilaian kompetensi *soft skill* karyawan dengan menerapkan empat kriteria. Keempat kriteria ini adalah kemampuan komunikasi, kemampuan bekerja sama, kejujuran dan kemampuan interpersonal. Analisis data menerapkan metode *AHP*, yang memungkinkan perhitungan matematis dengan berbagai kriteria. Hasil penelitian menunjukan nilai rasio konsistensi 0.053 [4]. Algoritma *AHP-PROMETHEE* I dapat diimplementasikan untuk menentukan calon penerima beasiswa BPP-PPA. Nilai kelayakan atau akurasi *AHP*-PROMETHEE I dalam menentukan calon penerima beasiswa BPP-PPA cukup baik karena mendekati pendapat pakar. Rata-rata akurasi sistem saat melakukan saat melakukan perangkingan menggunakan LF adalah 78%. Sedangkan rata-rata akurasi sistem saat melakukan perangkingan menggunakan EF adalah 85%. [5]

III. Metodologi

III.1. Identifikasi Masalah

Karyawan merupakan salah satu asset terpenting sebuah perusahaan, karenanya proses penerimaan sumber daya manusia memerlukan cara yang professional dan akurat agar menghasilkan sumber daya yang dapat mendukung kesuksesan sebuah perusahaan. Oleh karenanya obyektivitas sangat diperlukan untuk dapat menunjang setiap keputusan agar mendapatkan sumber daya manusia yang baik untuk jangka waktu yang panjang. Namun, hal ini sangatlah kontradiktif dengan yang diimplementasikan di lapangan. Seringnya penilaian yang berdasarkan subyektivitas merupakan salah satu contoh dari kegagalan pengambilan keputusan dalam proses penerimaan. Bila dibiarkan dalam waktu yang panjang hal tersebut dapat mempengaruhi kinerja sebuah organisasi sehingga berakibat pada gagalnya sebuah organisasi dalam mencapai tujuan.

III.1.1. Strategi Penyelesaian

Untuk menangani permasalahan tersebut, maka dibuat aplikasi yang lebih efisien dalam penyortiran data karyawan, dan sistem pengambilan keputusan yang bisa membantu klien dalam memutuskan karyawan yang paling tepat untuk menduduki posisi yang dibutuhkan klien. Dalam hal ini metode yang digunakan adalah *Analitycal Hierarchy Process* (*AHP*) dengan mempertimbangkan kriteria-kriteria yang telah ditentukan, kriteria tersebut terdiri dari pendidikan, *performance*, pengalaman dan penampilan.

III.1.2. Arsitektur dan Pola Kerja Sistem

Sistem pendukung keputusan ini terdiri dari matrik perbandingan kriteria dan matrik alternatif, dimana data kriteria ini didapatkan dari hasil *quisioner* dan matrik alternatif perbandingan dilakukan berdasarkan penilaian dari pengambil keputusan dengan menilai tingkat kepentingan suatu elemen dibandingkan dengan elemen lainnya.

Tabel 3.1 Matrik Perbandingan Kriteria

Kriteria	Pendidikan	Performance	Pengalaman	Penampilan
Pendidikan	1	1/3	1/5	3
Performance	3	1	1/2	4
Pengalaman	5	2	1	4
Penampilan	1/3	1/4	1/4	1

Berdasarkan tabel 3.1 diatas, maka didapatkan perbandingan sebagai berikut:

1. *Performance* cukup diutamakan dari Pendidikan
2. Pengalaman diutamakan dari Pendidikan
3. Pendidikan cukup diutamakan dari Penampilan
4. Pengalaman setara menuju cukup diutamakan dari *Performance*
5. *Performance* cukup diutamakan menuju diutamakan dari Penampilan
6. Pengalaman cukup diutamakan menuju diutamakan dari Penampilan

Hasil perbandingan dari masing-masing elemen akan berupa angka desimal. Sedangkan untuk angka bilangan bulat terdiri dari angka 1 sampai 9 yang menunjukan perbandingan satu elemen. Apabila suatu elemen dalam matrik perbandingan dalam matrik perbandingan dengan dirinya sendiri maka hasil perbandingannya diberi nilai 1. Untuk matrik perbandingan kriteria dalam bentuk desimal bisa dilihat pada tabel 3.2.

Tabel 3.2 Matrik Perbandingan Kriteria Bentuk Desimal

Kriteria	Pendidikan	Performance	Pengalaman	Penampilan
Pendidikan	1,000	0,333	0,200	3,000
Performance	3,000	1,000	0,500	4,000
Pengalaman	5,000	2,000	1,000	4,000
Penampilan	0,333	0,250	0,250	1,000
Jumlah	9,333	3,583	1,950	12,000

Untuk memperoleh prioritas secara keseluruhan maka pertimbangan-pertimbangan terhadap perbandingan berpasangan perlu disintesis. Dalam langkah ini, hal-hal yang dilakukan adalah:

1. Menjumlahkan nilai-nilai dari setiap kolom pada matrik
2. Membagi setiap nilai dari kolom dengan total kolom yang bersangkutan untuk memperoleh normalisasi matrik
3. Menjumlahkan nilai-nilai dari setiap baris dan membaginya dengan jumlah elemen untuk mendapatkan nilai rata-rata

Tabel 3.3 Nilai *Eigen* Matrik Perbandingan Kriteria

Kriteria	**Nilai *Eigen***				Jumlah	Rata-Rata
	Pendidikan	Performance	Pengalaman	Penampilan		
Pendidikan	0,107	0,093	0,103	0,250	0,553	0,138
Performance	0,321	0,279	0,256	0,333	1,190	0,298
Pengalaman	0,536	0,558	0,513	0,333	1,940	0,485
Penampilan	0,036	0,070	0,128	0,083	0,317	0,079
Jumlah						1,000

Bisa dilihat pada tabel 3.3 diatas, semakin tinggi jumlah nilai rata-ratanya, maka semakin tinggi tingkat kepentingan/hirarki dari elemen tersebut. Dalam matrik ini bisa dilihat dari 4 elemen yang dibandingkan, pengalaman menjadi elemen terpenting yang mempengaruhi penerimaan karyawan. Dan jika total nilai rata-rata nya tidak sama dengan 1, maka terindikasi adanya kesalahan dalam perhitungan matriknya.

Dalam pembuatan keputusan, tingkat konsistensi penting untuk diperhatikan karena sebuah keputusan tidak dibuat

berdasarkan pertimbangan dengan konsistensi yang rendah, dengan nilai maksimal *Consistency Ratio* (*CR*) <= 0,1 atau 10%.

Rumus Menghitung *Consistency Rasio* (*CR*) adalah: *CR = CI / IR*

Dimana:

CR = Consistency Rasio

CI = Consistency Index

IR = Index Random Consistency

Rumus Menghitung *Consistency Index* (*CI*) adalah: *CI =* (*lamda max*-n)/n-1

Dimana:

n = banyaknya elemen

Nilai *Index Random Consistency* (*IR*) didapat dari daftar indeks *random* konsistensi (RI) sebagai berikut:

Tabel 3.4 Daftar Indeks *Random* Konsistensi

n	1	2	3	4
RI	0.00	0.00	0.58	0.90

Hal-hal yang dilakukan dalam langkah ini adalah:

1 Mengkalikan setiap nilai pada kolom pertama dengan prioritas relatif elemen pertama, nilai pada elemen kedua dengan prioritas relatif elemen kedua dan seterusnya.

2 Jumlahkan setiap baris

3 Hasil dari penjumlahan baris dibagi elemen prioritas relatif yang bersangkutan

4 Jumlahkan hasil bagi diatas dengan banyaknya elemen yang ada hasilnya disebut lamda maks.

Lamda Max = (9,333 x 0,138) + (3,583 x 0,298) + (1,950 x 0,485) + (12,000 x 0,079) = 4,253

Consistency Index (*CI*) = (*Lamda Max*-n)/(n-1)

= (4,253-4)/(4-1)

= 0,084

Consistency Rasio (*CR*) = *Consistency Index (CI)/*

Index Random Consistency (*IR*)

= 0,084 / 0,90

= 0,094

Hasil *Consistency Rasio* (*CR*) adalah : 0.094 yang berarti CR <= 0.1, maka perbandingan kriteria tersebut konsisten, apabila nilai CR >= 0.1, maka perbandingan tidak konsisten dan harus diulang kembali mulai dari menentukan nilai perbandingan.

Setelah menentukan tujuan utama sebagai level teratas, akan disusun *level* hirarki dibawahnya sebagai alternatif yang cocok untuk membertimbangkan hasil keputusan. Data dibawah ini adalah sampel data untuk keperluan melengkapi data penelitian.

Tabel 3.4 Matrik Perbandingan Alternatif Untuk Kriteria Pendidikan

Pendidikan	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1	5	7
Karyawan 2	1/5	1	3
Karyawan 3	1/7	1/3	1

Berdasarkan tabel 3.4 diatas, maka didapatkan perbandingan sebagai berikut:

1. Karyawan 1 diutamakan dari Karyawan 2
2. Karyawan 1 lebih diutamakan dari Karyawan 3
3. Karyawan 2 cukup diutamakan dari Karyawan 3

Tabel 3.5 Matrik Perbandingan Alternatif Untuk Kriteria *Performance*

Performance	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1	1/2	3
Karyawan 2	2	1	5
Karyawan 3	1/3	1/5	1

Berdasarkan tabel 3.5 diatas, maka didapatkan perbandingan sebagai berikut:

1. Karyawan 2 setara menuju cukup diutamakan dari Karyawan 1
2. Karyawan 1 cukup diutamakan dari Karyawan 3
3. Karyawan 2 diutamakan dari Karyawan 3

Tabel 3.6 Matrik Perbandingan Alternatif Untuk Kriteria Pengalaman

Pengalaman	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1	1/4	1/4
Karyawan 2	4	1	1/2
Karyawan 3	4	2	1

Berdasarkan tabel 3.6 diatas, maka didapatkan perbandingan sebagai berikut:

1. Karyawan 1 cukup diutamakan menuju diutamakan dari Karyawan 2
2. Karyawan 1 cukup diutamakan menuju diutamakan dari Karyawan 3
3. Karyawan 3 setara menuju cukup diutamakan dari Karyawan 2

Tabel 3.7 Matrik Perbandingan Alternatif Untuk Kriteria Penampilan

Penampilan	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1	1/4	1/5
Karyawan 2	4	1	1/2
Karyawan 3	5	2	1

Berdasarkan tabel 3.7 diatas, maka didapatkan perbandingan sebagai berikut:

1. Karyawan 1 cukup diutamakan menuju diutamakan dari Karyawan 2
2. Karyawan 1 diutamakan dari Karyawan 3
3. Karyawan 3 setara menuju cukup diutamakan dari Karyawan 2

Hasil perbandingan dari masing-masing elemen akan berupa angka desimal. Sedangkan untuk angka bilangan bulat terdiri dari angka 1 sampai 9 yang menunjukan perbandingan satu elemen. Apabila suatu elemen dalam matrik perbandingan dalam matrik perbandingan dengan dirinya sendiri maka hasil perbandingannya diberi nilai 1. Untuk matrik perbandingan kriteria dalam bentuk desimal bisa dilihat pada tabel dibawah ini.

Tabel 3.8 Matrik Perbandingan Alternatif Untuk Kriteria Pendidikan

Pendidikan	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1,000	5,000	7,000
Karyawan 2	0,200	1,000	3,000
Karyawan 3	0,143	0,333	1,000
Jumlah	1,343	6,333	11,000

Tabel 3.9 Matrik Perbandingan Alternatif Untuk Kriteria *Performance*

Performance	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1,000	0,500	3,000
Karyawan 2	2,000	1,000	5,000
Karyawan 3	0,333	0,200	1,000
Jumlah	3,333	1,700	9,000

Tabel 3.10 Matrik Perbandingan Alternatif Untuk Kriteria Pengalaman

Pengalaman	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1,000	0,250	0,250
Karyawan 2	4,000	1,000	0,500
Karyawan 3	4,000	2,000	1,000
Jumlah	9,000	3,250	1,750

Tabel 3.11 Matrik Perbandingan Alternatif Untuk Kriteria Penampilan

Penampilan	Karyawan 1	Karyawan 2	Karyawan 3
Karyawan 1	1,000	0,250	0,200
Karyawan 2	4,000	1,000	0,500
Karyawan 3	5,000	2,000	1,000
Jumlah	10,000	3,250	1,700

Untuk memperoleh prioritas secara keseluruhan maka pertimbangan-pertimbangan terhadap perbandingan berpasangan perlu disintesis. Dalam langkah ini, hal-hal yang dilakukan adalah:

1. Menjumlahkan nilai-nilai dari setiap kolom pada matrik
2. Membagi setiap nilai dari kolom dengan total kolom yang bersangkutan untuk memperoleh normalisasi matrik
3. Menjumlahkan nilai-nilai dari setiap baris dan membaginya dengan jumlah elemen untuk mendapatkan nilai rata-rata

Tabel 3.12 Nilai *Eigen* Alternatif Untuk Kriteria Pendidikan

Pendidikan	**Nilai *Eigen***			Jumlah	Rata-Rata
	Karyawan 1	Karyawan 2	Karyawan 3		
Karyawan 1	0,745	0,789	0,636	2,171	0,724
Karyawan 2	0,149	0,158	0,273	0,580	0,193
Karyawan 3	0,106	0,053	0,091	0,250	0,083
Jumlah					1,000
Lamda Max = (1,343 x 0,724) + (6,333 x 0,193) + (11,000 x 0,083)					3,111
CI = (3,111-3) / (3-1)					0,056
CR = 0,056 / 0,58					0,096

Tabel 3.13 Nilai *Eigen* Alternatif Untuk Kriteria *Performance*

Performance	**Nilai *Eigen***			Jumlah	Rata-Rata
	Karyawan 1	Karyawan 2	Karyawan 3		
Karyawan 1	0,300	0,294	0,333	0,927	0,309
Karyawan 2	0,600	0,588	0,556	1,744	0,581
Karyawan 3	0,100	0,118	0,111	0,329	0,110
Jumlah					1,000
Lamda Max = (3,333 x 0,309) + (1,700 x 0,581) + (9,000 x 0,110)					3,005
CI = (3,005-3) / (3-1)					0,002
CR = 0,002 / 0,58					0,004

Tabel 3.14 Nilai *Eigen* Alternatif Untuk Kriteria Pengalaman

Pengalaman	**Nilai *Eigen***			Jumlah	Rata-Rata
	Karyawan 1	Karyawan 2	Karyawan 3		
Karyawan 1	0,111	0,077	0,143	0,331	0,110
Karyawan 2	0,444	0,308	0,286	1,038	0,346
Karyawan 3	0,444	0,615	0,571	1,631	0,544
Jumlah					1,000
Lamda Max = (9,000 x 0,110) + (3,250 x 0,346) + (1,750 x 0,544)					3,069
CI = (3,069-3) / (3-1)					0,034
CR = 0,034 / 0,58					0,059

Tabel 3.15 Nilai *Eigen* Alternatif Untuk Kriteria Penampilan

Penampilan	**Nilai *Eigen***			Jumlah	Rata-Rata
	Karyawan 1	Karyawan 2	Karyawan 3		
Karyawan 1	0,100	0,077	0,118	0,295	0,098
Karyawan 2	0,400	0,308	0,294	1,002	0,334

Karyawan 3	0,500	0,615	0,588	1,704	0,568
Jumlah					1,000
Lamda Max = (10,000 x 0,098) + (3,250 x 0,334) + (1,700 x 0,568)					3,033
CI = (3,033-3) / (3-1)					0,016
CR = 0,016 / 0,58					0,028

Hasil *Consistency Rasio* (*CR*) dari keempat alternatif bernilai <= 0.1, maka perbandingan kriteria tersebut konsisten, apabila nilai CR >= 0.1, maka perbandingan tidak konsisten dan harus diulang kembali mulai dari menentukan nilai perbandingan.

Setelah semua nilai perbandingan baik matrik kriteria dan alternatif didapat, langkah selanjutnya adalah melakukan perangkingan, untuk *total score* masing-masing calon karyawan.

Dalam langkah ini, hal-hal yang dilakukan adalah: score = (rata-rata pendidikan x pendidikan karyawan) + (rata-rata *performance* x *performance* karyawan) + (rata-rata pengalaman x pengalaman karyawan) + (rata-rata penampilan x penampilan karyawan).

Tabel 3.16 Peringkat Untuk Masing Kriteria dan Alternatif

Kriteria	Pendidikan	Performance	Pengalaman	Penampilan	Score
Karyawan 1	0,724	0,309	0,110	0,098	0,253
Karyawan 2	0,193	0,581	0,346	0,334	0,394
Karyawan 3	0,083	0,110	0,544	0,568	0,353
Rata-rata Kriteria	0,138	0,298	0,485	0,079	1,000

Bisa dilihat pada tabel 3.16 diatas, semakin tinggi *score*-nya maka semakin tinggi tingkat penerimaan karyawan tersebut. Dalam tabel ini bisa dilihat dari 3 elemen alternatif yang dibandingkan, karyawan 2 memiliki *score* rata-rata tertinggi dibandingkan dengan 2 elemen alternatif lainnya.

IV. Implementasi Dan Ujicoba

IV.1. Implementasi Program

Agar aplikasi penerimaan karyawan dengan metode *analitycal hierarchy process* (*AHP*) berbasis *web* dapat berjalan dengan baik, spesifikasi yang dipakai untuk implementasi sistem ini juga harus mendukung. Spesifikasi berikut bisa mendukung sistem saat ini, diantaranya adalah:

IV.1.1. Perangkat Keras (*Hardware*)

Perangkat keras (*hardware*) yang dipakai untuk implementasi aplikasi ini adalah sebagai berikut :

1. Laptop intel core i5
2. *Ram* / *Memory* 12 GB
3. *SSD* 256 GB

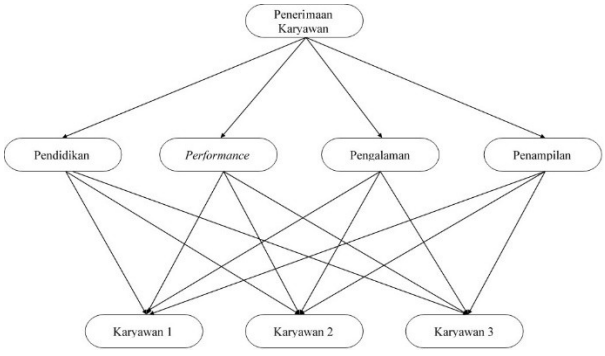
IV.1.2. Perangkat lunak (*Software*)

Perangkat lunak (s*oftware*) yang dipakai untuk implementasi aplikasi ini adalah sebgai berikut :

1. Sistem Operasi Microsoft Windows
2. Sublime Text
3. XAMPP
4. Web Browser

IV.2. Metode *Analitycal Hierarchy Process* (*AHP*)

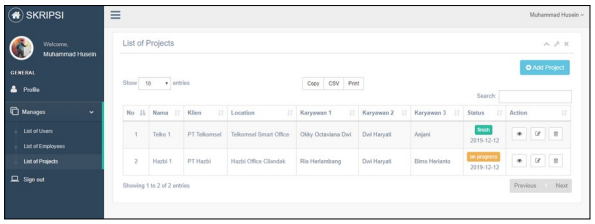
Metode *Analitycal Hierarchy Process* (*AHP*) dipilih karena sistem *AHP* sangat cocok untuk memperhitungkan validitas sampai dengan batas toleransi inkonsistensi berbagai kriteria dan alternatif yang dipilih oleh pengambil keputusan, dengan mengubah representasi permasalahan menjadi bentuk struktur multilevel, suatu masalah kompleks dapat diuraikan ke dalam bentuk kelompok yang diatur menjadi bentuk hierarki sehingga permasalahan akan terlihat lebih tersturktur dan sistematis.



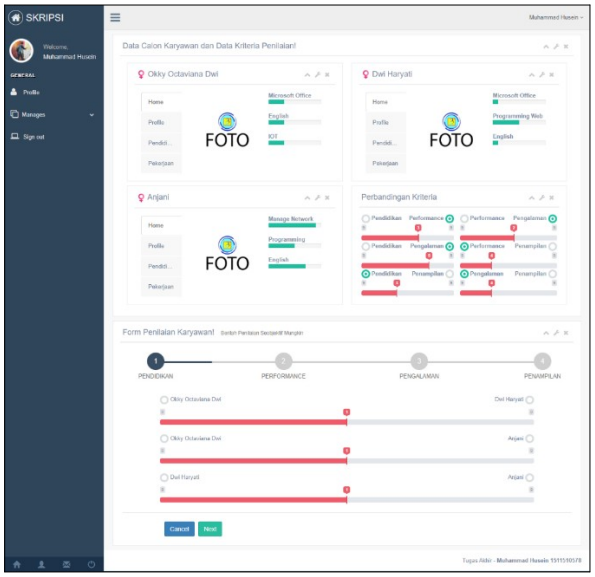
Gambar 4.1 Struktur Hierarki *AHP* Penerimaan Karyawan

IV.3. Tampilan Layar

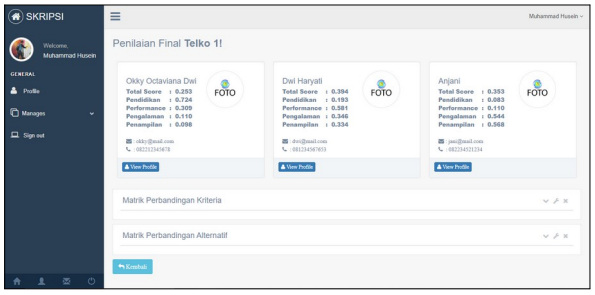
Pada bagian ini, diuraikan mengenai tampilan layar sistem penunjang keputusan penilaian penerimaan karyawan menggunakan metode *analytical hierarchy process* (*AHP*) di PT Kinarya Alihdaya Mandiri.



Gambar 4.2 Tampilan Layar Menu *List of Projects*



Gambar 4.3 Tampilan Layar Penilaian Menu *List of Projects*



Gambar 4.4 Tampilan Layar Hasil Penilaian Menu *List of Projects*

V. Pengujian Blackbox

Berdasarkan hasil pengujian *blackbox* dengan total modul yang dites berjumlah 30. dapat disimpulkan sistem yang dibuat dapat bekerja sesuai dengan yang diharapkan, dimana semua fungsi modul yang diuji, hasil ujinya menunjukan sistem dapat bekerja 100%.

VI. Pengujian *UAT* (*User Aceptance Test*)

Pengujian dengan *UAT* dilakukan dengan mengajukan beberapa pertanyaan terhadap 7 *audience* yang hadir saat demo sistem dilakukan. Hasil *user acceptance test* dinilai dengan 5 kategori, yaitu SS (Sangat Sesuai), S (Sesuai), KS (Kurang Sesuai), TS (Tidak Sesuai) dan TJ (Tidak Jawab).

Berdasarkan hasil pengujian *UAT* dapat disimpulkan sistem yang dibuat dapat bekerja sesuai dengan yang diharapkan, ini bisa terlihat dari total *vote audience* dimana kategori sesuai mendapatkan 52 poin atau 74%, kategori sangat sesuai mendapatkan 13 poin atau 19%, kategori kurang sesuai mendapatkan 5 poin atau 7%, sisanya kategory tidak sesuai dan tidak jawab tidak mendapatkan poin atau 0%.

VII. Kesimpulan

Setelah melewati tahap perancangan dan implementasi, kemudian dilakukan uji coba sistem dan evaluasi maka dapat ditarik kesimpulan sebagai berikut:

1. Fitur sign up yang disediakan dapat membuat proses pendataan calon karyawan lebih efisien.
2. Pencarian data karyawan yang sebelumnya semi manual dari Microsoft excel, saat ini bisa dicari cukup dengan mengetikan kata kunci yang diperlukan, sehingga lebih efektif.
3. Implementasi metode *Analitical Hierarchy Proses* (*AHP*) berdasarkan pengujian dengan metode *blackbox* didapatkan bahwa hasil yang didapat sudah memenuhi yang diharapkan 100%.
4. Dari pengujian *UAT* disimpulkan bahwa 85,7% *audience* setuju menyatakan bahwa sistem bekerja sesuai dengan yang diharapkan, dan 14,3% sisanya menyatakan sangat setuju. Dan untuk fungsi penilaian, sebanyak 71,4% *audience* setuju menyatakan bahwa sesuai dengan yang diharapkan, 28,6% menyatakan sangat setuju.

VIII. Saran

Sistem ini dibuat jauh dari sempurna, masih diperlukan banyak perbaikan-perbaikan yang dapat dilakukan untuk

dapat meningkatkan efektifitas kinerja sistem, beberapa saran yang dapat disimpulkan adalah sebagai berikut:

1. Data matrik kriteria dan data *skill* atau kemampuan dibuat *configurable* sehingga bisa disesuaikan untuk masing-masing posisi / jabatan yang dilamar.
2. Jumlah pencalonan karyawan yang sebelumnya dibatasi hanya untuk 3 orang karyawan pada tiap *project*, bisa dibuat *configurable* untuk menyesuaikan kemungkinan pengembangan bisnis dimasa yang akan datang.
3. Dibuat verifikasi untuk setiap karyawan yang mendapatkan nilai rata-rata tertinggi dalam suatu *project*, namanya otomatis dihide dan ditandai dengan status *not available* untuk waktu yang telah ditentukan.
4. Dengan adanya informasi tambahan pada *field skill*, calon karyawan dalam melakukan penilaian diri sendiri menjadi lebih akurat karena ada data yang terukur untuk dibandingkan dengan *skill* yang dimiliki.

DAFTAR PUSTAKA

[1] Saefudin, Sri Wahyuningsih. (2014). "Sistem Pendukung Keputusan Untuk Penilaian Kinerja Pegawai Menggunakan Metode *Analytical Hierarchy Proccess* (*AHP*) pada RSUD serang" ISSN: 2406-7768

[2] Markus Hendrawan SA. (2014). "Sistem Pendukung Keputusan Rekrutmen Karyawan di PT Indo Beras Unggulan Menggunakan Metode *Analytical Hierarchy Proccess* (*AHP*)" ISSN: 2089-9033

[3] Aji Sasongko, Indah Fitri Astuti, Septya Maharani. (2017). "Pemilihan Karyawan Baru Dengan Metode *Analytical Hierarchy Process* (*AHP*)" ISSN: 1858-4853

[4] Rusydi Umar, Abdul Fadhil dan Yuminah. (2018). "Sistem Penunjang Keputusan Dengan Metode *AHP* Untuk Penilaian Kompetensi *Soft Skill* Karyawan" ISSN: 2621-038X

[5] Nining Nahdiah Satriani, Imam Cholissodin, Mochammad Ali Fauzi. "Sistem Pendukung Keputusan Penentuan Calon Penerima Beasiswa BBP-PPA Menggunakan Metode *AHP-PROMETHEE* I Studi Kasus : FILKOM Universitas Brawijaya" ISSN: 2548-964X

Implementasi Algoritma Vigenere Cipher dan Steganografi Least Significant Bit Untuk Mengamankan File Vigenere Chiper Algorithm and Least Significant Bit Steganography Implementation for Securing File

Delima Sari [1)], Windarto [2)], Ahmad Pudoli [3)]

[1,2,3)] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753
delimahtg.d5@gmail.com [1)], windarto@budiluhur.ac.id [2)], ahmad.pudoli@budiluhur.ac.id [3)]

ABSTRAK — Perkembangan teknologi informasi dan komunikasi pada zaman ini mengalami kemajuan yang sangat pesat. Komputer sebagai media penyimpanan dan pertukaran data merupakan suatu kebutuhan yang tidak dapat dipisahkan. Seringnya pencurian data yang terjadi saat pertukaran data, membuat data yang seharusnya hanya diketahui oleh pengirim dan penerima juga dapat dilihat oleh pihak yang tidak berkepentingan. PT Tasindo Mandiri Indonesia merupakan Perusahaan yang bergerak dalam bidang produksi tas. Perusahaan ini memiliki tiga cabang perusahaan. Banyak dokumen penting yang harus terjaga kerahasiaannya seperti data keuangan perusahaan, desain tas dan daftar bahan pembuatan tas. Pertukaran data antar cabang perusahaan PT Tasindo Mandiri Indonesia dilakukan melalui internet dan dokumen hanya diamankan dengan cara memberi password pada file. Dengan demikian, dokumen tersebut kurang aman dan dikhawatirkan dapat merugikan PT Tasindo Mandiri Indonesia apabila terjadi peretasan. Dari permasalahan tersebut, dibutuhkan suatu metode untuk menjaga kerahasiaan dokumen-dokumen penting milik PT Tasindo Mandiri Indonesia yang dikirimkan melalui email. Metode yang dimaksud adalah dengan cara menyembunyikan dokumen menggunakan kriptografi dan steganografi. Metode kriptografi yang digunakan dalam penelitian ini adalah Vigenere Cipher, sedangkan metode steganografi yang digunakan adalah metode steganografi Least Significant Bit. Hasil yang didapatkan dari penelitian ini adalah aplikasi yang dibuat dapat mengamankan file dokumen milik PT Tasindo Mandiri Indonesia sebelum dikirimkan melalui email sehingga diharapkan dapat membantu PT Tasindo Mandiri Indonesia dalam mengamankan dan melindungi dokumen-dokumen penting dan kerahasiaan file tetap terjaga.

Kata kunci: Kriptografi, Steganografi, Vigenere Cipher, Least Significant Bit, Audio

ABSTRACK — Information and communication technology has been developed rapidly. Computer as a storage medium and data exchange is necessity inseparable. Frequent data stealing could be occurs when exchanging data through the internet, causing data that should only be known by the sender and the recipient also can be seen by the parties who don't have any interests. PT Tasindo Mandiri Indonesia is a company engaged in the production of bags. The company has three branches. Many important documents must be kept confidential such as company's financial data, bag design, and lists of bag's raw materials. Data exchange between branches of PT Tasindo Mandiri Indonesia is conducted through the Internet and documents are only secured by giving a password. Thus, in case of hacking the document is secure less and feared to be detrimental to PT Tasindo Mandiri Indonesia. From this problem, to maintain the confidentiality of important documents owned by PT Tasindo Mandiri Indonesia it takes a method to secure the documents. The method which referred to secure the documents is cryptography and steganography. The cryptographic method used in this study is Vigenere Cipher, while the Steganography method used is the Least Significant Bit steganography. This research obtained a result an application to secure documents owned by PT Tasindo Mandiri Indonesia, so it is to be expected helps PT Tasindo Mandiri Indonesia securing and

protecting their important and confidential documents before being sent by email.

Keywords: Kriptografi, Steganografi, Vigenere Cipher, Least Significant Bit, Audio

I. PENDAHULUAN

I.1. Latar Belakang

PT Tasindo Mandiri Indonesia merupakan salah satu perusahaan terkemuka di Indonesia. Banyak dokumen penting yang harus terjaga kerahasiaannya seperti data keuangan perusahaan, desain tas yang akan diproduksi dan daftar bahan-bahan yang digunakan untuk memproduksi tas tersebut. Pertukaran data antar cabang perusahaan PT Tasindo Mandiri Indonesia dilakukan melalui internet dan dokumen hanya diamankan dengan cara memberi password pada file. Dengan demikian, dokumen-dokumen tersebut dirasa kurang aman dan dikhawatirkan dapat merugikan PT Tasindo Mandiri Indonesia jika dan disalahgunakan oleh pihak yang tidak bertanggungjawab.

Untuk mengamankan sebuah dokumen digital dapat dilakukan dengan kriptografi dan steganografi. Salah satu metode kriptografi adalah Vigenere Cipher. Vigenere Chipe memiliki tingkat kesulitan untuk dipecahkan dengan melakukan kriptanalisis dengan metode analisis frekuensi karena dua huruf yang sama dalam teks-kode belum tentu bisa dideskripsikan menjadi dua huruf yang sama dalam teks-asli [1]. Sedangkan metode untuk penyisipan data dapat menggunakan steganografi Least Significant Bit (LSB). Metode ini banyak digunakan karena tidak terlalu kompleks dan pesan yang disembunyikan cukup aman, selain itu LSB merupakan salah satu metode yang paling sederhana [2].

Dalam penelitian ini dirumuskan masalah yaitu bagaimana meningkatkan keamanan data yang dimiliki oleh PT Tasindo Mandiri Indonesia dengan menerapkan algoritma kriptografi Vigener Chiper dan steganografi Least Significant Bit?

Penelitian ini dibatasi hanya untuk mengamankan jenis file berformat *.xls, *.xlsx, *.doc, *.docx, *.pdf, *.jpeg dan *.jpg dan file audio berformat *.mp3 sebagai media penampung.

I.2. Penelitian terkait

Dalam penelitian yang dilakukan oleh Irham Mu'alimin Arrijal membahas modifikasi algoritma Vigenere Cipher dengan konsep Vigenere Abstrak dan menerapkannya kedalam sebuah aplikasi yang memungkinkan pengguna dapat melakukan proses enkripsi dan dekripsi teks. Dalam penelitian ini algoritma yang dapat digunakan hanya algoritma yang telah ditambahkan ke aplikasi dan telah tervalidasi oleh testcase-testcase yang telah terdaftar pada database. Modifikasi yang dilakukan adalah dengan mengenkripsi setiap subsequence yang dipartisi dari plain text sesuai metode Vigenere Cipher dengan algoritma kriptografi kunci simetris yang dapat saling berbeda, dimana jumlah subsequence yang dihasilkan adalah sebanyak algoritma kriptografi kunci simetris yang digunakan. Modifikasi ini menghasilkan suatu cipher text yang sulit untuk di-decipher oleh cryptanalyst tanpa adanya kunci ataupun konfigurasi algoritma (susunan algoritma) yang digunakan. Berdasarkan analisa perancangan sistem, implementasi, dan pengujian sistem, maka dapat disimpulkan bahwa: penelitian ini telah berhasil menghasilkan suatu prototype aplikasi yang menerapkan algoritma kriptografi kunci simetris dengan modifikasi Vigenere Cipher [3].

Penelitian yang dilakukan oleh Zikrul Alim membahas cara untuk meningkatkan keamanan data pada komputasi awan dengan menggunakan algoritma Vigenere Cipher yang telah dimodifikasi. Modifikasi ini dilakukan karena pada algoritma Vigenere Cipher klasik panjang kunci dapat dipecahkan dengan pengujian Kasiski. Pada penelitian ini dilakukan beberapa pengujian yang terdiri dari pengujian ke-1, enkripsi dan dekripsi dilakukan dengan menggunakan algoritma Vigenere Cipher klasik. Pengujian ke-2, enkripsi dan dekripsi dilakukan dengan menggunakan algoritma Vigenere Cipher modifikasi. Plaintext yang digunakan adalah "FAKULTASILMUKOMPUTER" dengan kata kunci "USU". Pengujian ke-3 dilakukan kriptanalisis dengan menggunakan metode brute force terhadap hasil enkripsi dari pengujian ke-1 dan ke-2. Analisis pada pengujian ke-3 telah menunjukkan bahwa serangan yang dilakukan dengan metode brute force terhadap algoritma Vigenere Cipher yang telah dimodifikasi menunjukkan peningkatan keamanan terhadap serangan dengan metode brute force [4].

Penelitian yang dilakukan oleh Adi Widarma membahas bagimana meningkatkan keamanan data dengan mengkombinasikan kriptografi klasik Vigenere Cipher dengan kriptografi modern Electronic Code Book (ECB). Dari hasil penelitian ini dapat disimpulkan bahwa teknik kemanan data dengan mengkombinasikan Vigenere Cipher dengan kriptografi Electronic Code Book (ECB) dapat meningkatkan keamanan data, hal ini dikarenakan meningkatnya kompleksitas dua algoritma hasil ciphertext yang menjadi jauh lebih rumit daripada menggunakan satu algoritma [5].

Penelitian yang dilakukan oleh Hendro Eko Prabowo bertujuan untuk memberikan prosedur pengamanan pada data teks dengan metode algoritma modifikasi vigenere cipher. Hasil simulasi menunjukkan bahwa metode Vigenere Cipher memiliki pengulangan kata pada final key sehingga memiliki peluang informasi pesan dapat diprediksi dengan nilai peluang informasi dapat diprediksi terbesar adalah 74,07 %.

Sementara dengan menggunakan metode modifikasi Vigenere Cipher tidak didapatkan pengulangan kata pada final key sehingga informasi pesan tidak dapat diprediksi. Berdasarkan hasil pengujian terhadap algoritma modifikasi Vigenere Cipher adalah hasil enkripsi tidak memiliki pola perulangan huruf atau kata [6].

Penelitian yang dilakukan oleh Benni Purnama membahas bagaimana meningkatkan keamanan data dengan menggunkan algoritma kriptografi kunci berlapis. Dari hasil penelitian ini didapat bahwa pengamanan pesan melalui metode vigenere cipher dengan penggunaan kunci secara berlapis dapat meminimalisir kelemahan yang terjadi pada metode vigenere cipher terutama dengan menggunakan metode kasiski [7].

Kerahasiaan dan keamanan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan atau informasi melalui jaringan dan internet. Penelitian oleh Ulan Ari Anti dilakukan untuk menyembunyikan informasi yang sifatnya rahasia kedalam sebuah media video. Metode yang digunakan untuk menyembunyikan informasi adalah dengan menggunakan teknik steganografi Least Significant Bit (LSB) dan End Of File (EOF). Metode EOF dan LSB ditentukan oleh durasi, jumlah frame dan besar dimensi video. Dalam penelitian ini didapatkan hasil bahwa semakin besar ukuran file pesan rahasia yang disisipkan, maka akan semakin kecil tingkat kebehasilan proses penyisipan file pesan rahasia ke dalam file video [8]

Penelitian steganografi menggunakan Least Significant Bit (LSB) pada citra digital sebagai media penampung pesan rahasia umumnya menggunakan citra 8-bit hingga 24-bit dimana penyisipan atau penyembunyian pesan dilakukan di bit-bit kurang berarti elemen abu-abu untuk citra grayscale atau elemen merah, hijau dan biru (RGB) untuk citra berwarna. Penelitian oleh Ahmad Aidil Fitri membahas tentang bagaimana menyembunyikan sebuah file text kedalam sebuah citra digital bitmap berwarna dengan kedalaman 32-bit. Teknik penyisipan LSB pada penelitian ini mengalami peningkatan karena citra digital yang digunakan yaitu 32-bit dimana memiliki 4 elemen warna yaitu merah, hijau, biru dan alfa (RGBA). Hasil yang diperoleh dari penelitian ini adalah daya tampung atau kapasitas pesan rahasia yang dapat disisipkan lebih besar dan tetap menghasilkan kualitas citra stego yang baik dengan nilai Mean Square Error kurang dari 2 dan nilai Peak Signal-to-Noise Ratio diatas 45dB. [9]

Pada penelitian yang dilakukan oleh Rimbun Siringoringo membahas bagaimana menggabungkan steganografi metode LSB dengan dengan kriptografi metode AES, dimana pesan yang disisipkan terlebih dahulu dienkripsi dengan menggunakan metode AES. Hasil dari enkripsi tersebut kemudian disisipkan ke media citra digital. Dengan penggabungan kedua metode ini, pesan akan sulit untuk dipecahkan, karena memiliki dua tingkat keamanan. Dari penelitian ini didapatkan kesimpulan bahwa embedding pesan mempengaruhi nilai pixel pada koordinat tertentu pada cover image dan semakin banyak karakter yang disisipkan pada cover image maka nilai PSNR nya semakin kecil. Hal tersebut mengindikasikan bahwa kualitas citra semakin menurun dan nilai PSNR berbanding lurus dengan nilai MD citra. [10]

Penelitian yang dilakukan oleh Michael Sitorus membahas bagaimana meningkatkan keamanan sebuah pesan teks dengan melakukan enkripsi yang kemudian pesan yang telah dienkripsi akan disembunyikan kedalam sebuah media lain dengan menggunakan teknik steganografi. Metode yang dipakai adalah Least Significant bit insertion (LSB). Dari hasil uji coba, diketahui bahwa dengan metode Least Significant Bit Insertion (LSB) penyisipan dan ekstraksi pesan dapat dilakukan dengan baik. Jenis pesan yang dapat disisipkan adalah pesan teks. [11]

Penelitian yang dilakukan oleh Aliy Hafiz membahas bagaimana sebuah teknik steganografi Least Significant Bit dapat meningkatkan keamanan sebuah data. Hal ini dilakukan untuk mengamankan data yang terkoneksi pada jaringan internet yang tidak aman. Penyisipan dilakukan dengan menyembunyikan pesan yang kedalam sebuah citra digital. Hasil dari penelitian ini didapatkan bahwa penyisipan pesan tersembunyi berupa data dapat dilakukan ke dalam wadah citra digital berformat JPEG dan format citra digital lainnya, pesan yang disembunyikan juga data diekstraksi dari citra digital tanpa mengalami kerusakan. Terjadi perubahan kualitas pada ukuran citra digital, namun secara kasat mata perbedaan antara gambar sebelum dan sesudah disisipkan pesan tidak terlihat. Selain itu dalam penelitian ini juga didapatkan bahwa waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh spesifikasi komputer yang digunakan dan ukuran citra digital yang digunakan untuk menyembunyikan pesan [12].

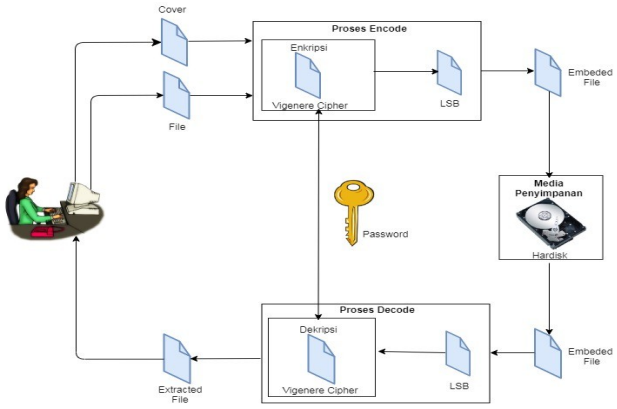
II. METODE PENELITIAN

II.1. Metode Penyelesaian

PT Tasindo Mandiri Indonesia memiliki masalah pada saat pertukaran data antar cabang perusahaan yang dilakukan melalui internet. Dokumen-dokumen penting seperti data keuangan, desain tas dan daftar bahan-bahan yang digunakan untuk membuat tas hanya diamankan menggunakan password biasa pada file, sehingga data-data tersebut masih rentan untuk dibobol dan diketahui oleh pihak yang tidak berhak untuk melihat. Dengan adanya situasi tersebut, maka pengguna khawatir akan adanya penyalahgunaan yang dapat berdampak pada kerugian perusahaan.

Untuk menyelesaikan masalah yang telah diuraikan di atas, maka dibutuhkan suatu metode penelitian untuk menerapkan algortima yang telah ditentukan untuk mengamankan dokumen rahasia yang dimiliki oleh PT Tasindo Mandiri Indonesia. Metode penyelesaian masalah yang digunakan yaitu dengan dengan mengenkripsi file menggunakan metode algoritma kriptografi Vigenere Cipher kemudian menyisipkannya ke dalam file audio dengan menggunakan metode steganografi LSB (Least Significant Bit) sehingga hanya pihak tertentu saja yang mengetahui isi file dan kerahasiaan file tetap terjaga. Data yang digunakan sebagai uji coba aplikasi pengamanan dokumen ini adalah data keuangan, data desain tas, dan data daftar bahan pembuatan tas yang dimiliki oleh PT Tasindo Mandiri Indonesia selama tahun 2014-2019. File dokumen tersebut diperoleh secara langsung dari PT Tasindo Mandiri Indonesia pada bagian accounting dan marketing.

Gambar 1 menjelaskan secara umum penerapan metode yang diusulkan dalam pembuatan aplikasi pengamanan dokumen ini. Pada proses encode, dibutuhkan dua buah masukan yaitu file dokumen rahasia dan file penampung. Alurnya adalah sebagai berikut: pengguna memilih file berformat *.xls, *.xlsx, *.doc, *.docx, *.pdf, *.jpeg atau *.jpg. Selanjutnya memilih file audio dengan format *.mp3 sebagai media penampung. Kemudian pengguna memasukan kunci keamanan untuk kemudian melakukan proses enkripsi menggunakan metode Vigenere Cipher dan menyisipkan file dokumen tersebut ke file audio menggunakan metode Least Significant Bit. Setelah proses selesai, file audio yang telah disisipi akan disimpan dalam media penyimpanan. Sedangkan pada proses ekstraksi dibutuhkan satu buah masukan yaitu file audio mp3 yang telah disisipi file dokumen. Pengguna memasukkan embeded file kemudian memasukan kunci keamanan yang sama pada saat proses encoding. Setelah proses ekstraksi berhasil dilakukan, keluaran yang dihasilkan berupa file dokumen asli.

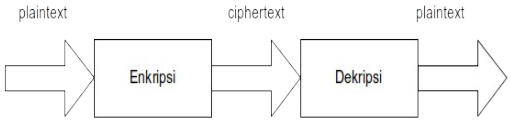


Gambar 1. Arsitektur Sistem

II.2. Vigenere Cipher

Vigenere Cipher termasuk algoritma simetrik dikarenakan algoritma ini menggunakan kunci yang sama untuk proses enkripsi dekripsi dan hasil enkripsinya termasuk algoritma polyalphabetic karena hasil enkripsi satu huruf tidak digantikan menjadi sebuah huruf tetap. Penemu Vigenere Cipher adalah Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada karya bukunya berjudul "La Cifra del. Sig. Goivan Battista Bellaso" pada tahun 1553. Nama Vigenere sendiri diambil dari seorang bernama Blaise de Vigenere. Hal ini dikarenakan beliau menemukan kunci yang lebih kuat lagi yaitu dengan metode autokeycipher meskipun algoritma ini dasarnya ditemukan oleh Giova Battista Bellaso.

Proses enkripsi dan dekripsi pada Vigenere Cipher dilakukan per karakter. Apabila suatu pesan yang dimasukkan lebih panjang daripada panjang kuncinya maka penggunaan kunci akan diperulang sampai seluruh pesan mendapatkan huruf kunci. Pada setiap baris di dalam bujursangkar Vigenere menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher, dimana jumlah pergeseran huruf plainteks ditentukan nilai numeric huruf kunci tersebut (yaitu, a=0, b=1, c=2, d=3, e=5…, z=25).



Gambar 2 Proses Kriptografi Secara Umum

Tabel 1. Daftar Urutan Huruf Alphabet yang Digunakan dalam Enkripsi-Dekripsi

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Model matematis algoritma Vigenere Cipher dapat dihitung dengan menggunakan persamaan (1) dan (2):

Enkripsi : $Ci = Pi + ki \bmod 26$ (1)

Dekripsi : $Pi = Ci - ki \bmod 26$ (2)

Kunci pada Vigenere Cipher dipakai berulang kali sebanyak pesan yang akan dienkripsi. Semakin beragam huruf alfabetik yang dipakai sebagai kunci, maka semakin kuat juga keamanan algoritma Vigenere Cipher ini.

II.3. Proses Enkripsi Algoritma Vigenere Cipher

Dalam contoh ini, panjang kunci lebih pendek daripada panjang plainteks maka kunci diulang secara periodik sampai panjang kunci sama dengan panjang plainteks. Setelah dilakukan pengulangan maka kunci menjadi:

Plainteks : KEAMANAN

Kunci : CIPHER

Dengan menggunakan rumus secara matematis: Ci = (Pi + Ki) mod 26 maka didapat hasil perhitungan seperti tabel 2

Tabel 2. Enkripsi Vigenere Cipher

Plainteks (P)	K	E	A	M	A	N	A	N
Indeks	10	4	0	12	0	13	0	13
Kunci (K)	C	I	P	H	E	R	C	I
Indeks	2	8	15	7	4	17	2	8
(P+K) mod 26	12	12	15	19	4	4	2	21
Cipherteks	M	M	P	T	E	E	C	V

Dari tabel 2. didapat hasil cipherteksnya adalah "MMPTEECV".

II.4. Proses Dekripsi Vigenere Cipher

Proses dekripsi Vigenere Cipher dengan menggunakan kunci "CIPHER". Dengan menggunakan rumus secara matematis : Pi = (Ci - Ki) mod 26 maka didapat hasil perhitungan seperti tabel 3.

Tabel 3. Dekripsi Vigenere Cipher

Cipherteks (C)	M	M	P	T	E	E	C	V
Indeks	12	12	15	19	4	4	2	21
Kunci (K)	C	I	P	H	E	R	C	I
Indeks	2	8	15	7	4	17	2	8
(C-K) mod 26	10	4	0	12	0	13	0	13
Plainteks	K	E	A	M	A	N	A	N

II.5. Metode Least Significant Bit

Least Significant Bit merupakan metode yang sederhana dalam proses menyembunyikan data, yaitu dengan cara mengganti bit yang kurang penting/least significant bit dari setiap sampling point dengan rentetan bit binary dari data yang disembunyikan. Secara matematis LSB melakukan pengubahan nilai bit paling rendah dari sampel audio dengan nilai bit pesan yang akan disisipkan.

File penampung atau cover dari metode LSB adalah audio digital yang berupa file MP3 dan bit–bit pesan atau data rahasia yang akan disisipkan ialah file yang telah terenkripsi dengan algoritma Vigenere Cipher. Keluarannya adalah file MP3 yang telah disisipi dengan bit–bit pesan rahasia.

Contoh:

Misalkan data yang ingin disisipkan berupa teks "sec". Kalau direpresentasikan ke dalam binary, maka kata "sec" diubah menjadi binary seperti ditunjukkan pada Tabel 4.

Tabel 4. Perubahan Karakter Menjadi Binary

Karakter	*Binary*
s	01110011
e	01100101
c	01100011

Misalkan media suara yang akan disisipi mempunyai panjang 24 byte, dengan nilai yang ditunjukkan pada Tabel 5.

Tabel 5. Media Penampung

Byte			
00000000	00000000	00000001	00000001
00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001
00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001
00000001	00000001	00000001	00000001

Binari dari kata "sec" kemudian diurutkan "01110011 01100101 01100011". Setiap 1 bit dari kata "secret" akan menggantikan bit terakhir dari setiap byte media penampung, maka stego yang dihasilkan ditunjukkan pada Tabel 6.

Tabel 6. Urutan Byte Media Penampung Setelah Dilakukan Penyisipan

Byte			
00000000	00000001	00000001	00000001
00000000	00000000	00000001	00000001
00000000	00000001	00000001	00000000
00000000	00000001	00000000	00000001
00000000	00000001	00000001	00000000
00000000	00000000	00000001	00000001

III. Hasil Dan Pembahasan

III.1. Rancangan Pengujian

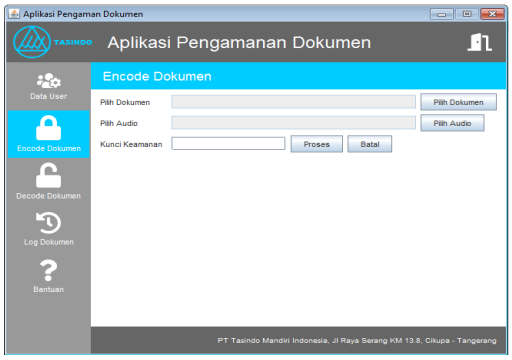
Rancangan pengujian dilakukan terhadap pengujian fungsi dari sistem, bertujuan untuk mengetahui fungsi dasar yang ada didalam aplikasi ini. Adapun rencana kasus uji pada pengujian fungsi dasar sistem ini dapat dilihat pada Tabel 7.

Tabel 7. Pengujian Fungsi Dasar Sistem

Kelas Uji Coba	Daftar Pengujian	Hasil yang Diharapkan

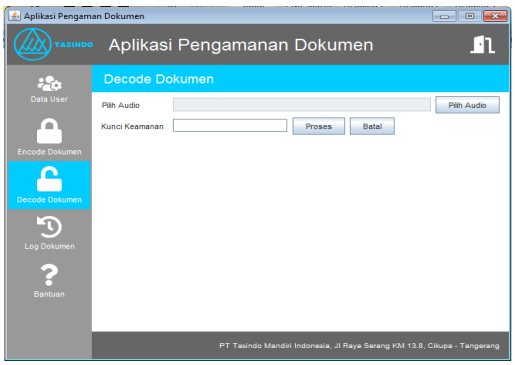
Fungsi *Login*	*Input login* admin dengan memasukkan *username* dan *password* benar	Sistem dapat menampilkan pesan *login* berhasil kemudian tampil halaman menu utama admin yang terdiri dari beberapa menu, yaitu: data *user*, *encode* dokumen, *decode* dokumen, *log* dokumen dan bantuan
	Input login admin dengan memasuk-kan *username* dan *password* salah	Sistem dapat menampilkan pesan login gagal, *username/ password* tidak sesuai dan halaman menu utama admin tidak tampil
	Input login user dengan memasukkan *username* dan *password* benar	Sistem dapat menampilkan pesan *login* berhasil, kemudian tampil halaman menu utama *user* yang terdiri dari beberapa menu, yaitu: data *user*, *encode* dokumen, *decode* dokumen dan bantuan
	Input login user dengan memasukkan *username* dan *password* salah	Sistem dapat menampilkan pesan login gagal, username/password tidak sesuai dan halaman menu utama user tidak tampil
Fungsi Menu Data *User*	*Input* ganti *password* admin	Data *password* baru dapat disimpan di *database*
	Input tambah *user* admin	Data *user* baru dapat disimpan di *database*
	Input ganti *password user*	Data *password* baru dapat disimpan di *database*
Fungsi Menu *Encode* Dokumen	Pilih dokumen	Dapat memasukkan *file* dokumen dengan format .xls, .xlsx, .doc, .docx, .pdf, .jpeg dan .jpg.
	Pilih audio	Dapat memasukkan *file* audio dengan format mp3
	Input password kurang dari 8 karakter	Dapat menampilkan bahwa pesan kunci terlalu pendek, demi keamanan diharapkan 8 karakter atau lebih
	Input password sama dengan atau lebih dari 8 karakter	Proses *encode* dokumen dapat dijalankan
Fungsi Menu *Decode* Dokumen	Pilih audio yang sudah di*encode*	Dapat memasukkan *file* audio yang sudah di-*encode* dengan format mp3
	Input password salah	Menampilkan pesan bahwa *decode* dokumen gagal, kunci keamanan salah
	Input password benar	Dapat memproses *decode* dokumen, kemudian data disimpan dan menampilkan pesan bahwa *decode* dokumen berhasil

Berikut ini adalah tampilan layar dan flowchart yang menggambarkan alur proses dari menu encode dokumen.



Gambar 3. Tampilan Layar Halaman Menu Encode Dokumen

Berikut ini adalah tampilan layar dan flowchart yang menggambarkan alur proses dari menu decode dokumen. Pada halaman ini, pengguna dapat melakukan dekripsi file atau mengembalikan file ke-bentuk semula.



Gambar 4. Tampilan Layar Halaman Menu Decode Dokumen

III.2. Hasil Pengujian

Pengujian dilakukan terhadap kesesuaian proses untuk membuktikan apakah saat proses encode, file dokumen dapat dienkripsi dan disisipkan ke dalam file audio, atau sebaliknya pada saat proses decode apakah file dokumen yang telah dienkripsi dan disisipkan ke file audio tersebut berhasil dikembalikan kebentuk semula tanpa mengurangi, menambah, dan memodifikasi isinya.

Berikut adalah hasil dari pengujian encode dokumen. File dokumen dienkripsi dan disisipkan ke dalam audio berformat file *.mp3

Tabel 8. Hasil Encode Dokumen

Nama File	Ukuran File		
	Dokumen (Kb)	Audio Cover (Kb)	Hasil Encode (Kb)
Pola Tas 1.jpeg	187	3113	3113
Pola Tas 2.jpeg	219	3185	3185
Swig.doc	238	4652	4652
Pola Tas 3,jpeg	294	3260	3260
Sycamore.doc	317	5418	5418
Blackbird.xls	377	7062	7062
Jones.pdf	423	8218	8218
Desain Phoenix.pdf	427	5418	5418
Desain Phoenix.pdf	427	6390	6390
Copilot.xls	501	5489	5489
Desember 2019.xls	534	7482	7482
4533.xls	559	9282	9282

Tabel 9. Hasil Encode Dokumen

Nama File	Ukuran File		
	Dokumen (Kb)	Audio Cover (Kb)	Durasi (ms)
Pola Tas 1.jpeg	187	3113	228,39
Pola Tas 2.jpeg	219	3185	253,07
Swig.doc	238	4652	370,67
Pola Tas 3,jpeg	294	3260	397,86
Sycamore.doc	317	5418	452,16
Blackbird.xls	377	7062	502,68
Jones.pdf	423	8218	475,11
Desain Phoenix.pdf	427	5418	904,37
Desain Phoenix.pdf	427	6390	561,49
Copilot.xls	501	5489	564,71
Desember 2019.xls	534	7482	729,09
4533.xls	559	9282	674,62

Berikut adalah hasil dari pengujian decode dokumen. File audio yang telah disimpan akan dikembalikan ke-bentuk semula. Berikut hasil yang ditampilkan pada proses decode dokumen.

Tabel 10. Hasil Decode Dokumen

Nama File	Ukuran File		
	Hasil Encode (Kb)	Hasil Decode	Durasi (ms)
Hasil Dekripsi 1.jpeg	3113	187	235
Hasil Dekripsi 2.jpeg	3185	219	265
Hasil Dekripsi 3.jpeg	3260	294	387
Hasil Dekripsi 4.pdf	5418	427	485
Hasil Dekripsi 5.pdf	6390	427	459
Hasil Dekripsi 6.pdf	8218	423	459
Hasil Dekripsi 7.xls	5489	501	549
Hasil Dekripsi 8.xls	7482	534	490
Hasil Dekripsi 9.xls	9282	559	704
Hasil Dekripsi 10.doc	4652	238	849
Hasil Dekripsi 11.doc	5418	317	718
Hasil Dekripsi 12.doc	7062	377	476

III.3. Evaluasi

Evaluasi program merupakan salah satu hal yang perlu dilakukan dalam pengembangan aplikasi, hal ini dilakukan untuk mengetahui hasil dari penelitian yang dibuat. Setelah dilakukan analisa dari hasil pengujian aplikasi dalam penelitian ini, didapatkan bahwa:

1. Aplikasi pengamanan dokumen ini dapat melakukan proses enkripsi dan penyisipan dengan baik. Proses penyisipan berhasil jika ukuran file dokumen tidak lebih besar dari jumlah byte sampel data audio yang akan disisipi file dokumen.
2. Waktu proses encode dan decode dokumen dipengaruhi oleh besarnya kapasitas file dokumen
3. Hasil pengujian menunjukkan bahwa size audio mp3 sebelum dan setelah penyisipan tidak mengalami perubahan.
4. Pada proses decode, file dokumen yang berhasil diekstrak sesuai dengan file dokumen yang disisipkan. Kesesuaian ditinjau dari size dan bentuk file dokumen.
5. Penyisipan bit-bit file dokumen ke dalam sampel data audio mp3 mempengaruhi kualitas suara. Semakin besar file dokumen yang disisipkan ke file audio maka semakin banyak derau yang ditimbulkan.

Kelebihan Aplikasi

1. Aplikasi ini dapat melakukan enkripsi dan juga penyisipan dokumen ke file audio, sehingga membuat keamanan file rahasia lebih aman.
2. Ukuran file audio sebelum dan sesudah disisipkan tidak mengalami perubahan.
3. Proses encode dan decode dokumen menggunakan kunci yang sama

4. Aplikasi ini memiliki user interface yang sederhana sehingga mudah dimengerti oleh para pengguna dan terdapat menu bantuan untuk membantu pengguna dalam menggunakan aplikasi ini.
5. Aplikasi ini mudah menambah pengguna baru sesuai dengan kebutuhan perusahaan.

Kekurangan Aplikasi

1. Tidak bisa diakses selain aplikasi desktop.
2. Aplikasi ini hanya dapat menyisipkan dokumen ke file audio berekstensi .mp3
3. File dokumen yang bisa diamankan maksimal 3 Mb.
4. Setiap satu proses penyisipan hanya bisa mengamankan satu file dokumen.
5. Untuk file dokumen yang memiliki kapasitas besar, membuat proses encode dan decode dokumen membutuhkan waktu yang lama.
6. Banyaknya derau dalam audio tergantung pada besarnya kapasitas file dokumen.

IV. Kesimpulan Dan Saran

IV.1. Kesimpulan

Melalui proses pengumpulan informasi, pemecahan masalah, perancangan dan uji coba aplikasi ini, dapat disimpulkan beberapa hal, yaitu:

1. Pengamanan dokumen dengan kriptografi menggunakan Vigenere Cipher dan steganografi menggunakan Least Significant Bit (LSB) telah berhasil diimplementasikan dalam sebuah aplikasi pengamanan dokumen berbasis desktop. Dengan demikian diharapkan dapat membantu PT Tasindo Mandiri Indonesia dalam mengamankan dokumen-dokumen penting terkait data keuangan, desain tas dan daftar bahan pembuatan tas sehingga dokumen-dokumen tersebut akan lebih aman.
2. Pada tahap decode dokumen, dokumen yang telah disisipkan dapat dikembalikan ke-bentuk semula dan tidak mengalami perubahan.
3. Dari hasil pengujian, telah dibuktikan bahwa kebutuhan waktu proses encode dan decode dipengaruhi oleh ukuran file dokumen. Semakin besar ukuran file dokumen asli maka semakin lama pula kebutuhan waktu prosesnya.

IV.2. Saran

Beberapa saran yang dapat diberikan untuk pengembangan aplikasi ini di masa mendatang, yaitu:

1. Media penyisipan diharapkan dapat dilakukan ke dalam media video.
2. Aplikasi ini diharapkan dapat mengamankan file yang berkapasitas lebih besar dari 3 Mb.
3. File dokumen yang dapat disisipkan hanya satu file untuk satu kali proses, untuk pengembangan selanjutnya diharapkan dapat menyisipkan file berekstensi zip sehingga pengguna dapat mengamankan beberapa dokumen sekaligus.

Daftar Pustaka

[1] D. Ariyus, “Pengantar Ilmu Kriptografi,” Penerbit Andi, 2008, doi: 10.1017/CBO9781107415324.004.

[2] H. K. A. Darmayanti, “SISTEM STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN LEAST Corresponding Author : maherza.qhadafi@gmail.com,” vol. 1, no. 1, 2016.

[3] I. M. Arrijal, R. Efendi, and B. Susilo, “Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks,” Pseudocode, vol. 3, no. 1, pp. 69–82, 2016, doi: 10.33369/pseudocode.3.1.69-82.

[4] Z. Alim and Y. Cancer, “Meningkatkan Keamanan Data Cloud Computing Menggunakan Algoritma Vigenere Cipher Modifikasi,” Times, 2016.

[5] A. Widarma, H. F. Siregar, and M. D. Irawan, “Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB),” J-SAKTI (Jurnal Sains Komput. dan Inform., 2019, doi: 10.30645/j-sakti.v3i2.157.

[6] B. Purnama, “Pengamanan Pesan Rahasia Melalui Kriptografi Vigenere Cipher Dengan Kunci Berlapis,” J. Ilm. Media Process., 2014.

[7] H. E. Prabowo and A. Hangga, “Enkripsi Data Berupa Teks Menggunakan Metode Modifikasi Vigenere Cipher,” Semin. Nas. Apl. Teknol. Inf., pp. 1–4, 2015.

[8] U. A. Anti, A. H. Kridalaksana, and D. M. Khairina, “Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF),” Inform. Mulawarman J. Ilm. Ilmu Komput., vol. 12, no. 2, p. 104, 2017, doi: 10.30872/jim.v12i2.658.

[9] A. Fitri, Ahmad Aidil, Mulya, Megah, "Steganografi pada Citra Digital Berwarna 32-Bit Menggunakan Least Significant Bit," J. Inform., vol. 2, no. 1, pp. 169–172, 2016.

[10] R. Siringoringo, M. Informatika, F. Ekonomi, and U. M. Indonesia, "Analisis Psnr Pada Steganografi Least Significant Bit Dengan," J. Method., vol. 2, no. 1, pp. 124–130, 2016.

[11] M. Sitorus, "TEKNIK STEGANOGRAPHYDENGAN METODE LEAST SIGNIFICANT BIT(LSB)," J. Ilm. Fak. Tek. LIMIT'S, vol. 11, no. 2, p. 54, 2015, [Online]. Available: https://www.researchgate.net/profile/Michael_Sitorus/publication/308610177_TEKNIK_STEGANOGRAPHY_DENGAN_METODE_LEAST_SIGNIFICANT_BIT_LSB/links/57e8934808ae9e5e4558ccc1/TEKNIK-STEGANOGRAPHY-DENGAN-METODE-LEAST-SIGNIFICANT-BIT-LSB.pdf.

[12] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb)," J. Cendikia, 2019.

ISSN 2302-3252

ASOSIASI PERGURUAN TINGGI INFORMATIKA & ILMU KOMPUTER
(APTIKOM) WILAYAH 3