ISSN: 1978 - 8282

DIGITAL SIGNATURE :BEST PRACTICE SOLUTION FOR THE DISTRIBUTION OF LETTERS IN COLLEGE

Untung Rahardja[1]
Muhamad Yusup[2]
Ari Asmawati[3]

e-mail : untung@raharja.co, yusup@raharja.co,ariasmawati@raharja.co.

Diterima : 19 Desember 2012 / Disetujui: 21 Januari 2013

ABSTRACT

Purpose of implementation ofweb-based information systems that allow user stoaccess information anywhere and anytime. Especiallyin making letters out stillusea wet signature. So that has not been able to provide information quickly and accurately. Identified there are7 (seven) point concerns the handling and processing of the paperstoday. However, the problem can besolved by building a Digital Signature Designand is online, so it can reduce the error rate and the information obtainedis really precise, accurate and in accordance with the needs. Obviously with the directional flow methodology description, ranging from th eillustration Figure Digital Signature, Flow distribution sub part Digital Signature, Digital Signature Flowchart, cycle and Digital Signature Digital Signature Use Case. From the Literature Review,has been much research on the Digital Signature Algorithm and Digital Signature Scheme. In the implementation phaseof the prototype described in detail the design of Digital Signature, the program listings are shown to display a letter that has been approved and has been signed. It can be also generatedauthentication system called digital signature is a waytoen sure the authenticity of an electronic document and keep documents in a time sender can not deny that she has sent the document.

Keywords: Digital Signature, Letters, Authentication, Online.

ABSTRAKSI

Tujuan diterapkannya sistem informasi berbasis web yaitu untuk mempermudah pengguna dalam mengakses informasi dimanapun dan kapanpun. Terutama dalam membuat surat-surat keluar masih menggunakan tanda tangan basah.Sehingga belum mampu menyediakan

1. **Dosen Jurusan Sistem Informasi, STMIK Raharja**
   Jl. Jend Sudirman No. 40 Modern Cikokol-Tangerang Telp. 5529692
2. **Dosen Jurusan Teknik Informatika, AMIK Raharja Informatika**
   Jl. Jend Sudirman No. 40 Modern Cikokol-Tangerang Telp. 5529692
3. **Mahasiswa Jurusan Sistem Informasi, STMIK Raharja**
   Jl. Jend Sudirman No. 40 Modern Cikokol-Tangerang Telp. 5529692

informasi yang cepat dan akurat. Diidentifikasikan terdapat 7(tujuh) point permasalahan terhadap penanganan dan pengolahan surat-surat saat ini. Namun, masalah tersebutdapat terselesaikan dengan membangun sebuah Perancangan Digital Signature dan bersifat online, sehingga dapat mengurangi tingkat kesalahan dan informasi yang diperoleh benar-benar tepat, akurat dan sesuai dengan kebutuhan. Tentunya dengan metodologideskripsi alur yang terarah, mulai dari Figure ilustrasi proses Digital Signature, Alur sub bagian pendistribusian Digital Signature, Flowchart Digital Signature, siklus Digital Signature dan Use CaseDigital Signature. Dari Literature Review, telah banyak penelitian mengenai Digital Signature Algorithm maupun Digital Signature Scheme. Pada tahapan implementasi dijabarkan secara detail prototype dari perancangan Digital Signature ini, listing program yang ditampilkan sampai tampilan surat yang telah disetujui dan sudah di tandatangani. Maka dapat dihasilkan pula sistem otentikasi yang disebut tanda tangan digital yang merupakan cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut.

Kata kunci*:Digital Signature, Surat, Otentikasi, Online.*

PENDAHULUAN

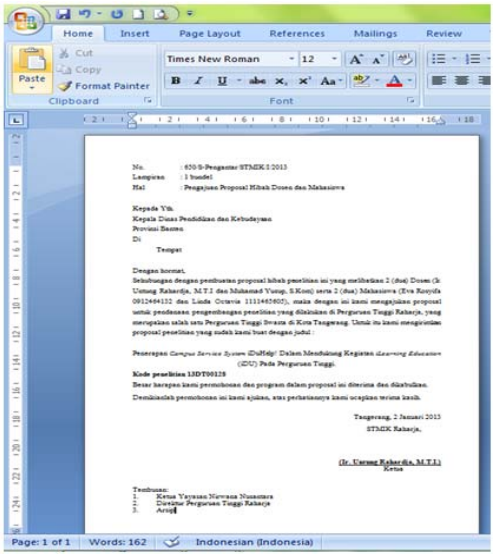
Saat ini perkembangan teknologi dalam dunia informatika dari waktu kewaktu mengalami kemajuan yang sangat pesat membuat semua instansi pemerintah dan swasta ingin mengembangkan dan menggunakan kecanggihan teknologi untuk meningkatkan kinerjanya dan pemenuhan terhadap kebutuhan atas suatu informasi saat ini tidak bisa lepas dari pemanfaatan komputer, dengan adanya informasi yang terkomputerisasi maka pekerjaan yang dihasilkan akan menjadi lebih efektif dan efisien. Beberapa alasan kenapa komputer saat ini sangat dibutuhkan dalam pemenuhan-pemenuhan kebutuhan informasi yaitu, adanya keinginan *user* untuk mendapatkan informasi secara efektif dan akurat, maupun menangani sistem informasi yang memiliki *database* yang sangat besar dan alasan-alasan lainnya termasuk proses pelayanan.

Perguruan Tinggi Raharja adalah sebuah lembaga pendidikan yang bergerak di bidang ilmu komputer.Seiring dengan perkembangannya, jumlah peserta didik dan dosen pengajar setiap semester terus bertambah.Untuk itu, Perguruan Tinggi Raharja dituntut meningkatkan sistem pengelolaan data dan sistem pelayanan dengan melakukan terobosan dalam pengembangan sistem informasi.

Namun demikian, untuk pengolahan surat-surat keluar masih menggunakan cara-cara lama di dalam pelaksanaannyayaitu pada penandatangannya masih menggunakan tanda tangan manual. Dimana tanda tangan merupakan alat untuk memvalidasi suatu kesepakatan. Selain itu memiliki beberapa kendala: pengolahan data masih mengandalkan program Microsoft Word, rendahnya ketelitian dalam pembuatan surat, serta tidak terintegrasinya antara sistem pemeriksaan data dengan sistem yang ada mengakibatkan sistem pembuatan surat yang berjalan kurang efektif dan efisien, serta informasi yang dihasilkan kurang akurat dan memerlukan waktu yang lama dalam hal penandatangan surat-surat keluar.Pada era digital saat ini terjadi proses legalitas suatu dokumen digital diperlukan juga suatu bukti yang bisa dijadikan sebagai dasar bahwa dokumen tersebut dikirimkan dan diakui oleh pihak yang membuatnya. Proses ini bisa diterapkan dengan menggunakan tanda tangan digital (*digital signature).*

PERMASALAHAN

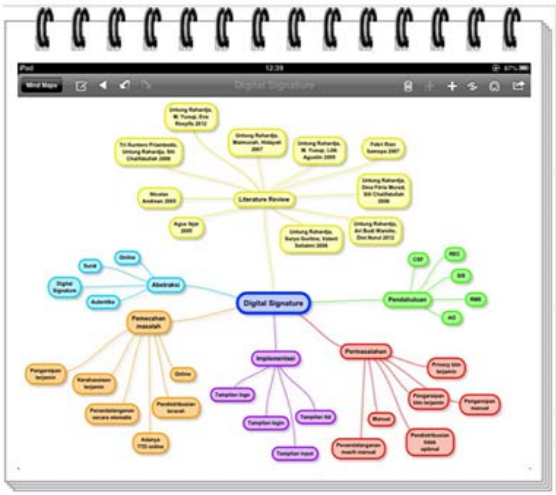
Melihat akan perkembangan informasi yang lengkap dan akurat, tentunya akan memberikan kepastian dan menghindarkan keraguan akan informasi tersebut serta keabsahan dari informasi tersebut. Walaupun demikian pada saat ini perguruan tinggi memiliki tempat khusus diberbagai bidang teknologi, yang merupakan unsur paling penting. Namun masihterdapat permasalahan harus dihadapi saat ini teutama segala kegiatan operasional. Dan dalam hal ini terdapat 7 (tujuh) permasalahan yang ada dalamhal penanganan surat menyurat dan pendokumentasian arsip saat ini,yaitu perihal keabsahan surat menyurat dalam hal penandatangananyakni salah satunya pengolahan surat-surat keluar masih menggunakan cara-cara lama didalam pelaksanaannya. Dengan permasalahan pertamapada penandatangan surat-surat keluar masih menggunakan tanda tangan manual. Dimana tanda tangan merupakan alat untuk memvalidasi suatu kesepakatan. Dan permasalahan kedua yaitu lemahnya proses legalitas suatu dokumen digital diperlukan juga suatu bukti yang bisa dijadikan sebagai dasar bahwa dokumen tersebut dikirimkan dan diakui oleh pihak yang membuatnya.Sedangkan permasalahan ketiga yaitu menggunakan pelayanan yang memiliki beberapa kendala diantaranya pengolahan data masih mengandalkan program Microsoft Word. Sehingga permasalahan keempat yaitu rendahnya ketelitian dalam pembuatan surat. Sedangkan permasalahan kelima yaitu tidak terintegrasinya antara sistem pemeriksaan data dengan sistem yang ada mengakibatkan sistem pembuatan surat yang berjalan kurang efektif dan efisien. Sedangkan permasalahan keenam yaitu informasi yang dihasilkan kurang akurat dan memerlukan waktu yang lama dalam hal penandatangan surat-surat keluar.Dan permasalahan yang terakhir yaitu permasalahan ketujuh, tidak bersifat online karena tidak tersimpan dalam suatu *database* sehingga tidak disajikan dalam bentuk *web page.*



Gambar 1. Tampilan pengolahan data pada program Microsoft Word

Dari gambar diatas, terlihat jelas bahwapengolahan data masih mengandalkan program Microsoft Word sehingga belum optimal dan gambar diatas menjadi bukti akan salah satu kekurangan penanganan surat. Sehingga didalamnya dapat diidentifikasikan secara keseluruhan terdapat 2 (dua) kekurangan yang telah dijabarkan diatas. Maka, untuk itu dari penjelasan di atas,dirumuskan 2(dua) permasalahan secara keseluruhan yaitu permasalahan pertama, perihal lemahnya proses legalitas suatu dokumen. Dan permasalahan yang kedua, yaituperihal integrasi sistem pemeriksaan data dengan sistem yang ada mengakibatkan sistem pembuatan surat yang berjalan kurang efektif dan efisien

Dari ketujuh permasalahan diatas dapat disimpulkan secara *detail* menurut penjabaran tentang penanganan surat menyurat dan pendokumentasian arsip yang tercantum dalam aplikasi *Mind Mapping*.Dikarenakan proses pembuatan aplikasi ini tidak mudah, dan membutuhkan proses yang bertahap, sehingga dilakukan proses pembuatan aplikasi yang sebenarnya.



Gambar 2.Mind MappingDigital Signature

Kegiatan operasional perihal pengolahan surat-surat keluar masih menggunakan cara-cara lama di dalam pelaksanaannya yaitu terutama pada penandatangan surat-surat keluar masih menggunakan tanda tangan manual. Dimana tanda tangan merupakan alat untuk memvalidasi suatu kesepakatan. Pada era digital terjadi proses legalitas suatu dokumen digital diperlukan juga suatu bukti yang bisa dijadikan sebagai dasar bahwa dokumen tersebut dikirimkan dan diakui oleh pihak yang membuatnya. Proses ini bisa diterapkan dengan menggunakan tanda tangan digital *(digital signature).* Permasalahan yang paling umum yaitu pengolahan data masih mengandalkan program Microsoft Word sehingga menimbulkan rendahnya ketelitian dalam pembuatan surat, serta tidak terintegrasinya antara sistem pemeriksaan data dengan sistem yang ada mengakibatkan sistem pembuatan surat yang berjalan kurang efektif dan efisien, serta informasi yang dihasilkan kurang akurat dan memerlukan waktu yang lama dalam hal penandatangan surat-surat keluar.

LITERATURE REVIEW

Sebelumnya, terdapat banyak penelitian yang dilakukan mengenai penanganan surat menyurat dan pendokumentasian arsip.Sehingga, dalam upaya pengembangan *Digital Signature* ini, dilakukan studi pustaka sebagai salah satu alat dari penerapan metode penelitian. Diantaranya adalah mengidentifikasi kesenjangan *(identify gaps)*, menghindari pembuatan ulang *(reinventing the wheel),*mengidentifikasi metode yang pernah dilakukan, meneruskan penelitian sebelumnya, serta mengetahui orang lain yang spesialisasi dan area penelitiannya sama dibidang ini. Beberapa *Literature Review*tersebut adalah sebagai berikut:

1. Penelitian ini dilakukan oleh Don Johnson,Alfred Menezes dan Scott Vanstone dari A1.Certicom Research, Canada, CA pada tahun 2001 yang berjudul *"The Elliptic Curve Digital Signature Algorithm (ECDSA)"*.Penelitian ini berisikan analisis Kurva Elliptic Digital Signature Algorithm (ECDSA) yang merupakan kurva eliptik analog dari Algoritma Tanda Tangan Digital (DSA). Itu diterima pada tahun 1999 sebagai standar ANSI dan pada tahun 2000 sebagai standar IEEE dan NIST. Itu juga diterima pada tahun 1998 sebagai sebuah standar ISO dan sedang dipertimbangkan untuk dimasukkan dalam beberapa standar ISO lainnya. Berbeda dengan masalah logaritma diskrit biasa dan masalah faktorisasi integer, tidak ada algoritma subexponential-waktu dikenal untuk masalah kurva eliptik diskrit logaritma. Untuk alasan ini, kekuatanperkeybit secara substansial lebih besar dalam algoritma yang menggunakan kurva eliptik. Jurnal ini menjelaskan ANSI X9.62 ECDSA, dan membahas terkait keamanan, implementasi, dan isu-isu interoperabilitas*[1]*.

2. Penelitian ini dilakukan oleh Mihir Bellare dan Sara K. Minerdari Conference Santa Barbara, California, USA pada tahun 2001 yang berjudul"*A ForwardSecure Digital Signature Scheme"*. Penelitian ini membahas skema tanda tangan digital di mana kunci publik tetap tetapi kunci penandatanganan rahasia diperbarui secara berkala sehingga dapat memberikan keamanan properti kedepan, kompromi kunci rahasia saat ini tidak memungkinkan musuh untuk menempa tanda tangan yang berkaitan dengan masa lalu. Hal ini dapat berguna untuk mengurangi kerusakan yang disebabkan oleh paparan kunci tanpa membutuhkan distribusi kunci. Konstruksi ini menggunakan ideidentifikasi dan skema tanda tangan, dan terbukti waktu pembuatannya juga cukup efisien[2].

3. Penelitian yang dilakukan oleh Teddy Marcus Zakaria dan Fandi dari Fakultas Teknologi Informasi Universitas Kristen Maranatha Jurusan Teknik Informatika, Bandung, Indonesia pada tahun 2008 yang berjudul "*Aplikasi Presensi Via PDA dengan Konektivitas Melalui Jaringan WiFi"*. Penelitian ini membahas mengenai pembuatan aplikasi mahasiswa menggunakan PDA dengan menggunakan jaringan *wifi*. Pengguna dapat bertindak sebagai operator. Selain itu, mendistorsi dan data cetak petugas, mahasiswa, subjek, jurusan, semester, kelas dan juga siswa kelas. Sementara pengguna bertindak sebagai dosen hanya dapat untuk melihat data yang ada didalam database, tanpa bisa mengubahnya. Implementasi aplikasi dengan menggunakan Visual Studio 2005 untuk desain dari antarmuka. Media penyimpan data adalah Microsoft SQL Server 2005 dan SQL CE. Hubungan antara aplikasi PC dan aplikasi *wifi* PDA dan digunakan untuk lulus layanan web[3].

4. Penelitian yang dilakukan oleh Untung Rahardja, Muhamad Yusup dan Lilik Agustin dari Perguruan Tinggi Raharja, Indonesia pada tahun 2009 yang berjudul *"Pengontrolan Mutu Sistem Informasi dengan Metode Database Health Monitoring"*.Pada penelitian ini

menjelaskan mengenai Database *Health Monitoring* (DHM), yang menggabungkan metode Database *Self Monitoring* (DSM), dan Server *Health Indicators* (SHI). DHM didefinisikan sebagai *dashboard system* yang menampilkan indikator sistem informasi dan indikator kapasitas penyimpanan data secara bersamaan, dengan adanya DHM dapat mengantisipasi segala kemungkinan data *anomaly* dengan menggunakan teknik pengendalian mandiri untuk memperbaiki mutu sistem informasi dalam pengendalian mandiri kapasitas peyimpanan. Untuk membuat sebuah aplikasi dibutuhkan sistem database, sebagai media penyimpan *input* data-data yang telah dimasukan dalam aplikasi, sehingga jika data-data tersebut dibutuhkan untukditampilkan pada *output* dan sistem yang dibuat dapat berjalan dengan baik[4].

5. Penelitian yang dilakukan oleh Untung Rahardja,Muhamad Yusup dan Eva Rosyifadari Perguruan Tinggi Raharja, Indonesia pada tahun 2012 yang berjudul*"Optimalisasi Key Performance Indicators (KPI) Melalui Pendekatan Balance Scorecard Upaya Mengimplementasikan Performance Management System (PMS) Pada Perguruan Tinggi"*.Dalam penelitian ini penulis menjelaskan bahwa bagaimana cara untuk menganalisis data, membuat laporan dengan menggunakan indikator dan pengukuran. Indikator merupakan alat pengukur minimal yang menyampaikan keadaan nilai data tunggal sekilas, dan sebagian besar digunakan untuk mewakili nilai keadaan *Key Performance Indicators*. Dalam mengelola dan mengukur kinerja suatu instansi lembaga pendidikan, khususnya perguruan tinggi dengan kinerja individu atau sumber dayanya, sehingga merupakan salah satu elemen penting bagi kesuksesan sebuah entitas lembaga pendidikan. Mengintegrasikan kinerja suatu lembaga pendidikan dengan kinerja individu bukan merupakan proses yang mudah, dan karenanya diperlukan sejumlah pendekatan yang sistematis untuk mengelolanya. Penerapan sistem manajemen strategis berbasis *Balance Scorecard* dapat digunakan sebagai suatu sistem pengukuran kinerja yang secara terus menerus akan memantau keberhasilan penerapan strategi suatu instansi lembaga pendidikan dan mengukur kinerja sumber dayanya secara komprehensif dan seimbang, tidak mementingkan kuantitas akan tetapi lebih mementingkan kualitas, sehingga kinerja lembaga pendidikan tersebut setiap saat dapat diketahui secara jelas. Kontribusi *Key Performance Indicators* dalam mengelola dan mengukur kinerja suatu instansi lembaga pendidikan merupakan suatu solusi dalam memberikan informasi sejauh mana keberhasilan mewujudkan target kerja yang telah ditetapkan, mengidentifikasi dan memonitor ukuran keberhasilan, tentunya dengan menunjukkan indikator kinerja yang jelas, spesifik dan terukur[5].

6. Penelitian yang di lakukan oleh Untung Rahardja,Ary Budi Warsito dan Dini Nurul Suvianti dari Perguruan Tinggi Raharja, Indonesia pada tahun 2012 yang berjudul "*Penerapan Aplikasi iDINI sebagai Media Penyimpanan Materi Perkuliahan iLearning Pada Perguruan Tinggi"*.Penelitian inimenjelaskan perihal permasalahan pendidikan yang masih rendah. Terutama sumber daya manusia. Indonesia merupakan tantangan berat bagi keadaan pendidikan diIndonesia. Diperlukan peningkatan mutu pendidikan Indonesia agar menghasilkan sumber daya manusia sesuai yang diharapkan, deteksi menurunnya prestasi peserta didik harus dimulai dari pendidik sebagai ujung tombak keberhasilan pendidikan. Metode ini dapat mengoptimalkan potensi intelektual, sosial dan emosional mahasiswa. Hal inimerupakan satu hal mengapa media pembelajaran sangat diperlukan dalam proses pembelajaran. Media pembelajaran merupakan salah satu komponen pembelajaran yang mempunyai peranan penting dalam proses pembelajaran. Pemanfaatan media seharusnya merupakan bagian yangharus mendapat perhatian guru sebagai fasilitator dalam setiap kegiatan pembelajaran. Olehkarena setiap pendidik perlu mempelajari

bagaimana menetapkan media pembelajaran agar dapat mengefektifkan pencapaian tujuan pembelajaran dalam proses belajar mengajar.Pada kenyataannya media pembelajaran masih sering terabaikan dengan berbagai alasan[6].

7. Penelitianyang dilakukan oleh Untung Rahardja, Suryo Guritno dan Valent Setiatmidari Perguruan Tinggi Raharja, Indonesia pada tahun 2008 yang berjudul *"Access Restriction Sebagai Bentuk Pengamanan Dengan Metode IP Token"*. Penelitian ini menjelaskan bahwa tujuan utama diterapkannya sistem informasi berbasis web adalah untuk memungkinkan *user* yang terhubung melalui jaringan dapat mengakses informasi dimanapun dan kapanpun. Akan tetapi, hal ini dapat menjadi bumerang bagi integritas dan keamanan data apabila akses tersebut melibatkan proses penting yang saling terkait atau berkesinambungan satu sama lain, yang sebenarnya hanya boleh diakses oleh *user* tertentu saja. Disamping itu, adanya pencegahan akses masuk bukanlah solusi yang tepat digunakan apabila informasi harus tetap dapat ditampilkan. Melalui metode IP Token, pembatasan akses *(access restriction)* dilakukan dengan cara yang bijak. Informasi seutuhnya dapat diakses oleh seluruh *user* yang terhubung melaluijaringan, sementara hak terhadap perubahan data hanya diberikan kepada satu *user* pemegang IP *Address* tertentu, yang mana kesenjangan perlakuan akses ini tidakdirasakan oleh *user* lainnya. Dalam artikel ini, diidentifikasikan masalah yang dihadapi perusahaan dalam hal pengendalian akses pada sistem informasi berbasis web, didefinisikan 7 (tujuh) ciri khas dari konsep *accessrestriction* dengan metode IP Token sebagai langkah pemecahan masalah, dan ditetapkan manfaat dari penerapan konsep baru tersebut. Selain itu, ditampilkan *listing* program yang ditulis menggunakan *script* ASP serta implementasinya untuk Absensi *Online* (AO) yang ada pada Perguruan Tinggi Raharja. Penerapan *access restriction* dengan metode IP Token pada sistem informasi berbasis web menghasilkan manajemen informasi yang jauh lebih efisien, sekaligus dapat menjaga integritas dan keamanan data secara lebih efektif pada sistem informasi berbasis web[7].

8. Penelitianyang dilakukan oleh Untung Rahardja, Dina Fitria Murad dan Siti Chalifatullahdari Perguruan Tinggi Raharja, Indonesia pada tahun 2008 yang berjudul *"Periodic Historical System Sebagai Evaluasi Strategis Dalam Mendukung Pengambilan Keputusan Manajemen"*.Penelitian ini menjelaskan perkembangan sistem informasi memiliki laju pertumbuhan yang sangat pesat, terutama sebagai media untuk memberikan informasi yang cepat dan akurat. Banyak perusahaan maupun organisasi menggunakan sistem informasi sebagai bahan evaluasi kinerja. Sebuah sistem informasi harus memiliki kemampuan yang baik, yaitu mampu memberikan informasi secara cepat dan akurat. Seiring berjalannya waktu maka informasi yang didapat akan semakin meningkat, tetapi informasi tersebut belum dapat terekam dan tersimpan dengan baik kedalam sebuah *history* sistem, dimana dapat merekam dan menyimpan seluruh informasi yang lama ataupun yang baru serta mampu memberikan informasi dari waktu kewaktu, walaupun informasi tersebut telah lampau, manajemen juga dapat menggunakan sistem tersebut guna membantu proses evaluasi strategis manajemen. Untuk mengatasi permasalahan ini, dibutuhkan suatu metodologi yang disebut *Periodic Historical System* (PHS). PHS didefinisikan sebagai teknik pengumpulan, pengintegrasian dan penyimpanan data yang bertujuan untuk memberikan informasi manajemen yang akurat dari waktu ke waktu serta bermanfaat untuk evaluasi manajemen dalam pengambilan keputusan. Diidentifikasikan5(lima) masalah yang timbul pada sistem informasi, mendefinisikan metode baru yang disebut PHS, menentukan 4 (empat) ciri khas dari PHS, merancang *algoritma* PHS, serta menguraikan 5 (lima) manfaat dari penerapan PHS. Aplikasi juga diurai dengan rincian database yang diperlukan serta *flowchart* diagram. Dengan metodologi PHS ini

dapat menjadi sebuah evaluasi terkini dalam mendukung kepentingan manajemen dalam pengambilan keputusan yang akurat[8].

9. Penelitian yang dilakukan oleh Tri Kuntoro Priyambodo,Untung Rahardja dan Siti Chalifatullahdari Perguruan Tinggi Raharja, Indonesia pada tahun 2008 yang berjudul*"Pengontrolan Mutu Sistem Informasi Dengan Metode Database Self Monitoring"* Penelitian ini menjelaskan tentang era globalisasi seperti sekarang ini, sistem informasi bukan hal yang asing lagi. Sistem informasi yang ada saat ini telah mendukung seluruh kegiatan organisasi maupun perusahaan didalam pengolahan data untuk menghasilkan informasi. Walaupun sistem informasi telah memberikan banyak manfaat, namun sistem tersebut belum dapat menampilkan indikator terhadap kemungkinan-kemungkinan kesalahan yang dapat terjadi pada sistem di dalam pengolahan data, sehingga mutu informasi masih dirasa rendah. Masalahnya adalah bagaimana sistem dapat mengantisipasi segala kemungkinan yang dapat menimbulkan permasalahan-permasalahan yang tidak diinginkan oleh manajemen. Untuk mengatasinya dibutuhkan suatu metodelogi yang disebut DSM (*Database Self Monitoring).* DSM didefinisikan sebagai *dashboard* yang menampilkan indikator untuk mengantisipasi segala kemungkinan. Dengan menggunakan teknik pengendalian mandiri dalam upaya peningkatan mutu dari sebuah sistem informasi. Dalam artikel ini, diidentifikasikan masalah yang dihadapi perusahaan dalam hal peningkatan mutu sebuah sistem informasi, didefinisikan 3 (tiga) ciri khas dengan menggunakan metode database *self monitoring*sebagai langkah pemecahan masalah, dan 6 (enam) manfaat dari penerapan konsep baru tersebut. Selain itu, ditampilkan *listing* program yang ditulis menggunakan *script* ASP. Dapat disimpulkan bahwa dengan metodelogi DSM ini dapat menjadi sebuah evaluasi terkini dalam meningkatkan mutu informasi sehingga mendukung seluruh kegiatan organisasi maupun perusahaan dengan lebih stabil, terkontrol dan termonitor lebih baik[9].

10. Penelitian yang dilakukan oleh Untung Rahardja, Maimunah dan Hidayati dari Perguruan Tinggi Raharja, Indonesia pada tahun 2007 yang berjudul *"Metode Pencarian Data dengan Menggunakan Intelligence Auto Find System (IAFS)"*. Penelitian ini menjelaskan bahwa pelayanan merupakan suatu nilai tambah yang harus dimiliki oleh suatu perguruan tinggi atau perusahaan jasa. Salah satu pelayanan tersebut yaitu dengan memberikan pelayanan yang cepat melalui metode pencarian data yang efektif dan efisien. Metode pencarian yang berlaku pada saat ini memiliki beberapa kendala, diantaranya tidak adanya tempat penyimpanan data yang terstruktur sehingga proses pencarian data tidak efektif dan efisien, masih banyak yang menerapkan sistem dengan bergantung mutlak pada karakter pencariansepenuhnya baik dilakukan secara manual maupun sudah secara terkomputerisasi. Hal ini bukan hanya menyebabkan proses pencarian data menjadi lama, tetapi juga sarat kesalahan karena *user* harus meng*input* keseluruhan *character* secara mutlak satu persatu. Untuk itu,dalam artikel ini penulis mengemukakan beberapa metodologi pemecahan permasalahan, diantaranya mengidentifikasikan setidaknya ada 2 (dua) masalah yang mendasar perihal metode pencarian yang lama, mendefinisikan konsep baru yang disebut IAFS, menentukan 4 (empat) ciri khas dari IAFS itu sendiri, merancang program IAFS itu melalui *flowchart*, dan terakhir membangun IAFS melalui Macromedia Dreamweaver MX dan Microsoft Access. Hasil akhir dari artikel ini yaitu sebuah konsep baru dengan menggunakan *Intelligence Auto Find System* (IAFS). IAFS ini memiliki definisi sebagai sebuah metode pencarian data yang dilakukan oleh komputer dengan menggunakan beberapa *alphanumeric character* dari kata kunci pencarian dan juga IAFS ini memiliki 4 (empat) ciri khas. Disamping itu, IAFS dapat dipakai dimanapun secara *online*. Metode IAFS ini menyediakan fasilitas pencarian baru, dimana *user* dapat mencari

seluruh data yang diinginkan dengan cukup meng*input* beberapa *character* terakhir dari kata kunci pencarian[10].

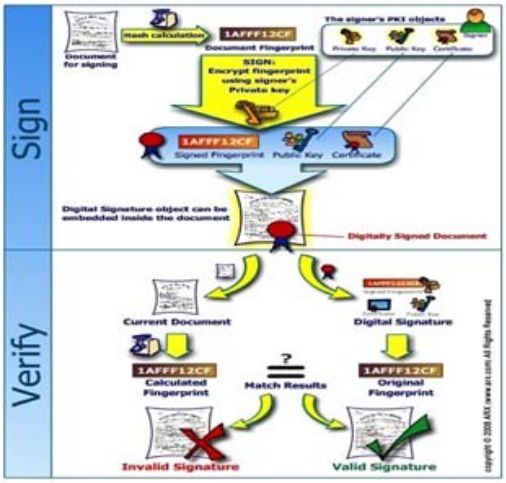
Dari sepuluh *Literature Review* yang ada, telah banyak penelitian mengenai *Digital Signature Algorithm, Digital Signature Scheme,* aplikasi dengan konektivitas melalui jaringan *wifi*,pengontrolan mutu sistem, *Performance Management System* (PMS) maupun *implementing* mengenai iDINI dan database *monitoring.*Disamping itu juga ada pembahasan mengenai *Key Performance Indicators* maupun pengambilan keputusan manajemen.Namun dapat disimpulkan bahwa belum ada peneliti yang secara khusus membahas mengenai *Digital Signature* untuk penanganan surat menyurat dan pendokumentasian arsip upaya untuk memaksimalkan sistem yang ada.

PEMECAHAN MASALAH

Setelah mengamati dan meneliti dari beberapa permasalahan yang terjadi pada sistem yang berjalan, sehingga untuk mengatasi berbagai masalah diatas, makadiperlukan4 (empat) alternatif pemecahan dari permasalahan yang dihadapi yaitu diantaranya alternatif pemecahan masalah yang pertama dengan membuat Perancangan *Digital Signature* berbasis web yang merupakan sebuah paradigma baru, dimana setiap administrasi mengirimkan surat-surat keluar yang sudah jadi melalui email, dan penerima hanya *verifikasi* dengan membuka *key* yang sudah diberikan secara *online*. Hal ini dapat meringankan beban kerja pada administrasi dalam meminta persetujuan sebuah dokumen. Sehingga waktu yang dibutuhkan lebih cepat. Di samping itu, akan menjadi lebih mudah bagi penerima dokumen untuk mendeteksi kesalahan yang mungkin terjadi di dalam memeriksa dokumen tersebut. Pemecahan masalah yang kedua yaitu dalam proses pengolahan surat-surat keluar dapat dilakukan secara *online*, sehingga waktu yang dibutuhkan untuk pemeriksaan surat-surat tersebut lebih cepat karena acc dilakukan secara *online* dan dalam bentuk *softcopy*. Pemecahan masalah yang ketiga yaitu dengan menerapkan perancangan *Digital Signature* secara *online* yang terintegrasi dengan *database* tanda tangan pemeriksa berupa kode atau inisial dengan memberikan key kepada masing-masing administrasi dalam penerimaan dokumen dan penerima memeriksa dokumen tersebut kemudian menyetujui dokumen tersebut dengan *Digital Signature* berupa kode atau inisial. Sehingga pada alternatif pemecahan masalah yang keempat yaitu dengan menerapkan aplikasi pengarsipan atau pendokumentasian surat-surat keluar secara *online.*

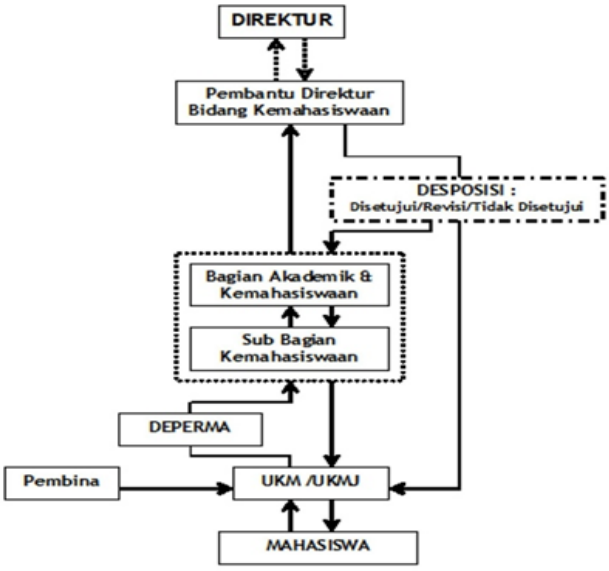
Oleh karena itu berdasarkan analisa dari segi kekurangan serta kebutuhan saat ini, kebutuhan terhadap sistem hendaknya dapat melihat dan menambahkan data-data serta informasi yang dibutuhkan, demi mengoptimalkan sistem informasi yang ada pada perguruan tinggi sehingga dapat memaksimalkan berbagai bentuk pelayanan dan kinerja yang baik secara keseluruhan. Selain itu dapat memberikan informasi yang akurat dan *up to date* sehingga informasi yang didapatkan relevan sesuai dengan kebutuhan.

Sehingga, segala hal pada dasarnya untuk mengatasi berbagai masalah diatas, maka diperlukan proses yang cepat dan efisien.



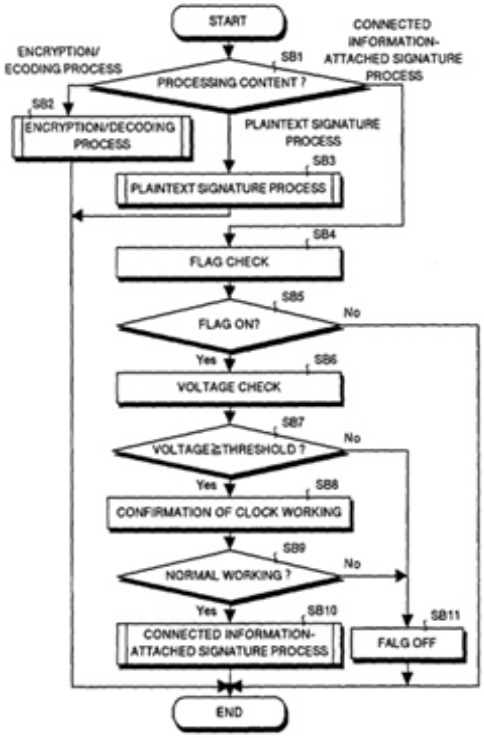
Gambar 3. Figure ilustrasi proses Digital Signature

Gambaran *figure* ilustrasi proses *Digital Signature*diatas, dapat dilakukan pula dengan jalan alternatif yang memudahkan untuk melakukan proses tersebut, yaitu melalui alur sub bagian.Dan dibawah ini merupakan gambaran alur salah satu sub bagian pendistribusian surat yang berjalan saat ini.



Gambar 4. Alur sub bagian pendistribusianDigital Signature

Gambaran *figure* ilustrasi proses *Digital Signature* diatas, dapat dilakukan pula dengan jalan alternatif yang memudahkan untuk melakukan proses tersebut, yaitu melalui alur *flowchart.*Dan dibawah ini merupakan gambaran alur *flowchart* pendistribusian surat yang berjalan saat ini.



Gambar 5. Flowchart Digital Signature

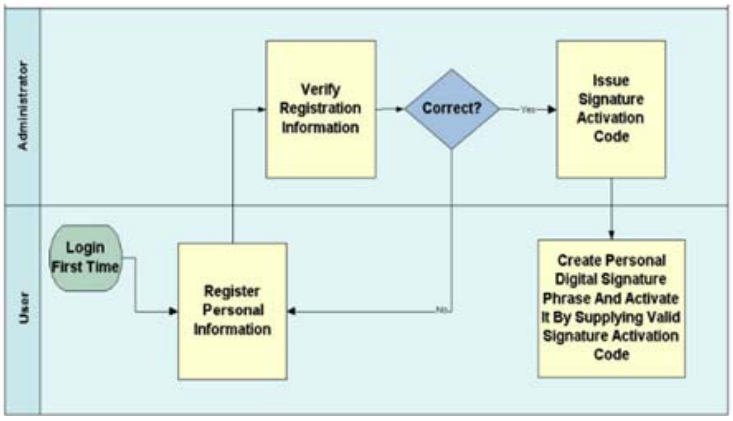
Gambar diatas merupakan alur*Flowchart Digital Signature* yang akan dituangkan berdasarkan sumber-sumber informasi yang telah didapat. Sehingga untuk rancangan aplikasi dimulai dengan beberapa tahapan pembuatan, dimulai dengan mengumpulkan ide-ide dasar serta aplikasi pendukung dalam pembuatan *Digital Signature*

Metodologi yang digunakan yaitu analisa dan perancangan mulai dari menganalisa sistem yang berjalan melalui Unified Modeling Language (UML), menggambarkan sistem yang diusulkan melalui UML, serta membangun sistem dengan menggunakan Macromedia Dreamweaver.

Langkah selanjutnya merupakan tahapan akhir, merupakan pengaplikasian *project* kedalam *database*sesuai alur siklus *Digital Signature* itu sendiri dan mengimplementasikannya sesuai alur *flowchart* diatas.

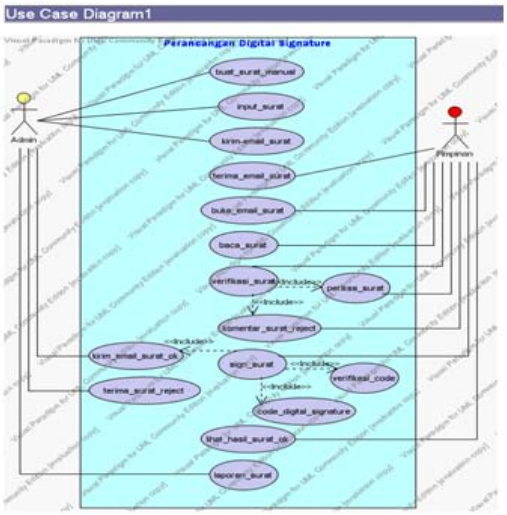
Gambar 6. siklus Digital Signature

Sehingga tahapan pembuatan siklus *Digital Signature* dapat digunakan, sehingga terlebih dahulu untuk melakukan *register*. Dibawah ini alur *register* untuk *user* dalam pembuatan *Digital Signature.*



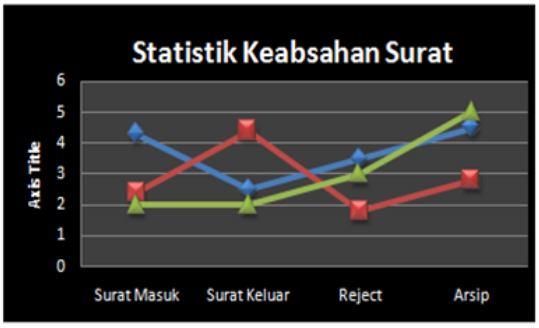
Gambar 7. Alur Register

Metode pengembangan yang digunakan meliputi 2 (dua) bagian pokok, yaituMetode Analisis, dilakukan melalui empat tahapan yaitu: survey atas sistem yang sedang berjalan, analisis terhadap temuan survey, identifikasi kebutuhan informasi, dan identifikasi persyaratan sistem. Adapun alat bantu (*tools*) yang penulis gunakan adalah berupa *Unified Modeling Language* (UML), yang dibuat dengan menggunakan *software* UML. Sedangkan untuk metode Perancangan, yang digunakan adalah Perancangan Terstruktur melalui tahapan: pembuatan UML dan pembuatan implementasi rancangan*Digital Signature*.



Gambar 8. Use CaseDigital Signature

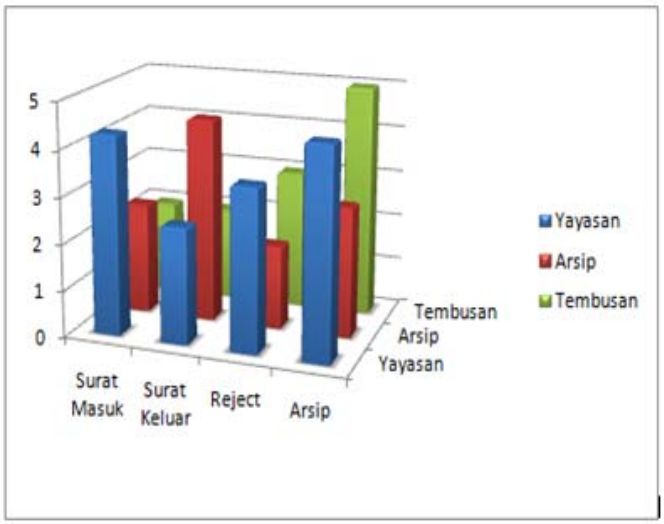
Sistem yang berjalan pada saat ini di Perguruan Tinggi Raharja terutama dalam membuat surat-surat keluar masih menggunakan tanda tangan basah, sehingga belum mampu menyediakan informasi yang cepat dan akurat, maka untuk itu dibutuhkan sebuah sistem yang dapat membantu administrasi didalam mengolah surat-surat. Solusi untuk mengatasi permasalahan tersebut yaitu dengan membangun sebuah Perancangan *Digital Signature* dan bersifat *Online*, sehingga dapat mengurangi tingkat kesalahan dan informasi yang diperoleh benar-benar tepat, akurat dan sesuai dengan kebutuhan. Hasil akhir yang dicapai yaitu terbentuknya suatu sistem email otomatis dengan yang menggambarkan analisa sistem yang berjalan dalam pendistribusian digital surat-surat keluar dan rancangan sistem yang diusulkan dengan menggunakan email otomatis. Pendokumentasian surat-surat keluar. Selain itu, dihasilkan pula sistem otentikasi yang disebut tanda tangan *digital*yang merupakan cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Sehingga statistik diagram garis perihal otentikasi surat tersebut tetap stabil.



Gambar 9. Graphstatistik Digital Signature

Tampak pada gambar diatas, merupakan tampilan grafik diagram garis perkembangan sistem otentikasi yang disebut tanda tangan *digital*yang merupakan cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Sehingga statistik diagram garis perihal otentikasi surat tersebut tetap stabil.

Sedangkan jika diukur melalui statistik diagram batang, maka hasilnya adalah sebagai berikut :



Gambar 10. GraphDiagram Batang Digital Signature

Membuat Perancangan *Digital Signature* berbasis web yang merupakan sebuah paradigma baru yang dipantau melalui statistik perkembangan setiap harinya, dimana setiap administrasi mengirimkan surat-surat keluar.Menghasilkan desain dan mengimplementasikan Perancangan *Digital Signature* yang terkomputerisasi secara optimal pada Raharja Enrichment Centre (REC) guna menghasilkan informasi yang lebih cepat dan akurat. Selain itu pula menghasilkan sistem pendokumentasian surat-surat keluar guna mengukur surat-surat yang keluar pada Raharja Enrichment Centre (REC). Perancangan *Digital Signature* yang terintegrasi guna pendistribusian surat-surat keluar lebih efisien dan adanya *paperless* di Raharja Enrichment Centre (REC). Sehingga sistem yang dihasilkan melalui pendistribusian digital guna menghasilkan informasi yang relevandan tepat pada waktunya (*timeliness*).

IMPLEMENTASI

Tampilan aplikasi (*application*) *Digital Signature* memiliki berbagai macam *fiture* yang dapat digunakan, yang terdiri dari :

Tampilan *Prototype* Aplikasi *Digital Signature*.

Logo aplikasi tersebut sudah dalam bentuk *icon apps for* iPad dan merupakan logo *Digital Signature*.

Gambar 11. PrototypeLogo Digital Signature.

Tampilan *Prototype* Layar Menu Utama *Digital Signature*

Untuk dapat masuk ke dalam tampilan menu utama program Perancangan *Digital Signature*, pada *address bar*. Setelah itu, tekan tombol "*go*" atau "*enter*" pada *keyboard* sehingga akan tampil halaman seperti pada gambar di bawah ini. Pada tampilan Menu Utama *Digital Signature* dibawah ini, terdapat 4 tombol yang menuju ke link tiap submenu yaitu input surat yang berfungsi sebagai *admin/user*, *list* surat dan statistik serta kirik dan saran.

Gambar 12. Prototype Tampilan Layar Menu Utama Digital Signature

Tampilan *Prototype ViewLogin* Input Surat

Tampilan input surat tersebut seorang admin diharuskan untuk *login* terlebih dahulu.

Gambar 13.PrototypeViewLogin Input Surat

Tampilan Informasi Input Surat

Tampilan menu input surat tersebut seorang admin untuk menginput nama surat dimana surat sebelumnya sudah dibuat dengan dokumen *html*terlebih dan disimpandalam *database* secara otomatis akan terkirim ke *email otomatis* sesuai tujuan surat tersebut.

Gambar 14.PrototypeInformasi Input Surat

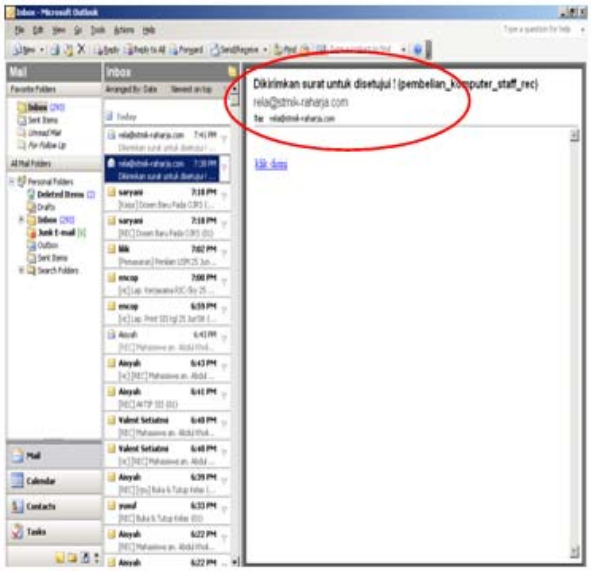
PrototypeList Surat Admin

Setelah tampilan input surat terisi, maka akan terinput dan terkirim email otomatis dan menuju list surat admin. Tampilan list surat admin adalah tampilan dimana admin dapat melihat surat-surat yang sudah di*sign*dan surat-surat yang belum di*sign.*

Gambar 15. PrototypeList Surat Admin

Prototype Isi Surat untuk Disetujui

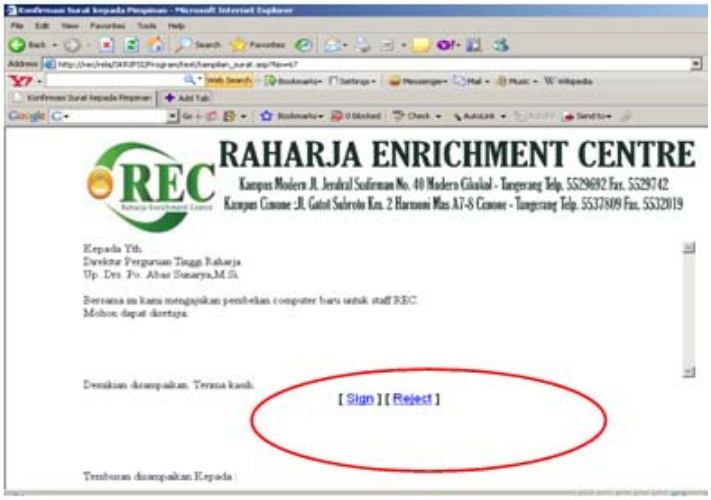
Setelah admin menginput surat maka secara otomatis akan terkirim email otomatis yang berisi minta persetujuan surat tersebut.



Gambar 16. PrototypeIsi Surat Untuk Disetujui Melalui AEMS

Tampilan surat untuk disetujui atau direject melalui AEMS

Pimpinan menerima email otomatis tersebut dan membaca email tersebur kemudian memeriksa surat tersebut berikut tampilan surat yang akan disign atau direject oleh pimpinan.



Gambar 17. Surat Untuk Disetujui Atau Direject Melalui AEMS

Prototype Verification Code

Apabila pimpinan menyetujui surat tersebutdan tidak ada perbaikan pada surat tersebut pimpinan akan memilih *"sign"* yang kemudian akan muncul tampilan *Verification Code.*

Gambar 18. *Prototype* Tampilan *Verficication Code*

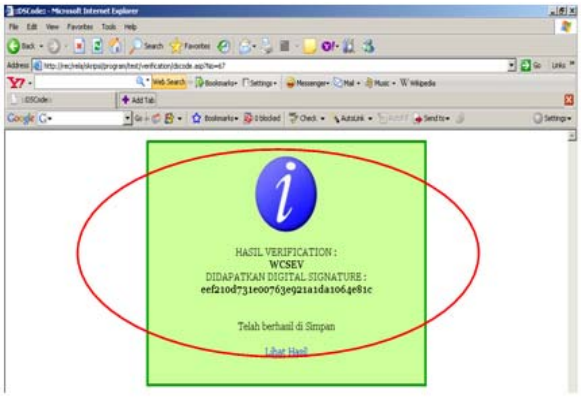
Prototype Tampilan Pesan Kesalahan Pada *Verficication Code*

Sebelum menandatangani surat tersebut pimpinan diminta untuk mengisikan *verification code* tersebut dengan benar sebelum di *submit,* apabila dalam mengisi *verification code* terdapat kesalahan akan tampak pesan kesalahan.

Gambar 19. Tampilan Pesan Kesalahan Pada *Verficication Code*

Tampilan surat untuk disetujui atau direject melalui AEMS

Apabila hasil *code* pada *verification code* tersebut diisi dengan benar dan mengklik tombol "*submit*" . setelah mengisi *verification code* tersebut maka akan menghasilkan *Digital Signature.*



Gambar 20. PrototypeTampilan Digital Signature

*Prototype*Tampilan Surat yang telah disetujui dan sudah di tandatangani.

Digital Signature sebagai bukti verifikasi dari dokumen tersebut bahwa telah disetujui isinya dan telah ditandatangani setelah itu surat akan berisi tanda tangan si penerima surat tersebut dan kembali ke pada si pengirim surat melalui *email otomatis*. Berikut hasil dari surat yang telah disetujui. Setelah surat di setujui dan ditandatangani serta surat tersebut sudah memiliki *Digital Signature Code* maka akan terkirim *email otomatis* kepada admin.

Gambar 21. Tampilan Surat yang telah disetujui dan sudah di tandatangani

Tampilan *Listing* Program *List* Surat

Dibawah ini merupakan *view detaillisting* program *Listing* program *list* surat pada Perguruan Tinggi Raharja, yaitu sebuah sistem informasi tentang penanganan surat menyurat

pada Perguruan Tinggi Raharja dengan menggunakan *Digital Signature*, *listing* program yang akan ditampilkan yaitu *listing* program untuk *List* Surat.

```
<% Set koneksi=Server.CreateObject("ADODB.connection")
Koneksi.Open "provider=msdasql;driver={SQL Server};server=REC;database=RELA;"
Sql="select * from Digital_Signature where perihal <> null or perihal <>'' or perihal <>' ' "
set rs=koneksi.execute(Sql)
%>
<html>
<head>
<title>::: Data Surat :::</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
td {font-family: verdana; font-size:0.75em;}
div.box {border:none; border-size:thin; border-color:333333; width:700; align:center;
background:#99CC99; }
h1,h2,h3,h4,h5,h6 {font-family:verdana;}
</style>
</head>

<body topmargin="0">
<table width="561" height="149" border="0" align="center">
 <tr>
  <td background="banner_list_surat.jpg"> </td>
 </tr>
</table>
<table width="700" border="1" align="center" cellpadding="2" cellspacing="1"
bordercolor="#009900">
 <tr bgcolor="#CCFF99">
  <td width="46"> <div align="center">No</div></td>
  <td width="79"> <div align="center">TGL</div></td>
  <td width="203">DOKUMEN</td>
  <td> <div align="center">AEMS</div>
   <div align="center"></div></td>
  <td width="232"> <div align="center">DS CODE</div></td>
 </tr>
 <% while not rs.eof
 no = no + 1
 %>
 <tr>
  <td><div align="center"><%=no %></div></td>
  <td><div align="left"><%= rs("Tgl") %></div></td>
  <td>
        <% if rs("ds_code") = "" then %>
        <a href="tampilan_surat.asp?No=<%=rs("No") %>"><%= rs("Perihal") %></a>
        <% else %>
        <a href="tampil_ok.asp?DsCode=<%=rs("Ds_code") %>"><%= rs("perihal")
%></a>
        <% end if %>
        </td>
  <td> <div align="center"><a href="aems.asp?DsCode=<%=rs("Ds_Code")
%>">Email</a></div>
    <div align="center"></div></td>
  <td><div align="center"><%= rs("ds_Code") %></div></td>
 </tr>
 <% rs.movenext
 wend %>
</table>
</body>
</html>
```

Gambar 22. Listing program list surat

KESIMPULAN

Perancangan *Digital Signature* yang diusulkan berdasarkan uraian yang telah dijelaskan diatas, yaitu aplikasi Perancangan *Digital Signature* yang diusulkan telah menggunakan*database*Microsoft SQL Server 2005 didalam penyimpanan datadan pembuatan surat yang menggunakan *file-file HTML*, dimana data tersebut kemudian ditampilkan dan diolah melalui *file-file ASP*sehingga menjadikan sistem tersebut terkomputerisasi lebih baik dibanding dengan pengolahan data yang semula dilakukan secara manual. Dengan demikian, dimungkinkan untuk dilakukannya manajemen terhadap data secara lebih "*smart*" dengan

cara memanfaatkan kemampuan dan kelebihan dari aplikasi yang digunakan.Disamping itu, dengan diterapkannya Perancangan *Digital Signature* yang secara *online* menjadikan proses surat-surat keluar menjadi lebih efisien. Pengolahan surat pun dapat dilakukan secara *online*. Hal ini dimanfaatkan oleh sistem yang diusulkan untuk melakukan *email* otomatis dalam pengiriman surat-surat tersebut.Dilakukannya pengukuran terhadap tingkat pengarsipan dan pendokumentasian surat-surat lebih teratur karena sistem pengarsipan yang digunakan yaitu secara *softcopy*. Dengan adanya perancangan *digital signature* dapat menghasilkan informasi yang cepat dan akurat melalui pendistribusian digital sehingga integritas data dapat dijamin.

DAFTAR PUSTAKA

[1] J. Don,M. Alfred, V. Scott "The Elliptic Curve Digital Signature Algorithm (ECDSA)". International Journal of Information Security Volume 1, Issue 1, pp 36-63. A1Certicom ResearchCanada : CA,2001.

[2] B. Mihir, M.K. Sara "A ForwardSecure Digital Signature Scheme", Annual International Cryptology Conference Santa Barbara, California : USA,1999.

[3] Z. M. Teddy, Fandi. "Aplikasi Presensi Via PDA dengan Konektivitas Melalui Jaringan WiFi". Jurnal Informatika Vol.4 No. 1.Fakultas Teknologi Informasi Universitas Kristen Maranatha Jurusan Teknik Informatika, Bandung : Indonesia,2008.

[4] R. Untung, Y. Muhamad, A. Lilik."Pengontrolan Mutu Sistem Informasi dengan Metode Database Health Monitoring" Pages : 214-230CCIT Journal Vol.2 No.3. Perguruan Tinggi Raharja : Indonesia,2009.

[5] R. Untung, Y. Muhamad,R. Eva. "Optimalisasi Key Performance Indicators (KPI) Melalui Pendekatan Balance Scorecard Upaya Mengimplementasikan Performance Management System (PMS) Pada Perguruan Tinggi". CCIT Journal ISSN : Vol.6 No2.Perguruan Tinggi Raharja : Indonesia,2012.

[6] R. Untung, W. B. Ary, S. Nurul Dini. "Penerapan Aplikasi iDINI sebagai Media Penyimpanan Materi Perkuliahan iLearning Pada Perguruan Tinggi".CCIT Journal ISSN : Vol. 6 No.5. Perguruan Tinggi Raharja : Indonesia,2012.

[7] R. Untung, G. Suryo, S. Valent. "Access Restriction Sebagai Bentuk Pengamanan Dengan Metode IP Token". CCIT Journal ISSN : 1978-8282 Vol.1 No.3. Perguruan Tinggi Raharja : Indonesia,2008.

[8] R. Untung, M. F. Dina, C. Siti."Periodic Historical System Sebagai Evaluasi Strategis Dalam Mendukung Pengambilan Keputusan Manajemen". CCIT Journal ISSN : 1978-8282 Vol.1 No.2. Perguruan Tinggi Raharja : Indonesia,2008.

[9] P. T. Kuntoro, R. Untung dan C. Siti."Pengontrolan Mutu Sistem Informasi Dengan Metode Database Self Monitoring" CCIT JournalISSN :1978-8282 Vol.1 No.3. Perguruan TinggiRaharja : Indonesia,2008.

[10] R. Untung, Maimunah, Hidayati. “Metode Pencarian Data dengan Menggunakan Intelligence Auto Find System (IAFS)”. CCIT JournalISSN : 1978-8282 Vol.1 No.1. Perguruan Tinggi Raharja : Indonesia,2007.

[11] R. Untung, N. Mia, Hidayati. “Peningkatan Kinerja Distributed Database Melalui Methode DMQ Base Level”. CCIT Journal ISSN : 1978-8282Vol.4 No.3. Perguruan Tinggi Raharja : Indonesia,2010.

[12] K. Ismi. “Kajian IT Governance Untuk Peningkatan Produktivitas Operasional Pelayanan Publik”. Jurnal CCIT ISSN Vol. 6 No.4. Perguruan Tinggi Raharja : Indonesia,2012.

[13] W. Ford, M.S. Baum. “Secure Electronic Commerce: Building the infrastructure for digital signatures and encryption” Prentice Hall, Inc. New Jersey : USA, 1997.

[14] R. Untung, W. Retantyo, B. Shakinah. “Data Mart Query (DMQ) Solusi Mempercepat Display Data Dalam Distributed Database System” Proseding Seminar Nasional Aplikasi Teknologi Informasi (SNATI) Yogyakarta : Indonesia, 2010.