ISSN 2085-4552

Penggunaan Teknik Data Mining untuk Manajemen Resiko Sistem Informasi Rumah Sakit

Ni Made Satvika Iswari

Institut Teknologi Bandung, Bandung, Indonesia

Diterima 30 November 2011
Disetujui 12 Desember 2011

***Abstract*— Rumah sakit merupakan sebuah organisasi yang sangat kompleks. Didalamnya terdapat berbagai elemen, seperti dokter dan perawat yang melakukan tugasnya, yaitu menyediakan layanan kesehatan. Perkembangan saat ini, seluruh data informasi rumah sakit disimpan secara elektronik dalam sistem informasi rumah sakit. Informasi inilah yang akan digunakan untuk menentukan resiko-resiko yang dapat menghambat berjalannya sistem informasi dengan baik. Adapun teknik yang digunakan adalah teknik *data mining*, yang bernama *risk mining*. Pada makalah ini, akan dijelaskan mengenai teknik *risk mining*, untuk menganalisis resiko pada sistem informasi rumah sakit. Selain itu, pada bagian analisis akan dilakukan perbandingan antara pendekatan teknik *data mining* ini dengan proses manajemen resiko yang diperkenalkan oleh NIST.**

Index Terms*—sistem informasi, rumah sakit, manajemen resiko, *data mining*, *risk mining

I. PENDAHULUAN

Sejak tahun 1980, informasi kesehatan untuk rumah sakit mulai disimpan secara elektronik sebagai sistem informasi rumah sakit dan meningkat secara tajam[1]. Data yang disimpan pada sistem informasi ini adalah seluruh informasi yang menunjang proses bisnis dari sebuah rumah sakit, mulai dari data laboratorium sampai data pasien. Data yang disimpan akan digunakan kembali untuk kebutuhan-kebutuhan tertentu, oleh karena itu dibutuhkan sebuah teknik untuk penggunaan data kembali, salah satunya dengan penggalian data atau *data mining*.

Penggalian data (*data mining*) dapat didefinisikan sebagai proses menemukan pola dan tren yang tidak diketahui sebelumnya dalam basis data dan menggunakan informasi tersebut untuk membangun model prediktif[2]. Penggunaan teknik penggalian data untuk kasus medis masih sangat baru digunakan dan masih banyak masalah yang harus diselesaikan dengan teknik ini[3].

Agar dapat menjalankan fungsinya dengan baik, sistem informasi rumah sakit harus mampu menghindari adanya kesalahan (*error*) demi memberikan pelayanan yang aman, nyaman, dan memuaskan bagi pasiennya. Adapun kesalahan yang umumnya terjadi dapat diklasifikasikan dalam tiga buah kategori. Kategori yang pertama adalah kesalahan sistematis (*systematic errors*), yaitu kesalahan yang dikarenakan adanya masalah dalam sistem atau alur kerja. Kategori yang kedua adalah kesalahan personal (*personal errors*), yaitu kesalahan yang dikarenakan kurangnya keahlian dari staff medis. Kemudian kategori yang terakhir adalah kesalahan acak (*random errors*). Mendeteksi kesalahan sistematis dan personal merupakan hal yang penting, sehingga dapat dicegah dengan aksi yang tepat, dan penggalian data merupakan teknik yang diharapkan dapat digunakan untuk menganalisis kesalahan-kesalahan tersebut.

Makalah ini akan menjelaskan mengenai pengaplikasian teknik penggalian data untuk menangani masalah-masalah yang telah dijelaskan sebelumnya. Untuk itu, akan dijelaskan mengenai teknik penggalian resiko (*risk mining*), dimana data yang mengandung informasi resiko akan dianalsis dengan menggunakan teknik penggalian data dan hasilnya digunakan untuk mencegah resiko yang mungkin terjadi.

II. MANAJEMEN RESIKO SISTEM INFORMASI

Resiko merupakan dampak negatif dari adanya suatu kelemahan dalam sebuah sistem, dengan berdasarkan probabilitas dan dampak dari kemunculannya[4]. Adapun manajemen resiko merupakan proses untuk mengidentifikasi resiko, menilai resiko, dan mengambil langkah untuk mengurangi resiko sampai pada level yang dapat diterima. Tujuan utama dari proses ini adalah agar sebuah organisasi dapat mengelola sistem informasinya dalam kaitannya dengan resiko yang mungkin terjadi.

Menurut Stoneburner, et al, manajemen resiko terdiri dari tiga proses utama, yaitu penilaian resiko (*risk assessment*), mitigasi resiko (*risk mitigation*), serta evaluasi dan penilaian (*evaluation and assesment*) [4]. Proses yang pertama, yaitu penilaian resiko merupakan proses awal untuk mengenal terlebih dahulu resiko-resiko yang mungkin muncul pada suatu sistem informasi. Adapun proses ini meliputi identifikasi dan evaluasi resiko beserta dampak yang mungkin terjadi akbat resiko tersebut. Selain itu pada proses ini juga direkomendasikan tindakan untuk mengurangi resiko yang mungkin terjadi. Proses kedua, yaitu mitigasi resiko merupakan proses nyata yang dilakukan untuk mengurangi resiko yang terjadi. Adapun proses ini meliputi penentuan prioritas, implementasi, dan pemeliharaan tindakan yang tepat untuk mengurangi resiko seperti yang telah direkomendasikan pada tahap penilaian resiko. Sementara proses yang terakhir, yaitu evaluasi dan penilaian, merupakan tahap evaluasi lebih lanjut untuk mengimplementasikan program manajemen resiko yang sukses.

III. SISTEM INFORMASI RUMAH SAKIT

Rumah sakit merupakan sebuah organisasi yang sangat kompleks, dimana para staff medis, termasuk dokter dan perawat memberikan pelayanan yang efektif dan istimewa untuk para pasien. Namun, organisasi yang kompleks tentu saja sangat sulit untuk melakukan perubahan dengan cepat. Perubahan yang cepat tersebut dapat menyebabkan terjadinya malpraktek oleh staff medis, dan kadang kecelakaan yang besar terjadi sebagai akibat dari deretan kecelakanan kecil.

Kecelakaan medis bukan hanya berupa kecerobohan dari dokter dan perawat, namun juga kesalahan resep ataupun efek samping obat. Penyebab dari kecelakaan tersebut tidak dapat diinvestigasi dengan baik dan tidak dapat diketahui apakah kecelakaan tersebut diklasifikasikan ke kategori kesalahan yang mana. Oleh karena itu, sangat penting untuk mengetahui bagaimana kecelakaan-kecelakaan tersebut dapat muncul dalam sebuah organisasi yang kompleks dan bagaimana mengklasifikasikan kecelakaan-kecelakaan tersebut berdasarkan kategori kesalahan yang telah disebutkan sebelumnya.

Seluruh informasi klinikal telah disimpan secara elektronik sebagai sistem informasi rumah sakit. Basis data menyimpan seluruh data yang berhubungan dengan tindakan medis, termasuk informasi akuntansi, pemeriksaan laboratorium, data pasien dan pengobatannya oleh staf medis. Bahkan laporan insiden dan kecelakaan juga disimpan pada basis data.

Berikut ini akan diberikan beberapa contoh skenario ancaman untuk sistem informasi rumah sakit. Skenario ini menyediakan deskripsi singkat mengenai isu dalam penanganan kesehatan dan dampak negatif yang dapat diatasi dengan pendekatan berbasis teknologi informasi.

A. Layanan Rumah Sakit yang Berhenti

Scenario: Kesalahan lokal pada rumah sakit, yaitu Unit Gawat Darurat terputus dari jaringan. Dengan demikian layanan IT menjadi tidak berjalan, sementara pasien terus-menerus berdatangan dan membutuhkan layanan kesehatan. Sistem layanan UGD tersebut seharusnya dapat terus berjalan untuk memberikan layanan kesehatan yang kritis.

Possible Design Mitigation: Untuk membuat mitigasi yang andal untuk skenario ini, sistem dapat mencakup kemampuan untuk membuat dan menyimpan secara lokal informasi kesehatan yang telah dibuat (foto medis, rekaman) walaupun akses LAN terputus. Disarankan untuk penyedia layanan kesehatan untuk memperhatikan pemulihan bencana ketika merencanakan penggunakan penyimpanan lokal. Rencana manajemen resiko yang sangat hati-hati termasuk persiapan adanya bencana dapat menghasilkan keseimbangan yang tepat untuk komponen ini.

Possible Operational Workarounds: Menggunakan staff tambahan, menggunakan peralatan yang tersedia pada departemen lain untuk fasilitas pelayanan yang sama, arahkan pasien ke fasilitas layanan kesehatan terdekat, atau bangun wireless yang aman sebagai solusi untuk berkomunikasi dengan jaringan.

B. Terjadinya Bencana yang Luas

Scenario: Penyediaan layanan kesehatan sebagai akibat dari bencana yang luas. Bencana tersebut dapat disebabkan oleh alam (seperti gempa bumi, tsunami, angin puting beliung, gunung meletus, dsb) atau disebabkan oleh ulah manusia (seperti teror, perang, dsb).

Selama terjadinya bencana ini, infrastruktur umum (seperti jaringan internet, jalan, sumber daya listrik, air, dsb) dapat terganggu, bahkan rusak. Lebih jauh lagi, bencana tersebut dapat menyebabkan kerusakan pada fasilitas kesehatan itu sendiri dan menghancurkan bagian dari infrastruktur layanan kesehatan, sehingga menyebabkan "*Health-care System Failure*". Situasi ini dapat menjadi lebih buruk jika bencana tersebut meningkatkan jumlah pasien yang datang ke fasilitas layanan kesehatan.

Possible Design Mitigations: Sistem memiliki mode darurat yang memungkinkan untuk identifikasi individu tanpa adanya otentikasi untuk mendukung tenaga kerja lokal.

Possible Operational Workarounds: Untuk bencana yang jarang terjadi seperti ini, tindakan mitigasi resiko sulit untuk ditentukan, karena mungkin tidak ada peralatan medis yang tersedia. Sementara itu, perencanaan berbagai kemungkinan sangat penting demi misi layanan kesehatan yang terus berlanjut. Dengan demikian, diperlukan adanya ketentuan bahwa data kritis layanan kesehatan harus diamankan dari perusakan seperti adanya bencana, dan jika memungkinkan, data tersebut harus dapat diakses dari fasilitas lainnya sebagai solusi cadangan.

C. Serangan Kejahatan yang Tidak Pandang Bulu

Scenario: Peralatan medis yang digunakan oleh pasien (seperi x-ray, ECG, ventilasi, CT, MRI, PET), ketika munculnya serangan terhadap perangkat lunak. Hal ini dapat merupakan efek samping dari serangan luas di dunia maya, dimana peralatan medis sebenarnya tidak dijadikan target spesifik. Serangan ini menggunakan peralatan teknologi yang dikenal sebagai virus, Trojan Horse, worm, dan sebagainya. Dalam keadaan ini, sistem harus dapat melindungi pasien dengan aman. Bencana dapat berdampak pada individu pasien dan penyedia layanan kesehatan apabila serangan dapat mengakses data personal.

Possible Design Mitigation: Selama operasi rutin, hanya layanan atau protokol jaringan yang penting untuk penggunaan yang tepat dari sistem yang diizinkan dan tetap aktif selama waktu tertentu. Mekanisme otentikasi ditempatkan untuk mengizinkan hanya point yang terpercaya (seperti IHE *Audit Trail and Node Autenthication integration Profile*) untuk berkomunikasi, untuk memblokir serangan. Untuk beberapa sistem, ketika akses jaringan gagal, desain mengizinkan untuk kembali namun tetap berfungsi dengan baik. Sebagai contoh, sistem pemantauan tanpa jaringan tidak akan mendukung tampilan terpusat untuk informasi pasien, namun disamping memantau, sistem tetap dapat melanjutkan operasinya dan tampilan. Beberapa sistem, seperti PACS *workstations*, tidak akan berfungsi ketika akses jaringan ke penyimpanan datanya terganggu. Dalam hal ini, sistem harus aman terhadap kegagalan untuk memungkinkan staff layanan kesehatan menuju langsung ke perangkat akuisisi untuk melihat gambar atau mencetak gambar dari perangkat akuisisi. Hal ini akan membutuhkan pemindahan media dari sistem akuisisi ke workstation.

Possible Operational Workaround: Biasanya, tindakan mitigasi resiko yang segera adalah menghilangkan akses jaringan dari perangkat ini. Namun, hal ini kurang tepat untuk beberapa perangkat yang membutuhkan akses jaringan yang berkelanjutan, dan hal ini dapat memungkinkan adanya konsekuensi medis yang parah untuk para pasien. Walaupun kebergantungan pada konektivitas jaringan meningkat, sistem ini biasanya mendukung alur kerja yang efisien dibandingkan menyediakan secara langsung fungsi *life-critical*. Secara umum, perangkat *life-critical* gagal kembali ke operasi yang tepat saat jaringan tidak berfungsi dengan baik. Sangat penting bagi Rumah Sakit memiliki rencana kemungkinan yang terjadi (*contigency plan*) untuk kesalahan fungsi jaringan, misalnya dengan menambah staff dengan cepat selama kegagalan jaringan berlangsung.

Sebagai basis dari manajemen resiko, aset-aset yang membutuhkan perlindungan, juga tujuan penggunaannya, harus didaftarkan. Berikut ini adalah beberapa aset khas, namun tidak disebutkan dengan lengkap, yang berupa perangkat keras maupun perangkat lunak yang digunakan untuk memroses informasi medis dan elemen kunci data:

1) Komponen/sistem aplikasi medis spesifik (seperti pembuatan gambar, komponen jaringan) dari infrastruktur teknologi informasi Rumah sakit.

2) Komponen/sistem aplikasi medis tidak spesifik (seperti *denial of service attack* dapat memblokir lalu lintas keseluruhan jaringan) dari infrastruktur teknologi informasi Rumah sakit.

3) Perangkat Lunak Aplikasi Medis itu sendiri.

4) Data konfigurasi perangkat lunak dan perangkat keras.

5) Data personal dari pasien.

6) Data personal dari staff layanan medis.

7) Informasi untuk mendukung prosedur layanan kesehatan, termasuk log penggunaan dan detil operator/pengguna.

Daftar ases ini harus dirinci lebih jauh untuk memulai tugas untuk mengenali ancaman yang terjadi terhadap masing-masing aset dan memungkinkan untuk mengidentifikasi dan mengimplementasi tindakan mitigasi resiko yang tepat. Membuat list aset dari sebuah sistem informasi rumah sakit tidak akan menyediakan informasi spesifik terhadap keadaan nyata. Secara umum, *network diagram* memberikan gambaran umum mengenai arsitektur teknologi

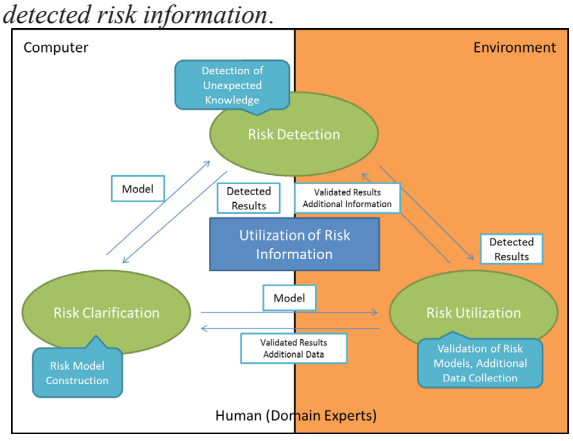
informasi dari peralatan yang dikembangkan atau keseluruhan jaringan rumah sakit. Hal ini memudahkan identifikasi sistem identik yang digunakan pada lokasi berbeda dengan instalasi yang sama (atau dengan penyedia layanan kesehatan yang sama) yang mungkin terkena dampak resiko yang sama, dan kebutuhan implementasi tindakan mitigasi resiko yang sama. Dengan mengunakan pendekatan jaringan secara keseluruhan, tim tunggal manajemen resiko dapat memperluas mitgasi potensial untuk penggunaan sistem pada berbagai implementasi jaringan.

IV. TEKNIK DATA MINING UNTUK MANAJEMEN RESIKO SISTEM INFORMASI RUMAH SAKIT

Pendekatan teknik penggalian data dalam hal ini digunakan untuk memanfaatkan data resiko yang diekstraksi dari sistem informasi. Tsumoto, et al, pada tahun 2000 memperkenalkan teknik yang disebut penggalian resiko (*risk mining*), sebagai pendekatan teknik penggalian data untuk menangani masalah yang telah dijelaskan sebelumnya[5]. Teknik ini terdiri dari tiga buah proses, yaitu pendeteksian resiko (*risk detection*), klarifikasi resiko (*risk clarification*), dan pemanfaatan resiko (*risk utilization*). Adapun masing-masing proses tersebut akan dijelaskan pada subbab berikut ini. Gambar 1 menunjukan gambaran umum dari proses-proses yang terlibat dalam risk mining.

A. Risk Detection

Pada proses ini, dilakukan penggalian pola atau tipe lain dari informasi yang tidak terduga untuk *domain expert*. Hal ini dilakukan karena pola atau tipe lain informasi yang tidak terduga untuk *domain expert* akan sangat penting untuk mendeteksi kemungkinan dari kecelakaan yang berskala besar. Pengetahuan yang didapatkan dari proses ini kemudiaan dinamakan *detected risk information*.



Gambar 1. Gambaran Umum Proses *Risk Mining*

B. Risk Clarification

Pada proses ini, fokus ditujukan pada *detected risk information* yang dihasilkan dari proses *risk detection*. *Domain expert* atau penggali data dapat berfokus pada klarifikasi dari pemodelan mekanisme yang tersembunyi dari resiko. Apabila *domain expert* membutuhkan informasi dengan granulasi yang lebih baik, dapat dilakukan pengumpulan data yang lebih banyak dengan informasi yang rinci, dan mengaplikasikan teknik penggalian data kembali terhadap data yang baru dikumpulkan. Pengetahuan yang didapakan dari proses ini kemudian dinamakan *clarified risk information*.

C. Risk Utilization

Pada tahap ini, dilakukan validasi terhadap model resiko yang dihasilkan dari proses *Risk Clarification*. Kita harus mengevaluasi *clarified risk information* di lingkungan nyata untuk mencegah resiko terjadi. Jika informasi resiko tersebut tidak cukup untuk melakukan pencegahan, maka dibutuhkan analisis yang lebih mendalam. Dengan demikian, pengumpulan data tambahan dilakukan untuk siklus baru pada proses *risk mining*. Pengetahuan yang didapatkan dari proses ini dinamakan *utilized risk information*.

Adapun unsur-unsur teknik yang digunakan dalam proses *risk mining* akan dijelaskan sebagai berikut:

1) *Mining unbalanced data*: Kecelakaan dalam skala besar yang terjadi biasanya merupakan penyimpangan yang besar dari kecelakaan skala kecil, yaitu insiden. Karena kemunculan dari insiden sangat rendah, maka probabilitas dari kecelakaan besar mendekati angka nol. Padahal, kebanyakan metode penggalian data bergantung pada frekuensi dan penggalian untuk data yang tidak seimbang tersebut. Dengan probabilitas yang kecil, merupakan salah satu masalah yang sulit dalam penelitian penggalian data. Dengan demikian, untuk penggalian resiko, teknik untuk penggalian data yang tidak seimbang adalah hal yang penting untuk mendeteksi informasi resiko.

2) *Interestingness*: Pada teknik penggalian data yang tradisional, indeks untuk pola resiko bergantung pada frekuensi. Sementara itu, untuk mengekstrak pengetahuan yang tidak terduga atau yang menarik, kita dapat mengusulkan tindakan untuk mengekstrak pola dari data berdasarkan unsur ketidakterdugaan dan unsur kemenarikannya.

3) *Uncertainty and Granularity:Granular Computing:* Laporan insiden didalamnya termasuk informasi mengenai aksi para staff, yang didalamnya

dijelaskan secara subjektif dan tidak pasti, apakah diperhalus atau justri dilebih-lebihkan (granularitas informasi). Komputasi granular berhubungan dengan point ini.

4) Visualisasi: Memvisualisasikan kejadian yang terjadi dapat memungkinkan domain expert untuk mendeteksi informasi resiko, untuk mengklarifikasi mekanisme dari resiko, atau untuk memanfaatkan informasi resiko.

5) Menstrukturkan: Graph Mining: Resiko dapat dideteksi atau diklarifikasi hanya dengan hubungannya antara beberapa hal dalam struktur jaringan yang besar. Dengan demikian, mengekstraksi struktur parsial dari jaringan yang tersembunyi dalam data merupakan teknik yang sangat penting, dengan fokus pada informasi resiko berdasarkan hubungan antara hal-hal yang ada.

6) *Clustering*: Faktor kesamaan dapat menemukan hubungan antara objek yang sama yang tidak terlihat sama. Atau kejadian yang dapat terjadi sendiri-sendiri dapat dikelompokkan menjadi beberapa kejadian yang "serupa", sehingga kita dapat menemukan keterhubungan antara kejadian-kejadian tersebut. Untuk tujuan ini, clustering atau pengelompokkan merupakan teknik yang sangat penting.

7) *Evaluation of Risk Probability*: Unsur probabilitas memiliki kinerja yang sangat tidak stabil ketika penentuan ruang sampel tidak stabil. Terutama ketika kita mengumpulkan data secara dinamis, ketidakstabilan tersebut sering muncul. Dengan demikian, pemikiran yang mendalam dalam mengevaluasi probabilitas sangatlah penting.

8) *Human Computer Interaction*: Proses ini sangat penting untuk proses penggalian resiko karena beberapa hal yang akan dijelaskan. Pertama, informasi resiko dapat diperoleh dengan cara diskusi mendalam terhadap hasil penggalian diantara domain expert karena hasil penggaliann hanya menunjukkan bagian kecil dari total informasi resiko. Karena *domain expert* memiliki pengetahuan, yang tidak dijelaskan pada kumpulan data, mereka dapat mengkompensasi pengetahuan yang kurang utnuk mendapatkan hipotesis atau penjelasan dari hasil penggalian. Hal yang kedua, hasil penggalian dapat membuat domain expert memiliki pengertian yang mendalam mengenai alur kerja dari sistem. Interpretasi dari hasil penggalian dalam mendeteksi resiko dapat menyebabkan pengumpulan data baru untuk klarifikasi resiko. Hal yang teakhir, interaksi manusia-komputer memberikan aspek baru untuk pemeliharaan resiko. Domain expert tidak hanya berfokus pada kinerja dari hasil klarifikasi resiko, namun juga melihat kemungkinan lainnya dari aturan (*rules*) pada penggalian data yang terlihat tidak terlalu penting, dibandingkan dengan aturan untuk klarifikasi resiko dan juga mengevaluasi kemungkinan untuk mendesain koleksi data yang baru.

V. ANALISIS

Pada bagian ini akan dilakukan analisis terhadap penggunaan teknik penggalian data untuk menunjang proses manajemen resiko dibandingkan dengan metode manajemen resiko konvensional, seperti yang diperkenalkan oleh National Institute of Standards and Technology (NIST).

Seperti yang telah dijelaskan pada Bab II, mengenai tahap-tahap yang dilakukan untuk melakukan manajemen resiko terhadap sebuah sistem informasi.Adapun tahapan-tahapan tersebut adalah penilaian resiko (*risk assessment*), mitigasi resiko (*risk mitigation*), serta evaluasi dan penilaian (*evaluation and assesment*). Sementara, tahapan-tahapan yang digunakan untuk manajemen resiko dengan pendekatan teknik penggalian data diantaranya adalah pendeteksian resiko (*risk detection*), klarifikasi resiko (*risk clarification*), dan pemanfaatan resiko (*risk utilization*).Adapun perbandingan dari masing-masing tahap tersebut akan dibahas satu per satu.

A. Risk Assesment vs Risk Detection

Proses penilaian resiko (*risk assessment*) pada metode yang diperkenalkan oleh NIST merupakan paling awal dalam manajemen resiko sistem informasi. Adapun pada proses ini akan dilakukan identifikasi dan evaluasi resiko-resiko yang mungkin muncul dalam sebuah sistem informasi beserta dampak yang mungkin ditimbulkan oleh resiko terebut. Proses ini dinilai sama dengan proses awal pada manajemen resiko dengan pendekatan teknik penggalian data, yaitu *risk detection*. Hanya saja, pada pendekatan teknik penggalian data, belum ada rekomendasi tindakan untuk mengurangi resiko yang mungkin terjadi seperti yang telah dilakukan pada tahap penilaian resiko (*risk assessment*). Padahal, rekomendasi awal mengenai tindakan yang tepat untuk mengurangi resiko diperlukan untuk membuat proses manajemen resiko menjadi lebih terarah dan memiliki tujuan awal. Apabilia proses manajamen resiko tersebut menjadi lebih terarah, maka proses akan lebih efektif dan membutuhkan waktu yang lebih singkat.

B. Risk Mitigation vs Risk Clarification

Risk mitigation merupakan proses kedua pada proses manajemen resiko yang diperkenalkan oleh

NIST. Pada proses ini dilakukan tindakan nyata untuk mengurangi resiko berdasarkan rekomendasi tindakan yang dihasilkan pada tahap *risk assessment*. Sementara pada *risk clarification*, yang merupakan proses kedua manajemen resiko dengan pendekatan teknik penggalian data, baru akan dilakukaan pembangunan model resiko yang telah didapatkan dari tahap sebelumnya, yaitu pendeteksian resiko. Pada tahap ini, pemodelan resiko dilakukan dengan teknik penggalian data, sehingga dapat berjalan dengan cepat. Namun, hasil pemodelan belum tentu menggambarkan keadaan yang sebenarnya. Oleh karena itu, tetap diperlukan pengawasan *domain expert* agar hasil pemodelan yang dihasilkan lebih sesuai.

Pemodelan yang dihasilkan dalam tahap *risk clarification* merupakan gambaran keadaan yang sebenarnya dalam sistem informasi yang diamati. Pemodelan ini digunakan untuk menentukan tindakan yang tepat untuk mengatasi resiko yang telah terdentifikasi. Oleh karena itu, tahap ini sesuai dengan tahap rekomendasi awal yang merupakan bagain dari tahap *risk assesment* (NIST). Karena pada *risk clarification* dilakukan dengan teknik penggalian data, maka hasil pemodelan dapat dihasilkan dengan cepat. Dengan demikian, pendekatan teknik penggalian data dapat lebih cepat dalam hal pemodelan, namun belum mengeksekusi tindakan untuk mengurangi resiko pada tahap kedua ini.

C. Evaluation and Assessment vs Risk Utilization

Proses *evaluation and assesment* pada metode yang diperkenalkan oleh NIST merupakan proses akhir, yang merupakan tahap evaluasi lebih lanjut untuk mengimplementasikan program manajemen resiko yang sukses. Sementara proses akhir dari metode dengan pendekatan teknik penggalian data adalah *risk utilization*, yaitu proses validasi model resiko yang dihasilkan dari proses sebelumnya , yaitu *risk clarification*. Pada tahap *risk utilization*, apabila model tidak sesuai untuk digunakan, maka akan dilakukan pengumpulan data kembali yang lebih rinci. Dengan demikian, hasil pemodelan yang dihasilkan pada proses ini dipastikan benar-benar sesuai dengan keadaan nyata yang ada di lapangan.

Kedua proses akhir ini dinilai sesuai, karena sama-sama mencakup evaluasi terhadap implementasi resiko berdasarkan analsis-analisis yang telah dilakukan pada tahap sebelumnya. Tujuannya sama, yaitu agar implementasi tindakan untuk mengurangi resiko dapat dilakukan dengan tepat, dan bukan malah menambah masalah baru.

VI. KESIMPULAN

Rumah sakit merupakan sebuah organisasi yang sangat kompleks. Didalamnya terdapat berbagai elemen, seperti staf medis dan para perawat yang melakukan berbagai layanan untuk pasien dengan cara yang efektif dan aman. Sejak tahun 1980, segala informasi kesehatan untuk rumah sakit mulai disimpan secara elektronik sebagai sistem informasi rumah sakit. Data yang disimpan pada sistem informasi ini adalah seluruh informasi yang menunjuang proses bisnis dari sebuah rumah sakit. Data yang disimpan tersebut, suatu saat tentu akan digunakan kembali. Data tersebut tentunya disimpan dalam jumlah yang sangat besar, oleh karena itu diperlukan sebuah teknik agar penggunaan kembali data dapat dilakukan dengan lebih efektif dan efisien. Salah satu teknik yang diusulkan adalah penggalian data (*data mining*).

Agar dapat menjalankan fungsinya dengan baik, sistem informasi rumah sakit harus mampu menghindari adanya kesalahan (*error*) demi memberikan pelayanan yang aman, nyaman, dan memuaskan bagi pasiennya. Adapun kesalahan yang umumnya terjadi pada sebuah sistem informasi dapat diklasifikasikan ke dalam tiga buah kategori, yaitu kesalahan sistematis (*systematic error*), kesalahan personal (*personal error*), dan (*random error*). Dengan demikian, proses manajemen resiko dilakukan untuk mengidentifikasi kesalahan – kesalahan ini sebagai resiko yang harus dihindari dan menentukan tindakan yang tepat untuk mengurangi resiko yang mungkin terjadi.

Pada makalah ini, dijelaskan mengenai penggunakan teknik penggalian data untuk menemukan data yang dapat menjadi resiko yang dapat mengancam keberjalanan sistem informasi rumah sakit. Teknik tersebut dinamakan penggalian resiko (*risk mining*). Sesuai dengan namanya, teknik tersebut digunakan untuk menggali data yang tersimpan di basis data untuk menemukan informasi yang diidentifikasi sebagai resiko.

Pada bagian analisis, telah dilakukan analisis perbandingan antara pendekatan teknik penggalian data dan metode manajemen resiko yang diperkenalkan oleh NIST. Berdasarkan analisis tersebut, diketahui bahwa penggunaan pendekatan teknik penggalian data untuk manajemen resiko dapat menghasilkan pemodelan keadaan sistem informasi yang lebih akurat berdasarkan rules yang telah ditentukan sebelumnya. Selain itu, proses pemodelan ini juga dapat dilakukan dengan efektif dan efisien. Hasil pemodelan yang dihasilkan oleh *risk mining* kemudian digunakan untuk menentukan tindakan untuk mengurangi resiko yang

mungkin terjadi.

Sementara itu, proses manajemen resiko yang diperkenalkan oleh NIST cenderung lebih lengkap dan rinci. Dengan demikian, kedua pendekatan ini dapat digabungkan untuk memberikan hasil analisis yang lebih baik dan lebih cepat. Misalnya, tahapan-tahapan yang digunakan dalam manajemen resiko mengikuti tahapan-tahapan pada manajemen resiko yang diperkenalkan oleh NIST, sementara teknik yang digunakan dalam setiap tahapnya dilakukan dengan pendekatan teknik penggalian data. Dengan demikian, hasil analisis yang didapatkan akan lebih akurat dan cepat.

Daftar Pustaka

[1] Li, Jing-song, et al. 2011. *Data Mining in Hospital Information System*. China, Shejiang University.

[2] Kincade, K. 1998. *Data Mining: Digging for Healthcare Gold*. Insurance & Technology, 23(2), IM2-IM7.

[3] Jabasheela, Dr.L. 2011. *Rule Based Approach for Mining Risk Factor in Hospitals.*International Journal of Engineering Trends and Technology.

[4] Stoneburner et al, 2002. *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology.

[5] Tsumoto, Shusaku. 2000. *Data Mining for Risk Management in Hospital Information Systems*. Shimane University.