# Analisis Kebutuhan Keamanan Sistem Dengan Menggunakan Metodologi SQUARE: Studi Kasus Pengembangan Sistem Informasi Rumah Sakit Berbasis Open Source ERP (Open Sikes)

**Hadi Syahrial**
*Universitas Budi Luhur*
*E-mail: hadisyahrial@gmail.com*

**ABSTRAK**

*Keberhasilan pengembangan sebuah sistem informasi rumah sakit sangat bergantung kepada aspek keamanan informasi seperti terjaminnya kerahasian, keutuhan, dan ketersediaan data dan informasi yang disimpan dan diolah oleh sistem tersebut. Saat ini sedang dikembangkan sebuah sistem informasi rumah sakit berbasis open source ERP yang dinamakan Open Sikes. Untuk mengetahui lebih awal kelemahan-kelemahan pada sistem tersebut maka diterapkan analisis kebutuhan keamanan informasi dengan menggunakan metodologi SQUARE. Hasil akhir yang diharapkan adalah dengan lebih awal ditemukenalinya kelemahan-kelemahan pada sistem tersebut, maka rekomendasi untuk memperbaiki kelemahan-kelemahan tersebut dapat diberikan, sehingga dapat dibangun sebuah sistem informasi rumah sakit berbasis open source ERP yang lebih aman.*

**Kata kunci**: Sistem informasi rumah sakit, Open Source ERP, Open Sikes, analisis kebutuhan keamanan sistem, metodologi SQUARE. (KEBANYAKAN)

## 1. PENDAHULUAN

Data dan informasi merupakan sumber daya yang sangat strategis dalam pengelolaan rumah sakit. Kebutuhan akan data dan informasi disediakan melalui penyelenggaraan Sistem Informasi Kesehatan (SIK), yaitu dengan cara pengumpulan, pengolahan, analisis data serta penyajian informasi. Saat ini SIK masih terfragmentasi serta belum mampu menyediakan data dan informasi yang handal, sehingga SIK masih belum menjadi alat pengelolaan pembangunan kesehatan yang efektif.

Perkembangan Teknologi Informasi dan Komunikasi (TIK) yang pesat memberikan kemudahan dalam pengembangan Sistem Informasi Kesehatan. Saat ini sudah ada kebutuhan-kebutuhan untuk memanfaatan TIK dalam SIK (eHealth) agar dapat meningkatkan pengelolaan dan penyelenggaraan pembangunan kesehatan.

Penguatan SIK dilakukan dengan mengembangkan model SIK yang terintegrasi. SIK yang terintegrasi adalah sistem informasi yang menyediakan mekanisme saling terhubung antar sub sistem informasi dengan berbagai cara yang sesuai. Dengan demikian data dari satu sistem secara rutin dapat mengalir, menuju atau diambil oleh satu atau lebih sistem yang lain.

Dengan SIK terintegrasi, data entri hanya perlu dilakukan satu kali, data yang sama akan disimpan secara elektronik, dikirim dan kemudian diolah. Fasilitas pelayanan kesehatan baik milik pemerintah maupun swasta wajib menyampaikan laporan sesuai standar dataset minimal dengan jadwal yang telah ditentukan.

Open Source Sistem Informasi Kesehatan (Open Sikes) adalah sistem komputerisasi yang memproses dan mengintegrasikan seluruh alur proses bisnis layanan kesehatan dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk mendukung kinerja dan memperoleh informasi secara cepat, tepat dan akurat. Open Sikes berbasis Open Source dengan menerapkan model Enterprise Resource Planning (ERP) dalam integrasi sistem. Open Sikes juga menggunakan teknologi berbasis web dan sudah mendukung untuk bisa diakses secara mobile. Sehingga Open Sikes sudah menerapkan metode *Online Ready* dan *Mobile Ready*.

Seiring dengan meningkatnya pemanfaatan layanan kesehatan yang terintegrasi khususnya pada Open Sikes, akan semakin banyak pihak-pihak yang berusaha mencari kelemahan-kelemahan yang ada. Celah keamanan ini dapat dijadikan sebuah motif serangan yang beragam jenis dan tingkat kecangihannya. Dikarenakan Open Sikes menggunakan Open Source ERP, maka keamanannya juga bergantung pada Open Source ERP yang digunakan. Penelitian ini dilakukan untuk menganalisis kebutuhan keamanan informasi dengan menggunakan metodologi SQUARE, sehingga rekomendasi bisa diberikan sejak tahap awal pengembangan sistem agar dapat dihasilkan sebuah sistem informasi rumah sakit yang aman. Open Source ERP yang digunakan pada penelitian ini adalah OpenERP.

## 2. LANDASAN TEORI

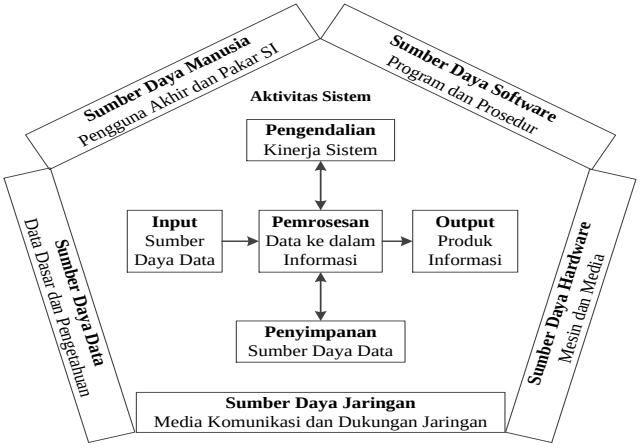
Menurut O'Brien, sistem informasi merupakan kombinasi yang terorganisir dari manusia, *hardware*, *software*, jaringan komunikasi dan sumber dayadata untuk mengumpulkan, memasukkan, dan memproses data dan menyimpannya, mengelola, mengontrol dan melaporkannya sehingga dapat mendukung perusahaan atau organisasi untuk mencapai tujuan [8]. Dapat didefinisikan juga bahwa sistem informasi adalah suatu sistem yang terdiri dari beberapa subsistem atau komponen *hardware*, *software*, *brainware*, data dan prosedur untuk menjalankan input, proses, output, penyimpanan, dan pengontrolan yang mengubah sumber data menjadi informasi.

Terdapat tiga alasan mendasar untuk semua aplikasi bisnis dalam menggunakan sistem informasi, peran utama sistem informasi dalam aplikasi bisnis tersebut menurut O'Brien adalah:[8]

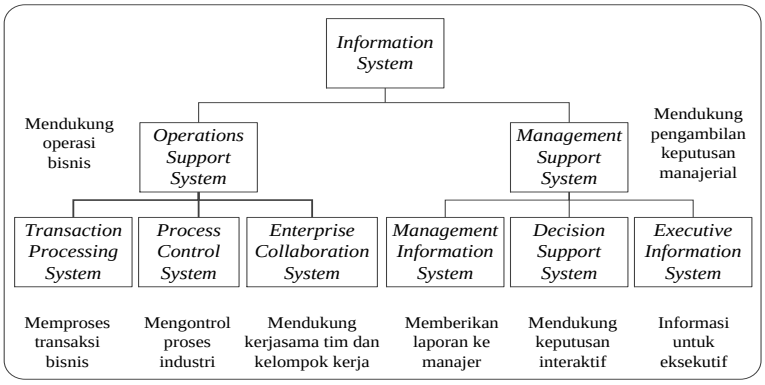
1. Mendukung proses dan operasi bisnis.
2. Mendukung pengambilan keputusan. Sistem informasi membantu para manajer dan pelaku bisnis untuk membuat keputusan yang lebih baik.
3. Mendukung berbagai strategi untuk keunggulan kompetitif. Mendapatkan kelebihan strategis atas para pesaing melalui penggunaan sistem informasi.

Gambar II-1 mengilustrasikan model sistem informasi yang menunjukkan kerangka konsep dasar komponen dan aktivitas sistem informasi. Komponen atau sumber daya sistem informasi tersebut adalah:

1. Sumber Daya *Hardware*. Berupasemua peralatan dan komponen fisik yang digunakan dalam pemrosesan informasi, yaitu peralatan input, peralatan proses, peralatan output, dan media penyimpanan.
2. Sumber Daya *Software*. Meliputi semua rangkaian perintah pemrosesan informasi dalam wujud instruksi-instruksi dan prosedur yang membuat komputer melakukan pekerjaan tertentu.
3. Sumber Daya Jaringan. Meliputi media komunikasi dan dukungan jaringan.
4. Sumber Daya Data. Meliputi data dasar berbentuk alfanumerik, teks, gambar, audio, video, dan bentuk data lainnya.
5. Sumber Daya Manusia (SDM). SDM dibutuhkan untuk pengoperasian semua sistem informasi. Sumber daya manusia ini meliputi pengguna akhir dan pakar sistem informasi.




Gambar II-1 Komponen Sistem Informasi [8]




Gambar II-2 Klasifikasi Sistem Informasi [8]

Secara konseptual, O'Brein mengklasifikasikan aplikasi sistem informasi berdasarkan tujuan utama sistem informasi yang mendukung operasi bisnis dan mendukung pengambilan keputusan manajerial dalam Gambar II-2:

Manajemen rumah sakit adalah serangkaian kegiatan manajemen mulai dari tahap perencanaan sampai tahap evaluasi yang berorientasi pada aspek input (pelanggan, dokter, sarana, prasarana dan peralatan), proses (pelayanan medik) dan output (kepuasan pasien). Peran Sistem Informasi Rumah Sakit yang utama adalah dalam mendukung pengendalian mutu pelayanan medis, penilaian produktivitas, analisis pemanfaatan dan perkiraan kebutuhan, perencanaan dan evaluasi program, menyederhanakan pelayanan, penilaian klinis dan serta pendidikan.

Sistem Informasi Rumah Sakit (SIRS) adalah suatu proses pengumpulan,pengolahan dan penyajian data rumah sakit. Sistem informasi ini mencakup semua Rumah Sakit umum maupun khusus, baik yang dikelola secara publik maupun privat sebagaimana diatur dalam Undang-Undang Republik Indonesia Nomor 44 Tahun 2009 tentang Rumah Sakit.

Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan himpunan atau kegiatan dan prosedur yang terorganisisasikan dan saling berkaitan serta saling ketergantungan dan dirancang sesuai dengan rencana dalam usaha menyajikan info yang akurat dan tepat waktu di rumah sakit. Selain itu, sistem ini berguna untuk menunjang proses fungsi-fungsi manajemen dan pengambilan keputusan dalam memberikan pelayanan kesehatan di rumah sakit. Sistem tersebut, saat ini ditujukan untuk menunjang fungsi perencanaan dan evaluasi dari penampilan kerja rumah sakit antara lain adalah jaminan mutu pelayanan rumah sakit yang bersangkutan, pengendalian keuangan dan perbaikan hasil kerja rumah sakit tersebut, kajian dalam penggunaan dan penaksiran permintaan pelayanan kesehatan rumah sakit oleh masyarakat, perencanaan dan evaluasi program rumah sakit, penyempurnaan laporan rumah sakit serta untuk kepentingan pendidikan dan pelatihan.

Metodologi SQUARE (*System Quality Requirements Engineering*) adalah sembilan langkah proses yang dikembangkan untuk membantu dalam melakukan analisis kebutuhan keamanan sistem. Metodologi SQUARE dikembangkan oleh *Carnegie Mellon Software Engineering Institute*, dan menunjukkan potensi besar untuk diadopsi oleh industri dalam mengembangkan aplikasi perangkat lunak dan sistem yang aman.

## 3. METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah metodologi SQUARE yang terdiri dari sembilan langkah proses yang dikembangkan untuk membantu menganalisis kebutuhan keamanan sistem sebagai berikut:

Langkah 1: *Definition*

Mendeskripsikan sistem informasi rumah sakit yang akan dibangun (Open Sikes) dan mendefinisikan istilah-istilah keamanan informasi untuk sistem yang akan dianalisis yang disepakati di dalam rumah sakit.

Langkah 2: *Safety and Security Goals*
Menganalisis tujuan dan persyaratan keamanan sistem yang diperlukan oleh rumah sakit untuk memastikan keamanan secara keseluruhan sistem dan ketersediaan (*availability*) setiap saat.

Langkah 3: *System Architecture*
Menjelaskan arsitektur Open Sikes yang sedang dibangun.

Langkah 4: *Use Case*
Menggambarkan diagram *Use Case* aplikasi menggunakan UML (*Unified Modeling Language*) dan menjelaskannya dalam tabel use case untuk masing-masing kasus penggunaan. Use Case memberikan garis besar fungsi sistem dari perspektif pengguna, dengan klasifikasi hak istimewa tingkat pengguna dengan Access Control List (ACL). Penggambaran untuk use case meliputi:pengguna yang berinteraksi dengan sistem, digambarkan sebagai seorang aktor.

Langkah 5: *Misuse Case*
Mengidentifikasi kemungkinanan ancaman dan kasus potensi penyalahgunaan aplikasi yang disepakati dalam organisasi. Tujuannya adalah untuk mengetahui kerentanan dalam aplikasi yang ada dan memberikan rekomendasi arsitektur dan kebijakan dalam mengurangi kerentanan untuk mengamankan komponen kritis Open Sikes. Digambarkan dalam bentuk diagram misuse case.

Langkah 6 : *Attack Tree*
*Attack tree* adalah pendekatan formal untuk memeriksa misuse case atau kasus penyalahgunaan dan untuk memverifikasi bahwa rekomendasi arsitektur misuse case atau kasus penyalahgunaan dan kebijakan yang diambil cukup dapat mengatasi semua potensi kerentanan yang dapat menyebabkan terjadinya penyalahgunaan.*Attack tree* merupakan representasi hirarkis banyak jenis pelanggaran keamanan yang didasarkan kepada misuse case. Setiap skenario di attack tree diperiksa secara rinci untuk melihat apakah ada sekumpulan rekomendasi yang cukup dapat mengurangi risikonya. Jika ada skenario yang saat ini tidak tercakup, tambahan arsitektur atau rekomendasi kebijakan perlu dipertimbangkan dan ditambahkan ke daftar rekomendasi. Dengan kata lain,

attack tree adalah visualisasi rinci misuse case dan elemen penting dari validasi untuk arsitektur dan rekomendasi kebijakan dari misuse case.

Langkah 7: *Prioritization*
Tahap metodologi *SQUARE* difokuskan pada prioritas persyaratan keselamatan dan keamanan. Untuk memprioritaskan persyaratan keselamatan dan keamanan digunakan misuse case dan kategorinya untuk menentukan *misuse case* mana yang paling penting untuk menjamin survivabilitas dari Open Sikes. Dengan mengevaluasi setiap misuse case (kasus penyalahgunaan) dan atributnya, akan mampu membuat daftar prioritas kerentanan dan penyalahgunaan yang merugikan Open Sikes.

Langkah 8: *Categorizing and Detailing Recommendation*
Membuat daftar kategori dan memberikan rekomendasi detail terhadap arsitektur dan kebijakan persyaratan penerapan keamanan system. Semua solusi teknis yang ada kemudian diteliti berdasarkan pada tingkatan prioritas misuse case, yang akan menyediakan semua yang diperlukan langkah-demi-langkah keamanan dan teknis dalam rangka implementasi pada komponen inti dari Open Sikes.

Langkah 9: *Inspect Requirements*
Dalam situasi ideal, semua misuse case atau kasus penyalahgunaan yang diprioritaskan tinggi (menengah dan rendah) akan diatasi dan diselesaikan untuk melindungi Open Sikes. Namun, karena keterbatasan jumlah sumber daya yang tersedia, hanya bagian tertentu dari misuse case dan secara inheren, arsitektur dan kebijakan rekomendasi harus dipilih. Untuk mengoptimalkan bagian ini, model matematika dirumuskan untuk memecahkan kombinasi terbaik dari *misuse case*. Hasilnya dalam tabel yang mereferensikan *use case* mana harus ditangani berdasarkan anggaran yang terse

## 4. HASIL PENELITIAN

Dalam melakukan analisis kemanan menggunakan metodologi SQUARE terdiri dari sembilan langkah yaitu *Definitions, Safety and Security Goals, System Architecture, Use Case, Misuse case, Attack Tree, Prioritization, Categorizing and Detailing Recommendation, Inspect Requirements.*

### *4.1 Definitions*

Mendefinisikan istilah-istilah keamanan yang akan disepakati. Istilah-istilah keamanan tersebut adalah sebagai berikut :

Tabel IV-1 Definisi

| |
|---|
| Beberapa definisi serangan pada sistem:<br>a. FTP Bounce Attack, menggunakan server ftp orang lain untuk melakukan serangan.<br>b. Daniel of Service (DoS), jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.<br>c. Distributed DoS (DDoS), salah satu jenis serangan Denial of Service yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi zombie) untuk menyerang satu buah host target dalam sebuah jaringan.<br>d. Serangan Injeksi SQL, pada serangan ini objek yang diserang adalah halaman web yang menggunakan Structured Query Language (SQL) untuk melakukan query dan memanipulasi database.<br>e. Password Attack, serangan untuk meng-*crack* sebuah password. |

### *4.2 Safety and Security Goals*

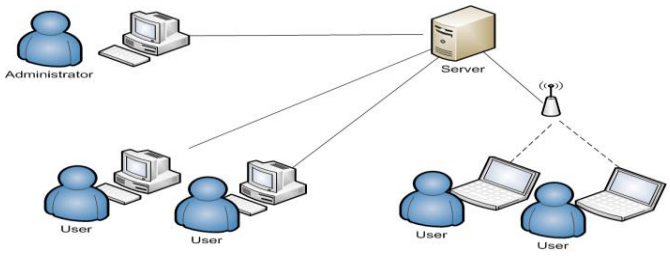
Menganalisis tujuan keamanan Sistem Informasi Rumah Sakit Open Sikes, untuk memastikan keamanan secara keseluruhan sistem dan ketersediaan (availability) setiap saat.

Tabel IV-2 Analisa Tujuan Keamanan

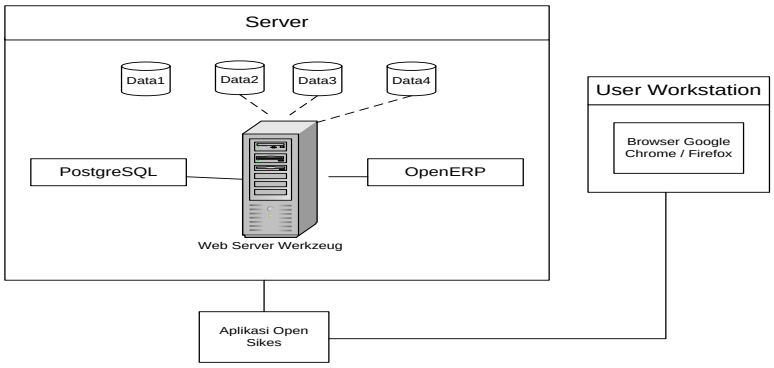
| | |
|---|---|
| Tujuan Keamanan | - Melakukan kontrol yang efektif atas konfigurasi sistem dan penggunaan.<br>- Kerahasiaan, akurasi, dan integritas data sistem harus terjamin.<br>- Sistem ini akan tersedia untuk digunakan bila diperlukan. |

### *4.3 System Architecture*

Melakukan analisis arsitektur Sistem Informasi Rumah Sakit Open Sikes.



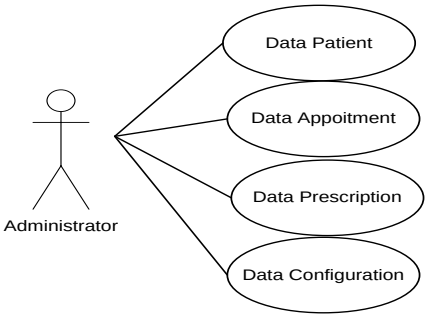

Gambar IV-1 Topologi Jaringan



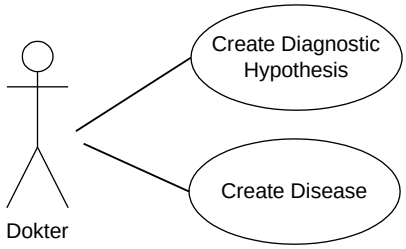

Gambar IV-2 Arsitektur Sistem

### *4.4 Use Case*

Penggambaran use case meliputi pengguna yang berinteraksi dengan sistem yang digambarkan sebagai seorang aktor.




Gambar IV-3 Use Case Admin Panel



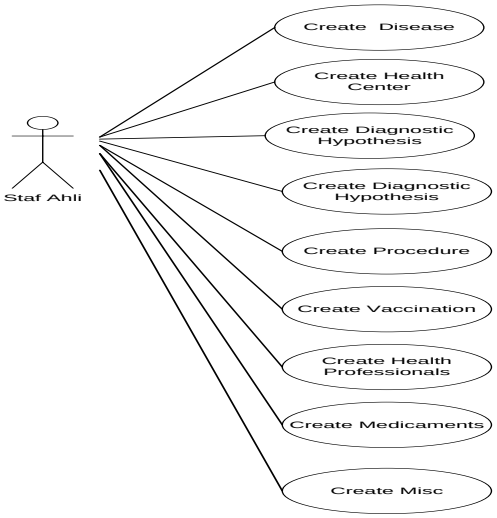

Gambar IV-4 Use Case Menu Dokter

Tabel IV-3 Tabel Admin Panel

| | |
|---|---|
| Nomor | UC-01 |
| Use Case | Admin Panel |
| Deskripsi | Administrator megkonfigurasi seluruh admin panel |
| Actor | Administrator |
| Asumsi | Administrator dapat mengontrol seluruh aplikasi |
| Langkah-langkah | 1. Log in menggunakan menu admin<br>2. Sistem akan memeriksa autentifikasi username dan password dan akan menghubungkan admin panel<br>3. Administrator mengkonfigurasi dan mengontrol seluruh aplikasi |
| Misuse case yang berkaitan | 1. Log in oleh orang yang tidak memiliki autorisasi pada sistem<br>2. Pegahapusan data admin pada database |

Tabel IV-4 Tabel Menu Dokter

| | |
|---|---|
| Nomor | UC-02 |
| Use Case | Menu Dokter |
| Deskripsi | Dokter hanya dapat mengedit menu dokter |
| Actor | Dokter |
| Asumsi | Dokter mengontrol menu dokter |
| Langkah-langkah | 1. Log in menggunakan menu dokter<br>2. Sistem akan memeriksa autentifikasi username dan password dan akan menghubungkan menu dokter<br>3. Dokter dapat mengkonfigurasi dan mengontrol seluruh menu dokter |
| Misuse case yang berkaitan | 1. Log in oleh orang yang tidak memiliki autorisasi pada sistem<br>2. Pegahapusan data dokter pada database |



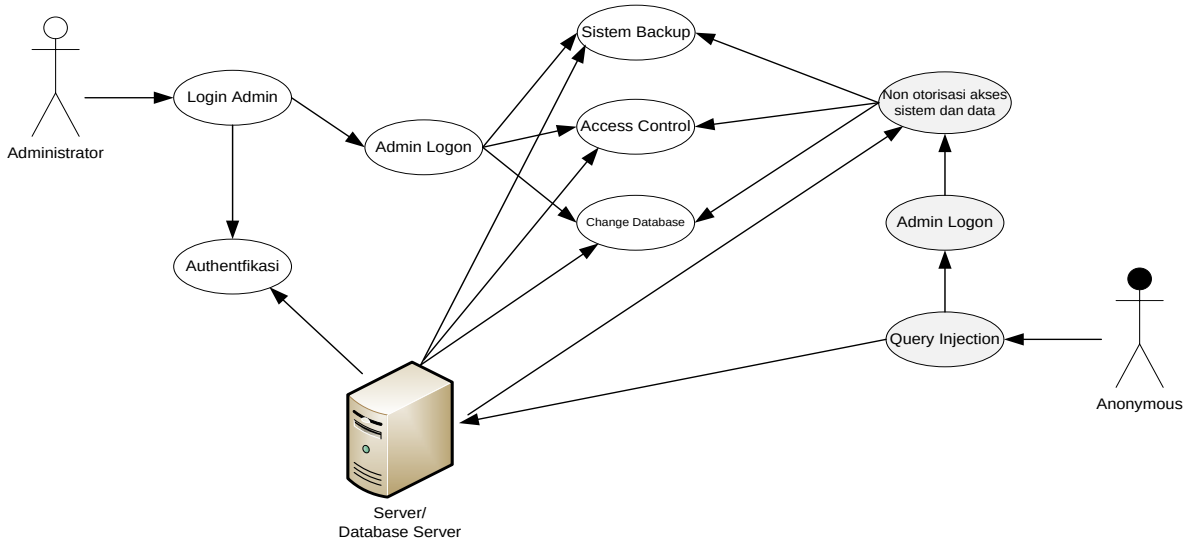

Gambar IV-5 Use Case Menu Staf Ahli

Tabel IV-5 Tabel Menu Staf

| | |
|---|---|
| Nomor | UC-03 |
| Use Case | Menu Staff Ahli |
| Deskripsi | Staf Ahli hanya dapat mengedit menu Staf Ahli |
| Actor | Staf Ahli |
| Asumsi | Staf Ahli mengontrol menu staf ahli |
| Langkah-langkah | 1. Log in menggunakan menu Staf ahli<br>2. Sistem akan memeriksa autentifikasi username dan password dan akan menghubungkan menu staf ahli<br>3. Staf ahli dapat mengkonfigurasi dan mengontrol seluruh menu staf ahli |
| Misuse case yang berkaitan | 1. Log in oleh orang yang tidak memiliki autorisasi pada sistem<br>2. Pegahapusan data staf ahli pada database |

### *4.5 Misuse case*

Merupakan anomali-anomali yang terjadi akibat serangan-serangan yang tidak diinginkan pada sistem, yang akan mengancam keamanan sistem.



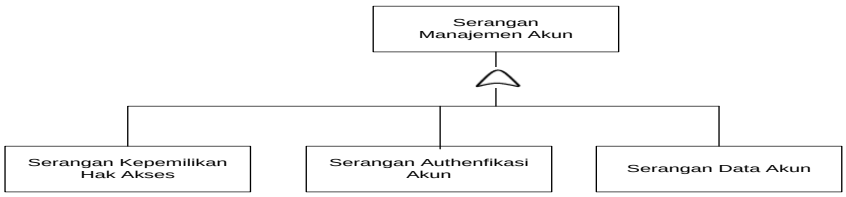

Gambar IV-6 Misuse Case

| No | Kategori | Penjelasan |
|---|---|---|
| 1 | Nama | Unauthorized Login, |
| 2 | Ruang Lingkup | Login Admin Panel dan Sistem data base |
| 3 | Prioritas | High |
| 4 | Lingkungan | Internet |
| 5 | Mis Actor | Anonymous |
| 6 | Akses Level | Sistem Administrator |
| 7 | Entry point | Aplikasi dan sistem database |
| 8 | Atribut keamanan | *Confidentiality*, *Integrity*, dan *Availability* |
| 9 | Deskripsi | Sistem akan disusupi oleh seseorang yang tidak memiliki otoritas. Dan dapat melakukan perubahan, pengambilan dan perusakan data. |
| 10 | Penyerangan | High: serangan dilakukan dengan injeksi SQL |
| 11 | Pre kondisi | Sistem akan dimasuki dan database admin akan didownload atau dihapus |
| 12 | Asumsi | Script dan file vulnerability |
| 13 | Post kondisi | - Sesorang yang tidak memiliki otoritas tidak dapat menyusup kedalam sistem<br>- Seseorang tidak dapat menghapus database |
| 14 | Profil potensi mis actor | Penyerangan dapat menggunakan script browser pada yang bertujuan menginjeksi SQL |
| 15 | Ancaman | Kehilangan dan kerusakan data pada sistem |
| 16 | Ancaman yang berkaitan | - Serangan Manajemen Akun<br>- Serangan Password<br>- Serangan Injeksi SQL |
| 17 | Rekomendasi Arsitektur (AR) | - Penggunaan firewall<br>- Penggunaan protocol HTTPS |
| 18 | Rekomendasi Kebijakan (PR) | - Penggunaan tanda tangan digital untuk sistem login<br>- Konfigurasi file pada sistem<br>- Penggunaan password yang kuat<br>- Aplikasi harus di patch secara berkala<br>- Penggantian password secara berkala |

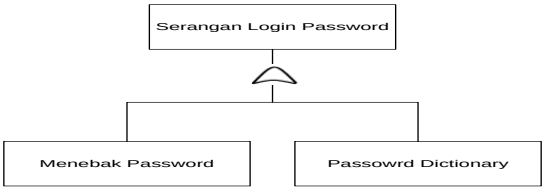
### *4.6 Attack Tree*

Melakukan pendekatan formal untuk memeriksa misuse case dan memverifikasi rekomendasi arsitektur dan kebijakan yang diambil dapat mengatasi kerentanan Sistem Informasi Rumah Sakit Open Sikes

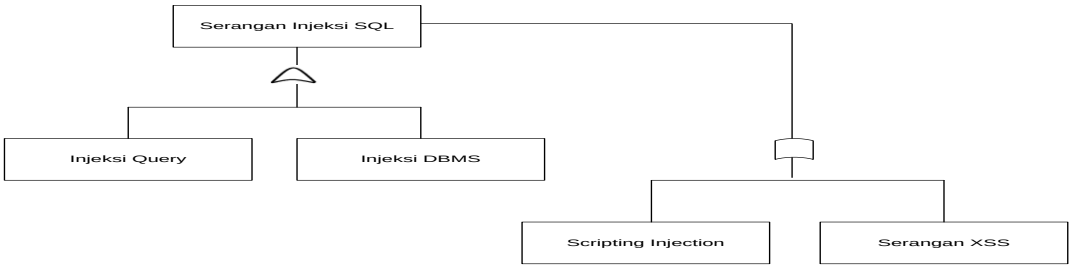
1. Pohon Serangan Manajemen Akun (MC 01)
2. Pohon serangan login password (MC 02)
3. Pohon serangan Injeksi SQL (MC 03)




Gambar IV-7 Pohon Serangan Manajeman Akun




Gambar IV-8 Pohon Serangan Login Password




Gambar IV-9 Pohon Serangan Injeksi SQL

### *4.7 Prioritization*

Memprioritaskan keamanan pada Open Sikes berdasarkan *misusecase* yang sudah dibuat. Dalam memprioritaskan ancaman mana yang lebih berbahaya, maka digunakan tabel priortitas ancaman yang harus ditanggulangi.

### *4.8 Categorizing and Detailing Recommendation*

Kategorisasi dan rekomendasi diambil berdasarkan analisa terhadap serangan yang terjadi untuk melindungi sistem ini. Kategorisasi diambil dari beberapa misuse case yang terjadi untuk merunjuk suatu rekomendasi yang akan dilakukan baik pada kebijakan maupun arsitektur sistem. Adapun kebutuhan keamanan pada Sistem Informasi Rumah Sakit Open Sikes adalah sebagai berikut :

Tabel IV-7 Pemerioritasan

| | |
|---|---|
| Tujuan | *Confidentiality*, *Integrity*, dan *Availability* |
| Kebutuhan | - UA: Keamanan sistem login dan server<br>- AC : Kemanan pada sistem<br>- PV: Database yang terjaga kerahasiaannya |
| Kategori | - *Unauthorize* Attack(UA)<br>- Access Control (AC)<br>- Privacy (PV) |
| Rekomendasi | - Pemasangan firewall pada server<br>- Penggunaan tanda tangan digital untuk sistem login<br>- Patching pada sistem aplikasi |

Tabel IV-8 Pengkategorian dan Rekomendasi

| Misuse Case | A1 | A2 | A3 | Rata-rata | Prioritas |
|---|---|---|---|---|---|
| MC 01 | 8 | 9 | 7 | 8.00 | Tinggi |
| MC 02 | 7 | 6 | 7 | 6.67 | Sedang |
| MC 03 | 7 | 8 | 6 | 7.00 | Tinggi |

## 5. PENUTUP

Dari hasil penelitian, penulis dapat memberikan kesimpulan bahwa metodologi SQUARE sangat membantu dalam melakukan analisis kebutuhan keamanan sistem dalam pengembangan sistem informasi rumah sakit berbasis open source ERP (Open Sikes).

## DAFTAR PUSTAKA

[1] Dawson, Christian, W. *Project in Computing and Information System: a Student Guide, 2nd Edition.* Addison-Wesley, 2009.
[2] Monk, Ellen, Wagner, Bret, *Concepts in Enterprise Resource Planning*, Cengage Learning, 2009
[3] Dennis, Alan, at.al. *"Systems Analysis and Design with UML – 3rd Edition".* John Wiley & Sons, Inc, 2009.
[4] Fahmy, Syahrul, Haslinda Nurul, et.al. "Evaluating the Quality of Software in e-Book Using the ISO 9126 Model." International Journal of Control and Automation, vol. 5 (2012).
[5] Jogiyanto, H, M. *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis.* Yogyakarta: ANDI, 2008.
[6] Kementrian Kesehatan RI, Roadmap Sistem Informasi Kesehatan, 2011
[7] Krutz,R.L. & Vines, R.D. *The CISM Prep Guide : Mastering the five domains of Information Security Managemen*t, Wiley Publishing, Indianapolis,2003.
[8] O'Brien, A, James. *Introduction to Information Systems, 12 th ed.* Dialihbahasakan oleh Fitriasari, Dewi dan [9] Deny, A, Kwary. Jakarta: Salemba Empat, 2006.
[10] Open Information System Security Group, *Information Systems Security Assessment Framework (ISSAF)*. 2008